Forsvarsdepartementet

Deres ref./dato:	Vår ref.:	Dato:
2016/2699-1/FD II 5/SIH	ONYH/ASTO	5. januar 2016

Høringsuttalelse – rapport fra Lysne II-utvalget om digitalt grenseforsvar

1. Innledning

Vi viser Forsvarsdepartementets utsendelse av rapport avgitt av Lysne II-utvalget om digitalt grenseforsvar med frist for høringsuttalelse 6. januar d.å.

NRK forstår behovet for et digitalt grenseforsvar, men mener utvalgets forslag bryter med grunnleggende menneskerettigheter knyttet til personvern og ytringsfrihet. Vi skal i det følgende utdype vår begrunnelse for denne vurderingen.

Utvalget foreslår å innføre et såkalt digitalt grenseforsvar (heretter forkortet DGF). Forslaget innebærer at myndighetene kan få tilgang til alle metadata og innholdsdata fra alle nordmenn, ikke bare de som er mistenkt for noe kriminelt. DGF omfatter all elektronisk kommunikasjon mellom Norge og utlandet. I praksis vil det innebære at også det meste av den kommunikasjonen som foregår mellom to personer *i* Norge, vil være omfattet. Systemet begrenses ikke til kommunikasjon mellom personer, men vil også omfatte informasjon som den enkelte lagrer på sin mobiltelefon kun for egen bruk.

Utvalget skriver selv:

> *"Kablene som krysser grensen inneholder mye mer enn kommunikasjon mellom Norge og utlandet. Alt vi foretar oss på sosiale medier krysser disse kablene. De fleste nye, internettbaserte meldings-, chatte- og taletjenester vi benytter oss av krysser landegrensen, selv om både avsender og mottager av meldingene og samtalene er nordmenn som befinner seg i Norge. Når du tar backup av telefonen din over nettet, kan all informasjon*

RA44, Postboks 8500 Majorstuen, 0340 Oslo
Bjørnstjerne Bjørnsons plass 1
+47 23 04 82 04
+47 23 04 70 00
No 976 390 512 MVA
nrk.no

som befinner seg på telefonen din passere avlesningsutstyret." [Fra kronikk i Aftenposten 5. september 2016 fra utvalgets leder og medlemmer]

Utvalget foreslår med andre ord et svært omfattende overvåkingssystem – et overvåkningssystem uten sidestykke i norsk historie.

Forslaget til et DGF er begrunnet i ønsket om å avverge terrorisme og cyber-trusler mot Norge og norske interesser. Dette er selvsagt svært viktige hensyn.

NRK mener imidlertid at det konkrete forslaget til overvåkingssystem ikke i tilstrekkelig grad tar hensyn til menneskerettighetene personvern og ytringsfrihet. Utvalget har heller ikke foretatt de nødvendige avveininger og vurderinger som kreves for å kunne innføre et så inngripende tiltak som dette systemet innebærer. Særlig gjelder dette i forhold til kildevernet - som er en del av ytringsfriheten.

Grunnleggende menneskerettigheter som personvern og ytringsfrihet forutsetter at det foretas en proporsjonalitetsvurdering der de fordeler som kan oppnås ved inngrepet, må avveies mot de konsekvenser inngrepet vil kunne få nettopp for disse rettighetene. Vi kan ikke se at forholdet til kildevernet er vurdert i rapporten, og vurderingen i forhold til personvernet er etter vårt syn klart mangelfull.

Vi vil i det følgende konsentrere oss om forholdet til kildevernet. Vi minner imidlertid om at det er en nær sammenheng mellom kildevernet og personvernet. Et fungerende personvern er på mange måter en forutsetning for kildevernet, og for at media kan få informasjon fra kilder som innehar, eller kan få tilgang til, informasjon som kan sette deres egen sikkerhet i fare.

For ordens skyld skal her innledningsvis bemerkes at NRK naturligvis erkjenner at det allerede er en betydelig risiko for kilder å kommunisere digitalt gjennom internett eller ved mobilkommunikasjon. Denne risikoen kan imidlertid ikke brukes som selvstendig argumentasjon for å innføre overvåkingstiltak som griper alvorlig inn i kildevernet.

NRK mener forslaget til overvåkningssystemet i alvorlig grad vil svekke kildevernet og følgelig medias mulighet for å fylle en av sine viktigste samfunnsroller – nemlig å avdekke forhold av allmenn interesse. NRK støtter derfor ikke forslaget.

