



ØKOKRIM

Den sentrale enhet for etterforskning og påtale av
økonomisk kriminalitet og miljøkriminalitet

Samferdselsdepartementet
Postboks 8010 Dep
0030 OSLO

Deres referanse
09/585-HK

Vår referanse
201000004

Vår dato
12.04.10

HØRING - IMPLEMENTERING AV DATALAGRINGS-DIREKTIVET

Vi viser til departementets høringsbrev av 08.01.2010 med vedlegg.

ØKOKRIMs høringsuttalelse faller i to hovedpunkter. Først drøftes spørsmålet om det i Norge bør innføres en plikt for teletilbydere til å lagre trafikkdata. Deretter drøftes forslaget i høringsnotatet til utforming av regelverk for en slik lagringsplikt og politiets tilgang til de lagrede dataene.

Datalagringsdirektivet pålegger tilbydere offentlig elektronisk kommunikasjonsnett og -tjenester å lagre såkalte trafikkdata av hensyn til bekjempelsen av alvorlig kriminalitet. Det har hittil ikke vært ført noen statistikk over i hvor mange saker ØKOKRIM har innhentet trafikkdata som ledd i etterforskning. Det dreier seg om et begrenset antall saker. Det er likevel ØKOKRIMs erfaring at trafikkdata gir vesentlige og tidvis avgjørende bidrag til etterforskningen og irtteføringen av alvorlige økonomiske og miljørelaterte straffesaker, jf. særlig punkt 1.3 om dette. Videre er det grunn til å tro at ØKOKRIMs nytte av trafikkdata ville vært langt større dersom dataene hadde vært lagret hos tilbyderne i lengre tid, ettersom ØKOKRIM etterforsker former for kriminalitet som i hovedsak ikke oppdages før etter noe tid, jf. punkt 2.2 om dette. ØKOKRIM er også opptatt av at regelverket for politiets tilgang til trafikkdata utformes på en måte som opprettholder politiets mulighet til effektivt å nyttiggjøre seg dataene, jf. punkt 2.3 om dette.

ØKOKRIMs erfaring med og behov for trafikkdata er knyttet til etterforskningen av økonomisk kriminalitet og miljøkriminalitet. Øvrige deler av politiet og påtalemyndigheten kan ha andre erfaringer og behov, og avvikende eller manglende synspunkter i denne høringsuttalelsen på det som fremheves av andre organer, kan selvsagt ikke tas til inntekt for at disse erfaringene og behovene ikke har vekt.

1. Bør teletilbyderne pålegges lagringsplikt for trafikkdata av hensyn til kriminalitetsbekjempelse

1.1. Innledning

I debatten om Datalagringsdirektivet så langt har hensynet til personvernet stått i sentrum. Det har vært anført at lagring av trafikkdata vil krenke personvernet, virke

hemmende på enkeltmenneskets frimodighet og svekke befolkningens tillit til myndighetene ved at hele folket settes under mistanke. Etter vårt syn er det viktig at personvernet debatteres. Retten til en personlig sfære og kontroll over opplysninger som angår en selv er helt sentral i en rettsstat.

Men personvernens hensynet må ikke være det altoverskyggende utgangspunktet og avgjørende elementet i vurderingen av om lagringsplikt for trafikkdata skal innføres. ØKOKRIM slutter seg til høringsbrevets vurdering av at spørsmålet om lagringsplikt i hovedsak beror på en avveining av de hensyn som gjør seg gjeldende. Etter vår oppfatning står man her overfor en avveining av to likestilte hensyn – retten til personvern og retten til ikke å bli utsatt for krenkelser av sin fysiske og psykiske integritet. Den sist nevnte rettigheten har fått mindre oppmerksomhet i samfunnsdebatten, den nevnes ofte med en kort henvisning til sekkebetegnelsen ”kriminalitetsbekjempelse”. Behovet for kriminalitetsbekjempelse er imidlertid mangeartet og rommer i realiteten flere hensyn. Vi vil derfor først utdype vårt syn på hva som ligger i dette hensynet, jf. pkt. 1.2.

Betydningen av trafikkdata for etterforskningen av alvorlig kriminalitet har vært et omstridt tema i debatten. ØKOKRIM er ikke i tvil om at trafikkdata er av stor betydning for etterforskningen av alvorlig kriminalitet generelt, men vil i punkt 1.3 fokusere på hvorfor muligheten til å innhente trafikkdata er et viktig og effektivt virkemiddel i etterforskningen av alvorlig økonomisk kriminalitet og miljøkriminalitet.

Det er ØKOKRIMs syn at innføringen lagringsplikt for trafikkdata utgjør et forholdsmessig inngrep i personvernet. Dette utdypes i punkt 1.4.

1.2. Hensynet til kriminalitetsbekjempelse

Tilbake etter at en straffbar handling er begått, står som hovedregel en skadelidt person – et offer. Årsaken til at handlinger kriminaliseres er nettopp at lovgiver vurderer handlingen eller dens konsekvenser som så alvorlig at det anses nødvendig å reagere med straff, endatil med fengselsstraff i de tilfelle som er relevante her. Ofrene er dermed, direkte eller indirekte, blitt utsatt for en alvorlig krenkelse, for eksempel av sin fysiske eller psykiske integritet, sitt privatliv eller sin eiendom. Når lovgiver velger å gjøre en handling straffbar, skjer det med den overordnede målsetning å gjøre færrest mulig enkeltmennesker til ofre.

