Representantforslag 126 S

(2016–2017)

fra stortingsrepresentantene Knut Arild Hareide, Kjell Ingolf Ropstad og Hans Fredrik Grøvan

Dokument 8:126 S (2016–2017)

Representantforslag fra stortingsrepresentantene Knut Arild Hareide, Kjell Ingolf Ropstad og Hans Fredrik Grøvan om utvidet lagringsplikt av IP-adresser for å beskytte barn mot overgrep

Til Stortinget

Bakgrunn

Norge ligger i verdenstoppen i bruken av internettbasert teknologi. Nettbasert informasjon og tjenester preger dermed også hverdagen for både voksne og barn. Mens internett har gjort verden mindre og den teknologiske utviklingen betyr store fremskritt på svært mange områder, innebærer den også at avstanden mellom barn og potensielle overgripere er blitt mindre.

Som en illustrasjon på hvor alvorlig situasjonen er, viser forslagsstillerne til «Operasjon Dark Room», som politiet offentliggjorde i slutten av oktober 2016, hvor Vest politidistrikt hadde avslørt et større nettverk av personer som delte bilder og videoer som viste overgrep mot barn på internett. Politiet hadde etterforsket nettverket i ti måneder, noe som hadde resultert i et av norgeshistoriens største beslag av overgrepsmateriale. Ofrene var barn fra spedbarnsalder og opp til 15 år, fra både Norge og utlandet. 51 menn i alle aldre og samfunnslag var mistenkt for ulik involvering i nettverket. Minst fire av dem skal selv ha begått overgrep mot enkelte av barna som det ble delt overgrepsmateriale knyttet til. Overgrepsmaterialet ble spredt både i det åpne internettet og i det såkalte «mørke nettet», og i chattegrupper ble det drøftet metodikk for å begå overgrep mot barn og delt erfaringer mellom pedofile.

Dessverre er ikke de tilfellene som er avslørt gjennom «Operasjon Dark Room», enkeltstående. Leder for Oslo politidistrikts avsnitt for seksuallovbrudd, Kari-Janne Lid, forklarte til VG i mars 2016 om en kraftig økning i antallet nettovergrep som politiet blir kjent med, men at «vi avdekker bare toppen av isfjellet».

Etter forslagsstillernes syn har samfunnet en plikt til å verne barn mot overgrep i så stor utstrekning som mulig, herunder å sørge for at politiet har tilstrekkelige verktøy til å identifisere pågående overgrep som ennå ikke er anmeldt, og stille til ansvar overgriperne og andre personer som gjennom deling av overgrepsmateriale skaper et marked og et miljø for så vel overgrepsmateriale som for selve overgrepene. Mens teknologien er i stadig utvikling, er utfordringen å gi politiet de virkemidlene som er nødvendige for å verne barn mot nettovergrep. Et av de viktigste virkemidlene som politiet har etterlyst, er at internettilbydere i større grad lagrer abonnementsinformasjon som identifiserer hvilke abonnenter som disponerer ulike IP-adresser. Dersom denne informasjonen lagres over lengre tid enn i dag, kan den sikres av politiet dersom det senere kommer opplysninger som tilsier at en IP-adresse kan knyttes til nettovergrep eller annen alvorlig kriminalitet.

IP-adresser (Internet Protocol Address) er en unik identifikator eller adresse som tildeles en enhet som er tilkoplet internett. Siden det er tilbyderne av internettjenester som tildeler IP-adresser til sine abonnenter, lagrer de eller har mulighet til å lagre informasjon om hvilke abonnenter som disponerer hvilke IP-adresser. Abonnentinformasjon knyttet til IP-adresser avslører ikke noe innhold, kan sammenlignes med et telefonnummer, og gir kun mulighet for å identifisere hvilken abonnent som disponerte den aktuelle adressen i hvilket tidsrom. Denne informasjonen kan imidlertid være avgjørende i situasjoner

hvor politiet blir kjent med bilder eller videoer som deles på nettet og viser overgrep mot barn, og som gir grunn til å frykte at barn som figurerer i materialet, utsettes på for pågående overgrep, som illustrert i eksempelet innledningsvis fra «Operasjon Dark Room». Da kan tilgang til IP-adressen gi politiet opplysninger om et mulig gjerningssted hvor de kan lete etter offeret og mulige gjerningspersoner. En stor utfordring for politiet ved etterforskningen av slike nettovergrep er at tilbyderne i dag er pålagt sletting av denne informasjonen etter kort tid, slik at informasjon som kan bidra til å avsløre overgripere ved hjelp av IP-adressen, ofte er slettet før politiet får sikret den.

