Civita-notat
nr.9 2019

civita

Ny etterretningslov:

Nasjonal sikkerhet eller digital masseovervåkning?

Av Vivi Ringnes Wilhelmsen, statsviter, kommunikasjonsrådgiver og tidligere personvernombud i GK-gruppen

Sammendrag

Regjeringens forslag til ny lov om Etterretningstjenesten har vært ute på høring. Forslaget om etablering av et såkalt digitalt grenseforsvar, hvor etterretningstjenesten gis mulighet til å lagre datatrafikk som krysser landegrensen, er kontroversielt. Høringsinstansenes innspill var i hovedsak negative. Dette notatet ser på forslaget til ny lov, praksisen med tilrettelagt innhenting og innvendingene mot denne. Det foreslås en revidering av lovforslaget, der det vurderes nærmere om tilrettelagt innhenting gir de ønskede effekter og hvordan de veier opp for samfunnsmessige og økonomiske kostnader. Det forslås også en utvidet evaluering av personvernseffekter, nedkjølingseffekt, formålsglidning og tilretteleggingsplikt, og en vurdering av hvordan kontrollregimet kan styrkes.

Innledning

12. november 2018 sendte Forsvarsdepartementet *Forslag til ny lov om Etterretningstjenesten* ut på høring. Den nye loven skal erstatte Etterretningstjenesteloven fra 1998 og ruste Norge i møtet med et nytt trusselbilde. Særlig kontroversielt er forslaget om etablering av et såkalt digitalt grenseforsvar, hvor etterretningstjenesten gis mulighet til å lagre datatrafikk som krysser landegrensen.

Høringsinstansenes innspill, som nå er til vurdering i Forsvarsdepartementet, var i hovedsak negative. Debatten i de brede lag har derimot vært begrenset. Muligens er dette fordi det er svært krevende å danne seg et bilde av utfordringene, blant annet fordi tilhengere og motstandere kommuniserer svært ulike virkeligheter.

Høringsforslaget er på nærmere fire hundre sider. Det er teknisk, språklig og juridisk utilgjengelig, og hadde kun standard høringsfrist på tre måneder (uten kompensasjon for jul og nyttår).[1] Formålet med dette notatet er å oppsummere regjeringens forslag, samt drøfte hvordan vi kan balansere etterretningstjenestens behov opp mot personvern, ytringsfrihet og kildevern.[2]

Tilrettelagt innhenting, tidligere kjent som Digitalt grenseforsvar

Etterretningstjenesten er en essensiell del av Norges forsvar. Deres ansvarsområde er utlandsetterretning, mens PST og Politiet har ansvaret for innenlandsk informasjonsinnhenting. E-tjenesten skal derfor som hovedregel ikke samle informasjon om norske borgere eller virksomheter.[3] E-tjenesten skal gi beslutningstagere et godt kunnskapsgrunnlag og på den måten bistå i å sikre Norges eksistens, sikkerhet og interesser. Som en del av de hemmelige tjenestene er etterretningstjenestenes metodikk i stor grad unntatt offentligheten, men det nye lovforslaget gir noe mer overordnet innsikt, fordi det skal "*i stor grad lovfeste eksisterende metoder og praksis*"[4].

> (…) tilgang til grenseoverskridende elektronisk informasjon er egnet til å bidra til reell beskyttelse mot trusler som kan materialisere seg i eller gjennom det digitale rom. Departementet mener at dette kan tale for at tilrettelagt innhenting ikke bare bør innføres for å dekke myndighetenes behov for informasjon, men også for å sikre effektiv beskyttelse av den norske befolkningens menneskerettigheter.[5]

En trygg, legal forankring er et absolutt gode.[6] Etterretningstjenestens hemmelige natur begrenser offentlighetens innsikt, og samfunnets tillit er betinget av at tjenesten opererer i henhold til tydelige kjøreregler. Det er også et viktig poeng at gjeldende lov er 20 år gammel, noe som betyr at den overhodet ikke er dimensjonert for dagens hybride trusler[7]. Den tar ikke tilstrekkelig høyde for digitaliseringen og de utfordringene dagens sikkerhetssituasjon fører til.[8] Et tredje poeng som Forsvarsdepartementet understreker er at Norge er en liten aktør i større forsvarssamarbeid. De hevder at et digitalt forsvarsverk er essensielt for å sikre Norges plass i de internasjonale etterretningsmiljøene, hvor utveksling av data er valuta. Avhengighet av andre staters velvilje svekker Norges forhandlingsposisjon og øker vår sårbarhet. Ikke minst hevder etterretningstjenesten at informasjonen generert ved tilrettelagt innhenting/DGF vil gjøre Norge bedre i stand til å oppdage terrorisme og cyberangrep. Etterretningssjefen og forsvarsministeren trekker for eksempel frem dataangrep mot Helse Sør-Øst, fremmede makters opinionspåvirkning og sabotasjeforsøk rettet mot vital infrastruktur, som noe som kan unngås eller oppklares.[9,10,11,12]

> Etterretningstjenesten innhenter informasjon med to ulike utgangspunkter; Informasjon innhentes for å kartlegge målmiljøer og identifisere nye etterretningsmål, dette kalles *målsøking*. Når man har identifisert legitime etterretningsmål pågår innhentingen over tid for å finne mest mulig informasjon om etterretningsmålene og deres intensjoner, aktiviteter og nettverk. Dette kalles *målrettet innhenting.*[13]

Etterretningstjenesten hevder at norske data allerede samles inn av andre lands hemmelige tjenester. De mener at innføring av tilrettelagt innhenting dermed ikke vil medføre innsamling av data som ikke allerede er i hendene på andre stater eller kommersielle[14] aktører. En stor del av

norsk internettrafikk går via kabler til Sverige. Sverige, Frankrike, Storbritannia, Canada og USA har allerede et digitalt grenseforsvar. Finland og Nederland vurderer å innføre det.[15] NUPI slår fast i sitt høringssvar at

> Debatten handler altså ikke *om* vår digitale kommunikasjon skal kunne samles opp eller ikke. Det blir den i stor grad allerede, men snarere om av *hvem* og *hvordan* informasjon kan samles.[16]

Hva snakker vi egentlig om?

I praksis foreslår Forsvarsdepartementet en revidert versjon av Lysne II-utvalgets *Digitale Grenseforsvar* (DGF). Disse begrepene sammenblandes ofte i debatten. Kjernen i kontroversen er det departementet har døpt "tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon", forkortet til tilrettelagt innhenting. Det som skiller tilrettelagt innhenting og DGF er primært hvilke filtre og kontrollmekanismer som legges til grunn. Dette kommer jeg tilbake til.

Tilrettelagt innhenting gir E-tjenesten lov til å speile elektronisk kommunikasjon som passerer landegrensene.[17] [18] En slik digital "kopimaskin", såkalt bulk-innsamling, innebærer at metadata lastes ned og lagres.[19] Metadata er den overordnede beskrivelsen av data, "data om data", for eksempel informasjon om avsender, mottaker, format, hva slags enhet som brukes, telefonnummer, størrelse på fil og IP-adresse. Innholdsdata er den faktiske informasjonen som mottaker får tilsendt, for eksempel innholdet i en mail eller SMS. Informasjon (også kalt rådata) behandles i ulike lagre[20] og filtreringsmekanismer[21] før etterretningstjenesten kan benytte informasjonen i sine analyser.[22]

Slik tilrettelagt innhenting skisseres i lovforslaget vil bearbeiding av metadata være underlagt svakere restriksjoner enn innholdsdata, fordi det anses som et mindre inngrep i personvernet. Innhenting og lagring av sistnevnte type data forutsetter kjennelse fra domstolen.[23] Nederland har derimot valgt å ikke skille mellom de to datatypene, fordi metadata samlet gir mye informasjon om personers liv, sosiale relasjoner, politiske syn, seksuelle preferanser, helse og bevegelsesmønster. Metadata er også mer strukturert og dermed lettere å analysere maskinelt.

> Metadataene er, ifølge DGF-rapporten, som «utsiden av konvolutten». Analogien med konvolutten illustrerer hvor galt det kan gå når moderne teknologi skal forklares med «gammeldagse» eksempler. Dette blir som å si at en firefelts motorvei er som en sti, fordi begge går mellom to punkter. Det er ikke direkte usant, men for en fotvandrer som aldri har sett en bil før, ville det oppleves som en litt mangelfull opplæring.[24]

På internett er alle katter grå

Internett ble utviklet for å sikre det amerikanske forsvarets kommunikasjon under en atomkrig. Datatrafikken er derfor designet for å alltid velge "minste motstands vei" .[25] Den tar seg gjerne en tur utenlands, hvis det er raskeste rute mellom A og B. En epost fra en nordmann til en annen nordmann vil for eksempel gjerne ta en snarvisitt innom en amerikansk eller irsk server. Norske internettjenester har også i økende grad basert seg på infrastruktur i utlandet.[26] I realiteten vil bortimot all elektronisk kommunikasjon derfor automatisk passere landegrensen, på grunn av ruting, fordi en bruker en skytjeneste e.l., eller fordi programvaren har interne moduler som lenker utenfor landegrensen.[27]

Det finnes også mange måter å maskere opprinnelsessted på. Å bruke IP-adresse som "nasjonalitet" for datatrafikk er dermed lite fruktbart.[28] Det finnes ingen landegrenser i tradisjonell forstand på nett, og i praksis blir skillet mellom nasjonale og grensekryssende data dermed fiktivt.

