STORTINGET

Innst. 386 S

(2017–2018)

Innstilling til Stortinget
fra helse- og omsorgskomiteen

Dokument 8:197 S (2017–2018)

Innstilling fra helse- og omsorgskomiteen om Representantforslag fra stortingsrepresentantene Kjersti Toppe, Emilie Enger Mehl, Per Olaf Lundteigen, Nicholas Wilkinson, Torgeir Knag Fylkesnes og Mona Fagerås om å be regjeringen definere grunnleggende IKT-infrastruktur i helseforetakene inn under sikkerhetsloven

Til Stortinget

Bakgrunn

I dokumentet fremmes følgende forslag:

«1. Stortinget ber regjeringen definere IKT-infrastrukturen i helseforetakene inn under krav i sikkerhetsloven om skjermingsverdig informasjon.
2. Stortinget ber regjeringen sikre at informasjon knyttet til nasjonale sikkerhetsinteresser blir driftet og lagret i Norge.
3. Stortinget ber regjeringen sikre at outsourcing av utvikling og drift av kritiske nasjonale IKT-tjenester og system i helsesektoren avsluttes og at nye avtaler ikke kan inngås.»

Forslagsstillerne viser til at IKT-skandalen i Helse Sør-Øst har ført til at uvedkommende har kunnet få tilgang til sensitive pasientdata om 2,8 millioner nordmenn som hører til Helse Sør-Østs område. Dermed har sensitiv pasientinformasjon kunnet komme på avveie, og uvedkommende har kunnet kartlegge en infrastruktur som kunne brukes til sabotasje for å lamme Norge. Forslagsstillerne mener Norge må ta lærdom av dette og sikre at grunnleggende IKT-infrastruktur i helsesektoren blir definert som kritisk nasjonal infrastruktur som kommer inn under sikkerhetsloven. Fremtidig outsourcing av utvikling og drift av kritiske nasjonale IKT-tjenester og system innenfor helsesektoren må avverges.

8. januar 2018 ble Sykehuspartner, som er et foretak under Helse Sør-Øst RHF, varslet om at det pågikk unormal aktivitet i datasystemene i regionen. Helseforetaket mistenkte at profesjonelle sto bak, og PST og Kripos ble koblet inn i saken (NRK 16. januar 2018).

Forslagsstillerne mener at IKT-skandalen i Helse Sør-Øst har vist at lovverk og departementets praksis ikke sikrer helseopplysningene til Norges befolkning godt nok, og at dette utgjør en fare for rikets sikkerhet. At helseopplysningene til halve Norges befolkning ikke har vært trygge, rokker ved tilliten til helsevesenet. Forslagsstillerne mener at forsvarlig behandling av helseopplysninger er en av kjerneoppgavene til helsevesenet.

Forslagsstillerne viser til at helse- og omsorgsministeren i redegjørelsen i Stortinget 30. januar 2018 om IKT-skandalen og senere i media uttalte at helseforetakene var underlagt sikkerhetsloven.

Svaret i Dokument nr. 15:902 (2017–2018) klargjør at statsrådens forsikringer om at helseforetakene er lagt inn under sikkerhetsloven, ikke betyr at IKT-infrastrukturen blir underlagt sikkerhetsloven. Forslagsstillerne mener at IKT-infrastrukturen i helseforetakene klart må defineres som samfunnskritisk infrastruktur.

Komiteens merknader

Komiteen, medlemmene fra Arbeiderpartiet, Elise Bjørnebekk-Waagen, Tore Hagebakken, Ingvild Kjerkol, Tuva Moflag og Tellef Inge Mørland, fra Høyre, Torill

Eidsheim, Astrid Nøklebye Heiberg, Erlend Larsen og Sveinung Stensland, fra Fremskrittspartiet, Bård Hoksrud og Sylvi Listhaug, fra Senterpartiet, Hans Inge Myrvold, fra Sosialistisk Venstreparti, Sheida Sangtarash, fra Venstre, Carl-Erik Grimstad, og fra Kristelig Folkeparti, lederen Olaug V. Bollestad, ser at forslagsstillerne her peker på Helse Sør-Østs håndtering av IKT-infrastrukturen. Komiteen viser til at alle de regionale helseforetakene har et overordnet ansvar for å sikre pasientinformasjonen de forvalter, og se til at systemene er oppdatert og blir utviklet på en slik måte at de ivaretar behovet for en trygg og effektiv IKT-infrastruktur. Det er viktig at man har tatt lærdom av uheldig informasjonshåndtering og sikrer at helseforetakene vil rigge en sikker og god utvikling av sin IKT-infrastruktur.

