Samferdselsdepartementet

Postboks 8010 Dep.
0030 OSLO

Vår saksbehandler:	Kopi til	Vår dato	Vår referanse	Deres referanse
Jorunn Solgaard		17.03.2010	2007-0063	09/585-HK

Høringssvar - datalagringsdirektivet

De mest sentrale spørsmålene i debatten om datalagringsdirektivet har vært en avveining mellom samfunnets behov for verktøy i kriminalitetsbekjempelsen og personvernet.

Unio har behandlet høringsnotatet og har valgt å støtte implementeringen av datalagringsdirektivet. Dette er gjort under forutsetning av at personvernhensynet, risikovurdering for misbruk av lagrede trafikkdata samt andre samfunnsverdier, slik som demokrati og rettssikkerhetsgarantier, blir ivaretatt og tillagt stor vekt.

Individets rettssikkerhet og myndighetene
Det er etter vår oppfatning viktig at borgere i Norge opplever at lagring av trafikkdata kun brukes i den hensikt som datalagringsdirektivet legger til grunn. I dag er den norske stat bygd på tillit mellom myndighetene og borgerne. Dersom borgerne som følge av datalagringsdirektivet opplever at myndighetene urettmessig overvåker dem, kan tilliten forvitre og samfunnet vårt vil utvikle seg i en retning som vi ikke er tjent med.

Debatten om datalagringsdirektivet har vært preget av sterkt engasjement og tydelige fronter. Både forkjempere og motstandere har levert sterke synspunkt. De politiske ungdomspartiene er alle i mot implementering av datalagringsdirektivet. Slik engasjement må myndighetene ta med seg i den videre behandlingen av saken. Mange frykter at innføringen av direktivet er et stort skritt på veien mot et overvåkningssamfunn, heller enn et forsøk på å ivareta borgernes sikkerhet og bekjempe organisert kriminalitet.

Det er derfor viktig at regjeringen og Stortinget er lydhøre overfor slike argumenter. Opplever man som borger at politikerne ignorerer denne skepsisen til å innføre datalagringsdirektivet, vil tilliten til myndighetene kunne svekkes.

Ved innføring av datalagringsdirektivet må myndighetene påse at enkeltindividets rettssikkerhet blir ivaretatt gjennom kontroll med bruk av trafikkdata, og sikring mot misbruk av trafikkdata.

Datalagringsdirektivets rolle for å bekjempe alvorlig kriminalitet
Kriminalitetsutviklingen viser en stadig økende andel av organiserte og profesjonelle aktører kommer til Norge utelukkende for å begå kriminalitet. Det stilles krav til politiet fra samfunnet side at disse utfordringene møtes med profesjonalitet og effektive verktøy.

Dette er hovedgrunnen til at Unio på visse vilkår støtter implementering av datalagringsdirektivet.

For politiet og samfunnet er bruken av trafikkdata et viktig verktøy i bekjempelsen av organisert og annen alvorlig kriminalitet. Bruk av elektroniske spor har vokst i takt med den teknologiske utviklingen og kriminalitetsutviklingen. Dette blir benyttet innen en rekke sakstyper, som organisert vinningskriminalitet, drap, vold og sedelighet, økonomisk kriminalitet, narkotika, menneskehandel og saker som omfatter forebygging av terrorvirksomhet.

Den teknologiske utviklingen gjør at en stadig større andel av kommunikasjonen skjer elektronisk. Hele befolkningen, inkludert kriminelle, benytter slik kommunikasjon og legger igjen elektroniske spor. Det er nødvendig at politiet i sin etterforskning kan benytte seg av relevant og tilgjengelig informasjon om kriminell aktivitet.

Dersom politiet ikke får hentet ut trafikkdata, når vilkårene for uthenting er til stede, vil det gi et sterkere vern for kriminelle enn for de som samfunnet skal beskytte mot kriminell aktivitet. Vi viser i denne sammenhengen til den europeiske menneskerettsdomstolens dom mot Finland. Saken gjaldt politiets adgang til å hente ut trafikkdata i forbindelse med at ukjent person hadde lagt ut intim informasjon om en tolvåring på internett. Teleselskapet var bundet av lovpålagt taushetsplikt som medførte at de ikke kunne utlevere trafikkdataene til politiet. Finland ble dømt fordi de ikke hadde et system som ivaretok personvernet til den krenkede tolvåringen, jf EMK art 8.

