Norges institusjon for menneskerettigheter

Kommunal - og moderniseringsdepartementet
(Kun avgitt digitalt på www.regjeringen.no)

Deres referanse: 20/3645
Vår referanse: 2021/00021
Dato: 25.01.2021

Høringsuttalelse – endringer i ekomloven (lagring av IP-adresser mv.)

1. Innledning

Vi viser til Høringsbrev fra kommunal- og moderniseringsdepartementet og Justis- og beredskapsdepartementet av 9. oktober 2020.

Norges institusjon for menneskerettigheter (NIM) har som hovedoppgave å fremme og beskytte menneskerettighetene i tråd med Grunnloven, menneskerettsloven og den øvrige lovgivning, internasjonale traktater og folkeretten for øvrig.[1] NIM skal blant annet gi råd til Stortinget, regjeringen og andre offentlige organer om gjennomføringen av menneskerettighetene. Innspill i relevante høringsprosesser er en sentral del av vårt mandat. NIM vurderer høringsnotater i lys av de rettslige rammene og føringene som følger av statens menneskerettslige forpliktelser etter Grunnloven, Den europeiske menneskerettskonvensjon (EMK) og andre internasjonale konvensjoner.

NIM ble gjort oppmerksom på denne høringen i januar og har fått to uker utsatt høringsfrist. Vårt høringssvar kan ikke forstås uttømmende.

NIM er i utgangspunktet positiv til departementenes forslag om å pålegge tilbydere av ekomtjenester å lagre IP-adresser slik at politiet kan bekjempe alvorlig kriminalitet. NIM mener imidlertid at lagring av IP-adresser er mer inngripende enn hva departementene legger til grunn. Etter NIMs vurdering vil strafferammekravet på 1-2 år for å kunne utlevere IP-adresser til politiet og manglende rettssikkerhetsgarantier utgjøre et uforholdsmessig inngrep i retten til privatliv. Slik NIM leser høringsnotatet vil forslaget om utlevering av IP-adresser også kunne gripe inn i kildevernet. Av den grunn mener NIM at departementene bør utrede problemstillingen knyttet til kildevernet nærmere.

[1] Lov om Norges nasjonale institusjon for menneskerettigheter av 22. mai 2015 § 1.

2. Departementets forslag

Departementet foreslår å innføre en hjemmel som pålegger tilbydere av ekomtjenester å lagre IP-adresser, slik at politiet kan identifisere hvilken nettaktivitet en IP-adresse er benyttet til.[2] Formålet med lagringen av IP-adresser er å knytte IP-adresser til andre opplysninger politiet får for eksempel gjennom beslaglagte enheter, fra nettsteder mv. eller fra virksomheter som er blitt utsatt for datainnbrudd eller lignende. Lagringen vil dermed kunne bidra til å avdekke hvem som står bak nettaktivitet, kommunikasjon osv. over nett, som kan knyttes til straffbare forhold. Forslaget åpner opp for at de lagrede opplysningene kan gis til politi - og påtalemyndigheten når det er nødvendig for både til etterforsknings- og forebyggingsformål.

3. EMK artikkel 8

NIM er enig med departementene at ekomtilbyders lagring av IP-adresser og utleveringsadgangen av disse IP-adressene til politiet utgjør et inngrep i EMK artikkel 8.[3] EMD har lagt til grunn at ikke bare innsamlingen av innholdet i kommunikasjon (innholdsdata), men også av trafikkdata og metadata er et inngrep i privatlivet.[4] NIM deler videre departementenes vurdering av at myndighetene har positive forpliktelser etter blant annet EMK artikkel 8 til å sikre respekt for privatlivet, som kan tilsi at staten må bekjempe kriminalitet som rammer andres privatliv over nett.[5]

Inngrep i retten til privatliv vil kun være tillatt dersom tre vilkår er oppfylt. Sammenfattet kreves det at (i) inngrepet må ha hjemmel i lov, (ii) inngrepet må søke å ivareta et legitimt formål og (iii) inngrepet må være nødvendig (herunder forholdsmessig) for å ivareta formålet.[6]

I dette tilfellet vil hjemmelskravet oppfylles gjennom den lovendringen, og hensynet til politiets kriminalbekjempelse vil være et legitimt formål.