Komiteen ønsker å understreke at for å sikre effektivisering gjennom økt digitalisering av det norske samfunnet må IKT-løsninger og digitale tjenester være tilstrekkelig sikre og pålitelige. Virksomheter og privatpersoner må ha tillit til at systemer og nettverk både fungerer slik de skal, og ivaretar personvernet til den enkelte. God IKT-sikkerhet og evne til å håndtere uønskede digitale hendelser er en forutsetning for å oppnå denne tilliten.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Høyre, Fremskrittspartiet, Sosialistisk Venstreparti, Venstre og Kristelig Folkeparti, viser til at en vesentlig oppgave for regjeringen er å sikre en bærekraftig helsetjeneste. Det krever at man legger forholdene til rette for å ta i bruk de fremste metoder og benytte den teknologiutviklingen som skjer. Da må vi forholde oss til at mye av dette skjer og tilbys internasjonalt.

Et annet flertall, medlemmene fra Høyre, Fremskrittspartiet, Venstre og Kristelig Folkeparti, ser det slik at en avgrensning av drift, som forslagsstillerne her viser til, kan synes svært vanskelig. Foretakene har i dag ansvaret for å drifte, forvalte og utvikle IKT-infrastrukturen. Helsesektoren er i tillegg gjennomgående avhengig av internasjonal teknologi, både for maskinvare, basis programvare og systemer. Dette flertallet vil peke på at det kan synes vanskelig å overskue alle de ulike konsekvenser av et vedtak i tråd med dette representantforslaget. Dette flertallet vil understreke at eventuelle avgrensninger og endringer i lovverket for IKT-infrastrukturen i helseforetakene må utredes grundig før det kan konkluderes om det vil kunne bidra til ønsket utvikling av et moderne og sikkert helsevesen.

Komiteens medlemmer fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti viser til at IKT-skandalen i Helse Sør-Øst har vist at lovverk og departementets praksis ikke sikrer helseopplysningene til Norges befolkning godt nok, og at dette utgjør en fare for rikets sikkerhet. Disse medlemmer vil understreke at det ikke bare er helseforetakene som må ta lærdom, men også helseforetakenes eier, staten. Disse medlemmer viser til at den øverste ansvarlige for sikker forvaltning av nordmenns helseopplysninger er regjeringen ved helseministeren.

Disse medlemmer viser til at outsourcingen som ble gjennomført i Helse Sør-Øst av grunnleggende IKT-infrastruktur, ble gjort uten at statsråden som øverste ansvarlige eller andre involverte klart kunne redegjøre for hva som faktisk ble outsourcet (jf. bl.a. interpellasjonsdebatt i Stortinget 30. januar 2018). Dette er alvorlig. Resultatet av outsourcingen var et grovt tillitsbrudd overfor befolkningen med pasientinformasjon til 2,8 millioner personer på avveie. Helse Sør-Øst har måttet betale minst 280 mill. kroner til selskapet de hadde inngått kontrakt med, etter at prosjektet ble satt på vent. Kostnadene knyttet til hele prosessen er langt høyere og sluttsummen ikke klar på lenge enda. Dette er høye summer som må dekkes over offentlige budsjetter og kan gå ut over annen sykehusdrift. Disse medlemmer mener alvoret i denne situasjonen tilsier at det må komme endringer i hvordan vi forvalter grunnleggende IKT-infrastruktur i helseforetakene, og befolkningen må kunne være trygg på at deres pasientinformasjon er ivaretatt på beste måte. Derfor må IKT-infrastruktur inn under krav i sikkerhetsloven, systemer knyttet til nasjonale sikkerhetsinteresser må driftes og lagres i Norge, og outsourcing av utvikling og drift av kritiske nasjonale IKT-tjenester og system i helsesektoren må avsluttes og nye avtaler ikke inngås.

Disse medlemmer mener det er spesielt at flertallet i Stortingets behandling av denne alvorlige saken skriver at avgrensningen av drift «kan synes svært vanskelig» uten én eneste kilde, ett eneste støttende høringssvar eller andre fakta. Eksperter fra NITO, El- og IT-forbundet, Fagforbundet og Legeforeningen har levert høringssvar og er uenige med flertallet og mener forslaget kan gjennomføres.

Sikkerhetsloven og grunnleggende IKT-infrastruktur

Komiteen viser til forslag 1 i representantforslaget, om å be regjeringen definere IKT-infrastrukturen inn under krav i sikkerhetsloven om skjermingsverdig informasjon.