Ikke alle straffbare handlinger har direkte konsekvenser for eksempel for ofrenes fysiske eller psykiske integritet. I noen tilfelle er ofrene mer indirekte skadelidende, som for eksempel ved narkotikakriminalitet. I andre tilfelle er det skaden den straffbare handlingen påfører vårt økonomiske system eller samfunnet for øvrig som begrunner kriminaliseringen. Terrorisme og tilfeller av alvorlig korrupsjon er eksempler på kriminelle handlinger som er egnet til å svekke stabiliteten i samfunnet, jf. også NOU 2009: 15 side 68-69.

Kriminelle handlinger er imidlertid ikke bare skadelige i hvert enkelt tilfelle, men har samlet sett også en generell destabiliserende effekt på samfunnet. Opplever borgerne at trusselen om kriminalitet blir for stor, vil det skape en utrygghetsfølelse. Denne vil for eksempel kunne true samfunnsikkerheten ved at borgerne tar oppgaven med å beskytte seg og sine i egne hender. En slik utrygghetsfølelse vil også kunne svekke borgernes tillit til staten, en tillit som er en forutsetning for vår samfunnsorden og vårt demokrati.

Uavhengig av om det er enkeltindivider eller samfunnsinteresser som er beskyttelsesobjektet, er det tungtveiende hensyn som begrunner kriminaliseringen av straffbare handlinger i det konkrete tilfellet. For at strafferettens underliggende målsetninger skal kunne realiseres, er det nødvendig at politiet har virkemidler som er tilstrekkelig effektive i arbeidet med å begrense omfanget av den alvorlige kriminaliteten.

1.3. Lagringsplikt som effektivt kriminalitetsbekjempende tiltak

Til grunn for den lagringsforpliktelsen som følger av Datalagringsdirektivet ligger en felles forståelse blant alle EUs medlemsland om at trafikkdata er et viktig verktøy for politiet i forebyggingen og oppklaringen av alvorlig kriminalitet. Dette fremkommer i avsnitt 11 i direktivets fortale, der det heter at det *”er i undersøgelser blevet påvist, og medlemsstaterne har praktisk erfaring for, at trafikkdata og lokaliseringsdata har stor betydning i etterforskning, avsløring og retsforfølging av straffbare handlinger”* og at det derfor anses nødvendig å sikre på europeisk plan at slike data lagres i en viss periode og på direktivets betingelser.

Denne forutsetningen er blitt hyppig og kraftig bestridt i den norske debatten om direktivet, og dokumentasjon på effektiviteten er etterlyst, jf. for eksempel NOU 2009: 1 side 222.

Det finnes imidlertid flere uavhengige kilder som sier noe om betydningen av trafikkdata for avdekkingen av alvorlig kriminalitet. Vi viser særlig til Metodekontrollutvalgets utredning NOU 2009: 15 Skjult informasjon – åpen kontroll på side 216-222. Av utredningen fremgår at utvalget, som blant annet var bedt om å foreta en evaluering av reglene om skjulte tvangsmidler, ikke fikk foretatt evalueringen på den måten det ønsket, jf. særlig utredningen side 111-112. Til tross for dette inneholder utredningen informasjon fra flere kilder som sier noe om betydningen av trafikkdata for etterforskningen.

Metodekontrollutvalget viser for det første til den svenske regjeringens årlige rapport til Riksdagen, som blant annet inneholder regjeringens syn på effektiviteten av bruken av hemmelig teleovervåking, som er den svenske betegnelsen på politiets innhenting av trafikkdata. Effektiviteten beregnes ut fra andelen tilfeller der anvendelse av overvåkingen har hatt *”betydning for etterforskningen”*, nærmere bestemt der den har ledet til anvendelse av et annet tvangsmiddel mot mistenkte, for eksempel pågrep. Det er med andre ord en begrenset definisjon av *”betydning”* som legges til grunn, det er ikke tilstrekkelig at overvåkingen har brakt etterforskningen fremover på annen måte, for eksempel ved at den aktuelle mistanken har bortfalt eller andre enn mistenkte er blitt pågrepet. De svenske tallene viser at i årene 2005 til 2007 hadde bruken av trafikkdata slik betydning for etterforskningen i henholdsvis 47, 50 og 51 prosent av tilfellene der metoden ble brukt. Svenske myndigheter vurderte tallene fra 2007 som gode, og konkluderte med at *”användningen av hemliga tvångsmedel även under år 2007 har varit framgångsrik och utgjort ett nödvändigt och viktigt instrument i den brottsutredande verksamheten”*, jf. NOU 2009: 15 side 115.

For det andre viser utvalget til en undersøkelse fra Max Planck-instituttet for utenlandsk og internasjonal strafferett der politiets utbytte av trafikkdata i etterforskning og straffforfølging ble undersøkt ved en analyse av saksdokumenter, en spørreundersøkelse og dybdeintervjuer av relevante aktører. Ifølge utvalget viser de tyske forskernes

analyse av saksdokumenter at innhenting av trafikkdata ga resultater i 35 prosent av sakene der de ble innhentet, jf. NOU 2009: 15 side 117. 63 prosent av personene som ble dybdeintervjuet oppga at metoden var avgjørende viktig i etterforskningsfasen, og da særlig i etterforskningen av organisert kriminalitet, narkotikakriminalitet, ransforbrytelser, gjengkriminalitet og datakriminalitet.

