Datatilsynet

Forsvarsdepartementet
Postboks 8126 Dep
0032 OSLO

Deres referanse	Vår referanse	Dato
2016/2699-1/FD II 5/SIH	16/01693-2/SDK	18.01.2017

Høringsuttalelse - Rapport avgitt av Lysne II-utvalget om digitalt grenseforsvar - Forsvarsdepartementet

Vi viser til høringsbrev fra Forsvarsdepartementet om Lysne II-utvalgets rapport om digitalt grenseforsvar (DGF) av 5. oktober 2016, mottatt hos oss den 25. oktober.

Oversikt over innholdet i høringssvaret

1. Oppsummering - Masseinnsamlingen og overvåkingen av egen befolkning er i strid med menneskerettighetene og kan ikke innføres

Datatilsynet mener at DGF-løsningen som utvalget foreslår ikke kan innføres i Norge av flere grunner:

- Forslaget krenker personvernet vårt og rettighetene våre etter Den europeiske menneskerettskonvensjonen (EMK) artikkel 8 og Grunnloven § 102. DGF vil være i strid med menneskerettighetene, og kan derfor ikke innføres i Norge. EU-domstolens avgjørelse i de forente sakene C-203/15 og C-698/15 bekrefter dette synet. Domstolen fastslo at generell innsamling og lagring av kommunikasjonsopplysninger om en ubegrenset krets av personer er i strid med menneskerettighetene.

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr:	Hjemmeside:
Postboks 8177 Dep 0034 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no

- Tiltaket er svært omfattende. Den foreslåtte løsningen går for langt, tiltaket treffer oss alle, og den evner ikke en nødvendig grad av målrettethet. Mengden av opplysninger som vil bli samlet inn og lagret er enorm. Opplysningene vil i stor grad være private, og dataene sier mye om oss, våre tanker, våre relasjoner og våre liv.
- Tiltaket er for inngripende overfor enkeltmennesket, det vil si beskyttelsen av deres personopplysninger, vernet om den private sfære og individets frihet til å tilegne seg informasjon, knytte vennskap og være et sosialt menneske i en stadig mer internettbasert verden. Det gjelder også for sentrale, kollektive verdier i vårt samfunn som informasjons- og ytringsfrihet.
- DGF vil bidra til å forsterke den nedkjølingseffekten som vi i stadig større grad bør bekymre oss for.
- Vi mener at informasjonen i DGF-systemet er så nyttig for andre aktører på justis- og sikkerhetsfeltet, for eksempel i straffesaker, at en formålsutglidning må påregnes. Tiltaket vil slik, med stor sannsynlighet, bli mer inngripende enn det man i første omgang tar stilling til.
- Vi mener tiltaket krysser en prinsipiell linje som ikke bør krysses, nemlig at hemmelige tjenester besitter enorme mengder informasjon om egne borgeres kommunikasjon, løsrevet fra mistanke eller individuelle sikkehetsbekymringer.
- Løsninger for både innholdskryptering og metadatakryptering er lett tilgjengelig og er også vanlig i bruk. Dette betyr at DGF i hovedsak vil ramme den vanlige mann og kvinne som ikke gjør spesielle tiltak for å beskytte sin kommunikasjon – bevisste og kompetente trusselaktører kan i stor grad unngå å bli fanget opp av DGF.

DGF reiser en rekke spørsmål. Noen av disse gjelder statens menneskerettslige forpliktelser, og om den foreslåtte DGF-løsningen er forenlig med disse og med Grunnloven. Uansett står ett viktig politisk og prinsipielt spørsmål frem:

Vil vi at egne sikkerhetsmyndigheter skal masseinnsamle data om borgernes kommunikasjon – fullstendig løsrevet fra mistanke og individuelle sikkerhetsbekymringer – for å skaffe en database å søke i på jakt etter trusler?

Vi mener at svaret på dette må bli «nei». Et «ja» vil innebære et veiskille.

Den foreslåtte DGF-modellen er i mange henseende mer inngripende enn slik datalagringsdirektivet var tenkt utført i Norge. Opplysningene blir ikke lagret desentralisert hos den enkelte tjenestetilbyder, med en mulighet for uthenting på individnivå. Opplysningene om oss alle blir samlet sammen til et lager av metadata for søk etter det mistenkelige. Vi havner alle under lupen.

2. Om menneskerettighetene, Grunnloven og EU-domstolens avgjørelse fra i fjor

EU-domstolens avgjørelse fra desember 2016

DGF vil innebære en overvåking av kommunikasjonen til de fleste innbyggerne i Norge, uten hensyn til om menneskene som blir overvåket har vært involvert i en straffbar handling eller ikke. Scenariet som DGF tegner opp er parallelt med den konkrete situasjonen som var utgangspunktet for dommen om de svenske og engelske datalagringslovene som EU-domstolen avsa i slutten av desember i fjor.

I dommen i de forente sakene C-203/15 og C-698/15 fra 21. desember konkluderte EU-domstolen med at de svenske og engelske datalagringslovene er ulovlige. Domstolen er klar i sin uttalelse når den slår fast at generell innsamling og lagring av kommunikasjonsopplysninger om en ubegrenset krets av personer er i strid med menneskerettighetene. Slik datalagring kan bare være lovlig hvis den er målrettet, sier domstolen.

Domstolen uttaler at lagring av kommunikasjonsopplysninger er et inngrep i våre fundamentale rettigheter. Datalagringslovene i Sverige og Storbritannia utgjør særlig alvorlige inngrep i våre rettigheter og friheter, heter det i dommen. Domstolen påpeker at det faktum at datalagringen finner sted uten at brukerne blir informert om det, er egnet til å skape en følelse hos de berørte menneskene av at privatlivet deres er under konstant overvåking (se premiss 100).

Domstolen uttaler videre:

> «[...] selv om effektiviteten af bekæmpelsen af grov kriminalitet, og navnlig organiseret kriminalitet og terrorisme, i vidt omfang kan være afhængig af anvendelse af moderne efterforskningsteknikker, kan et sådant mål af almen interesse, hvor grundlæggende det end er, ikke i sig selv begrunde, at en national lovgivning, der foreskriver en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata, anses for nødvendig af hensyn til den nævnte bekæmpelse.» (premiss 103)

Det kan derimot lagres kommunikasjonsdata om enkeltmennesker under forutsetning av at det eksisterer en sammenheng mellom de dataene som skal lagres og en konkret trussel mot den offentlige sikkerhet (premiss 106). Dette betyr at databehandlingen bare kan tillates dersom den er rettet mot data vedrørende et tidsrom og/eller et geografisk område og/eller en personkrets, som på en eller annen måte vil kunne være innblandet i alvorlige lovovertredelser (...)» (ibid.).

Kravet om målretting er svært sentralt: Staten kan ikke lagre data om folk på bakgrunn av en generell frykt for alvorlig kriminelle handlinger – inkludert terrorisme – i fremtiden.

EU-domstolens avgjørelse og norsk rett

EU-domstolen tok utgangspunkt i kommunikasjonsverndirektivet artikkel 15(1), som den tolket i lys av artiklene 7 og 8 i EUs charter over fundamentale rettigheter. Kommunikasjonsverndirektivet er en del av norsk rett gjennom EØS, men charteret gjelder ikke direkte for Norge. Artikkel 7 i EUs charter tilsvarer imidlertid bestemmelsene som vi har i Grunnloven § 102 og i Den europeiske menneskerettskonvensjonen (EMK) artikkel 8. EMK er tatt inn i norsk lov og gitt forrang foran øvrig formell lovgivning, i medhold av menneskerettsloven fra 1999. Artikkel 8 i charteret tilsvarer reglene i personopplysningsloven og i Europarådets konvensjon 108 fra 1981, som Norge har ratifisert. At charteret som sådan ikke er en del av norsk rett, er altså uten betydning, som Lysne II-utvalget selv viser til i avsnitt 9.5.2 i rapporten.