Komiteen viser til statsrådens redegjørelse 30. januar 2018 om IKT-saken i Helse Sør-Øst, der det ble understreket at Helse- og omsorgsdepartementet etter sikkerhetsloven har ansvaret for forebyggende sikkerhet i helse- og omsorgssektoren. Departementet gjennomførte i 2014 en vurdering av sikkerhetslovens anvendelse for de regionale helseforetakene, helsefore-

takene og Norsk Helsenett SF. NSM bistod med råd og veiledning i denne vurderingen. Konklusjonen var at departementet anså at de regionale helseforetakene, helseforetakene og Norsk Helsenett SF var omfattet av sikkerhetsloven, jf. sikkerhetsloven § 2 første ledd. Dette innebærer at virksomhetene er omfattet av sikkerhetsloven med tilhørende forskrifter. Virksomhetene fikk ansvaret for å iverksette og utøve forebyggende sikkerhetstjeneste fra desember 2014.

Komiteen merker seg at vurderinger av forvaltning og drift av IKT-infrastrukturen i helseforetakene i dag gjøres innenfor rammen av sikkerhetsloven. I vurderingen av om hele eller deler av IKT-infrastrukturen er skjermingsverdig, er det avgjørende om det kan skade grunnleggende nasjonale funksjoner om funksjonen får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse.

Komiteen viser også til at vurderingen av sikkerhetsnivå og behov for forebyggende sikkerhetstiltak knyttet til IKT-infrastrukturen i helseforetakene vil kunne falle inn under krav i sikkerhetsloven om skjermingsverdig informasjon og vil således kunne være gradert informasjon. Dette er vurderinger som de regionale helseforetakene, helseforetakene og Helse- og omsorgsdepartementet arbeider med i samarbeid med NSM, Norsk Helsenett SF, Helsedirektoratet, Direktoratet for e-helse og Sykehusbygg HF.

Komiteens medlemmer fra Høyre, Fremskrittspartiet og Venstre viser til at først når dette er klart, vil det være naturlig å vurdere organiseringen.

Disse medlemmer ønsker, i tillegg til komiteens høring i denne saken, også å vise til Meld. St. 38 (2016–2017) om IKT-sikkerhet og de instanser som deltok på høringen der. I denne meldingen understreker regjeringen også viktigheten av å styrke IKT-sikkerhetskompetansen i Norge samt arbeide for at kompetansebehovene for IKT-sikkerhet i samfunnet og næringslivet blir ivaretatt. Dette er det også pekt på i Lysneutvalgets utredning, i Meld. St. 10 (2016–2017) Risiko i et trygt samfunn og i Meld. St. 27 (2015–2016) Digital agenda for Norge. Regjeringen har de siste årene lagt til rette for bedre utdanningskapasitet og økt forskning på IKT-sikkerhet. Beskyttelse av kritisk IKT-infrastruktur er sentralt i arbeidet regjeringen gjør når det gjelder IKT-sikkerhet, og en del av dette arbeidet skjer på internasjonale arenaer.

Disse medlemmer viser til at en solid IKT-infrastruktur må sørge for stabil og tilstrekkelig tilgang til nettverk, support, utstyr, programvare og tjenester av god kvalitet, samtidig som hensyn til personvern og sikkerhet ivaretas. Disse medlemmer merker seg videre at Helse- og omsorgsdepartementet på bakgrunn av konklusjonene i pågående samarbeid mellom Nasjonal sikkerhetsmyndighet, de regionale helseforetakene, Norsk Helsenett SF, Helsedirektoratet, Direktoratet for e-helse og Sykehusbygg HF, vil utpeke, klassifisere og holde oversikt over skjermingsverdig informasjon, informasjonssystem, objekter og kritisk infrastruktur innen sitt myndighetsområde, jf. ny sikkerhetslov § 17.

Komiteens medlemmer fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti viser til høringssvarene fra Fagforbundet, El- og IT-forbundet, NITO og Den norske legeforening, som alle støtter at grunnleggende IKT i helseforetakene bør defineres inn under sikkerhetsloven for slik å sikre pasientene bedre.

Disse medlemmer viser til sikkerhetsloven kapittel 6 og § 6-1. § 6-1 første ledd gir to alternative vilkår for at et informasjonssystem skal anses som skjermingsverdig:

1. Systemet behandler «skjermingsverdig informasjon» jamfør § 5-1
2. Systemet har i seg selv avgjørende betydning for «grunnleggende nasjonale funksjoner» jamfør § 6-1

Disse medlemmer mener begge vilkårene er oppfylt.

Disse medlemmer viser til cyber-angrepet Wanna Decryptor eller Wanna Cry, som blant annet rammet sykehus i Storbritannia. Mangel på riktig pasientdata kan føre til feil behandling, manglende behandling eller overbehandling. Når sykehus mistet tilgang til viktige pasientdata, måtte flere sykehus derfor stenge driften til de fikk kontroll på situasjonen. Feil og mangler i IKT-sikkerheten kan koste liv.

Disse medlemmer viser til at sikkerhetsbrudd i datasystemene i helseforetakene utgjør en vesentlig nasjonal sikkerhetsrisiko. I en beredskapssituasjon vil et lammet helsevesen føre til lidelse og død. Fordi helsevesenet opererer med løpende akuttsituasjoner, vil sikkerhetsbrudd i helsevesenet også kunne føre til lidelse og død i ellers normale situasjoner.