NRK mener forslaget til DGF vil være i strid med den rettslige beskyttelse kildevernet har etter EMK artikkel 10.

NRK mener videre at forslaget til DGF vil være i strid med EU-lovgivningen, herunder bestemmelsene om personvern og ytringsfrihet i Charter of Fundamental Rights. Vi viser her til EU-domstolens nylig avsagte avgjørelse av 21. desember 2016 i de forente sakene om Storbritannias og Sveriges nasjonale datalagringslovgivning (C-203/15 og C-698/15). Avgjørelsen er avsagt etter at Lysne II-utvalget avga sin rapport og vil bli kommentert nærmere under punkt 3 nedenfor.

2. Kildevern og medias særskilte rolle i et demokratisk samfunn

Medienes viktigste rolle i et demokratisk samfunn er å bringe frem informasjon av allmenn interesse og å være en "offentlig vaktbikkje" i forhold til alle maktfaktorer i samfunnet – herunder også offentlige myndigheter. Både Den europeiske menneskerettighetsdomstolen (heretter forkortet EMD) og Høyesterett har i en rekke dommer fremhevet medienes særskilte samfunns-rolle og begrunnet hvorfor mediene er gitt et særskilt vern etter EMK artikkel 10 om ytrings- og informasjonsfrihet.

Kildevernet er gitt en svært sterk beskyttelse etter EMK artikkel 10. Kildevernet er begrunnet i samfunnsinteressen i fri formidling av samfunnsrelevant informasjon og avdekking av kritikkverdige forhold. Det er de skader inngrep i kildevernet kan påføre informasjonsfriheten generelt som er det vesentlige. Dette omtales gjerne som «the chilling effect» eller den langsiktige nedkjølende effekten. Det er følgelig ikke hensynet til kilden eller skadevirkningene i den konkrete saken som er det primære. Kildevernet omfatter ikke bare informasjon som direkte avslører kildens identitet, men også informasjon som indirekte kan lede til at kilden avsløres. Etter praksis fra EMD og Høyesterett er kildevernet tilnærmet absolutt. Også upublisert materiale som ikke inneholder informasjon som kan føre til avsløring av kildens identitet, nyter et visst vern etter EMK artikkel 10.

Den avgjørende begrunnelsen for et rettslig sett tilnærmet absolutt kildevernet er således at ethvert inngrep i kildevernet vil ha en nedkjølende effekt på fremtidige potensielle kilder og medføre at medias informasjonskanaler tørker ut. Dermed vil medienes muligheter til å fylle sin samfunnsrolle forhindres.

Vi viser i denne forbindelse blant annet til Rt-2013-1290 og Rt-2015-1286, der Høyesterett understreker at det er den langsiktige effekten av inngrep i kildevernet som er det sentrale (Rt-2013-1290 avsnitt 29 og 34, Rt-2015-1286 avsnitt 54, 57 og 81), og der det fremgår at det selv ikke i forbindelse med etterforskning og forebygging av terrorvirksomhet ble tillatt inngrep i kildevernet.

Hensynet til ytringsfriheten, medienes rolle i et demokratisk samfunn eller kildevernet er ikke reelt vurdert i rapporten. Disse hensynene er ikke en gang nevnt i kapitlet som omhandler "Faktorer som taler mot DGF" (kapittel 6). Det eneste som ser ut til å være nevnt om kildevernet står i punkt 9.5.1:

> *"Ut over dette vil utvalget legge til at det har vurdert om det må oppstilles særlige regler til vern om kommunikasjon med yrkesutøvere med streng taushetsplikt. Kommunikasjon mellom en advokat og klient eller mellom en journalist og en kilde kan være viktige eksempler på det. Unnlatelsen av å vurdere dette nærmere ser ut til å være én av hovedinnvendingene i EU-domstolens avgjørelse om Datalagringsdirektivet. Utvalget har imidlertid ikke funnet å tilrå en slik begrensning for DGF. Det er flere grunner til det. En grunn er at det vil være teknisk vanskelig å gjennomføre filtrering uten en innrapporteringsordning på selektornivå. Slik innrapportering kan være lite realistisk og vil uansett vanskelig kunne etableres for personer i utlandet. Dernest vil filtrering kunne ha utilsiktede konsekvenser. Dersom tjenesten følger et legitimt mål i utlandet, antas filtreringsregelen å måtte medføre at kommunikasjon fra vedkommende til en «sperret» selektor i Norge ikke vil fremkomme. For det første vil dette være en omgåelsesmulighet for trusselaktører som ønsker å unngå tjenestens søkelys. For det annet vil manglende informasjon i enkelte tilfeller lede til at personer ikke «sjekkes ut» av et sakskompleks, med de negative konsekvenser dette kan ha for dem det gjelder. Endelig vil utvalget peke på at gruppen som skulle omfattes kan være uklar. Hva f.eks. med kommunikasjon med religiøse ledere i radikale tross-samfunn – skal det likestilles med den taushetsplikt som gjelder for betroelse til prester? Hvem skal i så tilfelle treffe beslutning om at dette likestilles? Videre vil det være problematisk å legge til grunn at all kommunikasjon til eller fra f.eks. en advokat eller journalist er dekket av taushetsplikt og derfor skal filtreres ut. Det vil åpenbart legge til rette for å bruke stilling som skalkeskjul for dem som har interesse av det. Utvalgets syn er etter dette at en ikke bør legge inn bestemte begrensninger for yrkesgrupper med taushetsplikt ved design og utforming av reglene for DGF."* [Vår understrekning]

Til tross for at en manglende vurdering av disse var sentralt i EU-domstolens begrunnelse for at Datalagringsdirektivet ble ansett for å være ulovlig, har utvalget ikke foretatt noen vurdering av hvilke *konsekvenser* DGF vil få for kildevernet - og derigjennom allmennhetens mulighet til å få tilgang på informasjon av allmenn interesse. Vi kan i det hele ikke se at det er foretatt noen vurdering av lovligheten av DGF i forhold til kildevernet.

NRK mener det er overraskende at en slik vurdering ikke er foretatt, ikke minst på bakgrunn av den ekspertutredningen som i 2015 ble laget etter oppdrag fra Justisdepartementet og Samferdselsdepartementet. Utredningens tittel er

"*Datalagring og menneskerettigheter*", og er skrevet av professor Hans Petter Graver og Henning Harborg og avgitt 1. oktober 2015. Vi mener rapporten underbygger vår vurdering om at forslaget til DGF vil være i strid med menneskerettighetene. Vi viser her til ekspertutredningen punkt 7.10 der det blant annet står følgende:

> *"Et særlig problem med lagring av kommunikasjonsdata er at lagringen vil komme til å omfatte kommunikasjon med personer hvis kommunikasjon nyter en særlig beskyttelse så som leger, prester, advokater og journalister. I sin dom peker EU-domstolen på, som en innvending mot DLD, at det ikke inneholder noen unntaksbestemmelser som gjør at det ikke kommer til anvendelse på personer hvis kommunikasjon er underlagt taushetsplikt, se avsnitt 58. Det er ikke helt klart om domstolen mener at dette er et moment i proporsjonalitetsvurderingen, eller om et slikt unntak er en betingelse for at lagring av kommunikasjonsdata i det hele tatt skal være lovlig. Det fremgår imidlertid av avsnitt 65 at det må foretas avgrensninger som må sikre at inngrepet i de grunnleggende rettighetene er begrenset til det strengt nødvendige, og at disse avgrensningene må følge av klare og presise regler. Siden inngrep i privilegert kommunikasjon reiser særlige spørsmål, må det i det minste foreligge klare regler for hvordan denne dataen skal skilles ut fra den øvrige mengden av data, samt hvordan de skal behandles.*
>
> ...
>
> *For kommunikasjonsdata kommer for pressen det særlige hensynet inn at det er kildens identitet som nyter vern, like mye som innholdet av den kommunikasjonen som har foregått mellom kilden og en journalist. Rene kommunikasjonsdata er derfor uten videre mer inngripende i pressens kildevern enn i for eksempel kommunikasjonen med advokater og leger hvor det i hovedsak er innholdet av kommunikasjonen som er beskyttet. Det er neppe teknisk mulig å utforme en lagringsplikt som unntar data om kommunikasjon som kan røpe privilegert informasjon fra lagring. ... Dersom EMK må antas å stenge for udiskriminerende lagring av kommunikasjon som kan inneholde privilegert informasjon uten at det foreligger en konkret situasjon eller mistanke som kan begrunne også en slik lagring, vil dette innebære at datalagring ikke kan innføres uten å komme i konflikt med EMK.*
>
> *Det er uansett klart at en datalagringsordning må differensiere mellom privilegert informasjon og annen informasjon når det gjelder tilgangen til og bruken av de lagrede data. Skal man beskytte denne typen kommunikasjon må det derfor være gjennom forbud mot utlevering og anvendelse av opplysninger kombinert med kontrollmekanismer. I størst mulig grad må det settes inn barrierer mellom dem som samler inn data og dem som er involvert i oppklaring eller etterforskning av saker. Ved siden*