Dommen betyr en annen konklusjon enn utvalgets

Lysne-utvalget antyder selv at DGF balanserer på en knivsegg mot det som menneskerettighetene tillater. Det er de kompenserende tiltakene som gjør at forslaget etter en helhetsvurdering blir akseptabelt, slik vi forstår utvalget. Etter dommen i sak C-203/15 er det tydelig at Lysne-utvalget har tatt feil. I dommens premiss 108 fremgår det klart at målrettet datalagring kan finne sted, men da under forutsetning av at lagringen «begrænses til det strengt nødvendige for så vidt angår kategorierne af data, der skal lagres, de omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af lagringen». Uinnskrenket og generell lagring kan *ikke* finne sted i et demokratisk samfunn.

Utvalget skriver i sine konklusjoner: «EU-domstolens underkjennelse av Datalagringsdirektivet setter ned noen grensesteiner, men det er flere relevante saker som nå er under forberedelse. Avgjørelser i disse sakene kommer etter at utvalget har avsluttet sitt arbeid. Når de foreligger, vil DGF naturligvis også måtte vurderes i lys av disse». Av rapporten for øvrig fremgår det at det må være sakene C-203/15 og C-698/15 utvalget her sikter til.

Nå har domstolen sagt sitt, og konklusjonen er at nasjonal lovgivning utelukkende kan hjemle avgrenset datalagring. *En lov som hjemler generell datainnsamling og datalagring vil være uforenlig med direktiv 2002/58 artikkel 15 og menneskerettighetene – en slik lov vil med andre ord være ulovlig.*

Eksisterer det en menneskerettslig forpliktelse for staten til å innføre DGF?

Utvalget antyder i rapportens pkt. 5.7 at etablering av DGF kan ha støtte i våre folkerettslige forpliktelser. Dette vil vi tilbakevise. EU-domstolen ville neppe ha kommet til den konklusjonen som det er redegjort for overfor, hvis så hadde vært tilfelle. Hans Petter Graver og Henning Harborg har dessuten i en utredning om datalagring og menneskerettighetene uttalt følgende: [1]

> «Som vi ser, går ikke forpliktelsene i disse konvensjonene lengre enn det som kan anses som akseptable etterforskningsmetoder etter internasjonale menneskerettigheter

[1] https://www.regjeringen.no/contentassets/93528bcf984a48a2a89c89cf757b35ef/utredningdldsdjd2015.pdf

og nasjonale forfatninger. Det kan neppe heller være grunnlag for å strekke plikten til å sikre menneskerettighetene etter EMK lengre enn dette. Man vil dermed ikke kunne utlede noen plikt til datalagring ut fra statens plikt til å sikre menneskerettighetene. Statens plikt går ikke lengre enn til å sikre dem med de midler som er tillatelige ut fra blant annet beskyttelsen av privatlivet. Sagt på en annen måte kan man si at plikten til å sikre menneskerettighetene kan utgjøre et lovlig formål for inngrep i rettigheter, men den kan ikke erstatte de andre elementene i vurderingen av inngrepets lovlighet og proporsjonalitet.»

Graver og Harborg uttaler, etter en lengre vurdering av datalagring opp mot EMK og Grunnloven, også:

> «Det kan etter vår oppfatning ikke utelukkes at de personvernmessige betenkelighetene ved overvåkningselementet er så fremtredende og tungtveiende at man simpelthen ikke kan anse datalagring nødvendig i et demokratisk samfunn».

3. Fra de få til oss alle

Vi antar at den jevne nordmann i dag regner med at landets hemmelige tjenester, og E-tjenesten i særdeleshet, ikke behandler personopplysninger om dem. Det store flertallet av oss representerer ingen trussel mot samfunnet. De fleste av oss har heller ikke kontakt med kretser vi mistenker kan være under spesiell oppmerksomhet. Vi regner med å være unntatt. Det er et godt tegn for et fritt samfunn dersom den alminnelige borger ikke føler at sikkerhetstjenester vedrører *dem*, som et objekt for kontroll.

DGF forrykker dette. Tiltaket treffer oss alle, og terskelen for når det skal samles inn metadata (signalet krysser landegrensen) er veldig lav sett i lys av dagens internettbaserte hverdag. Tilnærmet alle bruker internett i større eller mindre omfang, og internettbruk betyr at signaler krysser landegrenser. Det er med andre ord ikke bare små bruddstykker av den enkeltes kommunikasjon det vil lagres metadata om. Særlig for den yngre delen av befolkningen vil tiltaket få et enormt nedslagsfelt i forhold til deres totale kommunikasjon og informasjonssøking.

Stadig flere løsninger og kommunikasjonskanaler vil basere seg på internett i tiden fremover, og med det også falle innenfor hva det vil samles inn data om. I tillegg skal det samles inn data om telefonbruk hvor den ene parten er utenfor Norges grenser.

Trafikken som krysser landegrensene våre har som regel et startpunkt eller endepunkt i Norge. Norge er i beskjeden grad transittland for kommunikasjon videre til utlandet, slik utvalget også påpeker. Som igangsetter eller mottaker handler informasjonen om oss – ikke bare om personer med dårlige hensikter, «de der ute», bedrifter eller «noen andre». Det er ikke engang mulig å filtrere effektivt ut kommunikasjon mellom personer som begge er i Norge. Vi må anta at lageret med metadata vil inneholde vel så mye informasjon om det innenlandske og nordmenn i Norge, som det utenlandske. Det er paradoksalt at det er E-tjenesten, altså landets utenlandsetterretning, som vil besitte enorme mengder informasjon om borgernes kommunikasjon.

I et frihets- og personvernperspektiv er mengde og nedslagsfelt svært problematisk. Vi stiller også spørsmål ved om kombinasjonen av den mengde og antatte innlandsprofil dataene trolig vil få, lar seg forene med kravet i etterretningstjenesteloven § 4 om at E-tjenesten på norsk territorium ikke skal overvåke eller på annen fordekt måte innhente informasjon om norske fysiske eller juridiske personer.

4. Overordnet om forslaget til DGF

Innsamling og lagring er et inngrep

Innsamling og lagring av personopplysninger er et inngrep *i seg selv*. Dette er et viktig poeng i EU-domstolens avgjørelser i både DLD-dommen og dommen om de svenske og engelske datalagringslovene fra desember i fjor.

Fra tidligere debatter vet vi at dette poenget ikke alltid blir oppfattet, eventuelt underslått. Vi kan se en slags parallell til dette i debatter om overvåking, inkludert ulik forståelse av hva som legges i begrepet. Kun først når opplysningen blir gjenstand for gjennomsyn og vurdering av et menneske, vil enkelte kalle det overvåking. Forutgående masseinnsamling for kontrollformål, samt maskinell analyse av data, teller på en måte ikke.

Vi antar at det i debatten om DGF også vil være aktører som mener at personvernproblematikken kan isoleres til hva som konkret kommer frem i E-tjenestens søk i datalagerne. Da er det også lettere å argumentere for at inngrepet er begrenset. Dette er et forfeilet utgangspunkt. Konsekvensene starter ved innsamlingen. Etter vårt syn er selve innsamlingen og lagringen – at vi alle skal inn i databasen for undersøkelser – det mest problematiske ved den foreslåtte DGF-løsningen.

Vi mener utvalget i for alt for liten grad vektlegger det svært problematiske ved masseinnsamlingen *i seg selv*. Utvalget retter sitt fokus over på kontroll med tilgangen til dataene, og setter sin lit til at dette rettferdiggjør systemet som helhet. Vi mener dette bryter med sentrale poenger i EU-dommene om at innsamlingen i seg selv må la seg forsvare.