Disse medlemmer viser til at sykehus er viktige for å sikre grunnleggende sikkerhet i Norge gjennom helsehjelpen de gir. De utfører avgjørende nasjonale funksjoner. De grunnleggende datasystemene er nødvendige for at sykehusene skal fungere. Informasjonen er skjermingsverdig fordi sikkerhetsbrister kan lamme hele helsevesenet, og informasjonen er i seg selv svært sensitiv. Dermed er det nødvendig å definere IKT-infrastrukturen i helseforetakene inn under krav i sikkerhetsloven som skjermingsverdig informasjon.

Disse medlemmer fremmer på denne bakgrunn følgende forslag:

«Stortinget ber regjeringen definere grunnleggende IKT-infrastruktur i helseforetakene inn under krav i sikkerhetsloven om skjermingsverdig informasjon.»

Drift, utvikling og forvaltning

Komiteen mener alle pasienter skal være trygge på at deres sensitive personopplysninger ikke kommer på avveie, og at uvedkommende personer ikke får tilgang til opplysningene.

Komiteen viser til forslag 2 og 3 i representantforslaget om:

– å be regjeringen sikre at outsourcing av utvikling og drift av kritiske nasjonale IKT-tjenester og system i helsesektoren avsluttes og at nye avtaler ikke inngås.
– å be regjeringen sikre at informasjon knyttet til nasjonale sikkerhetsinteresser blir driftet og lagret i Norge.

Komiteens medlemmer fra Høyre, Fremskrittspartiet og Venstre viser til at utfordringene i det digitale rommet er grenseoverskridende – på tvers av land, sektorer og virksomheter – og at utviklingen går svært fort. Disse medlemmer ser svært positivt på at helseministeren har satt i gang en utredning med mål om å få en omforent forståelse av hva som skal til for å ha en trygg og riktig bruk av både nasjonale og internasjonale leverandører i helsetjenesten. Direktoratet for e-helse har levert sine anbefalinger til departementet (30. november 2017). Rapporten bekrefter at helse- og omsorgssektoren er avhengig av internasjonale leverandører innen IKT-området, og at det ikke er grunnlag for å konkludere med at det er tjenester som aldri vil kunne overlates til eksterne leverandører. Disse medlemmer vil understreke at det ikke trenger å være et motsetningsforhold mellom informasjonssikkerhet og tjenesteutsetting. Trygg outsourcing krever god bestillerkompetanse, høy lederoppmerksomhet og at virksomheten gjennomfører grundige risiko- og sårbarhetsvurderinger i hvert enkelt tilfelle ved eventuell utflytting av slike tjenester. Videre skal det innføres kontrollmekanismer som reduserer risiko til et akseptabelt nivå. Rutiner for krav og kontroll må utformes på bakgrunn av grundige risikovurderinger av de konkrete løsningene. Det må stilles krav til at leverandørene kan dokumentere at de vil oppfylle sikkerhetskravene, ved å beskrive nødvendige tiltak i sine tilbud og fremlegge sikkerhetsdokumentasjon. Leverandører som ikke oppfyller kravene, kan ikke tildeles kontrakt. I denne vurderingen kan eventuelle forhold i det landet tjenesten leveres fra, tas i betraktning. Disse medlemmer ser også at det i rapporten fra Nasjonal sikkerhetsmyndighet (NSM), Helhetlig IKT-risikobilde 2017, fremkommer at tjenesteutsetting av IKT-tjenester til profesjonelle aktører kan gi bedre sikkerhet, mer stabile og tilgjengelige tjenester og lavere og mer forutsigbare kostnader.

Komiteens medlemmer fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti viser til sikkerhetsbruddet i Helse Sør-Øst, der privatisering gjennom outsourcing av grunnleggende datasystemer første til at personer som ikke skulle ha tilgang, fikk tilgang til sensitive persondata. Utenlandske ansatte i kommersielle firmaer i Bulgaria, Malaysia og India fikk tilgang til pasientjournaler til 2,8 millioner nordmenn.

Disse medlemmer viser til høringen der Fagforbundet, NITO og El- og IT-forbundet opplyste at situasjonen der uvedkommende fikk tilgang til sensitive pasientdata, var en direkte konsekvens av outsourcingen. Det ble opplyst at outsourcing av grunnleggende pasientdata med dagens teknologi nødvendigvis fører til at uvedkommende får tilgang, fordi kontroll og vedlikehold av grunnsystemer gir tilgang til hele systemet og dermed også til pasientdata. Disse medlemmer viser til at samtlige på høringen blant annet på denne bakgrunn støtter representantforslaget.