Det finnes heller ingen effektive filter som skiller "de snille" og "de slemme" sin internettaktivitet eller "nordmann" fra "utlending". Det er ikke teknisk mulig å utvikle et såpass finmasket garn, og det er udiskutabelt at mye innenlandsk informasjon vil samles inn "på slump".[29] At norsk datatrafikk samles inn er altså ikke til unngå.

Store deler av kritikken mot lovforslaget dreier seg om hvor mye av nordmenns data som samles inn, om lovforslaget i sin nåværende form er lovlig etter Grunnloven og menneskerettighetene, hvilke kontrollmekanismer som må på plass, og hvordan man sikrer den nødvendige grense-dragningen mellom PST, politi og etterretningstjenestens virke.[30] Departementet mener at selv om data vil samles inn[31], vil behandlingen av disse være underlagt strenge restriksjoner. De anser derfor inngrepet som minimalt.[32]

Men for å finne et sort får i en saueflokk vil en datamaskin måtte vurdere hele flokken. Det vil være strenge restriksjoner på søk i data, men min påstand er at selv om dataene ikke behandles, så er nok de færreste komfortable med at myndighetene teoretisk sett kan sitte på din søke-historikk, legejournaler, informasjon fra sosiale medier (også privat som Snapchat, Facebook-innboks eller datingapper), SMS, e-post osv. Særlig fordi du ikke har mulighet til å vite om *dine* data behandles eller ikke. 67 prosent av nordmenn er enig eller delvis enig i at man bør få være anonym på nett.[33]

Retten til privatliv

Menneskerettighetserklæringen slår fast at alle mennesker har medfødte, iboende rettigheter som skal kunne nytes uten frykt for represalier.[34] En privat sfære er en forutsetning for reell forsamlingsfrihet, ytringsfrihet, deltagelse ved valg og selvutvikling. Personvern og retten til privatliv er derfor nedfelt i Den europeiske menneskerettighetskonvensjonen (EMK), Grunnloven og en rekke nasjonale lover. Den europeiske menneskerettsdomstolen har lagt til grunn at innsamling av kommunikasjonsinnhold, trafikkdata og metadata er et inngrep i privatlivet.[35] Staten er forpliktet til å respektere retten til privatliv, med mindre noe annet er helt nødvendig for å ivareta andre menneskerettigheter eller samfunnets sikkerhet.[36] [37]

Søk med utgangspunkt i en konkret person eller virksomhet vil kunne inkludere informasjon to ledd ut i kommunikasjonskjeden. Det vil si at en rekke personer vil kunne fanges opp fordi de har kontakt med noen som har kontakt med noen som er av interesse. Elektronisk Forpost Norge hevder at myndighetene i løpet av to uker teoretisk kan tilrettelegge for profilering og kategorisering av nesten hele Norges befolkning.[38] En Stanford-studie[39] slår fast at ett telefonnummer kan gi tilgang til metadata om 25 000 personer.[40] Departementet, derimot, hevder Stanford-studien ikke er overførbar til norske forhold, og hevder at bestemmelsen om to kommunikasjonsledd balanserer personvern, effektiv ressursbruk og godt etterretningsarbeid.[41] Uansett hva praksis blir under norske omstendigheter: loven vil ha et stort nedslagsfelt og gi Etterretningstjenesten fullmakt til omfattende, skjønnsmessige aktiviteter på norsk jord.[42]

Nedkjølingseffekten

Vi tilpasser atferden vår til omgivelsene. Hver og en av oss gjør ting alene eller i private rom som vi ikke gjør på bussen. Ikke ulovlige handlinger, men litt mindre sosialt aksepterte. For eksempel å prompe, baktale andre, pille nese eller se porno. Borgernes meningsdannelse skjer også både offentlig og privat. Det skjer i samtale med andre og ved at man innhenter ny informasjon. Når livet leves på nett kan potensielt alle dumme ideer, ufullstendige argumenter, informasjonssøk eller interaksjon med grupperinger lagres i evig tid. Privat kan vi formulere oss på måter som vi ikke vil være komfortable med å presentere til hvem som helst. Alle har nok vært litt "sleivete" på telefonen eller googlet noe de ikke ønsker å dele med en nabo eller ens sjef.

Tilrettelagt innhenting innebærer at etterretningstjenesten vil få en teoretisk tilgang til store mengder informasjon som ikke er relevant for deres oppgaveløsning.[43] Spørsmålet er dermed om dette vil føre til en såkalt *nedkjølingseffekt*. Den kan forstås som at folk avstår fra å ytre seg som de ellers ville ha gjort, eventuelt modifiserer eller sensurerer egne ytringer, som følge av frykt for at disse kan fanges opp av Etterretningstjenesten. Konsekvensen av slik selvsensur vil være mindre eller endret privat og offentlig meningsbryting, noe som vil innvirke negativt på den demokratiske debatten.[44]

Tanken om at "noen" følger med vil med stor sannsynlighet føre til at vi modererer vår atferd. Faktisk sier 62 prosent av amerikanere at de ville være "much less likely" eller "somewhat less likely" å snakke eller skrive om visse tema på internett hvis de visste at myndighetene fulgte med.[45] Nesten åtte av 10 mente at de ville være mer forsiktig med hva de ville si i visse internettdiskusjoner og hva slags informasjon de ville oppsøke på nett.[46] Da handler det ikke lenger bare om individets autonomi.

Departementet konkluderer likevel med at nedkjølingseffekten ikke kan påvises[47] fordi de anser at studier basert på premisser om at "alle overvåkes" ikke er relevant for norske forhold. Dette begrunner de med strenge søkekriterier og kontrollmekanismer. For den gjengse nordmann vil nok innsamling anses som en form for overvåkning selv om data ikke brukes. Spørsmålet er i hvilken grad det vil påvirke vår atferd både kortsiktig og over tid.

Det er riktig at nedkjølingseffekten er svært vanskelig å isolere[48] og at fenomenet ikke er forsket mye på. Men et par gode studier indikerer at konsekvensene av en (oppfattet) statlig overvåkning kan bli store. Jon Penney (2016) undersøkte for eksempel om Snowden-avsløringene påvirket amerikaneres bruk av Wikipedia. Han fant både en kortsiktig og en langsiktig effekt på folks søkehistorikk.[49] En annen studie, fra MIT, fant en fem prosents reduksjon i visse Google-søk rett etter Snowden-avsløringene.[50] PEN America Center fant at frykt for statlig overvåkning hadde ført til at nesten en fjerdedel av amerikanske forfattere hadde unngått visse samtaleemner på telefon, nesten en tredjedel hadde unngått visse typer atferd i sosiale medier, og nesten en tredjedel hadde avstått fra, eller vurdert seriøst, å ikke skrive om visse tema.[51] [52] Ni av 10 mener også at deres personlige data kan bli misbrukt, fordi de kanskje aldri blir slettet eller fullstendig trygt oppbevart.[53] Det er viktig å merke seg at ingen av disse studiene ser på ulovlig atferd, kun bruk av sentrale informasjonskilder i demokratiet vårt.

Man må også spørre seg om det viktigste er at alle faktisk blir overvåket eller om det er *opplevelsen* av å være overvåket som er avgjørende for folks atferd. *Frykt for overvåkning* tenderer også til å

endre atferd,[54] men departementet argumenterer for at vurdering av nedkjølingseffekten må "ta utgangspunkt i et infor mert kunnskapsgrunnlag knyttet til hva Etterretningstjenesten lovlig kan og ikke kan gjøre".[55] Her er det på sin plass å påpeke at Etterretningstjenestens hemmelige natur og lovforslagets vage formuleringer gir allmenheten få forutsetninger for å tilegne seg et informert kunnskapsgrunnlag. Det er et argument for at *borgernes opplevelse* er viktigst for en eventuell nedkjølingseffekt. Argumenter som at "vi må stole på spionene våre"[56] gir derimot bare de som frykter masseovervåkning vann på mølla.

Departementet beskriver i høringsnotatet en mulig positiv nedkjølingseffekt.[57] Den negative effekten medfører at folk vegrer seg for å ytre seg. Positiv nedkjølingseffekt baserer seg på det samme premisset, men at staten følger med forhindrer ulovlige handlinger, rasisme eller hatefulle ytringer. Overvåkningen får en preventiv effekt. Ved første øyekast, særlig etter en titt innom visse kommentarfelt, kan en positiv nedkjølingseffekt virke attraktivt. Men ytringsfrihet begrenset av frykt for sanksjoner er ikke positivt. Det er svært sannsynlig at en eventuell "positiv" nedkjøling særlig vil ramme de som befinner seg i ytterpunktene av meningsfellesskapet. Holdninger og oppfordring til handling kan da flytte seg til andre fora.