Betydningen av trafikkdata som bevis
Elektroniske spor omtales ofte som såkalte "tause vitner", og har fått en stadig større betydning for politiets arbeid spesielt relatert til bekjempelse av organisert og annen alvorlig kriminalitet. Utviklingen av arbeidsmetoder som benyttes i tunge, kriminelle miljøer, viser at vitner trues til taushet og gjør viktigheten av elektroniske spor desto større.

For å gi et bilde av hvor avgjørende trafikkdata er i etterforskningen av ulike straffesaker, redegjøres det i det følgende for noen sakstyper hvor trafikkdata er og har vært helt essensielt:

Mobile vinningskriminelle – seriesaker
OP Grenseløs i Vestfold har siden vinteren 2007 etterforsket og ført for retten en rekke saker som omfatter organiserte vinningskriminelle nettverk, hovedsakelig fra Øst-Europa. I samtlige av sakene har trafikkdata vært av helt avgjørende betydning. Basestasjonssøk fra åsteder (søk etter hvilke telefonnummer som har vært i nærheten av gjerningsstedet på aktuelt tidspunkt) har bl.a. medført at man har kunnet knytte omfattende seriesaker sammen, som har funnet sted i flere politidistrikt.

I den personrettede etterforskningen har trafikkdata innhentet fra mistenkte/siktede vært av avgjørende betydning for å kunne avdekke oppholdssted, reisevirksomhet, kriminell virksomhet og nettverkstilhørighet.

Drap, vold og sedelighet
I voldssaker blir det om mulig innhentet trafikkdata fra både mistenkt, siktet og fornærmede dersom dette ansees å ha relevans for saken. Er gjerningspersonen ukjent blir det innhentet basestasjonssøk for å forsøke i sirkle inn aktuell person. Trafikkdata er også her viktig for å kontrollere forklaringer som blir gitt, eventuelle aktuelle knytninger mellom fornærmede og gjerningsperson, nettverk, bevegelser og eventuelle ytterligere impliserte.

Trafikkdata blir i tillegg til å identifisere gjerningspersoner og nettverk benyttet i utstrakt grad for å avdekke hvilke telefonnummer som bør avlyttes for deretter å kunne identifisere og pågripe bakmenn for virksomheten. Saker som dette har ofte internasjonale dimensjoner hvor

trafikkdata er helt avgjørende for en god, samordnet etterforskning. Det internasjonale aspektet samt sakenes kompleksitet og omfang, gjør arbeidet svært ressurskrevende.

Internettrelaterte seksuelle overgrep
Den teknologiske utviklingen og Internett har skapt en ny arena for seksuelle overgrep. Identifisering av IP-adresser tilhørende overgripere eller personer som deler filer med f. eks barnepornografisk innhold, er helt avgjørende for at man skal kunne straffeforfølge gjerningspersonene. Ovennevnte saker har ofte internasjonale forgreninger, hvor filer med barnepornografisk innhold spres til store deler av verden på kort tid.

Utfordringen i dag er at tilbyderne av Internettjenester i Norge er pålagt å slette data etter 3 uker. Dette medfører svært begrensede muligheter for norsk politi til å kunne avdekke overgripere og personer som deler overgrepsmateriale over Internett. Problemet er at informasjonen som kan være med å identifisere gjerningspersoner er slettet, og at man derfor i praksis ikke klarer å etterforske og rettslig forfølge ovennevnte saker.