Hva som faktisk skjer med opplysningene er heller ikke det eneste relevante for vurdering av personvernkonsekvenser. Som vi har vist lenger oppe, er dette poenget viktig i EU-domstolens avgjørelser. En eventuell opplevelse av å være overvåket, eller frykt for at opplysninger kommer ut av sin sammenheng og fremstår som mistenkelige, vil være konsekvenser som er reelle for de som opplever dem, og løsrevet fra hva som faktisk skjer med deres opplysninger bak lukkede dører. Dette har særlig relevans for debatten om DGF. E-tjenestens bruk av opplysningene vil skje under hemmelighold. Eksakt hva som skjer, og om akkurat dine opplysninger blir vurdert av et menneske, vil være noe du ikke vil vite eller få innsyn i.

Hva DGF er – masseinnsamling, masseovervåking og høystakkprinsippet

Vi må stille oss spørsmålet om hva DGF egentlig er. I rapporten brukes verken ordene masseinnsamling eller masseovervåking om utvalgets forslag. Det er imidlertid nettopp hva tiltaket handler om.

Ordet *masseinnsamling* passer utvilsomt innsamlingen som utvalget foreslår. Den omfattende datainnsamlingen, basert på lave terskler for «relevans», og det brede nedslagsfeltet av berørte personer, kan ikke kalles noe annet. Det er spesielt det såkalte metadatalageret, men også kortidslageret, som her er aktuelt.

Den foreslåtte løsningen innebærer kontroll av alle, slik er DGF *masseovervåking*: Den omfattende innsamlingen gjøres for *kontrollformål*. Innsamlede data om kommunikasjon, privatpersoners kommunikasjon inkludert, blir ikke bare passivt liggende. Dataene samles inn for å bli gjennomsøkt, for å finne spesifikk kontakt eller sammenheng E-tjenesten er ute etter. Alle data i lageret blir undersøkt opp mot søkekriteriene. Sagt annerledes: du og din kommunikasjon blir sjekket – det er ikke bare alle de andre.

"You need the haystack to find the needle," sa daværende direktør i NSA, Keith Alexander, i kjølvannet av Snowden-avsløringene[2]. Det såkalte metadatalageret, som er den sentrale komponenten i DGF-løsningen, er fundamentert på høystakkprinsippet. Den dagligdagse kommunikasjon og bruk av internettbruk vil (med enkelte unntak) automatisk inngå som en del av en høystakk, som igjen skal brukes til å finne nålen. Dette er ikke bare svært problematisk sett fra personvern- og frihetsperspektiv. At tiltaket bygger på masseinnsamling av kommunikasjonsdata får også følger. Sentralt står mengden overskuddsinformasjon, sannsynligheten for formålsutglidning og nedkjøling. Dette vil vi komme mer tilbake til senere.

Mål og midler

Målet med DGF er å oppdage trusler slik som digital spionasje eller terror, ta de riktige stegene for å avverge eller begrense, og for å kunne analysere hva som skjer eller har skjedd. Problemet ligger i hva som blir *middelet*. Data om det det alminnelige menneskets kommunikasjon og informasjonsinnhenting trekkes massivt inn *som et middel*. Masseinnsamling og masseovervåking blir resultatet og konsekvensen av hva man forsøker å få til.

Målrettede tiltak, tiltak som treffer alle og summen av presset mot vårt personvern

Samfunnet må velge løsninger som handler om målrettede tiltak, og avstå fra masseinnsamling og overvåking av alle. Utvalgets forslag mangler den innsnevringen og målrettingen av datainnsamlingen som EU-dommen fra desember i 2016 krever. At søkene er målrettede, er en selvfølge, og det avløser ikke kravet om at selve datainnsamlingen må være formålsrettet.

---

[2] http://www.economist.com/news/united-states/21582536-public-opinion-may-be-shifting-last-against-government-intrusiveness-secret

Som samfunn må vi til en viss grad akseptere inngripende, men målrettede midler, så lenge tersklene er høye nok og at rettsikkerhetsgarantier blir ivaretatt. Målrettethet er ikke bare et godt personvernprinsipp. Den politiske evnen til å si nei og til å avstå fra ikke-målrettede tiltak, er en nødvendighet for å ivareta vårt personvern i det lange løp. Vi kan ikke lenger legge til grunn at tekniske begrensninger, kostnader ved datalagring og prosesseringskraft vil holde innsamling og overvåking på et begrenset nivå.

Norge står ikke uten midler for å ivareta de hensynene DGF settes i sammenheng med. Det gjelder ikke minst midler i kampen mot terror. Å legge frem DGF på toppen av de tiltakene som allerede er etablert, viser villighet til å rykke frem på to spor samtidig - både målrettede tiltak og tiltak som treffer alle. Uavhengig av den siste EU-dommen, er dette en ikke ønskelig utvikling.

Etter 11. september 2001 har Norge innført en drøy håndfull «antiterrorpakker». Sist ute var endringer i straffeprosessloven (Prop 68 L) i juni 2016 om skjulte tvangsmidler, noe som inkluderte dataavlesning som et nytt skjult tvangsmiddel. I denne forbindelse ble det argumentert med at tiltakene var målrettede og ikke favnet alle[3].

Ville debatten i forbindelse med Prop 68 L fortont seg på samme måte dersom man visste at masseinnsamling ville kommet i tillegg? Vi tror ikke det. Vi står nå i fare for at nyere utvidelser av inngripende metoder i forbindelse med Prop 68 L har blitt akseptert med bakgrunn i at det ville være et riktigere veivalg enn alternativet, og i betydelig grad også kunne demme opp for rop om masseinnsamling. I verste fall får vi altså begge deler.

Uansett er det å kombinere rettede tiltak med tiltak som rammer alle et spørsmål om summen av det press vårt personvern settes under. Behovet for en personvernkommisjon på justissektoren (i bred forstand) er mer prekært en noen gang. Dette vil komme tilbake til i siste del av brevet.

5. Nærmere om løsningen – lagre, filtre og søk

Korttidslageret

Korttidslageret skal inneholde korte tidsintervaller med ufiltrert informasjon, og vil dermed omfatte både metadata og innhold fra nær sagt alles kommunikasjon. Dataene lagres i opptil 14 dager. Når mesteparten av befolkningens kommunikasjon krysser landegrensene, er det klart at korttidslageret, selv ved korte intervaller, vil inneholde store mengder detaljerte opplysninger om norske borgere. Utvalget beskriver korttidslageret som nødvendig for å kunne gjøre et fornuftig utvalg av kommunikasjonsbærere, for å forstå hva slags kommunikasjon som går på bæreren, samt for å kunne drive kontinuerlig oppdatering av filtrene i DGF.

---

[3] «Nye metoder for å bekjempe alvorlig kriminalitet» http://www.dagbladet.no/2016/03/11/kultur/meninger/debatt/overvakning/kriminalitet/43481128 «Overvåkingen skal ikke rettes mot folk flest» https://www.regjeringen.no/no/aktuelt/overvakingen-skal-ikke-rettes-mot-folk-flest/id2501864/

Vi mener det er verdt å merke seg hvorfor behovet for et korttidslager oppstår i utgangspunktet. Den tekniske løsningen for DGF er innrettet slik at det skal masseinnsamles metadata om all grensekryssende kommunikasjon. En stor andel av dette vil være opplysninger om norske borgere som E-tjenesten ikke skal ha tilgang til, og det oppstår dermed et behov for filtreringsmekanismer. Her har utvalget valgt en løsning med såkalt negativ filtrering, ved at man spesifiserer det som skal filtreres vekk. For standard telefoni og SMS vil dette være overkommelig, men for andre kommunikasjonsplattformer er det en langt mer kompleks oppgave. For å håndtere dette problemet etableres korttidslageret, slik at E-tjenesten kan gjøre vedlikehold av filtreringsmekanismene basert på ufiltrert innhold og metadata. Vi mener det er et paradoks at det må etableres et lager som inneholder mer detaljerte opplysninger enn det man forsøker å korrigere.

En konsekvens av korttidslageret er at den enkelte må ta inn over seg at all informasjon (ikke bare metadata) kan bli samlet inn av E-tjenesten. Da man ikke vet når det skjer, må den den enkelte ta utgangspunkt i at alt kan bli sett av personell i E-tjenesten.