Disse medlemmer viser til høringssvaret fra El- og IT-forbundet, som viser til at sikkerhetsbruddene i Helse Sør-Øst, Nødnett og Statoil har en viktig fellesnevner. IKT skulle outsources, og det ble gitt garantier om sikkerhet som det i ettertid viste seg var umulig å overholde.

Disse medlemmer viser til at helseforetakene driver i et evighetsperspektiv. Større investeringskostnader for egen drift er dermed mer økonomisk bærekraftige i et offentlig helsevesen. Outsourcing av grunnleggende systemer skaper en uholdbar konkurransesituasjon som helseforetakene taper på over tid. Når den private kontrakten kommer opp til mulig fornyelse, er trolig mange andre datasystemer avhengige av det spesifikke grunndatasystemet. Den kommersielle tilbyderen kan dermed ta mer betalt, fordi kostnadene ved et bytte kan bli høye for helseforetaket fordi grunndatasystemet påvirker mange andre datasystemer.

Disse medlemmer fremmer følgende forslag:

«Stortinget ber regjeringen sikre at outsourcing og drift av kritiske nasjonale IKT-tjenester og -systemer i helsesektoren avsluttes, og at nye avtaler ikke kan inngås.»

Disse medlemmer mener internasjonalt samarbeid er viktig for utvikling av IKT-systemer til bruk i helsevesenet. Disse medlemmer mener Norge fortsatt skal kjøpe IKT-tjenester for eksempel til drift av kliniske systemer som MR-maskiner og CT-skannere. Om klinisk utstyr i helseforetakene legges inn under sikkerhetsloven, vil det medføre at personell fra eksterne leve-

randører må sikkerhetsklarereres og trolig få kun tidsbegrenset adgang til systemene. Eksterne aktører vil få tilgang til en dedikert server uten å ha tilgang til store mengder opplysninger. Dette vil skje i nært samarbeid med offentlig IKT-personell og relevante myndigheter. Begrenset vedlikehold av dedikerte tjenester som MR, hjerte- og lungeutstyr og øyeutstyr vil kunne gjennomføres av eksterne aktører når dette er nødvendig.

Dette vedlikeholdet vil gjerne skje i samarbeid mellom internt og eksternt personale. Formålet med slik involvering av eksterne aktører vil ofte være kompetanseoverføring til internt personale. Helseforetakene vil kontinuerlig overvåke sine skjermingsverdige informasjonssystemer for å forebygge, avdekke og motvirke hendelser, jf. ny sikkerhetslov § 6-4. Hendelser som er relevante for sikkerhetsarbeidet, skal registreres. Disse medlemmer mener på denne bakgrunn det vil være uproblematisk å legge systemer med klinisk utstyr og andre lignende systemer inn under sikkerhetslovens bestemmelser. Det vil fortsatt være mulig å outsource slike systemer til internasjonale selskaper. Fordi driften av grunnleggende IKT-infrastruktur har andre utfordringer enn kliniske systemer, er effektene av å underlegge dem sikkerhetsloven forskjellige.

Komiteens medlemmer fra Senterpartiet og Sosialistisk Venstreparti viser til at norske lover gjelder i Norge. IKT-systemer som driftes fra India eller Kina, er underlagt lovene i landet de opererer fra. Helseforetak kan kontraktsfeste sikkerhetskrav ut over landenes egne krav gjennom lovverk, men som vi allerede har sett i Helse Sør-Øst-saken, blir lovnader om sikkerhet brutt, og selv da ønsker ikke alle å annullere avtalen. Disse medlemmer viser til høringssvaret fra Fagforbundet, der forbundet skriver at

«den reelle kontrollen over informasjonssystemene vil være betraktelig mindre dersom de ligger i utlandet. Den fysiske tilgjengeligheten til systemet vil være mindre dersom de ligger i utlandet. Videre vil informasjonen måtte sendes gjennom et eget nett, dersom ikke en fremmed makt skal kunne fange opp informasjonen via samtrafikkpunkter».

Disse medlemmer viser til høringssvaret fra NITO, der de skriver at norske myndigheter har bedre kontroll med at selskaper (som eventuelt vinner et anbud for drift av IKT-systemer) følger norske lover og regler om selskapene befinner seg i Norge.

Disse medlemmer mener på denne bakgrunn det er viktig å sikre at informasjon knyttet til nasjonale sikkerhetsinteresser blir driftet og lagret i Norge.

Disse medlemmer fremmer følgende forslag:

«Stortinget ber regjeringen sikre at informasjon knyttet til nasjonale sikkerhetsinteresser blir driftet og lagret i Norge.»

Uttalelse fra justiskomiteen

I tråd med Stortingets vedtak 12. april 2018 er helse- og omsorgskomiteens utkast til innstilling blitt forelagt justiskomiteen til uttalelse.