Datakriminalitet
Teknologien åpner som tidligere nevnt kontinuerlig for nye muligheter og arenaer for de kriminelle. Kriminalitetsutviklingen på dette området omfatter bl.a. datainnbrudd, nettbank- og kredittkortbedrageri, id-tyveri samt trakassering og trusler over Internett. Ulikt andre straffesaker finnes det her ingen andre alternative etterforskningsmetoder eller spor da kriminaliteten foregår "i den elektroniske verden". Sporene vil nesten alltid innbefatte en IP-adresse, men også her er utfordringen at lagringstiden er så kort at det setter store begrensninger for etterforskningen av disse sakene. Sakene har også her svært ofte internasjonale dimensjoner. Utveksling av informasjon og samordning av etterforskningen i et internasjonalt politisamarbeid er ressurskrevende og ikke minst tidkrevende. Et rigid regelverk med pålagt sletting av data etter 3 uker gir også her store utfordringer når det gjelder å løse oppgaven vi er satt til med å bekjempe kriminalitet av denne typen.

Forslag til innføring av strafferamme
Politiet får i dag utlevert trafikkdata dersom det antas å ha verdi som bevis i straffesaken. I forslaget som foreligger fra regjeringen ligger det en betydelig skjerpelse i forhold til dagens hovedregel, da det foreslås en strafferamme på fengsel i 3 år eller mer som grunnlag for å få utlevert data. En slik innskjerpelse vil kunne begrense politiets muligheter til å oppklare alvorlig kriminalitet.

Som eksempel på viktige saker hvor det kan bli vanskelig å få tilgang til trafikkdata dersom foreslåtte strafferamme innføres, er saker der barn og unge blir utsatt for mobbing, trakassering, sjikane eller trusler via internett/mobiltelefon. Dette er intet ukjent fenomen i dagens samfunn, og et særdeles viktig område å sette inn ressurser på.

Et annet område som kan nevnes er miljøkriminalitet. Lave strafferammer vil gjøre at sakene blir desto vanskeligere å etterforske dersom man i fremtiden ikke får tilgang til viktig trafikkdata.

Fremtidsutsiktene - garanti for sikring av personvernet
Den teknologiske utviklingen av elektronisk kommunikasjon og data skjer i et enormt tempo. Det er ingen indikasjoner på at vi i dag verken har nådd grensen for hva som kan lagres eller hvor mye som kan lagres. På 1980-tallet var kostnadene med datalagring store, og kostnaden virket begrensende i forhold til hva som ble lagret. I dag er virkeligheten en helt annen, man kan nærmest lagre ubegrensede mengder data uten at det medfører ytterligere kostnader. Videre er det slik at vi allerede i dag, via overvåking, kan hente ut innhold informasjonen som sendt over telefon, mobiltelefon og internett, altså ikke bare trafikkdata. I dagens teknologiske virkelighet er det høyst sannsynlig at man i nær fremtid, med enkle grep, vil også kunne lagre innholdsdata.

I dag krever datalagringsdirektivet at vi bare skal lagre trafikkdata, men hva gjør vi dersom et nytt EU-direktiv pålegger oss å lagre innholdet av kommunikasjonen. Vår vurdering er at skrittet fra å bare lagre trafikkdata til også å lagre innholdsdata, vil være kort.

Vi krever at myndighetene sikrer at man ikke, "i de gode intensjoners hensikt", forplikter seg til å lagre mer enn trafikkdataene. Unio foreslår at dataene som skal lagres må listes opp i loven og oppramsingen må være uttømmende. Dersom andre data skal lagres, må dette skje gjennom endring av lov. Det nå være Stortinget som må ha kontroll på hvilke data som kan lagres, og ikke overlate endringer til EU eller andre overmyndigheter.

Lagring av trafikkdata
Unio er av den klare formening at det må være myndighetenes ansvar, både økonomisk og administrativt, å sikre en forsvarlig og trygg lagring av trafikkdataene. Årsaken til dette er at dataene som lagres kan brukes til å krenke personvernet. Det er viktig at borgerne er forsikret om at lagring og bruk av trafikkdata skjer i henhold til intensjonene, altså å forebygge og oppklare alvorlig kriminalitet, og at dataene kun kan hentes ut dersom det fins et rettslig grunnlag for dette.

Unio mener at det må være en klar grense for hvor lenge trafikkdata kan lagres, og at 12 måneder må være en absolutt øvre grense.

Vennlig hilsen
Unio

Ingjerd Hovdenakk
sekretariatssjef

Jorunn Solgaard
seniorrådgiver