På bakgrunn av disse kildene konkluderer et samlet Metodekontrollutvalg med at *”trafikkdata må antas å ha betydning i minimum 40 prosent av de sakene de brukes”*. Utvalget peker videre på at tallene som Personvernkommissjonen viste til ikke er hentet fra den tyske undersøkelsen, men fra en betenkning avgitt til den tyske forfatningsdomstolen som tar utgangspunkt i undersøkelsen. Utvalget sa seg også uenig i Personvernkommissjonens slutninger og uttalte *”at det ikke gir mening å se nytten av trafikkdata i sammenheng med oppklaring av det totale antallet kriminalsaker”*. Utvalget anførte at dersom nytteverdien skal sees i sammenheng med oppklaring av saker, må det eventuelt sammenliknes med oppklaring av den type kriminalitet det er tillatt eller ment brukt i etterforskningen av, og da særlig organisert kriminalitet og narkotikakriminalitet, jf. NOU 2009: 15 side 122.

ØKOKRIMs syn er at Metodekontrollutvalgets konklusjon kan legges til grunn som et minimum for hvilken betydning trafikkdata har for etterforskningen i saker der slike data innhentes, og at andelen i realiteten er betraktelig større. Videre er det ØKOKRIMs oppfatning at man ikke bare kan vektlegge andelen saker trafikkdata har betydning i, men også må ta hensyn til hvor stor denne betydningen er når dataene først viser seg betydningsfulle.

Det sier seg selv at trafikkdata kan være av avgjørende betydning ved at de påviser hvor en person befant seg da en kirke ble påtent eller hvem som sist ringte et drapsoffer rett før vedkommende ble drept. Dette er ikke bare typiske tilfelle der trafikkdata vil kunne være avgjørende bevis, men også eksempler på straffbare handlinger som ofte avdekkes etter at de er begått. Det har vært anført i debatten at andre etterforskningsmetoder kan være fullgode erstatninger for trafikkdata, for eksempel sikring av elektroniske data etter straffeprosessloven § 215a eller kommunikasjonskontroll etter straffeprosessloven §§ 216a og 216b. Selv om fokuset på å avverge kriminalitet før den begås har økt de siste årene, er hovedregelen fremdeles at politiet kommer inn i etterkant. For å kunne påvise brannstifterens oppholdssted eller drapsmannens kontakt med offeret, er kommunikasjonskontroll eller sikringspålegg nytteløst; det avgjørende vil være om trafikkdata fra gjerningstidspunktet ble lagret, før de kriminelle handlingene allerede er begått.

Videre har enkelte kriminalitetstyper *særtrekk som gjør trafikkdata særlig relevante og betydningsfulle*. Disse er også i hovedsak kriminalitetstyper som har økt i omfang og alvor de senere årene, jf. for eksempel redegjørelsen for kriminalitetsutviklingen i NOU 2009: 15 side 74-100. Det gjelder først og fremst kriminalitet som begås av flere personer i fellesskap, der kommunikasjonen mellom aktørene står sentralt.

Kommunikasjonen kan for det første være *det eneste elementet som knytter vedkommende til det straffbare forholdet*, noe som ofte er tilfelle for bakmenn i kriminelle virksomheter. Narkotikavirksomhet er et typisk eksempel på hvordan de som står bak organiseringen av virksomheten og som oppnår den største fortjenesten aldri vil ha fysisk kontakt med det som gjør handlingen straffbar – narkotikaen – men bare kan knyttes til dette gjennom sin kommunikasjon med de som faktisk håndterer stoffet.

ØKOKRIM har imidlertid også i en rekke saker erfart at den som initierer eller organiserer for eksempel et større bedragerikompleks, ikke nødvendigvis er den som fører kontakten med de bedratte, men gjør bruk av stråmenn eller profesjonelle medhjelpere til dette. Dersom pengestrømmene ikke kan spores tilbake til hovedmennene, for eksempel fordi stråmennene mottar pengene og tar dem ut i kontanter, vil kommunikasjonen med medhjelperne i praksis være det eneste som knytter hovedmennene til forbrytelsen.

For det andre kan selve *kommunikasjonen være den eneste komponenten som skiller en straffbar handling fra en lovlig handling*. Dette er tilfellet ved viktige former for verdipapirkriminalitet, for eksempel ulovlig innsidehandel og misbruk av innsideinformasjon. Objektivt sett er det ingenting som skiller et tilfelle av ulovlig innsidehandel fra en lovlig gjennomført transaksjon – den vil fremstå som og registreres på samme måte i alle systemer. Forskjellen på en lovlig handel og en ulovlig innsidehandel beror utelukkende på hvorvidt innsideinformasjon ble kommunisert til den handlende i forkant av handelen. Normalt vil ingen andre enn de impliserte selv kjenne til *om* det har vært noen kommunikasjon som har muliggjort overlevering av innsideinformasjon, og enn mindre *hva* innholdet i denne kommunikasjonen i så fall var. Dette er altså kriminalitet hvor den elektroniske kommunikasjon reelt sett er ”åstedet” for forbrytelsen, og hvor fraværet av fornærmede og vitner innebærer at ”åstedsundersøkelser” i form av gjennomgang av kommunikasjonsdata er den eneste muligheten politiet har for å avklare *om* det er begått en straffbar handling.

