



Representantforslag 103 LS

(2010–2011)

fra stortingsrepresentantene Trine Skei Grande og Borghild Tenden

Dokument 8:103 LS (2010–2011)

Representantforslag fra stortingsrepresentantene Trine Skei Grande og Borghild Tenden om gjennomføring av domstolskontroll ved uthenting av trafikkdata, samt styrking av politiets ressurser til å bekjempe alvorlig kriminalitet med digitale verktøy. Endringer i ekomloven

Til Stortinget

Bakgrunn

Om datalagringsdirektivet

Forslagsstillerne har merket seg en økende debatt og interesse rundt digital kriminalitetsbekjempelse. Den største debatten rundt dette i den senere tid har vært om hvorvidt datalagringsdirektivet bør innføres i norsk rett. Regjeringens lovforslag om gjennomføring i norsk rett er fremlagt i Stortinget som Prop. 49 L (2010–2011).

Forslagsstillerne har vært engasjert i debatten rundt dette direktivet i mange år som sterke motstandere. Direktivet er et eksempel på hva som kan skje når man glemmer rettsstatlige og demokratiske prinsipper som skal beskytte borgere mot statens overgrep, i dette tilfellet gjennom vilkårlig overvåkning. Forslagsstillerne er av den oppfatning at en lagring av lokasjonsdata, når man kommuniserer og hvem man kommuniserer med, er nesten like sensitivt som innholdsdata i seg selv. Historisk har man behandlet lagring av slike data med stor forsiktighet. Datalagringsdirektivet vil endre dette drastisk.

Forslagsstillerne er videre bekymret for hvilken virkning en konstant og massiv overvåkning av all kommunikasjon i Norge vil ha på borgernes frie samling, tanker og ytringer, en såkalt nedkjølende effekt. Det vises til Prop. 49 L (2010–2011) kapittel 3.2.2,

3.3.3 og 6.3, hvor mange høringsinstanser uttaler seg om konsekvensene for ytringsfrihet og personvern, og departementet selv ikke utelukker en slik effekt. Dette legges fra departementets side ikke vekt på, siden dokumentasjonen er begrenset, men forslagsstillerne mener denne dokumentasjonen i alle tilfeller bør eksistere før man vedtar datalagringsdirektivet, all den tid sterkt inngripende tiltak bør dokumenteres tilsvarende grundig. De samme bekymringer gjelder for pressens kildevern.

Forslagsstillerne mener det eksisterer en feiloppfatning om at trafikkdata må pålegges lagring. Forslagsstillerne viser til transport- og kommunikasjonskomiteens høring om datalagringsdirektivet 7. og 9. februar 2011, hvor Stopp DLD, IKT-Norge og Telenor fortalte grundig om hvorfor dette ikke stemmer. Forslagsstillerne er av den oppfatning at pålegg om lagring av visse typer data er unødvendig, og at et slikt pålegg heller bør tas opp på det tidspunkt de faktiske forhold endrer seg.

Det knyttes også sterk tvil til lagringssikkerheten av dataene som omfattes i direktivet. Til tross for at det kan stilles krav til sikkerhet, vil det alltid forekomme lekkasjer og utro tjenere. Forslagsstillerne mener at å begrense mengden data som lagres, er den eneste måten å sikre at slik informasjon ikke kommer på avveie. Så viktig som regjeringen og politimyndigheter mener datalagringsdirektivet er, må man kunne anta at de også mener at disse dataene er sensitive nok til å kunne misbrukes av kriminelle eller fremmede makter, og dermed bør behandles med en sikkerhet forslagsstillerne mener ikke kan garanteres. Forslagsstillerne viser til datainnbrudd hos Google og andre selskaper med høy informasjonssikkerhet i starten av 2010, hvor et angrep fra kinesiske adresser lyktes med å få tilgang til bl.a. industrihemmeligheter og trafikkdata tilhørende menneskerettighetsaktivister.

Forslagsstillerne merker seg at det diskuteres, bl.a. i proposisjonens kapittel 11.4.2, om at å kreve lagring innenfor Norge vil være vanskelig innenfor EØS-regler. Dette betyr, etter forslagsstillerens oppfatning, at man ikke kan kontrollere lagringssikkerheten i andre land utenfor de gjeldende rammer i EUs lovverk, og heller ikke ha kontroll på hvorvidt disse dataene kan leveres til fremmed makt etter lagringslandets regler. Dette er en uholdbar problemstilling som det ikke er gitt svar på.

Etter forslagsstillerens oppfatning vil direktivet også føre til en økt inngangskostnad for ekomlevedrører, og dermed svekke konkurransen i bransjen.