av et forbud mot å anvende opplysninger som kan røpe kommunikasjon med personer som er unntatt fra vitneplikt på grunn av yrkes- og kallsmessig taushetsplikt eller pressens kildevern, kan tenkes regler om sletting av slike data samt protokollering av at sletting er foretatt.

...

Selv om datalagringen ikke skal omfatte kommunikasjonens innhold, vil i noen tilfeller selve det forholdet at det har vært kontakt mellom en person og for eksempel en advokat, lege eller journalist i seg selv kunne røpe opplysninger som er beskyttet av taushetsplikten. Det er gjerne når slik informasjon ses i sammenheng med annen informasjon som politiet har, at den fortrolige karakteren av kommunikasjonsdata kan tre frem. Dette kan ikke minst være problematisk for pressen, hvor rene kommunikasjonsdata kan røpe pressens kilder.

....

Problemene med i det hele tatt å skille ut privilegert informasjon fra det materialet som utleveres av de lagrede kommunikasjonsdata, er forhold som i seg selv trekker i retning av at datalagring ikke kan gjennomføres uten å komme i konflikt med EMK. Uansett må det legges til grunn at uten at man etablerer ordninger som kan sikre dette på en betryggende måte, vil en lagringsordning ikke stå seg. Det å utforme en slik ordning vil kreve en betydelig teknisk innsikt og en innsikt i arten av data som vil bli omfattet av en lagring. Dette er en type innsikt vi ikke har, og vi vil derfor ikke begi oss inn på en konstruksjon av en slik ordning. Den som skal utforme en slik ordning må imidlertid oppfylle de kravene som EMD og EU-domstolen har satt til klarhet, forutberegnelighet og sikkerhet. Det betyr at ordningen klart må angi hvem som skal foreta silingen, hvilke kriterier og metoder den skal bygge på, retningslinjer for det skjønnet som må utøves i vurderingen av om kommunikasjonsdata kan røpe fortrolig informasjon og for vurderingen av om fortrolig informasjon likevel i unntakstilfeller skal utleveres. Silingen må skje ved en instans som er uavhengig av påtalemyndigheten og forvaltningen, og i den utstrekning den ikke skjer ved en domstol, være underlagt judisiell kontroll." [Vår understrekning]

Som det fremgår, mener ekspertutvalget at det er et åpent spørsmål om masselagring av data som innbefatter kildevernsensitiv informasjon, pr. definisjon er i strid med menneskerettighetene. Ekspertutvalget uttaler videre at de faktiske problemene med å skille ut slik informasjon fra det som lagres, i seg selv taler for at datalagringen er ulovlig. Under enhver omstendighet må datalagringsordningen skille mellom slik informasjon og annen informasjon, den må oppfylle de krav som er satt av EMD og EU-domstolen, silingen må skje av en uavhengig instans, osv.

Lysne-utvalget er selv inne på at det ikke er praktisk realistisk å skille ut slik privilegert informasjon. Allerede av den grunn vil DFG å være i strid med

menneskerettighetene. Videre skal "*etterretningspersonell*" ha ubegrenset tilgang til all data de siste 14 dager gjennom det såkalte "*korttidslageret*". Silingen vil således ikke bli foretatt av en "*uavhengig instans*" og vil også av den grunn være ulovlig.
Vi minner om at ekspertutredningen gjaldt Datalagingsdirektivet som kun omfattet metadata, mens DGF i tillegg omfatter innholdsdata og således innebærer et overvåkningssystem av en mye mer omfattende karakter.