4. Forholdsmessighetsvurderingen ved inngrep i artikkel 8

Det tredje vilkåret om nødvendighet ligger ifølge praksis fra Den europeiske menneskerettsdomstol (EMD) et sted mellom «uunnværlig» på den ene siden og «ønskelig» eller «nyttig» på den andre. Vurderingen må foretas konkret og helhetlig, der

[2] Høringsnotatet s. 23.

[3] Se bl.a. *Leander v. Sverige* (9448/81) og *Amann v. Sveits* (27798/95), *Breyer v. Tyskland* (50001/12) fra EMDs praksis om at myndighetenes lagring av data som har forbindelse til enkeltpersoners privatliv, omfattes av vernet etter EMK art. 8

[4] *Malone v. Storbritannia* (8691/79)

[5] K.*U. v. Finland* (2872/02).

[6] Slik dette fremgår eksplisitt av EMK art. 8 (2). NIM konsentrerer seg i det videre om EMK artikkel 8. Årsaken til dette er primært praktisk grunnet tilfanget av praksis om denne typer saker som knytter seg til EMK artikkel 8 – fra både EMD og fra Høyesterett. Høyesterett har slått fast at Grunnloven § 102 kan gjøres inngrep i etter mønster av disse vilkårene, se f.eks. Rt. 2015 s. 93 avs. 60. Selv om inngrepsvilkårene er noe ulikt utformet i SP art. 17, vil nok vurderingen bli sammenfallende med mønsteret som følger av EMK.

viktige rettesnorer er om inngrepet er egnet til å nå formålet, om formålet kan nås med mer lempeligere midler (minste inngreps prinsipp), om inngrepet svaret til et «tvingende samfunnsmessig behov». [7] Endelig vil dette bero på hvorvidt inngrepet totalt sett er forholdsmessig sett hen til formålet. Forholdsmessighetsavveiingen munner ofte ut i et spørsmål om myndighetene har funnet en «rimelig balanse» mellom formålet (behovet for inngrepet) på den ene siden og individets rettigheter på den andre.[8] Inn under vurderingen om myndighetene har funnet en rimelig balanse, er det i slike saker sentralt hvorvidt systemet og regelverket inneholder gode kontrollmekanismer og rettssikkerhetsgarantier for å minske risikoen for misbruk/vilkårlighet/formålsutglidning. Basert på inngrepets karakter og styrke, kan rettssikkerhetsgarantiene blant annet knytte seg til bruken av materialet, lagringstiden, sletting og mulighetene for klage/overprøving. I det følgende vil NIM vurdere forslaget opp mot ulike sider ved forholdsmessighetsvurderingen.

4.1. Inngrepets art

Et utgangspunkt for vurderingen om myndighetene har funnet en rimelig balanse mellom formålet på den ene siden og individets rettigheter på den andre, er hvor inngripende tiltaket er. Departementene skriver blant annet at «informasjon om hvilke IP-adresser abonnentene er tildelt, ikke i seg selv avslører noe om innholdet i abonnentens internettkommunikasjon eller om hvem abonnenten har kommunisert med».[9] I høringsnotatet går departementene gjennom EMDs syn på inngrepsgraden i *Breyer v. Tyskland* hvor ekomtilbydere var pålagt å registrere informasjon som identifiserer kunder med forhåndsbetalte SIM-kort (kundens telefonnummer, navn og adresse, fødselsdato og dato for kontraktsinngåelsen).[10] Departementene skriver: «Det ble i denne forbindelse vist til at det bare ble lagret en begrenset mengde opplysninger, som ikke inkluderte «highly personal information» eller gjorde det mulig å bygge «personality profiles» eller spore abonnentenes bevegelser, og som ikke omfattet opplysninger om «individual communication events», jf. avsnitt 92. Det ble lagt til grunn at «the interference was, while not trivial, of a rather limited nature», jf. avsnitt 95». Etter EMDs syn tilsa inngrepets art at lagringstiden (ut det påfølgende kalenderår etter registrering) og manglende domstolskontroll ikke utgjorde et uforholdsmessig inngrep i denne saken.[11] På side 36 i høringsnotatet skriver departementene at lagring av IP-adresser «nok må anses som noe mer inngripende» enn hva tilfellet var i Breyer-saken. Departementene konkluderer likevel med at lagring av IP-adresser ikke vil være så inngripende at uavhengig domstolskontroll er påkrevd.