Justiskomiteen har i brev av 29. mai 2018 uttalt at justiskomiteens medlemmer slutter seg til helse- og omsorgskomiteens utkast til innstilling, og har ingen ytterligere merknader.

Forslag fra mindretall

Forslag fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti:

Forslag 1

Stortinget ber regjeringen definere grunnleggende IKT-infrastruktur i helseforetakene inn under krav i sikkerhetsloven om skjermingsverdig informasjon.

Forslag 2

Stortinget ber regjeringen sikre at outsourcing og drift av kritiske nasjonale IKT-tjenester og -systemer i helsesektoren avsluttes, og at nye avtaler ikke kan inngås.

Forslag fra Senterpartiet og Sosialistisk Venstreparti:

Forslag 3

Stortinget ber regjeringen sikre at informasjon knyttet til nasjonale sikkerhetsinteresser blir driftet og lagret i Norge.

Komiteens tilråding

Komiteens tilråding fremmes av komiteens medlemmer fra Høyre, Fremskrittspartiet, Venstre og Kristelig Folkeparti.

Komiteen har for øvrig ingen merknader, viser til representantforslaget og rår Stortinget til å gjøre følgende

v e d t a k :

Dokument 8:197 S (2017–2018) – Representantforslag fra stortingsrepresentantene Kjersti Toppe, Emilie Enger Mehl, Per Olaf Lundteigen, Nicholas Wilkinson, Torgeir Knag Fylkesnes og Mona Fagerås om å be regjeringen definere grunnleggende IKT-infrastruktur i helseforetakene inn under sikkerhetsloven – vedtas ikke.

Oslo, i helse- og omsorgskomiteen, den 5. juni 2018

Olaug V. Bollestad
leder

Torill Eidsheim
ordfører

VEDLEGG

Brev fra Helse- og omsorgsdepartementet v/statsråd Bent Høie til helse- og omsorgskomiteen, datert 7. mai 2018

Dokument 8:197 S (2017-2018) - Representantforslag om å be regjeringen definere grunnleggende IKT-infrastruktur i helseforetakene inn under sikkerhetsloven

Jeg viser til brev fra helse- og omsorgskomiteen av 17. april 2018, vedlagt dokument 8:197 S (2017-2018). Helse- og omsorgskomiteen ber om min uttalelse på representantforslaget fra stortingsrepresentantene Kjersti Toppe, Emilie Enger Mehl, Per Olaf Lundteigen, Nicholas Wilkinson, Torgeir Knag Fylkesnes og Mona Fagerås om å be regjeringen definere grunnleggende IKT-infrastruktur i helseforetakene inn under sikkerhetsloven.

Ny sikkerhetslov, som ble behandlet i Stortinget i februar og mars i år, er forventet å tre i kraft 1. januar 2019. Den nye sikkerhetsloven har et utvidet virkeområde særlig knyttet til grunnleggende nasjonale funksjoner, og de virksomheter som har vesentlig betydning for disse funksjonene.

Det som er særlig relevant i spørsmålene i representantforslaget er å sikre et forsvarlig sikkerhetsnivå for skjermingsverdig informasjon, samt skjermingsverdige informasjonssystemer, objekter og infrastruktur når dette har betydning for nasjonale sikkerhetsinteresser, samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet.

Det er departementene som har det overordnede ansvaret for forebyggende sikkerhetstjeneste i sin sektor, jf. sikkerhetsloven § 4. Det er imidlertid viktig å peke på at dette ikke begrenser den enkelte virksomhets ansvar og plikter etter bestemmelsene i eller i medhold av denne loven. Videre har departementene ansvaret for å utpeke skjermingsverdige objekter innen sitt myndighetsområde, jf. sikkerhetsloven § 17.

Når ny sikkerhetslov trer i kraft, må virksomheter som har råderett over informasjon, informasjonssystemer, objekter eller kritisk infrastruktur av avgjørende betydning for understøttelsen av grunnleggende nasjonale funksjoner, gjennomføre nye risikovurderinger.

Forslag 1:

Stortinget ber regjeringen definere grunnleggende IKT-infrastruktur i helseforetakene inn under krav i sikkerhetsloven om skjermingsverdig informasjon.

Svar:

Helse- og omsorgsdepartementet har etter sikkerhetsloven ansvaret for forebyggende sikkerhet i helse- og omsorgssektoren. Departementet gjennomførte i 2014 en vurdering av sikkerhetslovens anvendelse for de regionale helseforetakene, helseforetakene og Norsk Helsenett SF. Nasjonal sikkerhetsmyndighet (NSM) bistod med råd og veiledning i denne vurderingen. Konklusjonen var at departementet anså de regionale helseforetakene, helseforetakene og Norsk Helsenett SF å være omfattet av sikkerhetsloven, jf. sikkerhetsloven § 2 første ledd. Dette innebærer at virksomhetene er omfattet av sikkerhetsloven med tilhørende forskrifter. Virksomhetene fikk ansvaret for å iverksette og utøve forebyggende sikkerhetstjeneste fra desember 2014.