Politiets hjemler – dagens situasjon

Forslagsstillerne mener de lovhjemler som allerede eksisterer, er tilstrekkelige for å bekjempe alvorlig kriminalitet også med digitale verktøy. Forslagsstillerne viser til Tyskland, hvor den gjeldende implementering av datalagringsdirektivet har blitt underkjent av forfatningsdomstolen. Der har det kommet forslag fra justisminister Leutheusser-Schnarrenberger om en såkalt hurtigfrys-løsning som et alternativ, hvor påtalemyndighet kan pålegge ekomlevedrører tvungen lagring såfremt en etterforskning er igangsatt, og deretter få utlevert data etter utleveringspålegg. Dette medfører at data ikke slettes mens etterforskningen pågår.

Dette eksisterer allerede i Norge gjennom våre forpliktelser gitt av Datakriminalitetskonvensjonen (Ot. prp. nr. 40 (2004–2005)) gjennom straffeprosessloven § 215 a. Forslagsstillerne oppfatter at verktøyet er lite brukt i Norge grunnet Post- og teletilsynets mulighet til å oppheve taushetsplikten, men vil være et godt verktøy når domstolskontroll for historiske data er gjennomført. Det stilles også tilfredsstillende krav med tanke på at dataene skal fryses «som ledd i etterforskning», når de «antas å ha betydning som bevis», og at det er «grunn til å tro at det er begått en straffbar handling».

Samtidig har man hjemmel til utlevering av slike data, jf. straffeprosessloven § 216 b, og videre gjennom vanlig utleveringspålegg. Dette er mer åpent enn datalagringsdirektivet tillater, og forslagsstillerne mener det vil være naturlig å harmonisere disse kravene uavhengig av lagringsløsning.

Forslagsstillerne har også lagt merke til at Norge, gjennom reservasjoner i Datakriminalitetskonvensjonen samt justiskomiteens innstilling, har uttalt at «[vi] ikke bør åpne for innhenting av trafikkdata i sanntid i mindre alvorlige straffesaker,» noe som reflekteres i dagens lovverk. Dette står etter forslagsstillerens oppfatning ikke i sammenheng med en gjennomføring av datalagringsdirektivet i norsk lov, som vil pålegge det som i praksis er en fullstendig bevisikring av alle borgeres bevegelser i sanntid, i til-

felle de skulle gjøre noe kriminelt. Å vedta datalagringsdirektivet vil bety et paradigmeskifte vekk fra eksisterende prinsipper.

Domstolskontroll på utlevering av trafikkdata

Dagens situasjon er med tanke på utlevering av trafikkdata ikke holdbar. Forslagsstillerne har sterke bekymringer knyttet til dagens praksis for utlevering av trafikkdata. Metodene som i dag brukes, har blitt kritisert av Metodekontrollutvalget i NOU 2009:15, spesifikt mangelen på forhåndskontroll via domstolene – domstolskontroll – når trafikkdata skal utleveres til politiet. Denne kontrollen er påkrevd av datalagringsdirektivet, og har dermed blitt fremlagt av regjeringen som om datalagringsdirektivet styrker personvernet. Dette stemmer ikke. Metodekontrollutvalget la frem endringsforslag til lovverket for å gjennomføre denne kontrollen, og det er ingen nødvendig sammenheng mellom datalagringsdirektivet og en slik domstolskontroll.

Forslagsstillerne er overrasket over fremstillingen av regjeringens forslag til gjennomføring av EUs datalagringsdirektiv. Regjeringen har lagt frem forslaget som om domstolskontroll ikke kan gjennomføres uten datalagringsdirektivet, og viser med dette en mangel på respekt for parlamentets evne og rett til å ta separate beslutninger, samt en vilje til å behandle grunnleggende rettsprinsipper som politiske verktøy for å tvinge gjennom sin mening.

Det har blitt nevnt fra flere hold at dagens praksis kan være i strid med Menneskerettighetskonvensjonens artikkel 8, og hvis dette skulle vise seg å stemme etter en domsavgjørelse, vil det skape usikkerhet rundt saker som allerede er ført i norsk rett hvor trafikkdata utlevert gjennom opphevelse av taushetsplikten har vært brukt som bevismateriale. Det er blant annet derfor en uholdbar situasjon at ikke dette problemet har vært løst tidligere, og separat fra gjennomføringen av datalagringsdirektivet.

Forslagsstillerne mener at domstolskontroll på trafikkdata må innføres snarest mulig. Dette vil bety at Post- og teletilsynets mulighet til å gi unntak fra telesekskapenes taushetsplikt vil forsvinne. En slik domstolskontroll vil videre måtte ta hensyn til de begrensninger som ligger i lovverket når taushetsplikten ikke skal oppheves.

Den foreslåtte lovendring (forslag I) er ment forstått på samme måte som forklart i NOU 2009:15 kapittel 20. Det vil si at politi og påtalemyndighet fremdeles vil ha tilgang til grunnleggende abonnementsinformasjon slik som navn, adresse, identitet bak et hemmelig nummer mv. uten at taushetsplikten oppheves, jf. ekomloven § 2-9 tredje og fjerde ledd. Forslagsstillerne ønsker videre å begrense tilgangen til dette til å gjelde alvorlig kriminalitet, slik datalagringsdirektivet krever.