Fortrolig kommunikasjon

> Etterretningstjenesten skal ikke behandle opplysninger som er fortrolig kommunikasjon mellom ... journalist og kilde ... , med mindre **vektige samfunnshensyn** gjør behandlingen strengt nødvendig. Beslutning om å behandle opplysninger etter første ledd treffes av sjefen for Etterretningstjenesten.[58] (min uthevning).

Flere instanser har også påpekt det problematiske ved at "bukken passer havresekken". Særlig betenkelig er det at Etterretningstjenesten selv skal vurdere om samfunnsnyttige behov er tungtveiende nok til å behandle fortrolig kommunikasjon mellom særlige yrkesutøvere (for eksempel advokat-klient, lege-pasient, journalist-kilde). Helseinformasjon er konfidensiell blant annet fordi vi ikke vil at noen skal unngå å oppsøke helsehjelp. Trygg kommunikasjon med advokat er en forutsetning for god rettshjelp. Kildevernet skal sikre at enkeltpersoner kan informere storsamfunnet om overgrep eller maktmisbruk uten å frykte sanksjoner. Hensynet går dermed langt utover den enkeltes personvern. Tilliten til at informasjon er fortrolig svekkes med en gang informasjonen samles inn,[59] uavhengig av om den behandles eller brukes. Til sammenligning kreves kjennelse fra domstolen når politiet skal benytte tvangsmidler ved kommunikasjonskontroll (straffeprosessloven kapittel 16a).[60]

At vurderingen om hva som defineres som "vektige samfunnshensyn" skal gjøres av tjenesten selv er ikke tillitsvekkende. Det reiser også andre spørsmål: må mediehus hjelpe etterretningstjenesten med å samle informasjon?[61] Hva med de som jobber freelance eller som (politiske) bloggere? Skal norske journalister på jobb i utlandet kunne overvåkes? Hva med varslere som ikke har kontaktet media (ennå)? Skal etterretningstjenesten publisere en liste over hvilke digitale helsetjenester som er "trygge"? Hvordan ekskluderes andre objekter (for eksempel en advokats andre klienter)? Kommunikasjon mellom stortingsrepresentanter, regjeringsmedlemmer og dommere har heller ikke

fått særskilt vern.[62] Departementet mener dette opprettholdes av etterretningstjenestens forbud mot innhenting av informasjon om nordmenn.

Formålsglidning

> Så snart informasjonen er samlet inn eller kapasiteten etablert, så vil andre interessenter potensielt hevde at det ikke er hensiktsmessig ut fra et ressurs- eller kapasitetsperspektiv å avgrense bruken av systemet kun til det opprinnelige formål.[63]

Formålsutglidning innebærer at personopplysninger som var innhentet til et bestemt formål senere benyttes til et nytt, annet formål.[64] I høringsforslaget fastslår departementet at et forbud mot deling av overskuddsinformasjon må formuleres så "klart og uinnskrenkelig som mulig".[65] Terrorhandlinger, samt anslag mot nasjonal sikkerhet, selvstendighet og grunnleggende interesser (straffelovens kapittel 17 og 18) ligger såpass tett oppunder Etterretningstjenestens ansvarsområde at informasjonsdeling anses som legitimt, hvis handlingen kan avverges.

Nesten all vår atferd logges digitalt. Mengden informasjon myndigheter *kan* besitte om sine borgere er større enn noen gang før i historien. Med Artificial Intelligence er også analysepotensialet uten presedens. I Kina ser at det er etablert et sosialt belønningssystem for å fremme god atferd. Saudi-Arabia og Russland viser også skremmende tendenser. Hvor skal Norge trekke grensen? Hvor mye informasjon skal vi samle inn og hvem skal få benytte seg av den? Kunnskap er makt og, som Kripos påpeker i sitt høringssvar, kunnskap forplikter.[66]

Det nasjonale statsadvokatembetet, Riksadvokaten, Kripos, PST og Innlandet politidistrikt har allerede tatt til orde for at retten til informasjonsdeling skal utvides og at informasjonen skal kunne benyttes som bevis i straffesaker. Det vil være svært vanskelig for norske politikere å stå i mot press om slike utvidelser når bestialske saker, som for eksempel Dark Room-avsløringene, rulles opp. Det er sannsynligvis også en stor belastning for etterretningspersonell å måtte ignorere alvorlige overgrep. Men hvilke saker som er ille *nok* og *når* noe kan avverges er det svært vanskelig å definere. Kripos peker på overgrep mot barn. Hva med (planlagt) drap? Hvor grove må voldtekter være? Hvor mange mennesker må utsettes for økonomisk utbytting? Er ID-tyveri ille nok?

Vi må gjøre noe! Er dette "noe"?

> Staten skal beskytte oss mot terror og andre ytre trusler som har betydning for Norge og norske interesser. Det betyr at myndighetene må ha tilgang på informasjon som kan bidra til å kartlegge slike trusler. Det vil et digitalt grenseforsvar bidra til.[67]

Tre argumenter trekkes frem for innføring av tilrettelagt innhenting/DGF: a) forhindre terror, b) forhindre sabotasje og spionasje mot vital infrastruktur, og c) bygge Norges posisjon som en attraktiv etterretningspartner og oppfylle våre NATO-forpliktelser. I tillegg uttrykkes det bekymring for at andre land forsøker å forme opinionen gjennom sofistikerte, digitale propagandakampanjer.

Forholdsmessighetsprinsippet krever at inngrepets skade eller uleilighet må balanseres opp mot målet. Det innebærer at tiltaket må være *nødvendig,* det må være *egnet* for å oppnå formålet og det må være den minst inngripende metoden tilgjengelig.[68] Det er vanskelig å se hvordan disse kravene er oppfylt med tilrettelagt innhenting. Forsvarsdepartementet presenterer ulike scenarier i høringsforslaget,[69] men det er slående hvor dominerende etterretningshensyn er i vurderingen.

En rekke høringsinnspill påpeker at bulk-innsamling vil føre til en gigantisk høystakk av data, som igjen vanskeliggjør jakten på den famøse nålen. Etterretningens mangel på data er sjelden årsaken til at terrorister lykkes. De fleste "vellykkede" terrorangrep er utført av personer som allerede er oppført på en eller annen liste.[70] Problemet er snarere for mye data. Vi makter ikke å se mønstre fordi informasjonsmengden blir for stor.[71] Det er også omdiskutert i hvilken grad digital masseovervåkning forbedrer nasjonal sikkerhet.[72] Nå er det naturlig nok svært komplisert å bevise at datainnsamling fungerer. Både fordi effektene vanskelig kan isoleres, og fordi etterretningsarbeid er hemmelighetsstemplet. Det er dermed bare de gangene man mislykkes å avverge et angrep at eksterne forskere får innsikt. Suksesshistoriene forblir i stor grad ubejublet.

Men lovforslaget innebærer en oppstartsinvestering på 700 millioner kroner og estimerte driftskostnader på mellom 100 og 150 millioner kroner i året.[73] De reelle kostnadene kan bli betraktelig høyere. Vi bør derfor spørre oss selv om dette er riktig ressursprioritering. Alle valg betyr i praksis at noe velges bort, og for eksempel Tekna er usikre på om nytteverdien står i samsvar med kostnadene knyttet til å implementere, drifte og videreutvikle et så ressurskrevende system.[74] Det mangler en kost/nytte-analyse som viser at dette er den beste bruken av pengene.[75]

Får vi det vi betaler for?

Eventuelle effekter av denne typen datalagring er betydelig svekket av at terrorister, og også sivile aktører som Apple, Google og Facebook, i økende grad benytter krypterte tjenester. Cisco/Gartner anslår at 60–80 prosent av internett-trafikken i 2019 vil være kryptert.[76] Lovforslaget åpner opp for at tjenestetilbydere må åpne krypteringsnøklene sine for etterretningstjenesten. Dette vil fort føre til at kompetente aktører benytter andre metoder. De kan kommunisere med annen type kryptering enn den tjenestetilbydere kontrollerer, bruke metoder som ikke legger igjen verdifulle metadata, eller maskere trafikken som norsk gjennom noder og såkalte virtuelle private nettverk (VPN) slik at trafikken automatisk filtreres ut. Mindre teknisk kompetente personer vil kanskje kunne fanges opp på chatforum og lignende, men før konkrete planer diskuteres vil rekrutterere med all sannsynlighet guide noviser inn på sikre plattformer. Sannsynligvis vil også de store datamengdene medføre en rekke falske positive treff.[77]

Det tredje argumentet for endringene tar utgangspunkt i at Norge er et lite land i en stor og til dels farlig verden. For å nyte tryggheten en NATO-allianse innebærer, er Norge nødt til å bidra. Men i lovforslaget legges det en del begrensninger på hvem informasjon kan deles med. Spørsmålet blir dermed hvor mye "kapital", i form av informasjon, tilrettelagt innhenting vil gi oss. Et prinsipielt spørsmål er også om Norge, som et liberalt demokrati, skal operere i randsonen av hva som (kanskje) tillates under Den europeiske menneskerettighetserklæringen[78] fordi "alle andre gjør det".