ØKOKRIM vil fremhevet ett eksempel på en sak om innsidehandel der trafikkdata fikk stor betydning både for etterforskningen og iretteføringen. Saken gjaldt bl.a. innsidehandel og annen misbruk av innsideinformasjon i forbindelse med tre forskjellige oppkjøpssituasjoner. Totalt er åtte personer tiltalt, hvorav seks er domfelt. Hovedforhandlingen mot fem av de tiltalte gikk over 31 dager og det ble ført over 50 vitner. Tre av de tiltalte ble dømt til de strengeste straffene som er utmålt i innsidesaker i Norge. Om bevissituasjonen heter det innledningsvis i tingrettens dom 11. juli 2007 (ikke rettskraftig) at det ikke for noen av tiltalepostene finnes enkeltstående bevis som i seg selv er avgjørende for skyldspørsmålet, men at det er et sammenfall av hendelser og en innbyrdes sammenheng mellom disse som etter vårt syn bør føre til domfellelse. For alle de tre hovedpostene går det igjen at retten viser til og legger vekt på framlagte trafikkdata. Avslutningsvis i dommen uttales bl.a.:

"Overfor er det konkludert med at det faktisk fant sted kommunikasjon mellom de tiltalte på tidspunkter som faller sammen med kjøp av aksjer og salg av aksjer. Det er et påfallende sammenfall i tid mellom denne kommunikasjonen, de aktuelle selskapsbegivenhetene og X tilgang til innsideinformasjon."

Det ble selvsagt også ført en rekke andre bevis for tingretten, men trafikkdataene var helt sentrale. Det ville helt enkelt ikke blitt noen domfellelser i dette sakskomplekset dersom politiet ikke hadde hatt tilgang til de aktuelle trafikkdata.

I enkelte tilfelle kan det endatil være at *kommunikasjonen utgjør den straffbare handlingen*. Dette vil særlig være tilfellet ved ulike former for psykisk medvirkning og oppfordring til, trusler om eller inngåelse av forbund om å begå straffbare handlinger. Igjen kan et illustrerende eksempel hentes fra verdipapirkriminaliteten: En straffbar tilskyndelse til innsidehandel etter verdipapirhandelloven § 3-3 begås når en person med innsideinformasjon oppfordrer eller på annen vis ansporer en annen til å handle.

Erfaringsmessig skjer dette gjennom bruk av elektroniske kommunikasjon, typisk ved bruk av telefon, e-post eller andre elektroniske kommunikasjonskanaler. I slike tilfelle er det kommunikasjonen av innsideinformasjonen som utgjør den straffbare handlingen. Sprederen av innsideinformasjonen vil dermed ikke kunne bli straffedømt dersom det ikke kan påvises at vedkommende har kommunisert med den handlende. I dagens elektroniske kommunikasjonssamfunn, vil dette som den store hovedregel måtte skje ved trafikkdata. Som beskrevet ovenfor vil heller ikke den som har mottatt innsideinformasjon etterlate seg andre objektivt registrerbare spor som viser at det er begått en kriminell handling. Skulle tilgangen til trafikkdata falle bort, innebærer det dermed at de straffebedene som kriminaliserer slike handlinger i praksis vil bli bortimot virkningsløse.

Problemstillingen over er ikke bare relevant med tanke på bekjempelse av innsidekriminalitet, men av betydning for bekjempelsen av *verdipapirkriminalitet* generelt. Et særtrekk ved verdipapirmarkedet er informasjonens helt sentrale funksjon. Det er informasjon som har økonomisk verdi for aktørene i verdipapirmarkedet. Reguleringen av verdipapirmarkedet kan i all hovedsak ses på som en regulering av informasjonsflyt. For å oppnå et rettferdig marked er det fastlagt en rekke straffebelagte plikter og forbud, som skal sikre at alle aktører har like muligheter til å skaffe seg relevant informasjon. Verdipapirkriminalitet er således brudd på regler om kommunikasjon av kursrelevant informasjon eller brudd på adferdsregler utløst av at man enten besitter konkret informasjon eller en særskilt posisjon og hvor kriminalitetens eneste objektivt registrerbare spor er selve kommunikasjonen. Skulle norsk politi bli den eneste politistyrken innenfor EØS-området uten tilgang til slike data, er det grunn til å frykte at en andel av de som driver med verdipapirkriminalitet vil legge sin virksomhet til Oslo Børs.

Flere av verdipapirkriminalitetens særskilte karaktertrekk som igjen gjør trafikkdataenes betydning avgjørende for straffeforfølgningen, preger også enkelte andre former for økonomisk kriminalitet. Dette gjelder blant annet enkelte typetilfeller av *kartellvirksomhet*, *brudd på konkurranselovgivningen*, *bedragerier* og *korruptjonssaker*. Etterforskningen av slike saker vil dermed også vanskeliggjøres dersom politiets tilgang til trafikkdata forsvinner.

Generelt er analyser av finansielle transaksjoner og pengestrømmer av sentral betydning i en stor andel av de sakene som etterforskes hos ØKOKRIM. Trafikkdata vil svært ofte kunne ha stor bevisverdi når pengetransaksjoner/kontoinformasjon sammenholdes med hvem som har telefonisk kontakt i tilknytning til transaksjonene. For eksempel der det kan vises til utstrakt telefonkontakt mellom enkeltpersoner på samme tidspunkt som det skjer en større overføring fra én konto til en annen, vil dette kunne gi anvisning på hvem som er den reelle mottaker av pengene. ØKOKRIM har etterforsket flere saker der man ved hjelp av trafikkdata kunnet avdekke hvem som var de sentrale aktørene i saken ved å se på intensiteten i kontakt mellom dem (uten at noen av disse er endt med bevisføring om dette i retten).