Metadatalageret

Metadatalageret er DGFs mest sentrale komponent, og også den mest inngripende med tanke på personvernet. Lageret vil inneholde inntil 18 måneder med data om befolkningens kommunikasjon. Målet er som tidligere nevnt å lage en høystakk for søk etter det mistenkelige. Enten for å oppdage når noe skjer akkurat nå, eller for å kunne gå tilbake i tid og se sammenhenger.

Det er på det rene at store deler av nordmenns kommunikasjon på internett i dag, passerer de norske grensene. Dette har sin bakgrunn i de fremvoksende IP-baserte kommunikasjonsplattformene, hvor personer og virksomheter i økende grad tar i bruk tjenester hvor den tekniske infrastrukturen befinner seg utenfor Norge. Eksempler på dette er meldingstjenester som WhatsApp, Snapchat, Facebook Messenger og andre typer nettbaserte tjenester som gjøres tilgjengelig via en skyplattform i utlandet. I utredningen går det også frem at metadatalageret vil «inneholde betydelig informasjon om kommunikasjon mellom nordmenn som på kommunikasjonstidspunktet befant seg i Norge» (side 54).

Nå går også mobiloperatørene over fra vanlig tale og SMS til IP-baserte tjenester. GSMA, en organisasjon som representerer interessene til nesten 800 mobiloperatører og 250 mobil-virksomheter rundt om i verden, har i et samarbeid med Google tatt sikte på å anlegge IP-dominans ved å etablere egne IP-baserte Rich Communications Service (RCS). RCS er en løsning som tar tradisjonell tale og SMS, og legger til funksjoner som direktemeldinger, deling av lyd og bilder, videosamtaler og fildeling på tvers av enheter. Allerede nå har de store norske kommunikasjonsaktørene tatt de første skrittene for bruk av RCS. Den løsningen de globale operatørene vil benytte kan også baseres på Googles løsninger (Jibe Platform from Google).

Felles for mange av disse tjenestene er at det vil være vanskelig å avdekke om kommunikasjonen skjer mellom nordmenn i Norge, og følgelig ikke skulle vært lagret i DGF.

Datatilsynet mener at analyse av metadata fra mange kilder over tid gir tilgang til svært sensitive opplysninger om en person. Dette understøttes fra flere hold, blant annet i en forskningsrapport fra Stanford University[4], publisert i mai 2016. Selv om rapporten kun ser på metadata fra tradisjonelle telekomtjenester slik som telefoni og SMS, var det mulig for forskningsgruppen å utlede svært sensitiv informasjon om de som deltok i studien. I DGF vil datagrunnlaget bli langt mer omfattende ved at det legges opp til innsamling og overvåking av metadata fra nær sagt alle typer kommunikasjon.

Vi har valgt å ta med noen enkle eksempler på hva metadata kan avsløre, disse er hentet fra rapporten «*Personvern 2014 – tilstand og trender*»[5] som vi skrev i samarbeid med Teknologirådet:

- Metadata avslører ikke innholdet i en samtale, men viser at du ringte gynekologen din, pratet i 23 minutter og like etter ringte en abortklinikk.
- Metadata avslører ikke innholdet i en samtale, men kan vise at du ringte Kirkens SOS krisetelefon fra gangbrua over E18.
- Metadata avslører ikke innholdet i din kommunikasjon, men kan vise at du benyttet deg av en nettdatingtjeneste for homofile.

Når metadata settes i riktig kontekst, kan de altså være vel så avslørende som selve innholdet i kommunikasjonen. Rapporten er uklar på hvilke typer, og den totale mengden av, metadata som vil bli lagret i DGF-systemet. Det er derfor vanskelig å danne seg et klart bilde av hvor stort omfanget av metadatalageret vil bli. Det nevnes at det i enkelte tilfeller også vil være vanskelig å skille på hva som er metadata og hva som er innholdsdata. Det uansett ingen tvil om at lageret vil bli svært omfattende. I tillegg legges det opp til en lagringstid på hele 18 måneder.

Innholdslageret

Det såkalte innholdslageret er svært inngripende når det gjelder informasjonen som lagres der. Her vil det lagres både innhold og metadata. Lageret er imidlertid av en helt annen art enn metadatalageret. Innsamlingen er målrettet, og DGF-domstolen har godkjent at det samles inn kommunikasjon tilknyttet disse objekter (personselektorer). For Datatilsynet fremstår det temmelig parallelt til rettslig kjennelse for andre skjulte tvangsmidler.

Filtre

Et sentralt mål med filtrene i DGF er å hindre innsamling av data som faller utenfor E-tjenesten sitt område. Det mest åpenbare tilfellet er kommunikasjon mellom to norske statsborgere som befinner seg i Norge.

Én mulighet ville vært å benytte en positiv filtreringsmekanisme, ved at det på forhånd spesifiseres hva som skal tillates å samles inn. Utvalget foreslår å innføre det motsatte for

[4] http://www.pnas.org/content/113/20/5536.full.pdf

[5] https://www.datatilsynet.no/Om-Datatilsynet/rapporter-og-utredninger/Personvern-2014-tilstand-og-trender/

innsamling av metadata ved at man spesifiserer hva som skal filtreres vekk. Som utvalget selv påpeker er dette komplekst og vanskelig å gjennomføre. Vår vurdering er at det i praksis blir umulig å håndtere sett i lys av den stadig økende bruken av IP-baserte kommunikasjonsplattformer.

Søk

Rapporten beskriver kort hvordan søkene i metadatalageret skal gjennomføres. Søkene skal enten gjøres på individer (personselektor) eller et handlingsmønster (modusselektor). Det skal føres kontroll med hvilke søk som foretas. Etter vår vurdering vil det være en stor risiko i forbindelse med søk. Det er i rapporten for eksempel påpekt at det alltid vil være en viss risiko for at dommerne i forbindelse med prøvingen for en domstol, etter hvert kan identifisere seg med tjenestens virke og oppgaver. Den samme risikoen er beskrevet for DGF-tilsynet. Prosessen for søk, som er viktig i forbindelse med DGF, fremstår som et svakt punkt hvor det er en stor mulighet for å gjøre feil.

Rapporten gjør det vanskelig å se hvor omfattende og inngripende søkene blir. Dette gjelder særlig ved bruk av modusselektorer for målutvikling, hvor det etter vår vurdering kan åpnes for vide søkekriterier med lang varighet (i rapporten omtales opptil ett år, og i enkelte tilfeller lenger). Dette gjør det vanskelig å foreta en konkret vurdering av personvernkonsekvensene ved det søkeregimet det legges opp til.

«To ledd ut» i kommunikasjonskjeden

I rapporten står følgende:

> «For søk basert på personselektorer knyttet til personer som domstolen har godkjent innhenting mot, antar utvalget at domstolens kjennelser i alle fall bør kunne inkludere to ledd ut i kommunikasjonskjeden.» (Side 58)

Denne tilsynelatende detaljen bør ikke overses. Vi forstår dette slik: Med utgangspunkt i at domstolen har godkjent innsamling mot person A, kan kjennelsen også tillate at det samles inn informasjon om hvem A kommuniserer med, samt hvem disse igjen kommuniserer med. To ledd ut blir beskrevet som «i alle fall», noe som kan bety at to ledd ikke blir forstått som et maksimum. Å inkludere flere ledd ut har stor betydning, og det er svært inngripende.

For det første fører det til at uthenting fra lagret (og videre bruk av disse dataene) kan få et stort nedslagsfelt når det gjelder antall personer. Flere ledd ut er et godt kjent prinsipp i forbindelse med Snowden-avsløringene. Før avsløringen kunne NSA gå tre ledd/hopp ut. Dette ble senere redusert til to.