Tilrettelagt innhenting kan nok derimot gi økt innsikt om utenlandsk påvirkningsarbeid rettet mot norsk opinion. Ved å kunne evaluere hvem som forsøker å påvirke oss, kan vi forhåpentligvis iverksette mottiltak og øke beskyttelsen. Propaganda rettet mot andre lands borgeres innbyggere er det lang tradisjon for, men digitale analyseverktøy gir oss helt andre dimensjoner av skreddersøm og gjennomslagspotensial. Samlet blir effekten potensielt så stor at Etterretningssjefen anser dette som en av de tre alvorligste truslene mot Norges sikkerhet.[79] Slik jeg leser Etterretningssjefens utsagn virker det som om tilrettelagt innhenting skal fungere som en form for alarmsystem, men han har ikke gått i detalj på hvordan det skal organiseres innenfor retningslinjene for lagring og søk.

En slik "mot-propaganda"-funksjon åpner også en mye større debatt. En ting er å lære borgerne "nettvett" og flagge "fake news", det er noe helt annet å åpne for at Etterretningstjenesten skal bidra til forming av den norske debatten. Dagens lovforslag åpner ikke for at E-tjenesten skal være meningspoliti, men kampen mot for eksempel trollfabrikker tilsier at man også må skissere mot-tiltak. E-tjenesten vil potensielt besitte mye kunnskap om hvilke budskap som "slår an" og hvordan de bør besvares.

Hvem skal vokte vokterne?

Departementet anser det ikke som nødvendig med forhåndsautorisering når kommunikasjon samles under transport (midtpunktsinnhenting) eller ved tvungen adgang til for eksempel en PC (endepunktinnhenting). De anser etterretningstjenesten som den mest effektive og kvalifiserte til å vurdere metodebruk. Samtidig anerkjenner de at tilrettelagt innhenting må underlegges et strengere kontrollregime fordi det omfatter store mengder norsk data.[80] De skriver

> Det er avgjørende at den som beslutter metodebruk har oversikt over alle tilgjengelige kapasiteter, har kunnskap om etterretningsfaglige, risikomessige og ressursmessige aspekter ved bruk av ulike metoder, forstår hvordan ulike metoder kan spille sammen og kjenner saksfeltenes viktighet i en nasjonal og internasjonal kontekst.[81]

EOS-utvalget vil (fortsette å) være den viktigste kontrollinstansen. Dennes metode er primært etterhåndskontroller i stikkprøve-format. Utvalget består av syv medlemmer i 20-30 prosent stilling, hvorav to har juridisk og teknologisk bakgrunn (2017).[82] Utvalget støttes av et sekretariat på elleve personer. Det årlige budsjettet ligger på rundt 15 millioner kroner, og sekretariatet vedtok i 2017 å opprette en teknologisk enhet på fem personer.[83] I juni 2017 ble antall pålagte årlige kontroller inspeksjoner utført av alle EOS-tjenestene redusert fra 23 til 13.[84] Utvalget mener selv at dette gir dem økt fleksibilitet, men at de verken har ressurser eller mandat til å kontrollere alt EOS-tjenestene gjør.

Høringsnotatet viderefører ikke Lysne II-utvalgets modell med et eget DGF-tilsyn. DGF-tilsynet skulle motta alle søk i sanntid, motta alle avgjørelser fra domstolen, ha tilgang til all informasjon om hvordan filtre blir implementert og ha tilgang til all informasjon om hvordan interne retningslinjer og domstolsavgjørelser ble oversatt til søkeprivilegier.[85] Lysne II-utvalgets DGF-tilsyn skulle svare til Samferdselsdepartementet, for å ha den nødvendige avstanden til Forsvarsdepartementet[86].

Departementet mener at et slikt tilsyn ikke er nødvendig fordi EOS-utvalget, oppnevnt av Stortinget i 1996 for å overse de hemmelige tjenestene, skal styrkes betraktelig. I høringsnotatet skisserer departementet at EOS-utvalget skal opprette fire nye årsverk gjennom bevilgninger på ca. fem millioner kroner.[87] I tillegg skal domstolskontrollen utvides, med 5-10 arbeidstimer per sak og mellom en og to millioner årlig i økte driftskostnader. 150- 250 000 kroner skal dekke salær når domstolen velger å oppnevne advokater. Til sammenligning økes altså driftsutgiftene for Etterretningstjenesten med 100-150 millioner i året, etter en investeringskostnad på rundt 700 millioner kroner.[88]

> Lovforslaget lar etterretningstjenesten selv, for alle praktiske formål, etter eget skjønn kunne gjennomføre de tiltak de selv finner nødvendig for å utføre sine vidt formulerte oppgaver.[89]

Domstolskontrollen er foreslått lagt til Oslo Tingrett. Det er positivt at man ikke oppretter en særdomstol a lá den amerikanske FISA-domstolen, som blir beskyldt for å være NSAs forlengende arm og "sandpåstrøer". Lukkede og spesialiserte enheter kan føre til bekymring for domstolens selvstendighet og at dommere identifiserer seg i for stor grad med tjenestene de skal kontrollere. Om domstolskontrollen blir oppfattet som en formalitet, innebærer det en alvorlig svekkelse av systemets legitimitet. En rekke faktorer i det skisserte lovforslaget skaper imidlertid bekymring for om domstolskontrollen vil være effektiv.[90] Formålsangivelsen som ligger til grunn for inngrep er vid, og Borgarting lagmannsrett skriver i sitt høringssvar at nær sagt all informasjon kan hevdes å ligge innenfor ett av formålene listet opp i kapittel 3.[91] Dermed blir det også svært vanskelig for domstolen å vurdere en begjæring som ikke gyldig. Til sammenligning: I 2016 avslo tingretten politiets begjæring om kommunikasjonskontroll i to av 135 saker. I begge sakene ble det gitt tillatelse etter anke.[92]

I utgangspunktet vil kun representanter for etterretningstjenesten møte i rettsforhandlinger, og det er også etterretningstjenesten som vil stille med eventuell fagekspertise. En særskilt advokat *kan* oppnevnes av domstolen, men denne personen vil (naturlig nok) ikke ha mulighet til å konferere med sin klient, som igjen svekker advokatens mulighet for effektiv prøvelse. Muntlige forhandlinger er heller ikke pålagt, med de mulighetene det kunne gitt for kontradiksjon og oppfølgingsspørsmål. En rekke høringsinstanser trekker også frem behovet for forhåndsgodkjenning ved domstolene, en ordning departementet hevder verken er praktisk, mulig eller effektivt.[93] Amnesty, Datatilsynet, Den Internasjonale juristkommisjon – norsk avdeling (ICJ-Norge), Elektronisk forpost, Nkom, NSM, Norges institusjon for menneskerettigheter, Norsk redaktørforening, EOS-utvalget, Tekna, samt flere jurister og dommere er noen av aktørene som har uttrykt bekymring for om det skisserte kontrollregimet vil være tilfredsstillende. Advokatforeningen og Borgarting Lagmannsrett går så langt som å stille spørsmål ved hvilken reell mulighet domstolen har til å utøve effektiv kontroll slik det er skissert i høringsforslaget.

Lovforslagets inngripende natur og tekniske kompleksitet medfører at begrenset kunnskap kan få store ringvirkninger i den enkeltes liv. Man bør derfor også vurdere om retten skal ta stilling til konkrete søkekriterier, da abstrakte selektorer knyttet til en person eller type atferd[94] vil gi E-tjenesten et betydelig rom for skjønn.[95] Manglende teknisk kompetanse kan kompenseres ved at fagkyndige meddommere utnevnes.[96] Etterretningstjenesten fikk i 2014 en personvernsrådgiver.[97] Denne stillingen bør bli oppgradert til personvernombud, med plikt til å delta i domstolforhandlinger.

For å søke i den type ustrukturerte datamengder som bulkinnsamling gir, kan man bruke automatiserte teknikker.[98] Det er dermed også verdt å påpeke at enkelte forskere advarer mot at datainnsamling i økende grad vil automatiseres, fungere predikativt og overta metodikk fra andre fagfelt.[99] I sum gir dette oss en økt sårbarhet for at algoritmer baseres på mangelfulle og udokumenterte prosesser, som igjen fører til bias, at falske positive vanskelig kan motbevises, og at metodisk overførbarhet overvurderes. Dette medfører en reell risiko for at et individ ikke er i stand til å motbevise det en algoritme har påvist av mønster eller sammenheng.[100] Verken problemstillinger knyttet til automatisering eller predikative kapabiliteter er adressert i høringsnotatet. Et aspekt som kan vurderes er spesifisering av et krav om innebygget personvern i alle utviklingsfaser av systemet, tilsvarende kravet i personopplysningsloven GDPR.