Også i etterforskningen av flere typer miljøkriminalitet vil trafikkdata kunne gi viktige bidrag, for eksempel ved at å påvise hvem som befant seg i nærheten på det tidspunkt miljøfarlig avfall ble dumpet eller et kunstverk ble stjålet, eller hvem en mistenkt kommuniserte med i samme periode. ØKOKRIMs erfaring viser at ulovlig jakt ofte er godt organisert virksomhet, noe trafikkdata vil være viktig for å kunne påvise. I en dom om ulovlig bjørnejakt avsagt i Sør-Østerdal tingrett 12. november 2009 (delvis

rettskraftig) er logger over trafikken mellom en GPS-peiler som var festet på en av hundene som ble brukt i jakten og én av de tiltaltes mobiltelefon brukt aktivt som bevis og grundig omtalt i dommen. Trafikkdataene ble blant annet ansett å vise at vilkårene i viltloven § 56 siste ledd var oppfylt i forhold til hovedmannen i saken. Retten konkluderte på følgende måte:

”Retten finner det bevist at A har gjort seg skyldig i å jage fredet vilt, senest fra det tidspunkt han deltok i samhandlingen med å sette hundepileren sin på Æ, og deretter ved å peile hunden mens hunden loset på bjørnen i en lengre periode, helt frem til A felte den.”

I tillegg til å bekrefte trafikkkdatas betydning for irettføringen av saker om ulovlig jakt, illustrerer dommen at trafikkkdata kan få økt betydning i tak med at vi tar i bruk nye tekniske hjelpemidler i hverdagen.

Som det vises til i høringsnotatet punkt 4.1 vil trafikkkdata kunne være betydningsfulle i etterforskningen av de former for kriminalitet som har tiltatt som følge av *den teknologiske utviklingen*. Økt tilgang til og bruk av Internett har generert både nye former for kriminalitet og nye versjoner av eller arenaer for tradisjonelle straffbare handlinger. Dette er sterkt merkbart innenfor området økonomisk kriminalitet, for eksempel i økningen av antall anmeldelse av straffbare handlinger som følge av *identitetstyverier*. Dette er også handlinger som i utgangspunktet fremstår som lovlige, men som er ulovlige fordi den som gjennomfører dem er en annen enn den vedkommende utgir seg for å være. Der de tapsbringende handlingene gjennomføres på Internett, kan den eneste måten å påvise at det dreier seg om et bedrageri på, være å knytte den aktuelle ip-adressen til en annen person enn den hvis identitet er stjålet. Det må legges til grunn at behovet for å påvise tilknytning mellom kriminelle handlinger begått på Internett og enkeltpersoner vil øke i tiden fremover. I forlengelsen av dette vil ØKOKRIM påpeke at Internett og andre elektroniske kommunikasjonskanaler i dag utgjør kritisk samfunnsstruktur. En rekke samfunnsoppgaver er flyttet og vil flyttes over i elektroniske fora, som for eksempel levering av selvangivelsen på altinn.no, banktjenester, andre offentlige tjenester og trolig også gjennomføringen av fremtidige nasjonale og lokale valg. Disse sentrale samfunnsstrukturene vil bli svært sårbare for kriminelle handlinger dersom ikke data om bruken av dem registreres. For å ha mulighet til å holde følge med utviklingen på dette området, bør slik vi ser det politiets mulighet til teknologisk etterforskning og tilgang til opplysninger om internettbruk styrkes, ikke svekkes, som vil være tilfelle dersom trafikkkdataene forsvinner.

1.4. Lagringsplikt som forholdsmessig tiltak

Til tross for at et tiltak må anses både som viktig og effektivt i bekjempelsen av alvorlig kriminalitet, er det klart at dette må veies opp mot graden av inngrep tiltaket innebærer i enkeltmenneskers personvern.

Dette følger for det første av Norges forpliktelser etter EMK artikkel 8 første jf. annet ledd. ØKOKRIM slutter seg til konklusjonen i høringsbrevets punkt 4.2 om at plikten til å lagre data som nedfelt i Datalagringsdirektivet ikke er i strid med EMK artikkel 8. Vi viser for øvrig til den nærmere drøftelsen av dette i artikkelen ”Datalagringsdirektivet – en menneskerettskrenkelse eller forpliktelse” av Ingvild Bruce, Lov og rett nr. 1-2/2010 side 6-26 og artikkelen ”Implementering av Datalagringsdirektivet – et nødvendig,

effektivt og forholdsmessig tiltak” av Ingvild Bruce og Trond Eirik Schea i Tidsskrift for strafferett nr. 1/2010 side 75-90.

Også uavhengig av våre menneskerettslige forpliktelser er det ØKOKRIMs syn at innføring av lagringsplikt bare kan rettferdiggjøres dersom avveiningen mellom hensynet til bekjempelse av alvorlig kriminalitet og hensynet til personvernet tilsier at dette er et forholdsmessig tiltak. I denne vurderingen er det etter ØKOKRIMs syn relevant at lagring av trafikkdata innenfor de rammer Datalagringsdirektivet oppstiller, vil utgjøre en relativt *liten andel av den samlede mengden personlige data som lagres i dag*. I tillegg til personregistre, kunderegistre, pasientregistre og informasjon som lagres hos finansinstitusjoner, legger et flertall av oss igjen en overveldende mengde elektroniske spor som ledd i våre hverdagslige gjøremål, slik som ved bruk av bankkort, betaling i bomring, bruk av kollektivtrafikk og på jobben.