En ny studie fra Stanford University har kalkulert hvor mange personer som kan bli omfattet ved to hopp/ ledd ut i forbindelse med telefoni. Dataene ble hentet inn fra 800 frivillige som gjennom en app ga tilgang til loggene på sin smarttelefon. Vi siterer her fra Stanford Universitys artikkel som presenterer studien[6]:

---

[6] http://news.stanford.edu/2016/05/16/stanford-computer-scientists-show-telephone-metadata-can-reveal-surprisingly-sensitive-personal-information/

> «By extrapolating participant data, the researchers estimated that the NSA's current authorities could allow for surveilling roughly 25,000 individuals – and possibly more – starting from just one "seed" phone user.»

Om NSAs adgang før endringene i 2013 (tre hopp) sier rapporten[7]:

> «Applied to the NSA's program, our results strongly suggest that until 2013, analysts had legal authority to access telephone records for the majority of the entire US population.»

Et annet resultat av «to ledd ut» er at enkelte mennesker har liten eller ingen mulighet til å forutse om de selv vil bli sett nærmere på av E-tjenesten. Vi vil også komme tilbake til «to ledd ut» i forbindelse med nedkjøling.

Nytteverdien av DGF

I rapporten pekes det på at den tiltagende bruken av sterk kryptering vil påvirke verdien E-tjenesten har av å kunne avlytte kommunikasjon ved riksgrensen. Dette skal delvis håndteres ved at teletilbydere får tilretteleggingsplikt for leveranse av datastrøm uten linkkryptering, men det vil ikke ha noen effekt på ende-til-ende kryptering. Flere OTT-tjenester (eksempelvis WhatsApp) har allerede implementert sterk kryptering i sine applikasjoner, og vil effektivt gjøre innholdsdata utilgjengelig i et elektronisk grenseforsvar.

Mulighetene for å omgå DGF er store, og løsninger for å gjøre dette er enkelt tilgjengelig i dag. VPN med IP-anonymisering og TOR (The Onion Router) er eksempler på teknologi hvor selv metadataene mister mye av sin verdi. Vi mener rapporten i altfor liten grad drøfter hvilke konsekvenser krypterings- og anonymiseringsteknologi vil ha for nytteverdien av de ulike masselagrene i DGF. Man vil ende opp med at det er enkelt for den som ønsker å slippe unna DGF å kryptere og dermed gjøre både innhold og metadata utilgjengelig.

Datatilsynet ser også at angrep fra utlandet kan gå via krypterte forbindelser til Norge, og at videre angrep dermed kan foregå på innsiden av grensene uten at det oppdages i DGF.

Inngripende

Den omfattende lagringen av kommunikasjon det legges opp til, vil omfatte en stor del av den enkelte borgers totale kommunikasjon. Det vil også være umulig for den enkelte borger å danne seg et bilde av hvilken kommunikasjon som vil være berørt av DGF eller ikke, siden det ikke alltid kommer frem hvilke skytjenester og kommunikasjonsveier som brukes av kommunikasjonsmotpartene. Slik informasjon om bruk av utenlandske løsninger blir av enkelte aktører hemmeligholdt blant annet av sikkerhetsgrunner.

I vår hverdag fremover vil en betydelig del av vår daglige aktivitet bli koblet opp mot internett, og spesielt utenlandske aktører. Flere og flere produkter blir koblet til internett og rapporterer detaljert all bruk til for eksempel produsenter i utlandet. Dette gjelder alt fra biler

[7] http://www.pnas.org/content/113/20/5536.full.pdf

til klokker og vaskemaskiner. Det enkelte lands myndigheters iver etter å kontrollere kommunikasjonen vil også medføre økt behov for kryptering av denne trafikken.

6. Nærmere om nedkjølingseffekt

Utvalget tar opp temaet nedkjølingseffekt flere steder i rapporten. Vi deler utvalgets bekymring, men vurderer faren for nedkjøling som resultat av DGF, som større enn det utvalget gjør.

Nedkjøling er relevant også i Norge

Datatilsynet har sett på temaet nedkjøling ved flere anledninger. I 2008 skrev vi en rapport på bestilling fra Fornyings- og administrasjonsdepartementet om konsekvenser for norske borgere av den såkalte FRA-loven i Sverige[8]. Vårt viktigste poeng var at vissheten om at kommunikasjonen kan fanges opp, potensielt kunne få en dempende effekt på frimodigheten og dermed ytringsfriheten i samfunnet.

Siden 2008 har kunnskapen om nedkjøling økt, og temaet har blir kraftig aktualisert gjennom Snowdens avsløringer. Etter 2013 har enkeltmennesket en helt annen mulighet til å kjenne til den omfattende myndighetsovervåkingen av internettbruk.

Rapporten «*Personvern 2014 – tilstand og trender*», skrevet sammen med Teknologirådet, hadde et eget kapittel om nedkjøling[9]. Utvalgets rapport refererer til noen av disse tallene, basert på en spørreundersøkelse fra november 2013.

Da vi skrev en tilsvarende rapport året etter[10], viste vi respondentenes svar på dette spørsmålet (stilt (omtrent halvannet år etter at de første avsløringene fra Snowden nådde media): «Har Snowden-avsløringene hatt noe å si for tenkningen din om nettovervåking, og for hva du gjør på internett i dag?». Snowden-saken satt fremdeles i manges i bevissthet. Noen oppga at de hadde endret på sine nettvaner:

- 17 prosent valgte alternativet «Ja, jeg tenker fremdeles på avsløringene, og har også endret noe på nettbruken min i dag».
- I tillegg valgte 27 prosent «Ja, jeg tenker fremdeles på avsløringene, men nettbruken min er ikke endret i dag».
- De resterende valgte svar som tilsa at de ikke tenkte på avsløringen og hadde ikke endret nettbruken sin, samt «vet ikke».

---

[8] https://www.datatilsynet.no/Om-Datatilsynet/rapporter-og-utredninger/2004-2014/Utredning-om-signalspaning-i-Sverige1/

[9] https://www.datatilsynet.no/Om-Datatilsynet/rapporter-og-utredninger/Personvern-2014-tilstand-og-trender/

[10] *Personvern 2015 – tilstand og trender*, side 15. https://www.datatilsynet.no/Om-Datatilsynet/rapporter-og-utredninger/personvern-2015---tilstand-og-trender2/

Et viktig poeng er at nedkjøling neppe treffer likt i alle samfunnslag. Det er særlig ulike former for minoriteter vi bør bekymre oss for. Utvalget nevner også forskningseksempler på dette. I en ny masteroppgave i kriminologi fra desember 2016, skrevet av Sven Henrik Ekholdt[11], kommer nedkjøling for minoriteter spesielt frem. Oppgaven handler om ungdom i Norge sine forestillinger, oppfatninger og opplevelser rundt overvåking av internett, og om man kan finne spor av en nedkjølingseffekt. Vi siterer her kort fra sammendraget: «Minoritetsungdommene ser ut til å ikke bare mene at muslimer overvåkes mer enn andre, men å også handle deretter, ved at de vegrer seg for å snakke om temaer de er redd kan bli assosiert feil.» Oppgaven har også en egen del om nyere forskning på feltet.

Nedkjølingseffekt må ikke ufarliggjøres til bare en bekymring, en rent teoretisk basert risiko vi ikke har sett slå til. Nedkjøling er en realitet, og det skjer i verden i dag. Nedkjøling kan heller ikke isoleres til totalitære regimer og sammenhenger med åpenbar offentlig maktmisbruk. Vi viser også her til EU-domstolens nylig avsagte dom i Tele2 Sverige mot Post- og Telestyrelsen:

> «Selv om en sådan lovgivning ikke tillader lagring af indholdet af en elektronisk kommunikation, … kan lagringen af trafikdata og lokaliseringsdata imidlertid have en indvirkning på brugen af de elektroniske kommunikationsmidler, og følgelig på brugerne af disse midlers udøvelse af deres ytringsfrihed, …» (premiss 101)

Vurdering av nedkjøling som resultat av DGF

Om sin foreslåtte løsning skriver utvalget:

> «Utvalget mener også at befolkningen, med de begrensninger og kontrolltiltak som er foreslått, vil kunne ha tillit til at dataene kun anvendes for E-tjenestens formål og at en eventuell nedkjølingseffekt derfor blir svært liten.» (Side 67)

DGF vil bidra til nedkjøling, slik vi ser det. Vi vil her trekke frem noen grunner til at nedkjøling som resultat av DGF ikke bør undervurderes, og hvorfor vi vurderer utfallet annerledes enn utvalget.