---

[7] *Breyer v. Tyskland* avs. 88.

[8] *Ibid*. avs. 91

[9] Høringsnotatet s. 2.

[10] Høringsnotatet s. 7-8.

[11] *Breyer*, avs. 96 og avs. 105-107.

Etter NIMs syn er lagring av IP-adresser med det formål å identifisere hvem som står bak nettbruk, adskillig mer inngripende enn å registrere kunder med forhåndsbetalte SIM-kort, slik tilfellet var i Breyer-saken. I dagens samfunn legger vi igjen omfattende informasjon om vårt privatliv på internett. I tilfeller hvor IP-adressen kobles opp mot annen informasjon eller hvor det innhentes IP-adresser knyttet til en enkeltperson i et gitt tidsrom, gripes det inn i enkeltmenneskets liv og preferanser. Dette er noe vesentlig annet enn å lagre abonnentopplysninger. Etter vår forståelse – med forbehold om at denne er riktig - vil dessuten lagring av IP-adresser kunne gi en grov oversikt over borgernes bevegelsesmønstre, ettersom lokasjonen til IP-adressen vil endre seg basert på hvilket nettverk man til enhver tid er tilkoblet. Om dette er et utslag, forhøyes inngrepsgraden vesentlig, slik at det bør stilles strengere vilkår for utlevering og andre rettssikkerhetsmekanismer enn hva forslaget legger opp til. Departementet viser til at Kripos i sin modell har estimert at politiet vil sende om lag 110 000 anmodninger om IP-adresser dersom forslaget går gjennom. Selv om det fremgår av høringsnotatet at det etter Kripos' vurdering er stor usikkerhet knyttet til estimatet, vil omfanget av lagrede IP-adresser etter NIMs syn kunne forhøye inngrepsgraden. Dette har betydning for hvilke negative konsekvenser forslaget vil ha, blant annet med tanke på mulig nedkjølingseffekt.[12] Ut fra dette mener NIM at lagring av og politiets tilgang til befolkningens IP-adresser er mer inngripende enn høringsnotatet reflekterer.

4.2. Statens positive menneskerettsforpliktelser

NIM har stor forståelse for at utvidet lagring av IP-adresser vil lette politiets kriminalbekjempende arbeid. Departementet skriver på side 1 i høringsnotatet at begrunnelsen for politiets tilgang til IP-adresser er «for å bekjempe alvorlig kriminalitet». Dette er et sentralt utgangspunkt for vurderingen av om inngrepet svarer til et tvingende samfunnsmessig behov, og om inngrepet totalt sett er forholdsmessig sett hen til formålet.

Staten har positive forpliktelser til å beskytte andres rettigheter og friheter, som særlig er utpenslet i praksis fra EMD knyttet til EMK artikkel 2 og 8 rundt forpliktelser til å beskytte retten til liv og privatliv. Det fremgår av domstolens praksis at statens sikringsplikter gjennomgående skjerpes når det er tale om beskyttelse av barn mot vold og overgrep, fordi barn er sårbare og har et særlig behov for beskyttelse. Statens plikt til å iverksette alle egnede tiltak for å beskytte barn mot vold, overgrep og omsorgssvikt fremgår også eksplisitt av barnekonvensjonen artikkel 19. Barnekonvensjonen artikkel 34 pålegger videre staten å beskytte barn mot alle former for seksuell utnytting og misbruk.