Den overveldende mengden av elektroniske spor og personlige opplysninger vi hver dag frivillig legger igjen etter oss, kan etter vårt syn tyde på at *befolkningen ikke anser slike data som så veldig personlige* eller sensitive. Det er dermed ikke nødvendigvis slik at lagring av trafikkdata vil virke særlig hemmende på folks personlige utfoldelse og frimodighet.

Det er videre av stor betydning for vurderingen av lagringens forholdsmessighet at det kun er data om *omstendighetene rundt kommunikasjon*, ikke om *innholdet i kommunikasjonen* som skal lagres. Innholdet i samtaler, SMS eller e-post skal altså ikke lagres, ei heller hvilke nettsteder man har besøkt. At trafikkdata er mindre sensitivt enn innholdsdata reflekteres i forskjellene i kriminalitetskravet for henholdsvis innhenting av trafikkdata og gjennomføring av kommunikasjonsavlytting. Det er også lagt til grunn i EMD-praksis, jf. P.G. og J.H. mot Storbritannia (dom 25.september 2001, saksnr. 44787/98) avsnitt 83-84.

Det har vært anført at innføringen av en plikt til å lagre trafikkdata er uforholdsmessig fordi det samme kunne vært oppnådd med andre, og mindre inngripende virkemidler. Som tidligere nevnt, finnes det imidlertid *ingen andre etterforskningsmetoder som kan utgjøre noen erstatning for trafikkdata*. Dette blir særlig tydelig i tilfelle der politiet kommer inn *etter* at den aktuelle straffbare handlingen er begått, og har behov for opplysninger om kommunikasjonen på gjerningstidspunktet. De metodene som er anført som alternativer, for eksempel sikring av elektronisk lagrede data etter straffeprosessloven § 215a, kommunikasjonsavlytting etter § 216a, pålegg om utlevering av fremtidige trafikkdata etter § 216b, er alle metoder som må igangsettes i forkant for å dekke handlingstidspunktet, og kan ikke brukes der politiet først kommer inn i ettertid. For ØKOKRIM er dette tilfellet i så godt som alle saker, jf. også nedenfor pkt. 2.2 om lagringstid.

Det kan derimot anføres at manglende tilgang til trafikkdata vil kunne *svække politiets muligheter til å bruke andre etterforskningsmetoder* på effektiv måte. Enkelte typer trafikkdata kan nemlig være nødvendige for at politiet skal kunne igangsette kommunikasjonskontroll etter straffeprosessloven §§ 216a og 216b. I en begjæring om kommunikasjonskontroll må politiet identifisere det eller de kommunikasjonsanleggene de ønsker å avlytte, for eksempel ved såkalte IMEI- eller IMSI-numre for mobiltelefoner eller ved nettverksadresser eller ip-adresser når det gjelder datamaskiner. Sluttes man å lagre disse dataene, vil mulighetene til å bruke kommunikasjonskontroll, som er en effektiv og nyttig etterforskningsmetode, svekkes.

Samtidig vil et tap av tilgang til trafikkdata også kunne resultere i at bruken av *andre og mer inngripende etterforskningsmetoder vil måtte økes* både i antall og omfang. Der man ved hjelp av trafikkdata som hovedregel enkelt vil kunne si hvor en person har befunnet seg på et visst tidspunkt, vil man måtte foreta bredere informasjonssøk, for eksempel ved intensiv spaning eller ransaking. Det vises til at trafikkdata ofte vil være med å utelukke eller frikjenne enkeltpersoner fra mistanke om involvering i straffbare handlinger. Bruk av alternative etterforskningsmetoder som vitneavhør eller ransaking vil også kunne føre til at viktig tid gå tapt og skade kunne skje i mellomtiden. Dette vil igjen kunne føre til at mistenkte rekker å destruere bevis eller forlate landet. Ved igangsetting av kommunikasjonskontroll vil politiet ikke ha den samme oversikten over nettverkene i den kriminelle virksomheten når avlytting igangsettes, noe som gjør at det kan gå lenger tid før man får samme forståelse av hvem som er aktørene og hva som foregår i saken. Manglende tilgang til trafikkdata vil dermed kunne føre til at politiets etterforskning vil måtte gjennomføres på langt mer inngripende måter enn tidligere.

Av betydning for forholdsmessigheten er også *vilkårene for tilgang til lagrede data og kontrollregimet som gjelder for lagringen* og oppbevaringen av disse, samt politiets tilgang til og bruk av dataene. Uten å foregripe de spørsmål som vil redegjøres for i punkt 2, vises det til at Regjeringens forslag etter ØKOKRIMs syn vil kunne danne grunnlag for et rettssikkert system med solid kontroll. Det understrekes at dagens teknologi byr på store muligheter til å etablere sikkerhetsregimer rundt lagringen av dataene, kontroll med tilgangen til og den videre bruken av dem, noe som gjør at en eventuell fare for misbruk må anses som minimal.

I lys av dette er det ØKOKRIMs klare oppfatning at innføring av *lagringsplikt for trafikkdata utgjør et forholdsmessig tiltak*, særlig i lys av betydningen for politiets mulighet til å bekjempe alvorlig kriminalitet.

2. Kommentarer til høringsforslaget

2.1. Innledning

Vi vil i det følgende knytte enkelte kommentarer til de delene av høringsforslaget som fremstår som spesielt viktige for politiets evne til å bekjempe alvorlig kriminalitet, nemlig hvor lenge trafikkdata skal lagres og vilkårene for politiets tilgang til dataene i den enkelte sak. Fokus rettes mot de kriminalitetstypene som faller innenfor ØKOKRIMs ansvarsområder.