Ikke andre land, men egen stat. Gjennom DGF vil Norge melde seg på som en aktør for innsamling og overvåking av grensekryssende kabeltrafikk, og slik sett bidra til å forsterke vår opplevelse av overvåking på internett. Ulike staters overvåking av grensekryssende trafikk er allerede er en realitet for den opplyste borger. For nordmenn vil DGF likevel stå i en særstilling, fordi det handler om egne myndigheter, ikke fremmede stater uten videre makt i det enkelte menneskes liv. Det er også et tiltak man kan stole på at vil omfatte en selv.

DGF er særlig egnet for nedkjølingseffekt. Vi er enige med utvalget i at myndighetsovervåking ikke er den eneste drivkraften bak nedkjøling. Kommersielle selskaper har enorme mengder informasjon om oss. I tillegg har vi betydningen av mer nære relasjoner,

---

[11] *«Jeg bryr meg ikke så mye, for jeg har ikke planer om å gjøre noe kriminelt» Norske ungdommers tanker om overvåking*, Sven Henrik Ekholdt, Masteroppgave i kriminologi, Høsten 2016, Universitetet i Oslo

for eksempel å legge bånd på seg etter hva foreldre, venner eller fremtidige arbeidsgivere vil tenke om informasjon om oss på nett.

Når det gjelder hva staten rår over derimot, har vi imidlertid vanskelig for se hvilke tiltak som i større grad er egnet for nedkjøling enn masseinnsamling av metadata om nettbruk (og telefoni til utlandet).

Tillit og gode kontrollordning er relevant, men kilden til nedkjøling ligger i tvilen. Vi er enige med utvalget i at den generelle tilliten i Norge, tilliten til E-tjenesten spesifikt, samt stramme føring for og kontroll med E-tjenesten, vil kunne dempe den nedkjølingen tiltaket ellers ville hatt. Vi er imidlertid ikke enige i at dette *i stor grad* avhjelper, eller nuller ut problemet, slik vi oppfatter at utvalget setter lit til. Detaljer om tilsynsordninger, juridiske og tekniske barrierer vil ikke være noe den vanlige borger har god oversikt over.

Mistillit til E-tjenesten eller frykt for negative reaksjoner er neppe drivkraften i en nedkjølingseffekt her. Vi tror derimot tvilen og ubehaget vil ligge bak: De fleste alminnelige og lovlydige borgere ønsker ikke å bli undersøkt av E-tjenesten. Selv om det skulle skje ved en ren inkurie, vil vi anta at de fleste opplever det som en ubehagelig tanke. Det er vanskelig for det enkelte menneske å forutse om nettopp deres opplysninger vil kommer frem i en eller annen sammenheng.

Ulike minoriteter vil rammes hardest og først. For en del av disse er det naturlig å anta at tilliten til myndigheter og E-tjenesten neppe er like god som i den øvrige befolkningen. Det vedrører vurdering av tillit som en demper av nedkjøling.

Avslutningsvis vil vi minne om hva vi tidligere har kalt «to ledd ut». For den enkelte er det umulig å vite om du kommuniserer med noen, som igjen kommuniserer med noen som E-tjenesten har fattet interesse for. På jobb, i frivillig arbeid og i foreninger, som foreldre i barnehage og skole, og i vårt øvrige liv i hjem og familie, kommuniserer vi med et vell av mennesker. To ledd ut-prinsippet mener vi har et særlig potensiale for nedkjøling.

«To ledd ut» vil dessuten treffe enkelte yrkesgruppe på en særlig måte. Eksempelvis vil to ledd ut ikke bare treffe advokaten eller journalisten selv, men også vedkommendes partner og andre han/ hun har i sin krets. Vi mener det også kan få uheldige sosiale konsekvenser. Et interessant spørsmål å stille seg er: Ville du etablere kontakt med en hyggelig og velintegrert innvandrer hvis du visste at vedkommende var i slekt med en som er radikalisert, og som din venn trolig hadde elektronisk kontakt med som bror/ fetter?

7. Nærmere om formål, formålsutglidning og videre flyt av opplysninger fra E-tjenesten

E-tjenestens brede formål

Et viktig poeng for utvalget er at DGF-systemet skal avgrenses til E-tjenestens formål. Dette handler ikke minst om å begrense personvernkonsekvenser. E-tjenestens interesseområde og

formål favner imidlertid svært bredt. Med det følger også et potensiale for stor bredde i hva DGF-systemet lovlig skal kunne brukes til.

For oss er det noe uklart om utvalget mener at DGF-systemet skal kunne brukes til E-tjenestens samfunnsoppdrag generelt, og slik tjenestens oppgaver er listet opp i etterretningstjenesteloven § 3, eller om bruksområdet skal snevres ytterligere inn. Ulike formuleringer peker i forskjellig retning. Ser vi kun på formuleringene i kapittel 9 om utvalgets vurderinger, legger vi til grunn at søk både må være innenfor tjenestens lovbestemte oppgaver og årlige politisk fastsatte prioriterte etterretningsbehov.

Etter vårt syn, er etterretningstjenesteloven § 3 uegnet som ytre ramme for bruk. Den er alt for vid. Bruk av DGF til å skaffe «informasjon om overnasjonale miljøproblemer» eller til nytte for «langtidsplanlegging og strukturutvikling i Forsvaret», er eksempler på en åpenbart uønsket bruk av systemet. Videre mener vi at «årlige politisk fastsatte etterretningsformål» (side 60) ikke gir en god nok forutberegnelighet.

Formålene terrorbekjempelse og cybertrusler

I rapporten fremstår ulike cybertrusler som en viktigere begrunnelse for DGF enn terrorbekjempelse. Vi mener rapporten gir en bedre begrunnelse for behovene i forbindelse med cybertrusler, og i utvalgets konklusjon (side 70-71) beskrives DGFs betydning som mer nødvendig for ulike cybertrusler enn for terrorbekjempelse. Norge står slett ikke uten midler i kampen mot terror, som vi tidligere har vært inne på.

Ville en løsning med cybertrusler som eneste formål, endret vesentlig på hva som er relevant å samle inn, hvilke opplysninger som er relevante å hente ut fra DGF-systemet, og for øvrig om løsningen ville begrenset personvernkonsekvenser, sammenliknet med DGF hvor også antiterror er et formål?

Hvis dette spørsmålet skal utredes senere, må andre relevante midler vurderes samtidig. Ikke bare hva som allerede finnes, som utvalget til en viss grad tar opp, men også hvilke endringer som kunne vært gjort med eksisterende tiltak (eller andre og nye tiltak) for å møte samme behov. Å velge det minst inngripende middelet er et sentralt personvernprinsipp. Her er det også en vesentlig svakhet i utredningen: Det lå ikke i utvalgets mandat å foreta vurderinger av alternative tiltak, kun tilleggsgevinster ved DGF, sammenliknet med eksisterende tiltak. Manglende vurdering av alternative løsninger nevnes som en svakhet også av andre høringsinstanser, for eksempel av SINTEF. Å gi E-tjenesten tilgang til grensekryssende kabelbåren trafikk, er ikke et mål i seg selv.

DGF og PST – er det bare E-tjenestens formål som betjenes?

Hvilken betydning vil DGF få for PST? I denne sammenhengen spesielt om DGF vil føre til en omfattende videreleverering av informasjon fra E-tjenesten til PST. Temaet er alt for lite eksplisitt beskrevet og vurdert, og det ville vært verd en egen analyse i rapporten.