[12] NIM viser her til Datatilsynets personvernundersøkelse av 2019-2020, hvor det blant annet ble avdekket at 16 prosent av befolkningen har unnlatt å delta i kommentarfelt hos en nettavis og Facebook, og ni prosent har unnlatt å søke hjelp/finne informasjon om mental helse, misbruk, avhengighet eller andre sensitive problemer i en søkemotor på nett fordi de er usikre på om myndigheter slik som politiet og PST kan få tilgang til informasjonen.

Departementene viser til EMDs dom *K.U. v. Finland* hvor domstolen konstaterte brudd på EMK artikkel 8, fordi den finske lovgivningen ikke i tilstrekkelig grad åpnet for utlevering av IP-adresser.[13] I denne saken hadde en ukjent person lagt ut en annonseside av en 12 år gammel gutt på en datingside. Videre ble det i annonsen gitt utrykk for at gutten var ute etter et intimt forhold med en gutt på hans alder eller eldre. Da politiet ba om å få utlevert IP-adressen, ble dette hindret av lovbestemt taushetsplikt for ekomtilbydere. Domstolen konstaterte at ytringsfriheten og retten til respekt av kommunikasjon er sentrale utgangspunkter, og at brukerne av internett må ha garantier for at deres privatliv og ytringsfrihet blir respektert. Disse rettighetene er imidlertid ikke absolutte, og må i visse tilfeller vike for andre hensyn. Staten har også positive forpliktelser for å hindre uorden og kriminalitet og beskytte andres rettigheter og friheter.[14]

Videre har EU domstolens storkammerdom av 6. oktober 2020 i de forente sakene C-511/18, C-512/18 og C-520/18 fastslått at generell og udifferensiert lagring av IP adresser kan kun aksepteres når formålet er «beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed». Den høye terskelen som her kommer til utrykk, reflekterer både hvor inngripende en generell og udifferensiert lagring av IP-adresser faktisk er, men også hvilke positive forpliktelser som påhviler statene.

Politiets behov for lagring av IP-adresser blir beskrevet på side 20 flg. i høringsnotatet. Departementene viser til at tilgangen til IP-adresser vil være et godt verktøy for å bekjempe internettrelaterte overgrep mot barn, trusler mot norske sikkerhetsinteresser og identifisering av ofre.

Ettersom internett er blitt en viktig arena for barn, er det helt nødvendig at staten iverksetter effektive tiltak for å beskytte barn på internett. NIM er derfor av den oppfatning av at ekomtilbyderes plikt til å lagre og politiets til IP-adresser vil kunne falle inn under statens positive handleplikt for å styrke barns vern mot vold, overgrep, seksuell utnytting og misbruk.

Departementene skriver imidlertid at politiet vil ha behov for å finne ut hvem som har benyttet en gitt IP-adresse, uavhengig av hvilke konkrete straffbare forhold det er tale om, ettersom kommunikasjonen i større grad er internettbasert.[15] Departementet har ikke endelig tatt stilling til hvilket strafferammekrav som bør settes, men foreslår at strafferammekravet bør settes til minimum ett eller to års fengsel. Det bes særlig om høringsinstansenes syn på hvilket strafferammekrav som bør oppstilles, og hvilken lagringstid som skal gjelde.

[13] Se høringsnotatet s. 10 og 25.

[14] *K.U v. Finland* avs. 49.

[15] Høringsnotatet s. 21 og 34.

Etter NIMs syn er det ikke helt god sammenheng mellom det foreslåtte strafferammekravet (vilkåret for utlevering) og hva departementene ellers skriver i høringsnotatet om politiets behov, som på side 1 oppgis å være å bekjempe alvorlig kriminalitet.

NIM kan heller ikke se at forslaget er i tråd med internasjonal rettspraksis.