Konklusjon

> 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 som befinner seg på telefonen din passere avlesningsutstyret.[101]

I høringsnotatet ønsker departementet en god offentlig debatt velkommen. En åpen, demokratisk debatt kan redusere nedkjølingseffekten, øke bevisstheten om samfunnets sårbarheter og øke kunnskapen om E-tjenestens virksomhet. Et tydelig juridisk rammeverk for hemmelige tjenester er også et absolutt gode. Det store arbeidet som er lagt ned fra departementets side er derfor aktverdig. Men ambisjonen burde vært støttet opp av en lengre høringsfrist, et pedagogisk forarbeid og en imøtekommende kommunikasjon fra forsvarsminister og etterretningssjefen. Slik debatten har vært til nå, og med de store inngrepene som forslaget åpner for, risikerer vi at den nye loven svekker tilliten til etterretningstjenesten og norske myndigheter.[102]

NUPI publiserte i februar 2019 et blogginnlegg kalt ”Å gjøre ingenting er uansvarlig”.[103] Det er det lett å si seg enig i. Etterretningstjenesten trenger verktøy for å utføre de oppgavene vi pålegger dem. Men det er uklart om dette er veien vi bør gå. At vi må gjøre ”noe” betyr ikke automatisk at vi må gjøre ”dette”. Lovforslagets prinsipielle, teknologiske og etiske refleksjoner rundt de samfunnsmessige konsekvensene er svært kortfattede. 71 av 77 høringssvar er delvis eller svært kritiske til lovforslaget.[104] Riksadvokatembetet går så langt som å si at “lovforslaget har betydelig lovteknisk forbedringspotensial”.[105] Innspillene som har kommet i høringsrunden er såpass omfattende at de tilsier at en substansiell omskrivning og en ny høringsrunde er på sin plass. Da kan vi få den substansielle og prinsipielle diskusjonen som et såpass inngripende verktøy behøver.

Særlig tre aspekter bør utdypes i et revidert forslag:

a. en utvidet utgreiing av hvordan tilrettelagt innhenting gir de ønskede effekter og hvordan de veier opp for samfunnsmessige og økonomiske kostnader
b. en utvidet evaluering av personvernseffekter, nedkjølingseffekt, formålsglidning og tilrette-leggingsplikt

c. hvordan kontrollregimet kan styrkes for å bøte på svakhetene formulert I en rekke høringsinnspill.

Forarbeidet kunne også i større grad diskutert hvilke retningslinjer som legges til grunn for automatisert analyse og maskinlære i bearbeidelsen av så store datamengder.

Gjennomgående er alle parter enige om at a) Etterretningstjenesten gjør en svært viktig jobb. De trenger tydelige og gode verktøy for å møte det moderne trusselbildet, b) digitale trusler er komplekse og utfordrer den tradisjonelle organiseringen av sikkerhetsarbeidet[106], c) personvern og menneskerettigheter er fundamentale verdier i det norske samfunnet som må hegnes om, og d) tilliten til de hemmelige tjenestene forutsetter tydelige kjøreregler og sterke kontrollregimer.

Balansegangen mellom rikets sikkerhet og individets rettigheter er vanskelig. Det er en fare for at lovforslaget i sin nåværende form "kaster barnet ut med badevannet", at vi ofrer våre verdier i forsøket på å sikre Norge. Det trengs en bredere offentlig debatt med flere lekfolk og fagmiljøer på banen. Slik får beslutningstagerne våre det nødvendige kunnskapsgrunnlaget for å vurdere lovforslagets mange implikasjoner.

Tusen takk til Civita for muligheten til å skrive dette notatet. Ikke minst vil jeg takke Marius Doksheim, Kristin Clemet og Therese Thomassen. Jeg ønsker også å rette en stor takk til Magnus Ask i Trancendent Group for verdifull sparring om kryptering og informasjonssikkerhet. Jeg er verken jurist eller teknolog, og alle feil eller ufullstendige forenklinger i notatet er utelukkende min feil.

Vivi Ringnes Wilhelmsen er statsviter med to mastergrader med fokus på digital narrativbygging, kriminelle grupperinger og hacking som våpen. Hun er en erfaren konsulent og har jobbet flere år som kommunikasjonsrådgiver i Geelmuyden Kiese. Hun har jobbet med digitalisering i inn- og utland, vært skandinavisk personvernombud for GK-gruppen, og brenner for personvern og informasjonssikkerhet.

Litteraturliste

Advokatforeningen, "Høringssvar – forslag til ny lov om Etterretningstjenestene", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=2eece877-1005-4269-9c81-2d91201eb1bf

Almås, Gry Blekstad, Digitalt diktatur, NrK, 05.02.19, https://www.nrk.no/urix/kinas-digitale-diktatur_-gar-du-pa-rodt-lys_-blir-du-uthengt-pa-storskjerm-1.14369439

Amnesty International, "Høringsuttalelse om Forslag til ny lov om Etterretningstjenestene", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=80ab5e7a-f6a0-456b-a925-fb28eec589c4

Arvesen, Eivind, "Regjeringens forklaringsproblem", *NrK Beta*, 18.02.2019, https://nrkbeta.no/2019/02/18/regjeringens-forklaringsproblem/?utm_source=NRKbeta+nyhetsbrev&utm_campaign=c839193aca-RSS_NRKbeta_DAILY&utm_medium=email&utm_term=0_91dcbbbf89-c839193aca-248369945, 15.03.2019.

Bakke-Jensen, Frank, "Balansegangen mellom samfunnssikkerhet og privatliv", *Digi.no*, 12.12.2018, https://www.digi.no/artikler/kommentar-balansegangen-mellom-samfunnssikkerhet-og-privatliv/453496, 15.03.2019.

Bakke-Jensen, Frank, "Kort sagt 29.november: Digitalt grenseforsvar", *Aftenposten,* 28.11.2017, https://www.aftenposten.no/meninger/debatt/i/BJJ6mQ/Kort-sagt_-onsdag-29-november, 20.03.2019

Borgarting lagmannsrett, "Høringssvar", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=48de27f0-2fb4-49db-af1f-d8996c7bf68a

Datatilsynet, "Høringsuttalelse", 06.02.19, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=e0b87829-2c74-4f2c-8066-c75801bcd0d5

Den internasjonale juristkommisjon – norsk avdeling (ICJ-Norge), " Høringsuttalelse – ny lov om etterretningstjenesten", https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=362e4e3c-b570-4dea-bac3-b99348898862

Den norske dataforening, "Høringssvar – ny lov om Etterretningstjenesten", 05.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=2a27751b-4586-4875-9780-dd70ccb88680

Elektronisk Forpost Norge, "Høringsbesvarelse", 11.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=e223a080-75b8-4c95-b327-611de68094db

EOS-utvalget, Årsrapport 2016, https://eos-utvalget.no/norsk/arsrapporter/content/text_14011994717841426512038624/1489492366181/_0804_001.pdf

EOS-utvalget, Årsrapport 2017, https://eos-utvalget.no/norsk/content/text_ed78f726-e398-40b4-89265e169ba74a64/1523359815630/_2017_eos_a_rsmelding_nett.pdf

Forsvarsdepartementet, "*Høring – Forslag til ny lov om Etterretningstjenesten",* 12.11.2018. https://www.regjeringen.no/contentassets/556459ec77bd448f828af034dd573e11/horingsnotat---forslag-til-ny-lov-om-etterretningstjenesten.pdf,

Friis, Karsten, "Digitalt Grenseforsvar: å gjøre ingenting er uansvarlig", NUPI, 04.02.2019, https://www.nupi.no/Nyheter/Digitalt-grenseforsvar-AA-gjoere-ingenting-er-uansvarlig, 10.03.2019.

Gerhardsen, Sarah McDonald, "71 av 89 høringssvar er kritiske til ny e-lov", *digi.no,* 06.03.2019, https://www.digi.no/artikler/71-av-89-horings-svar-er-kritiske-til-ny-e-lov-her-er-oversikten-og-argumentene/459613, 15.03.2019

Granick, Jennifer Stisa, "Mass Spying Isn't Just Intrusive – It's Ineffective", *American Spies: Modern Surveillance, Why You Should Care, and What to Do About It,* Sitert i Wired.com 03.02.2017, https://www.wired.com/2017/03/mass-spying-isnt-just-intrusive-ineffective/, 15.03.2019.