2.2. Lagringstid

Hensynet til etterforskningen av økonomiske straffesaker av det format som foregår hos ØKOKRIM tilsier åpenbart at trafikkdata lagres så lenge som mulig innenfor direktivets rammer. ØKOKRIM etterforsker kriminalitetstyper hvor det gjerne tar lang tid fra lovbruddet begås til mistanke i det hele tatt vekkes, for eksempel gjennom revisors kontroll med regnskaper eller kontrollorganers undersøkelser av hendelser eller virksomheter. Ikke sjelden tar også avdekkingsfasen hos ØKOKRIM lang tid; mistankegrunnlaget retter seg for eksempel innledningsvis kun mot én person for noen lovbrudd, mens det først etter en del etterforskning oppstår mistanke mot flere andre personer og/eller om andre alvorlige lovbrudd enn de først avdekkede. Dette gjelder særlig i de mest alvorlige og best organiserte sakene. I mange av ØKOKRIMs største

saker de siste årene har man således først kommet "i posisjon" til å begjære innhentet trafikkdata etter at dataene etter dagens ordning er slettet. Det er lite tvilsomt at et antall personer ansvarlige for alvorlig økonomisk kriminalitet har gått fri fra strafforfølgning på grunn av dette.

Innsidesaken beskrevet ovenfor på side 5 er også en illustrasjon på at enkelte andre personer enn de som ble tiltalt, først kom i politiets søkelys et stykke ut i etterforskningen – slik at trafikkdata for deres telefoner mv var slettet i mellomtiden. Det senere tidspunktet lå noe over ett år etter den aktuelle kommunikasjonen, slik at med lagringsplikt i halvannet år ville dataene vært tilgjengelige. Det ble ingen strafforfølgning mot de aktuelle personene.

Videre bygger, som sagt, mange av sakene hos ØKOKRIM på anmeldelser fra ulike kontrollorgan. Disse vil i forkant av anmeldelsen ofte ha brukt lang tid på å undersøke de aktuelle forholdene. Når departementene nå i høringsbrevets punkt 4.12 og 4.13 går inn for at det kun er politiet som skal ha tilgang til trafikkdata, blir det desto viktigere at lagringstiden er lang nok til at dataene fremdeles er tilgjengelig etter at kontrollorganene har avsluttet sine undersøkelser.

Hensynet til etterforskningen av alvorlig økonomisk kriminalitet tilsier derfor at tilbyderne bør pålegges å lagre trafikkdata i minst ett år.

2.3. *Politiets tilgang til data*

Departementene har foreslått at utlevering av trafikkdata bare skal kunne pålegges dersom noen med skjellig grunn mistenkes for et lovbrudd med en strafferamme på fengsel i tre år eller mer, eller dersom lovbruddet er særlig vanskelig å etterforske uten tilgang til data.

ØKOKRIM slutter seg til utgangspunktet om at inngripende etterforskningsmetoder bare bør kunne brukes i etterforskningen av alvorlig kriminalitet eller der det dreier seg om lovbrudd som av ulike årsaker er særlig vanskelige å etterforske uten slike metoder. Men departementenes forslag innebærer en innskrenking av politiets tilgang til trafikkdata i forhold til i dag på tre måter: det kreves skjellig grunn til mistanke, noe som ikke har vært tilfellet til nå, det kreves at mistanken er rettet mot en bestemt person og det kreves at lovbruddet må være av et visst alvor eller en viss karakter. Ettersom lagring og innhenting av trafikkdata etter ØKOKRIMs syn ikke er blant de mest inngripende etterforskningsmetodene, innebærer forslaget i høringsnotatet en *for* kraftig innskrenking av politiets tilgang til trafikkdata. ØKOKRIMs syn på hvorfor og hvordan de respektive vilkårene bør justeres, vil redegjøres for i det følgende.

2.3.1. *Kravet til forbrytelsens alvor eller karakter*

I høringsnotatet foreslås det som nevnt at utlevering av trafikkdata bare skal kunne pålegges dersom noen med skjellig grunn mistenkes for et lovbrudd med en strafferamme på fengsel i tre år eller mer, eller der det dreier seg om angitte lovbruddstyper som er særskilt vanskelig å etterforske uten tilgang til data. Disse er i følge forslaget spionasje, terrorvirksomhet som rammes av straffeloven § 104 a, brudd på taushetsplikt etter § 132 b, datakriminalitet etter § 145 annet ledd, § 145 a om telefonavlytting, § 162 om narkotikalovbrudd, § 317 om hvitvasking, § 390 a om forstyrrelse av privatlivets fred, samt bestemmelser om seksuallovbrudd mot barn.

De fleste av sakstypene som omfattes av ØKOKRIMs arbeidsområde oppfyller kravet til tre års strafferamme. Videre slutter ØKOKRIM seg til forslaget om at straffeloven § 317 skal være en av de særskilte forbrytelsene som kan gi grunnlag for utlevering av trafikkdata.