Utvalget er svært opptatt av at DGF-systemet skal brukes av E-tjenesten til dets formål, og bare det. For de som leser forslaget, vil fokuset på avgrensning til E-tjenesten kunne resultere

i at man beroliger seg med at det «bare» er E-tjenesten (som jo skal beskjeftige seg med utenlandsetterretning, og ikke oss), som vil ha og bruke dataene. Så enkelt er det ikke.

Vi forstår utvalgets forslag slik:

- Informasjon fra DGF som er overskuddsinformasjon for E-tjenesten, kan ikke leveres videre (og skal slettes). Dette er en innskrenkning for DGF-informasjon sett i forhold til dagens generelle regler for viderelevering av overskuddsinformasjon i Instruks om Etterretningstjenesten § 5 og Instruks om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste § 10.
- Informasjon som er av felles interesse kan utleveres til PST etter de samme prinsipper som i dag, men altså nå med en ny kilde med enorme mengder data:
  «Dette [at DFG-informasjon ikke kan brukes som bevis i straffesaker] er imidlertid ikke til hinder for at informasjon innhentet gjennom DGF som ikke er å anse som overskuddsinformasjon, kan deles med PST – herunder gjennom Felles kontraterrorsenter (FKTS) – på vanlig måte, som kan bruke informasjonen som inngangsverdi for egen metodebruk/etterforskning basert på PSTs hjemmelsgrunnlag. Dersom en etterforskningssak leder til tiltale, vil imidlertid DGF-innhentet informasjon delt med PST ikke kunne benyttes som bevis.» (side 61)
  Etter Instruks om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste § 10, skal tjenestene «så langt mulig» utveksle informasjon av felles interesse (innenfor rammen av «need to know» og hensynet til å beskytte kilder og metoder).
- PST, NSM, Tolletaten og andre myndigheter skal ikke selv kunne søke, og heller ikke kunne bestille informasjon fra DGF – ikke til eget formål i hvert fall, og som en selvstendig begrunnelse. Det springende punktet er om E-tjenestens søk lar seg forsvare i utenlandsetterretningsformål. Her er det ikke bare en formålsavgrensing, men også et mulighetsrom som ikke avklares av utvalget, for det er en forskjell på om noe er relevant for utenlandsetterretning og at informasjonen *kun* er relevant for utenlandsetterretning. Kan for eksempel PST be E-tjenesten undersøke noe så lenge svaret også antas å gi nyttig informasjon for E-tjenesten (søket må begrunnes i utenlandsetterretning)? Vi forstår utvalget slik at det ikke avgrenser mot at E-tjenesten *i praksis* kan foreta søk i DGF som er initiert/ønsket/etterspurt av andre myndigheter, så lenge søket også lar seg forsvare ut fra E-tjenestens formål: Vi viser her til følgende formulering på side 61 om dagens praksis, og som utvalget ikke mener bør endres:
  «Spesielt betyr dette at E-tjenesten ikke kan samle inn informasjon på anmodning fra andre myndigheter, uten at dette har et utenlandsetterretningsformål.»

Den praktiske konsekvensen av de to siste kulepunktene er vanskelig å forutse, og rapporten gir her liten hjelp. Når kommunikasjonsinformasjonen i DGF-systemet som hovedprinsipp har én ende i Norge og én utenfor landet, vil en og samme e-postutveksling, telefonsamtale eller annen kommunikasjon, ofte ha interesse for flere etater samtidig.

Det fremstår som hevet over enhver tvil at DGF vil øke informasjonsmengden fra E-tjenesten til PST vesentlig. Vi siterer her rapportens kapittel om faktorer som taler for DGF, og hvor PSTs syn legges frem:

> «DGF antas i vesentlig grad å styrke PSTs informasjonstilfang, og dermed gi sikrere og tryggere data å agere på, selv om det i forkant av en eventuell etablering selvsagt er vanskelig å si akkurat hvor stor effekt DGF vil ha, hvilket også vil bero på hvilket konsept som implementeres.» (side 32)

Vi kan ikke se at resultatet av den foreslått DGF-modellen bare blir utenlandsetterretning. Det er kanskje heller ikke meningen. At DGF ikke bare er utenlandsetterretning kan også ses i hvordan det argumenteres for hva PST må gjøre uten DGF:

> «Dersom DGF ikke etableres, antas dette å ha konsekvenser både for det digitale forsvaret av landet innenfor landegrensene, og for behovet for en bredere anlagt overvåking av aktører eller aktørgrupper fra PSTs side.» (Side 32)

I en stillingtaken til DGF, vil det ikke være riktig å legge til grunn at det ene og alene er E-tjenesten og deres formål som drar nytte av DGF.

Formålsutglidning må påregnes

Utvalget er tydelige på at innholdet i DGF er svært egnet for bruk av andre enn E-tjenesten:

> «Utvalget har tidligere gjort rede for at svært mange av de digitale spor nordmenn etterlater seg i sine daglige liv vil passere de punktene hvor DGF samler inn data. Det betyr at DGF-installasjonen vil kunne være et svært kraftfullt virkemiddel også for nasjonale myndigheter som har ansvar for innenlandske forhold. ... Brukt til overvåking av nordmenn i Norge har DGF et enormt potensial, ...» (Side 61)

Vi vil rose utvalget for de advarslene og forsøkene som er gjort for å demme opp for formålsutglidning. Spørsmålet er om tiltak og advarsler vil holde bruken av systemet uendret. Vi kan ikke se av rapporten om utvalget selv tror det vil holde over tid. Etter vårt syn er det lite sannsynlig. Ikke bare politiet, men også Skatteetaten og Tolletaten med flere kan ha interesse for de dataene DGF-systemet vil inneholde. Vi merker oss at ytterligere bruk enn den foreslåtte allerede har meldt seg i høringssvar. Norsk senter for informasjonssikring (NorSIS) skriver:

> «NorSIS mener at informasjon fra et DGF må brukes til å understøtte det nasjonale digitaliseringsarbeidet og gjøre hele samfunnet bedre i stand til å møte en økt digitaltrussel. Dette innebærer at informasjon som fremkommer med bakgrunn i et DGF må kunne deles med de som har behov for den.» (Side 3 og 4.)

Vi nevner her et knippe problemstillinger i forbindelse med formålsutglidning:

DGF-informasjon kan ikke brukes som bevis i straffesaker. Når bevisene faktisk finnes, og konkrete saker ikke fører til domfellelse på grunn av for svake bevis, vil da samfunnet akseptere denne begrensningen?

E-tjenesten kan ikke levere videre informasjon til andre myndigheter, og må selv slette informasjon, så lenge dataene ikke har relevans for eget formål. Rapporten sier:

> «I praksis vil dette si at dersom E-tjenesten – mot formodning og uten hensikt – skulle komme over informasjon om at en person har begått et drap, seksuelle overgrep mot barn eller deltatt i annen alvorlig kriminalitet som ikke er av relevans for E-tjenestens ansvarsområde, vil slik informasjon bli slettet uten videre oppfølging. Hensynet til rikets sikkerhet er viktigere enn å tillate bruk av denne overskuddsinformasjonen.» (Side 60)

Når konkrete saker kommer for dagen, vil da samfunnet akseptere at E-tjenesten verken kan eller skal varsle om alvorlig og farlig kriminalitet som de kommer over, men som ikke utgjør noen fare for rikets sikkerhet?

Vi viser her også til høringsuttalelsen fra Den internasjonale juristkommisjon – norsk avdeling (ICJ-Norge), hvor det settes spørsmålstegn ved om en slik begrensning lar seg forene med norsk lovgivning for øvrig (under overskriften «5. Nødrett og avvergingsplikt»).

Uthenting av DGF-informasjon må begrunnes i utenlandsetterretningsformål. Når dataene først er der, og kan gi svar, vil samfunnet da akseptere at PST ikke kan få tilgang til informasjon av ren innenlandsverdi? En form for bestillerrett for PST, for eget formål, vil være blant de mest sannsynlige formålsutglidningene etter vår vurdering.