På side 34 viser departementet til praksis fra EU-domstolen hvor det konstateres at «lagring av IP-adresser for kriminalitetsbekjempende formål bare rettferdiggjøres dersom formålet er å bekjempe «alvorlig kriminalitet». Departementets forslag om å lagre IP-adresser uavhengig av hvilket straffbart forhold det er tale om, vil gå vesentlig lenger enn føringene som kan utledes av EU domstolens storkammerdom i de forente sakene C-511/18, C-512/18 og C-520/18. NIM bemerker videre at i EMDs dom i nevnte *K.U v. Finland* ble finske myndigheter dømt for å ikke ha på plass effektive etterforskningsmidler når det gjelder å beskytte barns privatliv på internett i en sak hvor en person hadde stjålet et barns identitet og laget en kontaktannonse i barnets navn, dvs. i et alvorlig tilfelle. Det er imidlertid mer usikkert om sikringsplikten kan trekkes utover dette til vesentlig mindre alvorlige straffebud som den foreslåtte strafferammen på 1-2 år vil omfatte. Etter NIMs syn vil en slik utleveringsadgang ikke være begrenset til «alvorlig kriminalitet». NIM etterlyser en nærmere vurdering av hvordan det foreslåtte strafferammekravet står seg i forhold til den høye terskelen for slike inngrep særlig fra EU- domstolen. Etter NIMs vurdering vil det foreslåtte lave strafferammekravet kunne utgjøre et uforholdsmessig inngrep sett hen til formålet om å bekjempe alvorlig kriminalitet.

4.3. Kontroll- og rettssikkerhetsmekanismer

Som nevnt i punkt 4.1. legger departementene Kripos' estimat til grunn ved vurderingen av omfanget av anmodninger som følge av lovforslaget. Det estimeres at politiet årlig vil sende om lag 110 000 anmodninger til ekomtilbydere om utlevering av IP-adresser dersom forslaget blir vedtatt. Et slikt omfang anmodninger forhøyer risikoen for misbruk og vilkårlighet. Til dette vil det ha betydning om den enkelte blir kjent med informasjonsinnhentingen. Slik NIM leser høringsnotatet, vil slik innhenting foregå uten at den enkelte blir varslet om dette.

I høyesterettsdom (HR-2014-2288-A) som gjaldt bruk av overskuddsmateriale fra politiets kommunikasjonskontroll som bevis i en straffesak, ble det uttalt i avsnitt 30 at loven må ses «i lys av den forhøyede risikoen for misbruk og vilkårlighet som erfaringsmessig kan foreligge når myndigheter tillates å operere i hemmelighet – gi rimelige garantier knyttet til blant annet formen for lagring, bruken av materialet, mulighetene for å gi innsyn, sikkerhet og sletting». EMD er ganske intensiv i sin prøving om et system som overvåker innbyggerne er innrettet med rettssikkerhetsmekanismer som sikrer at systemet ikke misbrukes. EMDs dom *Szabó og Vissy v. Ungarn* fra 2016 gjaldt målrettet hemmelig overvåking, herunder overvåking av nettaktivitet og annen elektronisk kommunikasjon

med det formål å bekjempe terrorisme. Utgangspunktet for vurderingen av rettsikkerhetsmekanismer ble formulert slik:

> «The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society. »[16]

I saker hvor myndighetene tillates å innhente opplysninger som angår borgernes privatliv uten at borgerne får kjennskap til innsamlingen, har EMD i sin praksis innfortolket et krav til effektiv og uavhengig kontroll for å hindre myndighetsmisbruk, og at denne kontrollen bør ligge til den dømmende virksomhet i saker om skjult overvåking.[17] Tilsvarende doktriner er utviklet for saker om bulkinnsamling av data.[18] Hvilke krav til rettsikkerhetsmekanismer som vil oppstilles for masselagring av IP adresser vil til en viss grad bero på hvor inngripende et slikt tiltak anses å være.

Departementene mener at inngrepsgraden ved innhenting av IP-adresser, om enn noe mer inngripende, kan sammenliknes med det som var tilfellet i Breyer-saken hvor det var tale om innhenting av abonnentopplysninger av forhåndsbetalte SIM-kort.[19] På bakgrunn av dette konkluderes det med at det ikke er påkrevd med en uavhengig forhåndsgodkjenning av hver enkelt utlevering.