Blant de straffebud det foreslås unntak for er straffeloven § 132 b, som gjelder brudd på taushetsplikt ilagt av retten i forbindelse med benyttede tvangsmidler som ransaking eller beslag. ØKOKRIM støtter dette forslaget. Det er imidlertid uklart for ØKOKRIM om og eventuelt hvorfor det antas at etterforskningen av brudd på taushetsplikten etter straffeloven § 132 b er vanskeligere å etterforske uten tilgang til data enn brudd på andre typer taushetsplikt. Slik ØKOKRIM ser det, fremstår eksempelvis brudd på taushetsplikten etter vphl § 3-4 første ledd som etter § 17-3 annet ledd har ett års strafferamme, som minst like vanskelig å etterforske uten tilgang til data. I lys av at kilden regulært vil kunne være relativt mange personer, fremstår det som tilnærmet umulig å oppklare hvem kilden er uten tilgang til data, og det foreslås derfor at dette lovbruddet tas inn i oppregningen av de særskilte straffbare handlingene som kan gi grunnlag for utlevering av trafikkdata. Vi oppfordrer departementene til også å vurdere om andre straffebestemmelser om brudd på taushetsplikt bør kunne gi grunnlag for utlevering av data.

For øvrig ser vi at strafferammekravet vil være av større betydning for politidistriktene enn for ØKOKRIM. Vi påpeker i den sammenheng at en rekke straffeprosessuelle tvangsmidler står uten denne typen alvorlighetskrav men at det generelle prinsippet om forholdsmessighet gjelder. Det er for oss paradoksalt at et strafferammekrav på fengsel i 3 år skal innføres for så vidt gjelder trafikkdata spesielt.

2.3.2. *Kravet om skjellig grunn til mistanke mot en bestemt person*

Som det fremgår av høringsnotatet punkt 2.5, har Post- og teletilsynet i vurderingen av om trafikkdata kunne utleveres, lagt vekt på ”hvorvidt telefonen disponeres av en person som har straffeprosessuell stilling som siktet eller mistenkt”, likevel uten at dette har vært noe absolutt krav. Kravet om *skjellig grunn* til mistanke mot en *bestemt person*, vil således innebære en betraktelig skjerping av mistankekravet. Kravet vil etter ØKOKRIMs syn vanskeliggjøre etterforskningen av alvorlig kriminalitet betraktelig.

Departementenes høringsforslag bygger på en anerkjennelse av at enkelte typer lovbrudd er ”*særskilt vanskelig å etterforske uten tilgang til data*”. I relasjon til disse fremstår kravet om at skjellig grunn til mistanke må foreligge *før* man får tilgang til data paradoksalt, ettersom det ligger i erkjennelsen av disse vanskelighetene at det også vil være vanskelig å etablere skjellig grunn til mistanke uten tilgang til data. Opprettholdes kravet om skjellig grunn i slike saker, er det sannsynlig at mange lovbrytere hvis skyld kunne vært påvist ved tilgang til trafikkdata, vil gå fri fordi det uten slike data ikke en gang kan påvises skjellig grunn til mistanke.

Dette vil for eksempel gjelde etterforskningen av handlinger der kommunikasjonen er den eneste komponenten som skiller en straffbar handling fra en lovlig handling, altså der det er selve kommunikasjonen som gjør handlingen ulovlig, jf. også ovenfor i punkt 1.3 om betydningen av trafikkdata for etterforskningen av slike handlinger. I slike tilfelle vil trafikkdata være essensielle for i det hele tatt å påvise skjellig grunn til mistanke. For

ØKOKRIMs del gjelder dette særlig i etterforskningen av verdipapirkriminalitet, der det ulovlige består i kommunikasjon mellom parter.

Man kunne tenke seg en løsning der kravet om skjellig grunn til mistanke ble sløyet i relasjon til de lovbrudd som anses særskilt vanskelige å etterforske uten tilgang til data. I så tilfelle må det imidlertid foretas en vurdering av hvilke lovbrudd dette gjelder også innenfor den gruppen lovbrudd som har tre års strafferamme eller mer. Dette vil innebære en svært komplisert vurdering og også en komplisert lovteknisk løsning. ØKOKRIM foreslår derfor at kravet om skjellig grunn til mistanke fjernes fra regelen om utlevering av trafikkdata.

Uavhengig av dette forslaget, foreslår ØKOKRIM at man vurderer å fjerne kravet om at mistanken må knytte seg til en bestemt person. Dette vil trolig ikke utgjøre noen avgjørende forskjell i ØKOKRIMs saker, men resten av politiet har stor nytte av trafikkdata i saker der man enda ikke har noen mistenkt, for eksempel i forsvinningssaker, drapssaker etc., der man innhenter trafikkdata knyttet til et åsted.

2.3.3 Beslutningskompetanse

I høringsnotatet foreslås beslutningskompetansen lagt til retten, uten hastekompetanse til påtalemyndigheten. Straffeprosessens system er i Norge – i motsetning til mange andre europeiske land – at etterforskning er underlagt påtalemyndighetens kontroll. Generelt er det slik at straffeprosessuelle tvangsmidler hvor retten har beslutningskompetansen, likevel kan besluttes av påtalemyndigheten i hastetilfeller. Dette gjelder også for de mest inngripende tvangsmidlene som kommunikasjonsskontroll og romavlytting. Hastekompetansen er tildelt fordi det i en del tilfeller er nødvendig for at bevisene skal la seg sikre. Dette gjelder ikke mindre for trafikkdata enn for andre bevis. Vi foreslår derfor at det vurderes å innføre en bestemmelse om hastekompetanse til påtalemyndigheten også for så vidt gjelder trafikkdata.

Med vennlig hilsen

Trond Eirik Schea
ØKOKRIM-sjef

Ingvild Bruce
politiadvokat

Kopi: Riksadvokaten, Politidirektoratet