Vurderinger av forvaltning og drift av IKT-infrastrukturen i helseforetakene gjøres i dag innenfor rammen av sikkerhetsloven. I vurderingen av om hele eller deler av IKT-infrastrukturen er skjermingsverdig, er det avgjørende om det kan skade grunnleggende nasjonale funksjoner om funksjonen får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse.

Utvelgelse av skjermingsverdige objekter skal skje på grunnlag av verdi- skadevurdering, hvor det innenfor lovens formål særlig tas hensyn til objektets:

a) betydning for sikkerhetspolitisk krisehåndtering og forsvar av riket,
b) betydning for kritiske funksjoner for det sivile samfunn,
c) symbolverdi, og
d) mulighet for å utgjøre en fare for miljøet eller befolkningens liv og helse.

Helseforetakene og de regionale helseforetakene plikter å utøve forebyggende sikkerhetstjeneste i henhold til bestemmelsene gitt i eller i medhold av sikkerhetsloven, jf. sikkerhetsloven § 5. Videre pålegger loven de som er objekteiere en plikt til å foreslå hvilke objekter som er skjermingsverdige overfor departementet. Etter loven § 17 er det i sin tur departementet som har ansvaret for å utpeke skjermingsverdige objekter innen sitt myndighetsområde.

I felles foretaksmøte i de regionale helseforetakene i januar 2018 stilte jeg krav om at det skal gjennomføres tiltak som gjør at de regionale helseforetakene og helseforetakene i regionen er forberedt når ny sikkerhetslov trer i kraft. I tillegg har departementet tatt initiativ til et samarbeid med Nasjonal sikkerhetsmyndighet (NSM) for å forberede sektoren. De regionale helseforetakene, Norsk Helsenett SF, Helsedirektoratet, Direktoratet for e-helse og Sykehusbygg HF deltar også i dette arbeidet. Formålet er å identifisere om det er informasjon, informasjonssystemer, objekter eller kritisk infrastruktur som kan ha avgjørende betydning for understøttelsen

av grunnleggende nasjonale funksjoner. Det skal i tillegg gjennomføres verdi- og skadevurderinger ved helt eller delvis bortfall av disse funksjonene, og deres betydning for understøttelse av grunnleggende nasjonale funksjoner.

Helse- og omsorgsdepartementet vil på bakgrunn av konklusjonene i arbeidet utpeke, klassifisere og holde oversikt over skjermingsverdig informasjon, informasjonssystem, objekter og kritisk infrastruktur innen sitt myndighetsområde, jf. ny sikkerhetslov § 17. Departementet rapporterer til Nasjonal sikkerhetsmyndighet (NSM) med angivelse av klassifiseringsgrad (jf. ny sikkerhetslov § 7-1). Klassifiseringen skal som tidligere nevnt bygge på verdi- og skadevurderinger. Begrunnelsen for klassifiseringen skal inngå i departementenes og NSMs oversikt over skjermingsverdige informasjon, informasjonssystemer, objekter eller kritisk infrastruktur.

IKT-infrastrukturen i helseforetakene er et av områdene som blir vurdert i det nevnte samarbeidet med NSM. Disse vurderingene av sikkerhetsnivå og eventuelt behov for forebyggende sikkerhetstiltak for hele eller deler av IKT-infrastrukturen i helseforetakene vil kunne være sikkerhetsgradert informasjon. Dette er vurderinger som de regionale helseforetakene, helseforetakene og Helse- og omsorgsdepartementet arbeider med i samarbeid med NSM, Norsk Helsenett SF, Helsedirektoratet, Direktoratet for e-helse og Sykehusbygg HF.

Forslag 2:

Stortinget ber regjeringen sikre at informasjon knyttet til nasjonale sikkerhetsinteresser blir driftet og lagret i Norge.

Svar:

I min redegjørelse til Stortinget den 30. januar i år om tilgangsstyring og informasjonssikkerhet i Helse Sør-Øst, var jeg tydelig på at det er helt nødvendig at befolkningen har tillit til helsetjenestens håndtering av pasientopplysninger. Når svakheter i informasjonssikkerheten avdekkes, er det viktig å møte dette med en åpen debatt og gjennomføre grundige vurderinger for å iverksette nødvendige tiltak. I redegjørelsen var jeg også helt tydelig på regjeringens mål; Befolkningen skal ha tilgang til offentlig finansierte helsetjenester med høy kvalitet. En vesentlig oppgave for regjeringen er å sikre en bærekraftig helsetjeneste. Det krever utstrakt bruk av teknologi som gjør det mulig for helsepersonell å arbeide effektivt, levere helsetjenester på nye måter, behandle pasienter utenfor sykehuset og gi pasienten større kontroll over egen behandling og egen helse. Da må vi ta i bruk de fremste metoder og teknologi som finnes. Det krever at vi også må forholde oss til at mye av teknologiutviklingen skjer og tilbys internasjonalt.