Utfordringer for politimyndigheter

Debatten rundt datalagringsdirektivet har søkt alternativer til direktivet for å bekjempe kriminalitet. Som tidligere nevnt er forslagsstillerne overbevist om at de nødvendige hjemler allerede eksisterer, men at ulike politienheter, både under de ulike politidistrikter samt Kripos og Politiets sikkerhetstjeneste (PST), mangler ressurser i form av både økonomi og kompetanse til effektivt å bekjempe alvorlig kriminalitet med digitale verktøy. For eksempel uttalte Kripos i Teknisk Ukeblad (10. august 2009) at de kun har kapasitet til å behandle fem sakskomplekser i året i datakrimavdelingen, og ønsker seg større kapasitet.

Det er viktig at disse ressursene er til stede, og å innføre datalagringsdirektivet i norsk lov er et sterkt inngrep i personvernet som ikke nødvendigvis vil gi særlig effekt på kriminalitetsbekjempelse så lenge det ikke eksisterer ressurser til å ta verktøyene i bruk på en effektiv måte raskt etter igangsatt etterforskning.

Forslagsstillerne er opptatt av at myndighetsutøvelse ikke skal kunne velge de enkleste løsninger i alle tilfeller. Å ikke bruke de enkleste løsningene, som datalagringsdirektivet er et eksempel på, er i seg selv et forsvar av personvernet, da det tvinger frem prioritering av ressurser til inngripende tiltak for den mest alvorlige kriminaliteten. Forslagsstillerne er likevel klar over at ikke nok alvorlig kriminalitet kan bekjempes med de verktøyene som allerede eksisterer – ikke på grunn av manglende hjemler, men på grunn av ressursmangel. Forslagsstillerne ønsker å utbedre denne situasjonen.

Disse forslag er ment å gi en alternativ retning til innføring av datalagringsdirektivet i norsk rett, og være en start på arbeidet med å videre forbedre og raffinere personvernet og rettsikkerheten, samtidig som alvorlig kriminalitet kan bekjempes effektivt. Forslagsstillerne ønsker å gjennomføre domstolskontroll ved utlevering av trafikkdata samt innskrenke tilgangen til trafikkdata lik datalagringsdirektivet krever (forslag I, jf. merknader i NOU 2009:15 kap. 20.5), og å forbedre ressurs situasjonen i politiet med tanke på kriminalitetsbekjempelse med digitale verktøy (forslag III-V).

Forslag

På denne bakgrunn fremmes følgende

f o r s l a g :

A

Vedtak til lov

om endringer i lov av 4. juli 2003 nr. 83 om elektronisk kommunikasjon

I

I lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon gjøres følgende endringer:

§ 2–9 tredje ledd nytt fjerde punktum skal lyde:

Taushetsplikten er heller ikke til hinder for at det gis opplysninger til påtalemyndigheten eller politiet om hvilke kommunikasjonsanlegg som i et bestemt tidsrom har vært satt i forbindelse med hverandre, og andre data tilknyttet kommunikasjon, dersom det foreligger beslutning om utleveringspålegg.

§ 2-9 fjerde ledd skal lyde:

Anmodning fra påtalemyndigheten eller politiet om opplysninger som omhandlet i tredje ledd *første til tredje punktum* skal etterkommes med mindre særlige forhold gjør det utilrådelig.

II

Endringene trer i kraft umiddelbart.

B

Stortinget ber regjeringen fremme lovforslag som begrenser tilgangen til utlevering av trafikkdata, lik de forslag til og endring i straffeprosessloven §§ 210 b og 210 c og nye §§ 118 a og 210 d som foreslås i Prop. 49 L (2010–2011).

C

Stortinget ber regjeringen snarest igangsette en behovsutredning for å se på hvordan ulike enheter i politiet, herunder spesielt Kripos og PST, kan bekjempe alvorlig kriminalitet med digitale verktøy, med de eksisterende hjemler og verktøy gitt av lovverket. Utredningen bør ha spesielt fokus på hvilke ressurser i form av kompetanse og økonomi som må tilføres for å gjøre situasjonen tilfredsstillende.

Stortinget ber regjeringen følge opp resultatene av en slik behovsutredning senest i forslag til statsbudsjett for 2012.

D

Stortinget ber regjeringen fremme forslag som pålegger politiet å føre tilstrekkelig logg og statistikk over bruken av hemmelige tvangsmidler, herunder

kommunikasjonskontroll og kommunikasjonsdata, slik at det blir mulig å evaluere metodebruken bedre i ettertid.

Oslo, 24. februar 2011