Ethvert inngrep i kildevernet må – for å være lovlig – oppfylle vilkårene i EMK artikkel 10 nr. 2. Etter praksis fra EMD medfører det at det må foreligge en "*overriding requirement in the public interest*". Det er kun i helt eksepsjonelle tilfeller der det foreligger et altoverveiende samfunnsmessig behov for det at unntak fra kildevernet vil være tillatt. Etter det vi kan se er DGF i hovedsak begrunnet med at det er "*vanskelig å se for seg at en tilsvarende positiv effekt vil kunne oppnås på annen og mindre inngripende måte*", jfr. rapportens side 62. Dette tilfredsstiller selvsagt ikke den proporsjonalitetsvurderingen som skal foretas etter EMK artikkel 10. Rapporten inneholder ingen vurdering av hvilken langsiktig innvirkning DGF vil ha på kildevernet og dermed borgernes mulighet til å motta informasjon av allmenn interesse.

I proporsjonalitetsvurderingen skal den langsiktig skadelige "*chilling effect*" veies opp mot det man kan oppnå ved inngrepet. Vi mener det i rapporten heller ikke er foretatt noe betryggende vurdering av hva man kan oppnå med DGF. Det er allment kjent at kryptering – og kryptering som ikke lar seg forsere – brukes i stadig større utstrekning. Og dersom DGF skulle bli vedtatt, må det antas at kryptering vil bli brukt i enda større utstrekning. Verdien av det som kan oppnås med DGF vil således bli tilsvarende redusert. Det må antas at de som driver slik virksomhet som e-tjenesten ønsker å ramme i all hovedsak vil bruke slik kryptering.

3. EU-domstolens storkammeravgjørelse om Storbritannias og Sveriges datalagringslovgivning

Avgjørelsen slår fast at generell og ikke-diskriminerende lagring av metadata (trafikkdata og lokasjonsdata) er i strid med EU-retten.

Avgjørelsen gjelder ikke lagring av innholdsdata, kun lagring av metadata. Det ble likevel ansett som svært inngripende, både i forhold til personvernet og ytringsfriheten. EU-domstolen uttaler blant annet:

> *100 The interference entailed by such legislation in the fundamental rights enshrined in Articles 7 and 8 of the Charter is very far-reaching and must be considered to be particularly serious. The fact that the data is retained without the subscriber or registered*

user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance (...).

101 Even if such legislation does not permit retention of the content of a communication and is not, therefore, such as to affect adversely the essence of those rights (...), the retention of traffic and location data could nonetheless have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter.

EU-domstolen fastslår at heller ikke bekjempelse av terrorisme rettferdiggjør en generell, ikke-diskriminerende datalagring. Videre viser domstolen – på samme måte som i dommen om datalagringsdirektivet – til at yrkesgrupper som mottar taushetsbelagt/privilegert informasjon ikke er skilt ut. For at datalagring skal kunne være tillatt må lagringen begrenses mht. personer, type data, osv., til det som er absolutt nødvendig. Domstolen uttaler blant annet:

103 Further, while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight (...).

...

105 Second, national legislation such as that at issue in the main proceedings, which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception according to the objective pursued. It is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences. Further, it does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraphs 57 and 58).

108 However, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication

affected, the persons concerned and the retention period adopted, to what is strictly necessary

Videre slår domstolen fast at myndighetenes tilgang til informasjonen krever forhåndskontroll av en domstol eller et annet lignende uavhengig organ, samt at de personer som myndighetene har fått tilgang til informasjon om, skal varsles.

Etter det NRK kan se oppfyller forslaget til DGF ikke de krav som stilles i EUs storkammeravgjørelse. NRK legger derfor til grunn at man under enhver omstendighet ikke vil gå videre med forslaget, før det er foretatt en nærmere analyse av forslaget i forhold til den nå foreliggende storkammeravgjørelsen.

4. Nærmere om forslaget til kontrollmekanismer

I rapportens kapittel 9 redegjøres for de kontrollmekanismer utvalget ser for seg. Som kommentert under punkt 2, må det antas at overvåkningssystemet vil være i strid med menneskerettighetene til tross for forslagene om kontroll-mekanismer. Det er vanskelig å få oversikt over hvilke skranker og rettsikkerhetsgarantier de foreslåtte kontrollmekanismene i realiteten medfører. Vi vil her gi et par eksempler på forhold som medfører at kontrollmekanismene i liten grad representerer rettssikkerhetsgarantier, og som følgelig underbygger vår vurdering av at overvåkningssystemet antas å være i strid med menneske-rettighetene:

- Kontrollen er i stor grad etterfølgende. EMD har i en rekke avgjørelser påpekt at etterfølgende kontroll ikke er i samsvar med kildevernet. Dette, fordi skaden - den nedkjølende effekten - da allerede har skjedd. Kildevernet forutsetter ordninger som sørger for at myndighetene ikke får *tilgang* på informasjon som - direkte eller indirekte - kan føre til at kilden avsløres.