Slik vi har redegjort for ovenfor, utgjør lagring og utlevering av IP-adresser til politiet et betydelig inngrep i retten til privatliv (personvernet). På bakgrunn av dette er NIMs vurdering at en eventuell lagring og utlevering av IP-adresser må ledsages mer omfattende og effektive garantier mot misbruk og vilkårlighet. Selv om informasjonen ved lagring av IP-adresser isolert sett ikke gir grunnlag for å trekke presise slutninger om privatlivet, er det koblingen mot annen informasjon som forhøyer inngrepet. Videre gis det i høringsnotatet tilsynelatende få begrensninger på hvordan IP-adressen kan benyttes. Det vises til høringsnotatet s. 42 hvor departementene skriver:

> «Det understrekes at abonnementsinformasjon kan være nødvendig i en etterforskning for andre formål enn å identifisere ukjente gjerningspersoner. Informasjonen kan også være nødvendig blant annet for å identifisere eventuelle fornærmede og vitner, analyse og annen bearbeiding av innhentet

[16] *Szabó og Vissy v. Ungarn* (37138/14), avs. 57.

[17] *Klass mfl. v. Tyskland* (5029/71) avs. 55-56 og *Kennedy v. Storbritannia* (26839/05) avs. 167. *Roman Zahkarov v. Russland* (4714/06) avs. 233.

[18] Big Brother Watch mfl. v. Storbritannia (58170/13, 62322/14 og 24960/15).

[19] Høringsnotatet s. 36.

kommunikasjonsdata, eller for å muliggjøre innhenting av ytterligere materiale for eksempel gjennom beslag og utleveringspålegg.»

Dersom lagringen i tillegg gir politiet mulighet til å få informasjon om den enkeltes bevegelser eller informasjon om hvem den enkelte har samhandlet med over internett, mener NIM at utlevering fra ekomtilbydere til politiet antakelig bør forhåndsgodkjentes av en uavhengig myndighet for å oppfylle kravet etter EMK artikkel 8. Under enhver omstendighet må rettsikkerhetsmekanismene i forslaget styrkes betydelig for å ivareta prosessuelle krav etter EMK artikkel 8.

Departementene stiller heller ikke krav til hvor dataene skal lagres, ei heller hvordan disse skal lagres, ettersom gjeldende regelverk allerede inneholder krav for å sikre at ekomtilbydere oppfyller kommunikasjonsvernet, taushetsplikten og at sikkerhet overholdes.[20] NIM bemerker at gode og tydelige regler for lagring, herunder sikkerhet i systemene og mulighetene for innsyn og sletting, vil være sentrale i vurderingen av hvorvidt prosessuelle krav etter EMK artikkel 8 anses oppfylt. Hva gjelder den enkeltes rett til å be om innsyn i sine egne opplysninger, fremstår det uklart for NIM hvordan dette ivaretas når opplysningene ligger lagret hos ekomtilbyderne.

5. EMK artikkel 10 og kildevernet

NIM vil også knytte noen merknader til forslagets betydning for ytringsfriheten og kildevernet. Departementene drøfter problemstillinger knyttet til ytrings- og informasjonsfriheten særlig i høringsnotatet punkt 4.2 og 7.1.3 flg.