Guariglia, Matthew, "Too much surveillance makes us less free. It also makes us less safe", *The Washington Post,* 18.07.2017, https://www.washingtonpost.com/news/made-by-history/wp/2017/07/18/too-much-surveillance-makes-us-less-free-it-also-makes-us-less-safe/?noredirect=on&utm_term=.d93e2ee4d91c

Indregaard, Sigve, *Vi kan ikke se den grense inni nettet*, Morgenbladet, 13. oktober 2018, https://morgenbladet.no/aktuelt/2017/10/indregard-allkopi-pa-grensen

Indregaard, Sigve, *"Å stoppe hacking ved hekken",* Morgenbladet, 17. februar 2017, https://morgenbladet.no/aktuelt/2017/02/stoppe-hackingen-ved-hekken

Julsrud, Åsne, Erland Flaterud, Elizabeth Baumann, Anne Horn, Heidi Heggdal, Finn-Arne Selfors, " Høringsuttalelse til forslag om ny lov for Etterretningstjenesten", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=9791d23a-b98f-464e-abf8-2c8080bb582f

Kripos, "Høringssvar – forslag til ny lov om Etterretningstjenesten", 18.02.2019, https://www.regjeringen.no/contentassets/287d2d52ddb847849cddb49796456129/horingssvar-med-merknader---kripos.pdf?uid=Kripos

Kristiansen, Bjørn S., "Ber nordmenn stole på staten", Dagsavisen, 09.02.2019, https://www.dagsavisen.no/helg-nye-inntrykk/ettertanke/ber-nordmenn-stole-pa-staten-1.1275574?paywall=true, 15.03.2019

Lunde, Morten Haga, "Frykter du overvåkingssamfunnet? Utkast til ny e-lov bør berolige deg", *Aftenposten,* 04.02.2019, https://www.aftenposten.no/meninger/debatt/i/4dpVVg/Frykter-du-overvakingssamfunnet-Utkastet-til-ny-e-lov-bor-berolige-deg--Morten-Haga-Lunde, 15.03.2019

Lyon, David, "Surveillance after Snowden", *Polity Press,* Cambridge, 2015.

Lysne, Olav, Christian Reuch, Eva Jarbekk, Einar Lunde, Trond Grytting, "Derfor bør Norge etablere et digital grenseforsvar", *Aftenposten,* 05.09.2016, https://www.aftenposten.no/meninger/debatt/i/LL6wx/Derfor-bor-Norge-etablere-et-digitalt-grenseforsvar?spid_rel=2, 15.03.2019

Nasjonal Kommunikasjonsmyndighet Nkom, "Høringssvar – forslag til ny lov om Etterretningstjenesten", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=db44a957-54a6-47c4-9afc-d53f684826cd

Norges Forsvarsforening, " Etterretningssjefen:-Dataangrep mot Helse Sør-Øst kunne vært avverget", 05.03.2018, https://www.forsvarsforeningen.no/nyheter/etterretningssjefen-dataangrepet-mot-helse-sor-ost-kunne-ha-vaert-avverget/, 15.03.2019

Norsk Institusjon for menneskerettigheter, " Høringsuttalelse til e-loven", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=1b03fe18-1d1e-4be5-a7ce-5f1dc785695a

Norsk Journalistlag, "Høringsuttalelse om ny lov om Etterretningstjenesten", 08.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=881aaf63-58f1-4783-8c03-631c5f14c38f

NRK, "Høringsuttalelse fra NrK", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=dc790b05-c48e-4086-8352-e50f989d2268

Norsk Senter for Informasjonssikring, "Høringssvar til ny lov om Etterretningstjenesten", 31.01.2019. https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=efe41610-0c1b-4873-bd64-cbad381059fa

NUPI, "Høringssvar", 30.01.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=d4630119-b015-4ef7-8110-60be2a90c0be

PEN America Center, "Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor", 12.11.2013, https://pen.org/sites/default/files/2014-08-01_Full%20Report_Chilling%20Effects%20w%20Color%20cover-UPDATED.pdf

Penney, Jon, "Chilling effects: online Surveillance and Wikipedia Use", *Berkeley Technology Law Journal,* 2016, Vol. 31, No. 1, 117

Penney, Jonathon W., "Internet surveillance, regulation, and chilling effects online: a comparative case study", *Internet Policy Review - Journal of internet regulation*, May 2017, Volume 6, issue 2, https://policyreview.info/node/692/pdf

Regjeringen.no, "Spørsmål og svar om ny lov om Etterretningstjenesten og særlig om tilrettelagt innhenting", https://www.regjeringen.no/contentassets/41961c273e824333ac5c6e04cd65da2d/qa-e-lov.pdf

Riksadvokatembetet, "Høring – forslag til ny lov om etterretningstjenesten", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=26e56eae-1e99-4300-8ff1-368ff7802abc

SINTEF, "Høringsuttalelse vedrørende forslag til ny lov om Etterretningstjenesten", 18.02.2019, https://www.regjeringen.no/contentassets/287d2d52ddb847849cddb49796456129/horingssvar-med-merknader---sintef.pdf?uid=SINTEF

Stahl, Titus, "Indiscriminate mass surveillance and the public sphere", *Ethics and Information Technology*, March 2016, Volume 18, Issue 1, 34 – 35

TEKNA – Teknisk-naturvitenskaplig forening, "Høringsinnspill til lov om Etterretningstjenesten", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=c576f91f-c92d-4001-bc64-4c164fcd0717

Telenor Norge AS, "Høringssvar", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=cc113e20-03fe-4674-9055-a949da9e9505

Sluttnoter

1 Til sammenligning fikk forslaget til ny straffeprosesslov (NOU 2016: 24) frist på seks måneder. Flere instanser har påpekt eller kritisert den korte fristen: Amnesty, Befalets fellesorganisasjon, Datatilsynet, Den internasjonale juristkommisjon – norsk avdeling (ICJ-Norge), Den norske dataforening, Elektronisk forpost, International Comission of Jurists (ICJ) Norge - studentnettverk Bergen, Kripos, PST, NRK, Norges institusjon for menneskerettigheter, Norsk Presseforbund, Norsk redaktørforening, Oslo Tingrett, Piratpartiet , STAFO Etatsforeningen

2 Noen forenklinger har vært nødvendig, og jeg refererer derfor gjennomgående til supplerende kilder. Alle eventuelle feil og overforenklinger er mitt ansvar alene.

3 Det er også foreslått endringer i unntaksbestemmelsene, nærmere presentert i Hørinsgforslagets kapittel 8.

4 Forsvarsdepartementet, *"Høring – Forslag til ny lov om Etterretningstjenesten"*, 12.11.2018, https://www.regjeringen.no/contentassets/556459ec77bd448f828af034dd573e11/horingsnotat---forslag-til-ny-lov-om-etterretningstjenesten.pdf, 16.

5 Sitat Forsvarsdepartementet, "Høring – Forslag til ny lov om Etterretningstjenesten", 12.11.2018, 221

6 Det må påpekes at en av de mest betente stridstema i debatten er i hvilken grad lovforslaget er akseptabelt under Grunnloven, Den europeiske Menneskerettighetskonvensjonen (EMK) og Den europeiske menneskerettsdomstolen. Det er usikkert i hvilken grad omfanget av overvåkning er balansert mot inngrepet i personvernet og underlagt de nødvendige kontrollmekanismene. Domsavgjørelsene begge partene primært refererer til er i EU domstolens storkammer etter anke.

7 Også kalt sammensatte trussler. Aktøren benytter samler en rekke ulike virkemidler, for eksempel politiske, økonomiske, militære, sivile og informasjonsmessige, for å nå sitt mål. Dette kan for eksempel være svekking av demokratiske institusjoner, samfunnsmessig tillit eller lignende.

8 Geopolitisk polarisering og endring i sikkerhetsallianser, fake news, digital propaganda og valgpåvirkning, hacking. For å nevne noe.

9 Norges Forsvarsforening, "Etterretnigssjefen:-Dataangrep mot Helse Sør-Øst kunne vært avverget", 05.03.2018, https://www.forsvarsforeningen.no/nyheter/etterretningssjefen-dataangrepet-mot-helse-sor-ost-kunne-ha-vaert-avverget/, 15.03.2019

10 Frank Bakke-Jensen, "Balansegangen mellom samfunnssikkerhet og prvatliv", Digi.no, 12.12.2018, https://www.digi.no/artikler/kommentar-balansegangen-mellom-samfunnssikkerhet-og-privatliv/453496, 15.03.2019.

11 Morten Haga Lunde, "Frykter du overvåkningssamfunnet? Utkast til ny e-lov bør berolige deg", Aftenposten, 04.02.2019, https://www.aftenposten.no/meninger/debatt/i/4dpVVg/Frykter-du-overvakingssamfunnet-Utkastet-til-ny-e-lov-bor-berolige-deg--Morten-Haga-Lunde, 15.03.2019

12 Eivind Arvesen, "Regjeringens forsklaringsproblem", NrK Beta, 18.02.2019, https://nrkbeta.no/2019/02/18/regjeringens-forklaringsproblem/?utm_source=NRKbeta+nyhetsbrev&utm_campaign=c839193aca-RSS_NRKbeta_DAILY&utm_medium=email&utm_term=0_91dcbbbf89-c839193aca-248369945 , 15.03.2019.

13 Forsvarsdepartementet, "Høring – Forslag til ny lov om Etterretningstjenesten", 12.11.2018, 149

14 Kommersielle aktører besitter store mengder data om individer. Det er svært sannsynlig at Etterretningstjenester internasjonalt både kjøper og tilegner seg disse dataene. Dette er et svært komplekst og kontroversielt tema. Men fordi det ikke er adressert i høringsforslaget har jeg av plassgrunner valgt å se bort fra dette aspektet i notatet.