E-tjenesten kan kun bruke datalagerne til søk. Vil E-tjenesten over tid slå seg til ro med at metadatalageret ikke kan brukes til automatiserte analyser, til stordatanalyse for å finne ukjente sammenhenger og mønstre? Til sammenligning har PST tidligere formidlet ønske om ta i bruk stordataanalyse for å «kunne avdekke mønstre og trender, danne utgangspunkt for gode analyser og for å avsløre mistenkelig adferd hos enkeltindivider»[12].

For DGF er formålsutglidning ikke bare en fare, det må rett og slett påregnes. Tiltaket vil slik, med stor sannsynlighet slik vi ser det, blir mer inngripende enn man i første omgang tok stilling til. Dette må tas med i vurderingen av om man vil igangsette DGF. Det ligger i den foreslåtte modellens natur, bygd på masseinnsamling og overskuddsinformasjon, at ytterligere bruk vil tvinge seg frem.

8. Øvrige merknader

Personvernkommisjon på justisfeltet er mer presserende enn noen gang

Datatilsynet har ved gjentatte anledninger tatt til orde for en personvernkommisjon på justisfeltet (i bred forstand). Etter utvalgets anbefaling av DGF er behovet for en slik

[12] https://www.nrk.no/norge/pst-vil-samle-stordata-1.11890927

kommisjon større enn noen gang. Det behøves en helhetlig oversikt over personvernets kår i sektoren og en beskrivelse av hvilket inngrep totaliteten av dagens tiltak representerer, de hemmelige tjenestenes midler inkludert. Vi mener det under alle omstendigheter er uansvarlig å gå videre med planer om DGF uten en slik oversikt.

Utvalget nevner også behovet for en personvernkommisjon. I Samferdselsdepartementets høringsuttalelse skriver de at «det kan være behov for å behandle den totale sammenhengen mellom ulike inngrep mot kommunikasjonsvern og personvern i et større bilde.» (Side 1)

Behovet for utredning og offentlig debatt ved vurdering inngripende midler

Datatilsynet er svært positiv til fremgangsmåten med offentlig utredning og offentlig debatt som departementet her har redet grunnen for. Vi har tidligere gitt vår støtte til denne viktige anbefalingen i Lysne I-utvalgets rapport om digital sårbarhet. At vi er uenige i anbefalingen av den aktuelle DGF-løsningen, er et spørsmål på siden av dette.

Utvalget fikk lite tid til utredning

Utvalget ble nedsatt 24. februar 2016 og fikk en frist til 30. juni (rapporten ble levert i august). Vi mener tiden utvalget fikk er alt for kort for et så komplisert tema.

Eventuelt DGF-regelverk må på høring

Et digitalt grenseforsvar vil kreve nytt regelverk. Vi forutsetter at et slikt regelverk vil komme som en ny høring dersom det mot formodning skulle blir aktuelt å gå videre med DGF.

E-tjenesten som sekretariat er uheldig

I rapporten står det at E-tjenesten har ivaretatt sekretariatsfunksjonen for utvalget (side 9). Vi har forståelse for at behovet for hemmelighold i denne sammenheng har gitt utfordringer som ellers ikke ville vært til stede for et utvalg. Vi finner dette likevel uheldig, særlig da valget ikke utdypes eller forklares. E-tjenesten er organisasjonen som spørsmålet står om, og har stor egeninteresse av utfallet. Vi mener det er allment akseptert at et sekretariat ikke er strippet for innflytelse på fremstilling og vinkling.

Digital grenseovervåking vs. grenseforsvar

Ord er makt. Benevnelsen digitalt grenseforsvar, valgt at utvalgets oppdragsgiver, trekker oppmerksomheten bort fra det mest sentrale ved forsalget. På den måten høres tiltaket mindre problematisk ut. (Om det skal hete overvåkingskamera eller trygghetskamera er en tilsvarende diskusjon.) Tiltaket handler ikke om forsvar slik den vanlige nordmann forstår ordet. Det handler om noe mer snevert, nemlig begreper som «kontroll», «overvåking» eller «etterretning» (som kan være en del av et forsvar).

Tidligere sjef for E-tjenesten, Kjell Grandhagen, kalte det «digital grensekontroll»[13]. Det er et mer sakssvarende og ærlig begrep. Etter vårt syn bør begrepet digitalt grenseforsvar byttes ut med digital grenseovervåking, eventuelt digital grensekontroll.

Digitalisering og tillit

Vi merker oss at flere høringssvar tar opp at DGF kan redusere tilliten som digitaliseringen avhenger av. I sitt høringssvar skriver Direktoratet for e-helse:

> «Foreslåtte DGF har stort potensial for å redusere reell og opplevd konfidensialitet i digital kommunikasjon med helseopplysninger, og representerer derfor et vesentlig risiko-område.» Og: «Risikoen for redusert tillit til helsetjenesten i befolkningen og vegring mot digitale løsninger er særskilt viktige faktorer ...».

Difi trekker frem at utvalgets rapport ikke går inn på «i hvilken grad etablering av digitalt grenseforsvar kan medføre utfordringer, som at det blir større skepsis til digitalisering.».

SINTEF skriver:

> «Et DGF med rett til innsyn i kryptert trafikk kan tvinge norsk næringsliv samt forsknings- og innovasjonsmiljøer til å skaffe seg kostbare omveier i jakten på sikre kommunikasjons-løsninger. I tillegg risikerer vi at noen brukere vil unngå enkelte digitale tjenester på grunn av manglende tillit. Da vil digitaliseringen av samfunnet lide.»

DGFs mulige negative virkning for tillit til digital tjenester har et slektskap til nedkjølingseffekt. Vi mener bekymringene om negativ virkning på digitaliseringen bør tas på alvor.

Er DGF et mindre inngrep enn alternativt?

I rapporten skrives det at innføring av DGF vil dempe personvernkonsekvensene i forbindelse med E-tjenestens og PSTs (øvrige) virkemiddelbruk. For terrorbekjempelse separat sett, skriver utvalget at «fraværet av DGF i noen grad kan kompenseres med andre kapasiteter, men det er ikke gitt at slike kapasiteter vil innebære mindre overvåking/inngrep i personvernet enn DGF, antagelig snarere tvert om.» (Side 70) Rapporten sier også at «Det kan ikke utelukkes at tilgang til et godt regulert DGF vil kunne minske myndigheters press på informasjon lagret hos private aktører.» (Side 35)

I det store bildet teller DGF klart negativt for borgernes personvern. Vi vil fullstendig avvise en eventuell tanke om at DGF totalt sett reduserer personvernkonsekvenser.

---

[13] – Digital grensekontroll er et godt begrep. Vi kontrollerer både mennesker og varer som tas inn i landet. Skal vi tillate at det digitale rom blir et fristed for terrorisme, fremmed etterretning og organisert kriminalitet, spør han. https://www.nrk.no/norge/sliter-med-a-fange-opp-digitale-trusler-1.12425079

Alvoret og behovet for en «ødelegg DGF-rutine»

I rapporten finnes det en interessant og talende detalj. Utvalget skriver:

> «Det bør utvikles mekanismer og rutiner for både sletting av all informasjon lagret i DGF, og for ødeleggelse av DGF-utstyret. Disse mekanismene og rutinene bør innrettes slik at det kan iverksettes ved ikke-demokratisk maktovertakelse.» (Side 69)

Forslaget er klokt og nødvendig. Men behovet for en slette- og ødeleggelsesplan forteller oss noe mer, det illustrerer alvoret og hvilket maktmiddel DGF-systemet faktisk er.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Stian D Kringlebotn
seniorrådgiver

Kopi: Kommunal- og moderniseringsdepartementet
v/Statsforvaltningsavdelingen
Postboks 8112 Dep, 0032 OSLO