Etter gjeldende rett skal informasjon om hvilke IP-adresser som har vært benyttet av de enkelte abonnentene, slettes når det for tilbyderen ikke lenger er nødvendig å lagre informasjonen for blant annet kommunikasjons- eller faktureringsformål, og senest innen 21 dager. Dette betyr at tilbyderne i dag er pålagt en aktiv sletteplikt, og ingen kan lagre lenger enn 21 dager. I mange tilfeller slettes informasjonen også umiddelbart ved nedkobling eller etter få dager.

Stortinget har i forbindelse med implementeringen av EUs datalagringsdirektiv i norsk rett vedtatt lov 11. april 2011 nr. 11 («lagringsloven»), som forplikter teletilbydere til å lagre alle tele- og trafikkdata i seks måneder. Dette inkluderer IP-adresser, men også vesentlig mer informasjon fra telefoni og lignende. Som en vil komme tilbake til nedenfor, ble datalagringsdirektivet senere opphevet fordi det av flere domstoler ble ansett for å gå for vidt i å pålegge lagring av sensitiv informasjon, og lagringsloven er på denne bakgrunn aldri trådt i kraft. Konsekvensen av dette er dermed at selv om det allerede er lovfestet en lagringsplikt for IP-adresser, tråd denne ikke i kraft fordi den er vedtatt i samme lov som lagringsplikten for annen og mer omfattende informasjon. I fravær av ny lovregulering som kun gjelder lagring av IP-adresser, opprettholdes sletteplikten etter 21 dager.

Forslagsstillerne viser til at politiet selv anser den korte lagringstiden å være et stort hinder for avverging og oppklaring av alvorlig kriminalitet, herunder overgrep mot barn. I sitt høringsbrev til Justis- og politidepartementet i forbindelse med implementeringen av det såkalte datalagringsdirektivet i 2010 skrev KRIPOS:

«Norge har med dagens praksis hvor IP-logger kun lagres i 21 dager meget begrenset mulighet for å kunne avdekke både overgripere og personer som sprer overgrepsmateriale med base i Norge. Norge er i ferd med å bli en frihavn for denne typen kriminelle.

Anslagsvis to ganger i måneden mottar Kripos informasjon fra kolleger i utlandet om overgrepssaker hvor nordmenn er involvert. Problemet er at 21-dagersfristen er utløpt før Kripos mottar informasjon om konkrete IP-adresser fra internasjonale kollegaer. Kripos får stadig opplysninger om nordmenn som deler overgrepsmateriale over nettet. Bevisene er sterke, men gjeldende slettepraksis gjør informasjonen ubrukelig for etterforskerne.

Gjennom tjenesten tips.kripos.no mottar Kripos regelmessig henvendelser om mulig pågående overgrep, hvor etterforskningen ikke kommer videre på grunn av at IPhistorikken slettes nesten umiddelbart av noen teletilbydere (ISP'er). Ved å ha et regelverk som gjør at man i praksis ikke klarer å etterforske og iretteføre disse forbrytelsene klarer ikke Norge å oppfylle de internasjonale forpliktelsene vi har gjennom blant annet FNs barnekonvensjon artikkel 34. I realiteten innebærer dette at Norge jevnlig bryter FNs barnekonvensjon.

Internettrelaterte seksuelle overgrep – noen saks-eksempler;

Sak 1 (2009). I forbindelse med en politiaksjon i Mellom-Europa i juni 2009 fikk Kripos oversendt 709 unike, norske IP-adresser som var benyttet til å utveksle overgrepsmateriale (mot barn). Det betyr at mange personer i Norge har mottatt eller sendt filer med overgrepsmateriale på dette nettverket. På grunn av manglende lagring av trafikkdata var det ikke mulig å iverksette etterforskning mot mistenkte i Norge.

Sak 2 (2009). I begynnelsen av oktober 2009 fikk Kripos oversendt tilsvarende IP-adresser fra brasiliansk politi i forbindelse med en aksjon mot et nettverk for distribusjon av overgrepsmateriale der det var blitt utvekslet filmer av overgrep mot barn. Som følge av dette ble blant annet 121 personer arrestert i Spania. På grunn av manglende lagring av trafikkdata var det ikke mulig å iverksette etterforskning mot mistenkte i Norge.

