Digital Grenseforsvar, slik det er foreslått, innebærer massiv systematisk overvåkning av hele det norske folk og hele det norske næringsliv. Forslaget bør forkastes.

Lovstridig

Høringsnotatet påpeker en konflikt med Grunnloven §102. Den behandler derimot ikke punktet videre utover å antyde at «rett til respekt for sitt privatliv» samt «..og sin kommunikasjon» er relativt åpne for fortolkning. Da Norges viktigste dokument, Grunnloven, ble forfattet i 1814 besto kommunikasjon primært av brevutveksling. Det var klart, da som nå, at for å kunne ha et fritt demokratisk samfunn var man avhengig av ytringsfrihet, respekt for privatlivet og frihet fra overvåkning. Forslaget kan ikke sees på som annet enn helt klart i strid med grunnloven og dens intensjon.

Forslaget er i strid med menneskerettighetene. Det er også i konflikt med EU-domstolens kjennelse av onsdag 21/12 2016 om at nettverkstilbydere ikke kan pålegges *generell* lagring av trafikkdata, men kun pålegges å gi tilgang ved særskilte tilfeller hvor det er grunn til å mistenke alvorlige lovbrudd og tilgang skal da gis i et begrenset omfang.

Formålsglidning

Det uttalte formålet er å avverge større angrep mot Norge. Dersom etterretningen kommer over andre lovbrudd, vil de raskt komme i et etisk dilemma. Dette fordi etterretningen får tilgang til system for overvåkning av hele det norske folk, deres gjøren og laden. For eksempel vil militær etterretning få kjennskap til ulike sivile forhold. Dette vil kunne medføre en sammenblanding av militær etterretning og for eksempel politiets oppgaver. I hvilke tilfeller skal og skal ikke informasjon mottatt fra overvåkning av alles datatrafikk sendes videre? Et system for massiv systematisk overvåkning åpner store muligheter det er vanskelig å se konturene av.

Faren for formålsglidning må anses å være svært stor og potensielt farlig.

Norsk brukere av norske tjenester vil også overvåkes

Internett er, av design, bygd opp gjennom desentralisert løst sammenkoblede datamaskiner og nettverkskomponenter som selv bestemmer hvor data skal sendes. Som bruker av Internett har man dermed ingen kjennskap til hvilken vei, dvs. hvor, datatrafikken går. Man har heller ingen måte å påvirke dette på. Nettverkstrafikk kjenner således ingen grenser, og datatrafikk som går fra en bruker i Norge til en annen bruker i Norge, kan gå flere ulike veier både innenfor og utenfor rikets grenser. En overvåkning av all «grensetrafikk» vil dermed også innebære massiv overvåkning av trafikk mellom nordmenn og norske tjenester i Norge. Dette er spesielt aktuelt for utenlandske nettverkstilbydere som, av ulike årsaker, kan velge å rute trafikk sentralt via egne linjer ut av landet og så tilbake til landet igjen.

Datatrafikk kjenner ingen grenser – Digitalt Grenseforsvar vil overvåke alt og alle

Norske bruker av utenlandske tjenester vil alltids overvåkes

Svært mye av norske borgeres legitime datatrafikk forlater rikets grenser. Dette fordi mange tjenester holder til i utlandet, samt at datatrafikk også mellom norske parter, i stor grad går inn og ut av rikets grenser. Overvåkning av datatrafikk gir tilgang til disse opplysningene.

Noen eksempler på datatrafikk ut av Norge?

- Søk: Alle søk på Google, Bing m.fl. Bruk av Apple Siri, OK Google, Amazon Alexa, Microsoft Cortana
- Sosiale medier, vennskap, personlige meldinger: Facebook, Linkedin, Instagram, Google+
- E-post, dokumenter, regneark og presentasjoner: Microsoft Office 365, Google Apps
- Direktekommunikasjon: Facebook messenger, Apple Facetime, Skype, Whatsapp
- Helsedata: Fitbit, Apple, Whitings. Inneholder data om vekt, fettprosent, blodtrykk, oksygennivå, hjerterytme, fysisk aktivitet, fingeravtrykk og andre biometriske data.
- Alarmsystemer, GPS, kamera
- Alle nettsider du besøker utenfor Norge (og noen innenfor Norge)
- Diskusjonsforum
- Bilmodeller som rapporterer alt fra posisjon, hastighet til status på bilalarmen

Gjennom tilgang til data generert av den enkelte borgers datatrafikk er det i dag fint mulig å lage gode profiler av hver eneste borger. Dette inkluderer alder, kjønn, legning, trosretning, politisk tilhørighet og aktivitet, geografisk lokasjon og bevegelsesmønster, helse og sykdommer, familierelasjoner, utroskap, vennskap. Det eksisterer allerede systemer som kan tolke en persons sinnstemning ved å automatisk analysere språkbruk.

Innføring av Digitalt Grenseforsvar innebærer et grovt inngrep i personvernet til alle norske borgere.