- Gjennom det såkalte "*korttidslageret*" vil E-tjenesten ha tilgang til all informasjon den siste 14-dagers perioden. Selv om denne tilgangen etter utvalgets beskrivelse kun skal benyttes til "*teknisk vedlikeholdsarbeid av filtrene*" og "*oppdatering av filtrene*", vil det medføre at e-tjenestens medarbeidere faktisk har tilgang til informasjonen og følgelig vil den nedkjølende effekten inntre.

- I metadatalageret skal en spesialdomstol (DGF-domstolen) kunne gi tilgang til søk – ikke bare på person, men også på "*modus*" eller "*kommunikasjonsparametre*". Dette innebærer i realiteten at det åpnes for en svært vid søkeadgang der det må antas at kildevernet regelmessig

vil bli brutt. Dette, fordi det ikke er foretatt noe utskilling av kildevernsensitive data i datalageret. I denne sammenheng kan det også påpekes at utvalget skriver at DFG-domstolen vil måtte "*ta hensyn til at utenlandsetterretning ofte innebærer at man søker etter ukjente aktører basert på kjent modus, hvilket kan tilsi bred målutvikling før man gjennom analyse og videre tiltak kan skille ut den relevante informasjon for videre målrettet og presis innsamling*". Det legges med andre ord opp til at myndighetene skal ha en svært omfattende tilgang på informasjon, for så senere å kunne skille ut relevant informasjon.

- For søk på personer skal det være adgang til søk "*to ledd ut i kommunikasjonskjeden*". Videre skal det kunne gis tillatelse til søk i "*opp til ett år, i enkelte tilfeller muligens lenger*". Det legges således også her opp til svært vide fullmakter til søk.

- Den informasjonen e-tjenesten har samlet inn til utenlandsetterretnings-formål skal kunne deles med andre myndigheter når informasjonen er av relevans disse andre myndighetene. En slik adgang er problematisk i forhold til kravet om klarhet, sikkerhet og forutberegnelighet etter EMK.

- DGF-domstolsystemet innebærer flere klare mangler. For det første er det ingen ankemuligheter og ingen som særskilt ivaretar interessene til de som er blitt overvåket. I denne forbindelse skal det påpekes at de interesser som kildevernet bygger på ofte ikke blir til tilstrekkelig hensyntatt før saken blir behandlet av Høyesterett. Det kan her blant annet vises til den siste kildevernavgjørelsen behandlet i Høyesterett (Rt-2015-1286) der både tingretten og lagmannsretten enstemmig kom til at kildevernet måtte vike, mens Høyesterett enstemmig kom til at inngrepet var i strid med kildevernet. Videre er det nærliggende å anta at det skal mye til før en enslig dommer vil nekte E-tjenesten tilgang når det argumenteres med rikets sikkerhet, og det kan spørres hvilken reell mulighet for overprøving den enkelte dommer egentlig vil ha. Det foreligger også en fare for at dommerne ved en slik spesialdomstol – som bare skal bestå av noen få dommere og som skal tilhold i godkjente lokaler hos e-tjenesten - vil identifisere seg med tjenestens virke og oppgaver.

- Det åpnes også for at e-tjenesten kan iverksette søk uten å avvente domstolens tillatelse. Det skal da foretas en etterfølgende foreleggelse for domstolen og sletting av søk dersom domstolen avslår god-kjennelsen. NRK mener dette på ingen måte er tilfredsstillende i forhold til kildevernet.

5. Oppsummering

NRK mener forslaget til DGF er i strid med kildevernet. Vi mener det under enhver omstendighet ikke innføres uten en nærmere utredning av forholdet til kildevernet. Etter den nylig avsagte storkammeravgjørelsen fra EU-domstolen fremstår det videre som om forlaget er i strid med EU-retten. Det legges til grunn at man ikke går videre med forslaget – i alle fall ikke uten en nærmere analyse av de konsekvenser storkammeravgjørelsen får for forslaget.

Med vennlig hilsen

Olav A. Nyhus
Direktør
Juridisk, rettigheter og personal
olav.nyhus@nrk.no