Sak 3 (2006). En 42 år gammel mann fra Bergen opprettet kontakt med mindreårige gutter via ulike nettsamfunn. Når han chattet med guttene utga han seg for å være jevnaldrende med dem. Han avtalte møter med flere av de fornærmede. En av disse, en da 15-årig gutt som hadde avtalt å møte overgriperen på torget i Bergen, ante imidlertid uråd da han forstod at den han møtte var betydelig eldre enn han hadde utgitt seg for å være, og kontaktet politiet. Domfelte ble identifisert gjennom sporing av IP-adressen han hadde operert fra i sin kontakt med 15-åringen. Ved å undersøke hvilke andre IP-adresser domfeltes IP-adresse hadde vært i kontakt med klarte politiet etter hvert å identifisere flere ofre. 42-åringen ble i januar 2010 dømt til 10 års forvaring med en minstetid på 6 år. Han ble i tillegg dømt til å betale erstatning til 11 av ofrene.»

I tråd med at stadig mer kommunikasjon flyttes fra tradisjonelle kommunikasjonskanaler som telefon og over på IP-baserte plattformer, er den korte lagringstiden blitt et voksende hinder for politiets arbeid de seneste årene. I et skriv til Riksadvokatembetet fra mars 2017, vedrørende etterforskning av internettrelaterte overgrep mot barn, har KRIPOS blant annet beskrevet utfordringen slik:

«Internettrelaterte overgrep mot barn er et prioritert område for norsk politi. Kripos er politiets sentrale kontaktpunkt for mottak av informasjon om internettrelaterte overgrep mot barn fra nasjonale og internasjonale samarbeidspartnere. Eksempler er

informasjon mottatt via tipsmottaket til Kripos, hvor både bekymrede foreldre, organisasjoner og eksterne samarbeidspartnere (for eksempel nettsteder) kan tipse Kripos om mulige internettrelaterte overgrep mot barn. Andre eksempler er informasjon som mottas via National Center for Missing & Exploited Children (NCMEC), og sakskomplekser mottatt fra utenlandske politimyndigheter hvor etterforskingen viser at norske brukere kan knyttes til straffbare handlinger. I mange av disse tipsene og sakene er ofte identifikatoren en IP-adresse. Et sentralt første skritt vil da være at Kripos ut fra materialet forsøker å identifisere registrert bruker av IP-adressen på aktuelt tidspunkt, for derigjennom å komme nærmere en gjerningsmann og eventuelle fornærmede. Ofte har det allerede gått 21 dager eller nært opp til dette når Kripos mottar informasjon, og ikke sjelden er IP-adressen alene nøkkelen i identifiseringsarbeidet. Det fremstår for Kripos som et paradoks at man i forbindelse med økt politisk fokus hva gjelder bekjempelse av internettrelaterte overgrep mot barn ikke har funnet grunn for endring av regelverket hva gjelder lagringspraksis for denne knytningen. Særlig når dette er en lagring som i realiteten kan sammenlignes med lagring av abonnentinformasjon hva gjelder telefonnummer. Dagens situasjon, hvor teletilbyderne kan lagre IP-adresser i maksimalt 21 dager, resulterer utvilsomt i at et stort antall saker ikke kan oppklares og at fornærmede ikke identifiseres.»

Forslagsstillerne viser til at Norge gjennom tilslutningen til den europeiske menneskerettighetskonvensjonen (EMK) har en forpliktelse til å iverksette nødvendige tiltak for å verne borgerne mot kriminalitet, blant annet gjennom å gi politiet tilstrekkelige muligheter og virkemidler for effektiv rettshåndhevelse. For barns del oppstiller barnekonvensjonen artikkel 35 en plikt for myndighetene til å «treffe alle egnede nasjonale, bilaterale og multilaterale tiltak for å hindre» seksuell utnyttelse av barn.