Næringslivet, Norske datasenter og utenlandske investeringer i Norge

Massiv systematisk overvåkning vil kunne skade investeringsvilje fra utenlandske aktører i Norge og skade norsk næringsliv. Det har de senere årene vært høyt fokus på å tiltrekke seg utenlandske datasenter-aktører. Dersom man gjennom lov tillater norsk etterretning å overvåke all datatrafikk inn og ut av landet, vil dette svekke norske aktørers mulighet til å konkurrere om datasenter-tjenester. Videre vil selskaper som investerer i forskning og utvikling av høyteknologi i større grad ønske å benytte andre land som ikke har innført «Digitalt Grenseforsvar». Eksempelvis antas det at Snowdens avsløringer om lignende overvåkning i USA koster Amerikanske skytjeneste-leverandører milliarder av dollar hvert år i tapte inntekter, muligens 10-20% av omsetningen. Sverige har eksempelvis blitt mindre interessant som land for datasenter-tjenester etter FRA-loven ble innført. Unntaket er tjenester som lever av å dele alle opplysninger, slik som sosiale medier, nyhetstjenester ol.

«Snowden revelations may cost U.S. cloud providers billions, says study", Computerworld, 9 august 2013. Link: http://www.computerworld.com/article/2484779/cloud-computing/snowden-revelations-may-cost-u-s--cloud-providers-billions--says-study.html

Innføring av Digital Grenseforsvar kan påføre økonomisk skade for norsk Næringsliv

Norges omdømme som fritt, åpent demokratisk land

Viten om at et land har generell overvåkning av all datatrafikk vil kunne legge en demper på ytringer. Ytringsfriheten er en grunnpilar for å ha et fritt åpent demokratisk land. Overvåkning vil redusere åpenhet og derigjennom skade demokratiet. Norge vil bli rangert langt dårligere på indekser som rangerer ytringsfrihet, pressefrihet, personvern og demokrati. Dette vil igjen skade Norges omdømme i utlandet. Etter terrorangrepet 22 juli 2011 manet daværende statsminster Jens Stoltenberg til å møte truslene med mer demokrati og åpenhet. Dette med støtte fra samtlige politiske partier med positiv oppmerksomhet fra verdenssamfunnet. Innføring av generell overvåkning av hele det norske folk under påskudd av beskytte de samme innbyggerne setter den samme uttalelsen og de samme verdiene til side. Innføring av Digitalt Grenseforsvar vil kunne redusere nordmenns tillitt til norske myndigheter.

Digitalt grenseforsvar rammer Norges omdømme

Faren for misbruk og uautorisert tilgang

Rapporten påpeker misbruk fra egne ansatte uten å utdype mer om farene og omfang. Det er de senere årene avdekket at politiets ansatte misbruker egne systemer, at NAVs ansatte misbruker sine systemer og at sykehuspersonell snoker i andres journaler. Ofte skyldes misbruket egeninteresser og nysjerrighet. VDet må antas at et hvert system kan og vil bli misbrukt, ikke minst av ansatte selv. Misbruk er dessverre svært vanskelig, ofte umulig, å avdekke.

Faren for misbruk er høyst reell, vanskelig og avdekke og farene ved misbruk må ikke undervurderes.

Fremmede makters interesse for Digitalt Grenseforsvar

Data om all nettbruk kan være svært verdifulle også for utenlandsk etterretning. Det må antas at fremmede makter vil ønske å oppnå tilgang til de samme dataene. I hvilken grad kan eller skal norske myndigheter utlevere data innhentet via Digital Grenseforsvar til fremmede makter? Ved Snowden-avsløringene ble det for eksempel avdekket at amerikansk etterretning ba engelsk etteretning om å overvåke amerikanske borgere de selv ikke hadde tillatelse til å overvåke. Kan det samme skje i Norge?

Videre må det antas at fremmede makter vil forsøke å skaffe uautorisert tilgang til de samme systemene. Vi kjenner fra før tilfeller både i Norge og hos våre allierte, at fremmede makter får tilgang til forsvarssystemer, registre, kjernekraftverk, olje- og gassintallasjoner med mer. På hvilken måte mener man å sikre disse dataene bedre mot fremmede makter? Det må antas at fremmede makter vil kunne oppnå uautorisert tilgang til de samme dataene som norsk etterretning.

Fremmede makter vil kunne få tilgang til sensitive data om norske borgere og norsk næringsliv

Omgåelse av grenseforsvaret

For en person, organisasjon eller fremmed makt er det svært enkelt å omgå grenseforsvaret dersom man skulle ønske dette. Det finnes et utall måter å gjøre dette på. Digitalt Grenseforsvar gir således like mye beskyttelse som et fysisk grensegjerde som alle usett kan klatre over, krype under eller gå rundt. Da en hver som ønsker å omgå grenseforsvaret enkelt kan gjøre dette, står man igjen med et

system for å overvåke den lovlydige massen som ikke ser grunn til å «hoppe over gjerdet». Da faller også poenget med Digitalt Grenseforsvar bort.

Digital Grenseforsvar kan enkelt omgås av de som ønsker

Oppsummert

Forslaget innebærer stor fare for formålsglidning, åpner for misbruk, er potensielt skadelig for norsk næringsliv, er klart grunnlovsstridig, svekker personvernet, ytringsfriheten og demokratiet og bør forkastes.