15 Hårek Elvenes, sitert i Sigve Indregaard, *"Å stoppe hacking ved hekken",* Morgenbladet, 17. februar 2017, https://morgenbladet.no/aktuelt/2017/02/stoppe-hackingen-ved-hekken

16 NUPI, "Høringssvar", 30.01.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=d4630119-b015-4ef7-8110-60be2a90c0be

17 Lovforslaget skisserer at aktører som faller under ekomloven paragraf 1-5 nr. 16 og "Tilbydere av internettbaserte kommunikasjon- og meldingstjenester som er tilgjengelig for allmenheten"(OTT-tjenester som brukes til overføring av tekst, lyd og bilder) skal måtte bistå etterretningstjenesten. Det er svært uklart hvem som vil omfattes og i hvilken grad de må bistå. På grunn av plassutfordringer har jeg måttet prioritere ned denne viktige debatten, men den er behørlig behandlet i flere høringsuttalelser, for eksempel fra Datatilsynet.

18 Datatilsynet, "Hørinsuttalelse", 06.02.19, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=e0b87829-2c74-4f2c-8066-c75801bcd0d5, 10

19 Forsvarsdepartementet, *"Høring – Forslag til ny lov om Etterretningstjenesten",* 12.11.2018, 136

20 Tilrettelagt innhenting består av tre ulike datalager: Korttidslagret som lagrer innhold- og metadata for filtrering og teknisk utvikling; Metadatalagret som inneholder data etter passering av filter 2. Lageret inneholder 18 måneder med grensekryssende kommunikasjon. Søk krever domstolgodkjenning og baserer seg på personer og virksomheter (personseleketorer) eller for eksempel handlingsmønster og geografisk område (modusselektorer); og Innholdslagret: innholdsdata med tilhørende metadata etter passering av filter 3. Data må være målrettet mot spesifikt objekt og lagring krever domstolens godkjenning. Datatilsynet, *"Høringsuttalelse",* 06.02.19, 11 – 12

21 Tre filtre skal redusere datamengden innsamlet med tilrettelagt Innhenting: Filter 1 fjerner ikke-relevant data gjennom negativ filtrering, eksempelvis trafikk fra strømmetjenester. Filter 2 skal fjerne innholdsdata samt metadata utenfor e-tjenestens område. Det er en automatisk filtrering basert på e-tjenestens definisjoner og påfølgende liste av metadata. Filter 3 siler ut innholdsdata knyttet til domstolgodkjente overvåkingsobjekter. Datatilsynet, *"Høringsuttalelse",* 06.02.19, 10 – 11

22 Ønsker du en nyttig gjennomgang av de ulike lagrene og filterne anbefaler jeg Abelias eller Datatilsynets høringssvar https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?expand=horingssvar&lastvisited=e0b87829-2c74-4f2c-8066-c75801bcd0d5

23 Regjeringen.no, "Spørsmål og svar om ny lov om Etterretningstjenesten og særlig om tilrettelagt innhenting", https://www.regjeringen.no/contentassets/41961c273e824333ac5c6e04cd65da2d/qa-e-lov.pdf, punkt 30. Besøkt 05.04.2019.

24 Sigve Indregaard, *Vi kan ikke se den grense inni nettet*, Morgenbladet, 13. oktober 2018, https://morgenbladet.no/aktuelt/2017/10/indregard-allkopi-pa-grensen

25 Sigve Indregaard, *Vi kan ikke se den grense inni nettet*, Morgenbladet, 13. oktober 2018,

26 Telenor Norge AS, "Høringssvar", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=cc113e20-03fe-4674-9055-a949da9e9505

27 Den norske dataforening, "Høringssvar – ny lov om Etterretningstjenesten", 05.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=2a27751b-4586-4875-9780-dd70ccb88680, 1

28 For teleforner kan man for eksempel filtrere bort kommunikasjon hvor både sender og mottaker benytter landkode +47. Men det vil åpenbart være en metode med store svakheter og det eksisterer ingen tilsvarende sorteringsvariabel for internettsøk, epost, sosiale medier etc.

29 Forsvarsdepartementet ibekrefter dette i høringsnotatet s.136, dog de på s. 137 mener at overskuddsinformasjon relatert til norske rettsubjekter vil være meget liten.

30 Digtalt Grenseforsvar er dermed, etter min menig, mye mer dekkende begrepsbruk for hva lovforslaget innebærer enn tilrettelagt innhenting. Datatilsynet har på sin side valgt å beskrive datalagringen som "Digital masseovervåkning"

31 Det åpnes for at rådata kan lagres i 15 år, med mulighet for forlengelse hvis Etterretningssjefen anser det som nødvendig, samt at sletting kun skal være fra operative systemer.

32 Forsvarsdepartementet, *"Høring – Forslag til ny lov om Etterretningstjenesten",* 12.11.2018, 137

33 Norsk Senter for Informasjonssikring, *Høringssvar til ny lov om Etterretningstjenesten,* 31.01.2019. https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=efe41610-0c1b-4873-bd64-cbad381059fa , 2.

34 Amnesty International, "Høringsuttalelse om Forslag til ny lov om Etterretningstjenestene", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=80ab5e7a-f6a0-456b-a925-fb28eec589c4 , 1

35 Forsvarsdepartementet, "*Høring – Forslag til ny lov om Etterretningstjenesten",* 12.11.2018, 42.

36 Amnesty International, "Høringsuttalelse om Forslag til ny lov om Etterretningstjenestene", 12.02.2019, 1

37 Respekt for privatliv er både grunnlovsfestet i §102 og fastslått i Den europeiske menneskerettskonvensjonen (EMK) artikkel 8. Også vern av kilder med påfølgende konsekvenser for ytringsfriheten kan bli problematisk. Visse former for overvåkning antas også å kunne gjøre et inngrep i forenings- og forsamlingsfriheten etter Grunnlovens § 101 og EMK artikkel 11, eller religionsfriheten etter Grunnlovens § 16 og EMK artikkel 9. Forsvarsdepartementet, "*Høring – Forslag til ny lov om Etterretningstjenesten",* 12.11.2018, 34

38 Elektronisk Forpost Norge, "Høringsbesvarelse", 11.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=e223a080-75b8-4c95-b327-611de68094db, 5

39 Datatilsynet refererte blant annet til denne studien i sin Lysne II-høringsuttalelse

40 Forutsatt lovforslagets to kommunikasjonsledd og 18 måneders lagringstid.

41 Forsvarsdepartementet, "*Høring – Forslag til ny lov om Etterretningstjenesten",* 12.11.2018, 285

42 Kripos, "Høringssvar – forslag til ny lov om Etterretningstjenesten", 18.02.2019, https://www.regjeringen.no/contentassets/287d2d52ddb847849cddb49796456129/horingssvar-med-merknader---kripos.pdf?uid=Kripos , 6

43 Forsvarsdepartementet, "*Høring – Forslag til ny lov om Etterretningstjenesten",* 12.11.2018, 273

44 Forsvarsdepartementet, "*Høring – Forslag til ny lov om Etterretningstjenesten",* 12.11.2018, 272

45 Jonathon W. Penney, "Internet surveillance, regulation, and chilling effects online: a comparative case study", Internet Policy Review - Journal of internet regulation, May 2016, Volume 6, issue 2, https://policyreview.info/node/692/pdf , 8

46 *I would be more careful about what I say or discuss in certain contexts online*" :"strongly" agreeing (38%) or "somewhat" agreeing (40%) with that statement. (sitat Penney, 2016:9). "*Government monitoring of online activities would make them "more careful" about what they "search for online"*: strongly agree" (40%) and "somewhat agree" (38%) (sitat Penney, 2016:11).

47 Forsvarsdepartementet, "*Høring – Forslag til ny lov om Etterretningstjenesten",* 12.11.2018, 273

48 Forsvardepartementet trekker frem noen viktige metodiske utfordringer, som for eksempel subjektive vurderinger i spørreundersøkelser. At vi ikke kan påvise en direkte kausalitet betyr ikke at sterke tendenser kan ignoreres. Kontrollerte eksperimenter er uetisk og forskningssubjektene (mennesker) lever ikke i et vakum. Alle studier må gjennomføres etter etablerte standarder i samfunnsvitenskapene, men det blir overfladisk å konkludere med at nedkjølingseffekten ikke eksisterer fordi man filtrerer etter svært strenge søkekriterier.

49 Jon Penney, "Chilling effects: online Surveillance and Wikipedia Use", *Berkeley Technology Law Journal,* Vol. 31, No. 1, 117

50 Studien fokuserte kun på en begrenset tidsperiode. Funn er sitert i Jon Penney, "Chilling effects: online Surveillance and Wikipedia Use", *Berkeley Technology Law Journal, 2016,* Vol. 31, No. 1, 131 – 133

51 Rapporteringen har selvfølgelig potensielle metodiske utfordringer og det er usikker om effekten holder seg over tid, om utvalget er representativt etc. Men tallene er såpass dramtiske at indikasjonen studien gir bør tas på alvor.