Forpliktelsene til å ivareta ofres rettigheter gjennom virkemidler som gjør det mulig for politiet å etterforske saken, er anerkjent gjennom flere avgjørelser i den europeiske menneskerettighetsdomstolen (EMD). I dommen K.U. v Finland (2. desember 2008) var saksforholdet at noen hadde lagt ut en kontaktannonse på internett i navnet til en mindreårig gutt. I annonsen søkte gutten tilsynelatende etter jevnaldrende gutter for seksuell kontakt. Da dette ble oppdaget av gutten og hans familie, ble forholdet anmeldt til politiet, som ba om å få utlevert IP-adressen til den som hadde lastet opp annonsen. Anmodningen ble avslått fra kommunikasjonsleverandøren, og politiets begjæring om rettslig utleveringspålegg førte heller ikke frem, idet dette straffbare forholdet ikke ga hjemmel til utlevering av opplysningene etter finsk rett. EMD kom til at Finland hadde brutt sin plikt til effektiv beskyttelse av retten til privatliv etter artikkel 8 ved ikke å ha hjemmel for utlevering av opplysninger som var nødvendige for etterforskning og oppklaring av saken.

Domstolen uttalte blant annet:

«The Court considers that practical and effective protection of the applicant required that effective steps be taken to identify and prosecute the perpetrator, that is, the person who placed the advertisement. In the instant case, such protection was not afforded. An effective investigation could never be launched because of an overriding requirement of confidentiality. Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.»

Dommen viser at menneskerettighetene inneholder en plikt for statene til å sikre politiet tilgang til nødvendige bevis for å beskytte borgerne. Dette forutsetter blant annet tilgang til tilstrekkelige kommunikasjonsdata for å kunne oppklare straffbare handlinger som innebærer krenkelser av personers rettigheter. Et av de sentrale momentene i EMDs avgjørelse er at garantien for anonymitet på internett og i bruken av kommunikasjonstjenester ikke kan være absolutt. Dette er også et vektig argument for at statene i tilstrekkelig grad må sikre at slike data er tilgjengelige ut over det som telekommunikasjonsselskapene selv finner nødvendig å oppbevare. Regelverk omkring lagring av og tilgang til kommunikasjonsdata må utformes og praktiseres etter en avveining mellom konkurrerende grunnleggende rettigheter. På den ene siden individenes rett til en effektiv beskyttelse mot krenkelser, og på den annen side inngrep i kommunikasjonsfriheten som kan medføre inngrep i personvernet og ytringsfriheten.

Forslagsstillerne mener at hensynet til avverging og oppklaring av svært alvorlige straffbare handlinger, som bl.a. overgrep mot barn, taler for at tilbyderne av internettjenester pålegges å lagre informasjon om hvilke av deres abonnenter som har disponert ulike IP-adresser, i en avgrenset periode.

Forslagsstillerne understreker at personvernhensyn taler for en varsomhet med lagring av opplysninger, og viser til at også den europeiske menneskerettskonvensjon (EMK) artikkel 8 om retten til vern om privatliv samt Grunnloven § 102 forutsetter en avveining av personvernhensyn og hensynet til oppklaring av straffesaker. I EMK artikkel 8 nr. 2 fremgår at

«det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å

beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter».

Etter forslagsstillernes syn må det derfor foretas en avveining av på den ene siden hvor stort inngrep lagring av IP-adresser vil være for innbyggerne, herunder hvor omfattende og personlig informasjon som pålegges lagret og varigheten av lagringen. På den andre siden må det vurderes alvorlighetsgraden av de lovbruddene som kan tenkes avverget eller oppklart gjennom lagringen, og sannsynligheten for at alvorlige lovbrudd mot uskyldige kan avverges eller oppklares.

Et eksempel på for omfattende lagringsplikt med hensyn til personvernet er det ovenfor nevnte datalagringsdirektivet fra EU (2006/24/EF) fra 2006, som påla tilbydere av elektronisk kommunikasjon å lagre all trafikkdata for en periode som ikke kunne være mindre enn 6 måneder og inntil 24 måneder. Formålet var å kunne benytte dette i arbeidet med kriminalitetsbekjempelse. Trafikkdata er informasjon som er lagret hos tilbydere av elektronisk kommunikasjon, om abonnentenes bruk, bl.a. hvilke telefoner som har vært i kontakt med hverandre ved sms eller telefoni, varighet av samtaler, lokaliseringsdata for kommunikasjonsutstyr og også bruk av IP-adresser. Pålegg om lagring av trafikkdata generelt innebærer dermed lagring av vesentlig mer omfattende informasjon om personers kommunikasjon og bevegelser enn kun lagring av abonnementsinformasjon om IP-adresser. Stortinget vedtok i 2011 gjennomføring av datalagringsdirektivet for Norges del ved lov 11. april 2011 nr. 11 («lagringsloven»), som forpliktet teletilbydere til å lagre teledata i 6 måneder. Loven er imidlertid aldri trådt i kraft. Datalagringsdirektivet ble opphevet ved EU-domstolens storkammeravgjørelse av 8. april 2014. EU-domstolen fant at datalagringsdirektivet, slik det var utformet, ville være for vidtrekkende og uforholdsmessig med hensyn til retten til privatliv og personvernhensyn. I en senere avgjørelse fra EU-domstolen i den såkalte «Tele2-saken» fra desember 2016 foretok domstolen en prøving av lagringslovene i Sverige og Storbritannia, som i stor grad er parallelle til det ugyldiggjorte datalagringsdirektivet. EU-domstolen kom etter en konkret vurdering av hvor omfattende og detaljert informasjon som var pålagt lagret, til at generell lagringsplikt for all trafikk- og lokasjonsdata strider mot EU-charteret om vern om privatlivet, som langt på vei tilsvarer EMK artikkel 8.