NIM bemerker, som departementene, at ytringsfriheten er beskyttet av Grunnloven § 100, EMK artikkel 10 og FNs konvensjon om sivile og politiske rettigheter artikkel 19. Ethvert inngrep i ytringsfriheten må oppfylle de tre vilkårene for inngrep om lovhjemmel, formåls- og forholdsmessighet.[21]

Pressefriheten, herunder kildevernet, er en sentral del av ytringsfriheten, og nyter et særlig sterkt vern.[22] EMDs praksis viser at nødvendighetsvurderingen i kildevernsaker er svært streng. Dette er et område hvor EMD foretar en relativ intens prøving av nødvendigheten – og statens såkalte skjønnsmargin er tilsvarende begrenset. EMD har slått fast at hvor det foreligger risiko for at en kilde kan bli identifisert, må myndighetene sørge for å ha på plass klare og presise regler for å sikre at identiteten til kilden ikke blir kompromittert.[23] NIM vil også minne om at EMD dømte Norge i desember 2020 i en sak som gjaldt påtalemyndighetenes beslag og gjennomgang av data i en mobiltelefon som

[20] Høringsnotatet s. 32.

[21] Jf. Grunnloven § 100, særlig 2. og 3. ledd, samt EMK art. 10 nr. 2 og SP art. 19 nr. 3.

[22] Bl.a. understreket i EMDs praksis, jf. f.eks. *Goodwin v. Storbritannia* (17488/90) avs. 39–40, som er referert til senere av EMD og Høyesterett, og som også departementene viser til, jf. høringsnotatets s. 11.

[23] *Sanoma Uitgevers B.V v. Nederland*, (38224/03) avs. 92.

innehold korrespondanse mellom klageren og hans forsvarer.[24] Det avgjørende for domstolen var at det norske regelverket ikke inneholdt klare og presise prosessuelle garantier for å hindre at innholdet i advokatkorrespondansen ble kompromittert.[25]

NIM merker seg at departementene skriver at «lagring av IP-adresser [ikke] omfatter lagring av informasjon om innholdet i abonnentens internettkommunikasjon, hvem abonnenten har vært i kontakt med, eller hvor abonnenten befinner seg.»[26] Slik vi har skrevet ovenfor under punkt 4.1, med forbehold om at dette er riktig, vil lagring av IP-adresser kunne gi en grov oversikt over den enkeltes bevegelsesmønster. På s. 26 i høringsnotatet skriver departementene at «[n]år det gjelder ytringsfriheten, herunder kildevernet, er det etter departementenes vurdering tvilsomt om regler om IP-lagring i seg selv utgjør et inngrep i ytringsfriheten etter EMK artikkel 10.»

Likevel vil det, slik NIM forstår forslaget, etter omstendighetene kunne oppstå situasjoner hvor politiet, på bakgrunn av annen informasjon de har tilgjengelig, kan anmode om å få utlevert informasjon om hvem en IP-adresse har kommunisert med. Departementene synes å holde muligheten åpen for at det kan oppstå spørsmål om å benytte IP-informasjon for å identifisere en kilde.[27] NIM bemerker at terskelen for å gripe inn i kildevernet er at inngrepet må være «justified by an overriding requirement in the public interest».[28] Den høye terskelen for inngrep og den intense prøvingen, må forstås i lys av kildevernets begrunnelse. EMD har understreket, at begrunnelsen for vernet er hensynet til samfunnet som helhet: Uten et solid kildevern kan ikke pressen ivareta sine viktige samfunnsroller som offentlig vaktbikkje, informasjonskanal og tilrettelegger for den offentlige samtale – som alle er av vesentlig betydning for å realisere og sikre sentrale hensyn bak ytringsfriheten.[29]

Et inngrep i kildevernet kan derfor ikke kun vurderes på bakgrunn av de negative virkninger det vil ha i den konkrete sak. Det må vurderes helhetlig ut fra den negative virkning et slikt inngrep vil ha i en bredere samfunnsmessig kontekst. Dersom potensielle kilder ikke har tilstrekkelig tillit til at deres anonymitet vil bli ivaretatt, vil det kunne svekke

[24] *Saber v. Norge* (459/18).

[25] *Ibid*. avs. 57.

[26] Jf. høringsnotatets s. 23.