52 PEN America Center, *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*, 12.11.2013, https://pen.org/sites/default/files/2014-08-01_Full%20Report_Chilling%20Effects%20w%20Color%20cover-UPDATED.pdf

53 *"92% believe that personal data collected by the government will be vulnerable to abuse for many years because it may never be completely erased or safeguarded"* (sitat PEN, 2013)

54 Jonathon W. Penney, *Chilling effects: Online Surveillance and Wikipedia Use*, 27. april 2016.

55 Sitat Forsvarsdepartementet, *"Høring – Forslag til ny lov om Etterretningstjenesten",* 12.11.2018, 274

56 Hårek Elvenes, i Sigve Indregaard, *"Å stoppe hacking ved hekken" og* og Bjørn S. Kristiansen, "Ber nordmenn stole på staten", Dagsavisen, 09.02.2019, https://www.dagsavisen.no/helg-nye-inntrykk/ettertanke/ber-nordmenn-stole-pa-staten-1.1275574?paywall=true

57 Forsvarsdepartementet, *"Høring – Forslag til ny lov om Etterretningstjenesten",* 12.11.2018, 273

58 NRK, "Høringsuttalelse fra NRK", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=dc790b05-c48e-4086-8352-e50f989d2268, 8

59 Norsk Journalistlag, "Høringsuttalelse om ny lov om Etterretningstjenesten", 08.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=881aaf63-58f1-4783-8c03-631c5f14c38f

60 Datatilsynet, *"Høringsuttalelse",* 06.02.19, 21 og 37

61 Altså underlagt tilretteleggingsplikten

62 Datatilsynet, *"Høringsuttalelse",* 06.02.19, 21 og 37

63 Sitat Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016 punkt 6.2 s. 34, sitert i Forsvarsdepartementet, *"Høring – Forslag til ny lov om Etterretningstjenesten",* 12.11.2018.

64 Datatilsynet, *"Høringsuttalelse",* 06.02.19, 23

65 Sitat Forsvarsdepartementet, *"Høring – Forslag til ny lov om Etterretningstjenesten",* 12.11.2018, 264 – 265

66 Kripos, "Høringssvar – forslag til ny lov om Etterretningstjenesten", 18.02.2019, 10

67 Frank Bakke-Jensen, "Kort sagt 29.november: Digitalt grenseforsvar", *Aftenposten,* 28.11.2017, https://www.aftenposten.no/meninger/debatt/i/BJJ6mQ/Kort-sagt_-onsdag-29-november, 20.03.2019.

68 Forsvarsdepartementet, *"Høring – Forslag til ny lov om Etterretningstjenesten",* 12.11.2018, 152

69 Se høringsforslaget side 195 – 210.

70 Matthew Guariglia, "Too much surveillance makes us less free. It also makes us less safe", *The Washington Post,* 18.07.2017, https://www.washingtonpost.com/news/made-by-history/wp/2017/07/18/too-much-surveillance-makes-us-less-free-it-also-makes-us-less-safe/?noredirect=on&utm_term=.d93e2ee4d91c

71 Her kan man argumentere med at fremveksten av Artifical intelligence og maskinlæring bøter på dette, men det skaper igjen en rekke andre dilemma knyttet til for eksempel bias og domstolskontroll av maskinlæring.

72 Det samme fant *the President's Review Group on Intelligence and Communications Technologies,* som analyserte terroristhendelser fra 2001 til 2013. Se også for eksempel policy paper *Do NSA's Bulk Surveillance Programs Stop Terrorists?* Av Cahall et. Al. (2014) eller *What's the evidence mass surveillance works? Not Much* av Kirchner (2015) for ProPublica.

73 Forsvarsdepartementet, *"Høring – Forslag til ny lov om Etterretningstjenesten",* 12.11.2018, 303

74 TEKNA – Teknisk-naturvitenskaplig forening, "Høringsinnspill til lov om Etterretningstjenesten", 12.02.2019.

75 For eksempel så kan man argumentere for at bedre informasjonssikring i norsk næringsliv og offentlige etater vil forhindre mer spionasje og dataangrep enn etterretningstjenestens tilgang på grenseoverskridende elektronisk informasjon.

76 TEKNA – Teknisk-naturvitenskaplig forening, "Høringsinnspill til lov om Etterretningstjenesten", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=c576f91f-c92d-4001-bc64-4c164fcd0717

77 Hvordan skiller man for eksempel de som bare er nysgjerrige fra de som faktisk blir radikalisert? Det strider mot nordmenns rettsfølelse at alle som besøker for eksempel en viss nettside, forum eller ser en YouTube-film skal registreres og kunne overvåkes. Særlig når den enkelte legmann ikke har muligheten til å vite hvilke sider som "flagger deg".

78 Den internasjonale juristkommisjon – norsk avdeling (ICJ-Norge), "Høringsuttalelse – ny lov om etterretningstjenesten", https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=362e4e3c-b570-4dea-bac3-b99348898862, 3

79 Morten Haga Lunde, "Frykter du overvåkingssamfunnet? Utkast til ny e-lov bør berolige deg", *Aftenposten,* 04.02.2019, 15.03.2019

80 Forsvarsdepartementet, "Høring – Forslag til ny lov om Etterretningstjenesten", 12.11.2018, 180 – 181.

81 Sitat Forsvarsdepartementet, "Høring – Forslag til ny lov om Etterretningstjenesten", 12.11.2018, 180

82 EOS-utvalget, Årsrapport 2017, https://eos-utvalget.no/norsk/content/text_ed78f726-e398-40b4-89265e169ba74a64/1523359815630/_2017_eos_a_rsmelding_nett.pdf, 10

83 EOS-utvalget, Årsrapport 2016, https://eos-utvalget.no/norsk/arsrapporter/content/text_1401199471784142651203862 4/1489492366181/_0804_001.pdf

84 EOS-utvalget, Årsrapport 2017,, 9

85 Datatilsynet, "*Høringsuttalelse",* 06.02.19, 44

86 Nasjonal Kommunikasjonsmyndighet Nkom, "Hørinsgsvar – forslag til ny lov om Etterretningstjenesten", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=db44a957-54a6-47c4-9afc-d53f684826cd, 4

87 EOS-utvalget skriver i sin høringsuttalelse at de ønsker minst seks årsverk samt styrking av sekretariatetteknisk kompetanse.

88 Forsvarsdepartementet, "*Høring – Forslag til ny lov om Etterretningstjenesten",* 12.11.2018, 299 – 303

89 Advokatforeningen, "Høringssvar – forslag til ny lov om Etterretningstjenestene", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=2eece877-1005-4269-9c81-2d91201eb1bf, 3

90 Datatilsynet, "*Høringsuttalelse",* 06.02.19, 2

91 Borgarting lagmannsrett, "Høringssvar", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=48de27f0-2fb4-49db-af1f-d8996c7bf68a, 1

92 Datatilsynet, "*Høringsuttalelse",* 06.02.19, 41

93 Bla Julsrud et. al og Advokatforeningen, "Høringssvar – forslag til ny lov om Etterretningstjenestene", 12.02.2019, 3 – 5

94 Person- og moduselektorer

95 Norsk Institusjon for menneskerettigheter, "Høringsuttalelse til e-loven", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=1b03fe18-1d1e-4be5-a7ce-5f1dc785695a, 28

96 Advokatforeningen, "Høringssvar – forslag til ny lov om Etterretningstjenestene", 12.02.2019, 8

97 Forsvarsdepartementet, "*Høring – Forslag til ny lov om Etterretningstjenesten",* 12.11.2018, 86

98 Elektronisk Forpost Norge, "Høringsbesvarelse", 11.02.2019, 5

99 David Lyon, "Surveillance after Snowden", *Polity Press,* 2015.

100 SINTEF, Høringsuttalelse vedrørende forslag til ny lov om Etterretningstjenesten", 18.02.2019, https://www.regjeringen.no/contentassets/287d2d52ddb847849cddb49796456129/horingssvar-med-merknader---sintef.pdf?uid=SINTEF , 4

101 Lysne et. al, "Defor bør Norge etablere et digital grenseforsvar", *Aftenposten,* 05.09.2016, https://www.aftenposten.no/meninger/debatt/i/LL6wx/Derfor-bor-Norge-etablere-et-digitalt-grenseforsvar?spid_rel=2, 15.03.2019

102 Dette poenget trekkes frem i flere høringssvar, for eksempel av Tekna.

103 Karsten Friis, "Digitalt Grenseforsvar: å gjøre ingenting er uansvarlig", NUPI, 04.02.2019, https://www.nupi.no/Nyheter/Digitalt-grenseforsvar-AA-gjoere-ingenting-er-uansvarlig, 10.03.2019.

104 89 innsendelser, 12 svar fremstår nøytrale eller uten merknad. Sarah McDonald Gerhardsen, "71 av 89 høringssvar er kritiske til ny e-lov", *digi.no*, 06.03.2019, 15.03.2019

105 Riksadvokatembetet, "Høring – forslag til ny lov om etterretningstjenesten", 12.02.2019, https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=26e56eae-1e99-4300-8ff1-368ff7802abc, 2

106 For eksempel forståelsen av hva en territoriell grense er. For å sitere Sigve Indregard i Morgenbladet "Vi kan ikke se den grensen inni nettet", *Morgenbladet* 13. oktober 2017.