Det foreligger ikke, så langt forslagsstillerne er kjent med, noen tilsvarende avgjørelse fra EU-domstolen, Den europeiske menneskerettsdomstolen (EMD) eller norske domstoler hvor lagringsplikt kun for IP-adresser drøftes opp mot hensynet til personvernet. Forslagsstillerne peker imidlertid på at EU-domstolen i den såkalte «Tele2-saken» la stor vekt på graden av detaljert sensitiv informasjon som lagres gjennom fullstendige trafikkdata. Forslagsstillerne viser til at abonnementsinformasjon knyttet til IP-adresser inneholder vesentlig mindre informasjon, slik at en lagringsplikt kun for dette vil innebære et mye mindre inngrep for abonnentene enn lagringsplikt for fullstendige trafikkdata. Lagring av IP-adresser fremstår derimot mer sammenlignbart med annen tilsvarende avgrenset lagring av informasjon om borgernes aktiviteter eller bevegelser, som eksempelvis bilregistreringsnummer eller valutatransaksjoner til utlandet, som lagres aktivt i dag, og som ikke er vurdert å være i strid med EMK artikkel 8. Forslagsstillerne viser videre til at hvilken betydning lagring antas å ville ha for oppklaring og avverging av alvorlig kriminalitet, har vært fremhevet som et viktig moment av EU-domstolen. Basert på uttalelsene referert ovenfor fra politiet, antas lagring av IP-adresser å ha stor betydning for etterforskning og avverging av overgrep mot barn. På denne bakgrunn mener forslagsstillerne at EMK artikkel 8 vanskelig kan sies å være til hinder for lagringsplikt av kun IP-adresseinformasjon i en begrenset periode.

Som en ytterligere illustrasjon på vesensforskjellen mellom plikt til lagring av fullstendige trafikkdata i motsetning til kun abonnementsinformasjon knyttet til teledata, viser forslagsstillerne til at også Datatilsynet i forbindelse med Stortingets behandling av datalagringsdirektivet i 2011 støttet lagringsplikt for abonnementsinformasjon knyttet til IP-adresser, selv om Datatilsynet var motstander av de øvrige delene av datalagringsdirektivet.

Forslagsstillerne foreslår at regjeringen bes fremme de nødvendige forslag for Stortinget for å sikre at lagringsplikt for IP-adresser kan vedtas i en form som kan tre i kraft så raskt som mulig og uavhengig av den allerede vedtatte lagringsloven og de mer vidtgående bestemmelsene der knyttet til trafikkdata.

Når det gjelder lagringstidens lengde, viser forslagsstillerne til at politiet i forbindelse med behandlingen av datalagringsdirektivet ga uttrykk for at det var behov for lagring av informasjon i to år, men at stortingsflertallet gikk inn for en lagringstid på seks måneder. Forslagsstillerne mener at personvernbetraktninger tilsier at lagringstiden også for IP-adresser bør begrenses til seks måneder, og anser at dette vil være tilstrekkelig av hensyn til politiets etterforskning.

Forslag

På bakgrunn av dette fremmes følgende

f o r s l a g :

Stortinget ber regjeringen fremme forslag for Stortinget som sikrer at tilbydere av internettjenester lagrer abonnementsinformasjon og IP-adresser i minst seks måneder.

27. april 2017

Knut Arild Hareide **Kjell Ingolf Ropstad** **Hans Fredrik Grøvan**

Trykk og layout: Stortingets grafiske seksjon