[27] Jf. høringsnotatet s. 26 hvor departementene skriver at «[h]vis det i et konkret tilfelle likevel skulle oppstå spørsmål om å benytte IP-informasjon for å identifisere en kilde, vil det etter departementenes vurdering trolig være politiets fremgangsmåter for å skaffe til veie tilleggsinformasjon som IP-opplysningene i så fall må kobles med, som vil komme i forgrunnen ved vurderingen av skrankene i EMK artikkel 10.» Departementene viser til sine drøftelser av begrensningene i adgangen til å bruke tvangsmidler mot journalistiske virksomheter. Videre står det på s. 28 i høringsnotatet at «[d]et kan samtidig ikke helt utelukkes at det ved bruk av NAT i enkelte tekniske løsninger vil være nødvendig å lagre noe mer informasjon for å identifisere abonnenter, som også sier noen om destinasjon, for eksempel hvilken IP-adresse og porten man har kommunisert med», og departementet ber om tilbakemelding fra teletilbyderne om dette.

[28] Jf. bl.a. *Goodwin v. Storbritannia* avs. 39–*40, Sanoma Uitgevers B.V. v. Nederland* (38224/03) avs. 51 og *Financial Times og andre v. Storbritannia* (821/03) avs. 59–63.

[29] *Ibid*.

pressens kildetilfang generelt (gi en «nedkjølende effekt») – med de negative konsekvenser det vil ha for pressens mulighet til å utøve sine nevnte oppgaver på vegne av samfunnet. [30] Vi ser at også departementene viser til at «en plikt til IP-lagring vil kunne påvirke den reelle muligheten til å kunne ytre seg anonymt eller motta anonyme ytringer på internett, og med dette ha en «nedkjølende effekt» på ytringsfriheten.»[31]

NIM bemerker at i tillegg til å være beskyttet av ytringsfriheten mot statlige inngrep (statens negative plikt), har kildevernet også en klar side til statens positive plikt til å sikre ytrings- og informasjonsfriheten, jf. blant annet Grunnloven § 100 sjette ledd.[32] Slik NIM ser det, kan det ikke utfra vår forståelse av høringsnotatet utelukkes at det kan bli tale om inngrep i EMK artikkel 10. Det hadde vært ønskelig med en noe klarere teknisk beskrivelse av forholdene på dette punktet. Departementene skriver at dersom det blir tale om å innhente informasjon om en kilde, «vil det etter departementenes vurdering trolig være politiets fremgangsmåter for å skaffe til veie tilleggsinformasjon som IP-opplysningene i så fall må kobles med, som vil komme i forgrunnen ved vurderingen av skrankene i EMK artikkel 10», mens de viser til begrensningene i adgangen til å bruke tvangsmidler mot journalistiske virksomheter.[33] NIM er enig i at det vil stilles krav til rettssikkerhetsgarantier for det tilfellet at det kan bli tale om inngrep i kildevernet, men savner en omtale av hvordan disse rettssikkerhetsgarantiene vil anvendes hvor lagring av IP-adresser vil kunne kompromittere en kilde.

NIM er tilgjengelig for nærmere diskusjoner om ønskelig.

Vennlig hilsen
for Norges institusjon for menneskerettigheter

Adele Matheson Mestad	Anders Einar Broderstad
Direktør	Rådgiver

Dette dokumentet er elektronisk godkjent og har dermed ingen signatur.

---

[30] Se f.eks. Rt. 2013 side 1290 avs. 34, med henvisning til Rt. 2010 side 1381 (avs. 62), hvor Høyesterett fastslår at det må ses hen til «den mer langsiktige effekten av å skulle gjøre unntak – den såkalte 'chilling effect'», og at det i «det lange løp er [...] en risiko for at en mer utstrakt bruk av vitneplikt vil kunne medføre at viktige kilder blir borte».

[31] Høringsnotatet s. 25.

[32] Grl. § 100 (6): «Det påligger statens myndigheter å legge forholdene til rette for en åpen og opplyst offentlig samtale.» Den positive plikten følger også som en del av EMK og SP (dog ikke like eksplisitt av ordlyden), se f.eks. EMDs dom i *Appleby og andre v. Storbritannia* (44306/98) avs. 39-40.

[33] Høringsnotatet s. 26