Helsetjenesten er avhengig av et variert og godt tilbud fra private leverandører av IKT-løsninger og medisinsk-teknisk utstyr. Økt digitalisering stiller imidlertid også økte krav til arbeidet med informasjonssikkerhet og personvern. Jeg er opptatt av at dette arbeidet skal ha høy prioritet.

Det var derfor viktig for meg å få utredet og få en omforent forståelse av hva som skal til for å ha en trygg og riktig bruk av både nasjonale og internasjonale leverandører i helsetjenesten. Direktoratet for e-helse fikk derfor i 2017 i oppdrag å utarbeide en rapport. Et stort antall aktører var involvert i arbeidet: sentrale kompetansemiljøer, pasientorganisasjoner, fagorganisasjoner, tillitsvalgte, brukerorganisasjoner og IKT-næringen. Det ble også innhentet erfaringer fra andre samfunnsaktører, slik som Finanstilsynet, Telenor og Statoil.

Direktoratet for e-helse leverte sine anbefalinger til departementet den 30. november 2017. Jeg vil påpeke at rapporten ikke er en kontroll- eller tilsynsrapport, men et normativt underlag. Dette er i tråd med rollen til direktoratet. Rapporten bekrefter at helse- og omsorgssektoren er avhengig av internasjonale leverandører innen IKT-området, og at det ikke er grunnlag for å konkludere med at det er tjenester som aldri vil kunne overlates til eksterne leverandører. Videre er det et faktum at ansatte også hos de internasjonale leverandørene i relevante og nødvendige tilfeller vil måtte ha tjenestemessig tilgang til pasientinformasjon. Det må imidlertid alltid foreligge risikovurderinger og databehandleravtaler for å ivareta hensynet til informasjonssikkerheten. Jeg mener derfor at det ikke trenger å være et motsetningsforhold mellom informasjonssikkerhet og tjenesteutsetting.

Det er viktig å merke seg at det etter gjeldende rett ikke er forbud mot at norske virksomheter benytter nasjonale eller utenlandske IKT-leverandører fra EU/EØS-området. Tvert imot er det svært begrenset anledning til å avvise tilbud med den begrunnelse at oppdragstaker er etablert i, eller vil levere tjenester fra, et annet EØS-land. Det er ifølge anskaffelsesreglene mulig hvis dette har betydning for rikets sikkerhet, og når det er nødvendig for å ivareta vesentlige sikkerhetsinteresser. Det skal mye til for at beskyttelse av pasientopplysninger utfordrer rikets sikkerhet, i hvert fall dersom det stilles krav til leverandørene og det er etablert kontrollmekanismer basert på risikovurderinger. Ved bruk av IKT-leverandører utenfor EU/EØS-området er det særskilte krav som må oppfylles.

I NSMs rapport *Helhetlig IKT-risikobilde 2017* fremkommer det at tjenesteutsetting av IKT-tjenester til profesjonelle aktører kan gi bedre sikkerhet, mer stabile og tilgjengelige tjenester, og lavere og mer forutsigbare kostnader. Utflytting av slike tjenester kan også bidra til at virksomheten kan ha større fokus på sine kjerneoppgaver. Samtidig kan utsetting av tjenestene føre til økt risiko ved at det gis redusert kontroll over virksomhetskritiske verdikjeder. Hver enkelt virksomhet må

derfor gjennomføre grundige risiko- og sårbarhetsvurderinger i hvert enkelt tilfelle ved eventuell utflytting av slike tjenester.

Rapporten fra Direktoratet for e-helse viser til at oppdragsgiver i vurdering av tjenesteutsetting skal stille krav til informasjonssikkerhet, gjennomføring av risikovurderinger og at det foreligger databehandleravtaler. Det skal i tillegg innføres kontrollmekanismer som reduserer risiko til et akseptabelt nivå. Rutiner for krav og kontroll må utformes på bakgrunn av grundige risikovurderinger av de konkrete løsningene. Det må stilles krav til at leverandørene kan dokumentere at de vil oppfylle sikkerhetskravene, ved å beskrive nødvendige tiltak i sine tilbud og fremlegge sikkerhetsdokumentasjon. De regionale helseforetakene og helseforetakene er ansvarlig for å vurdere om kravene er oppfylt. Leverandører som ikke oppfyller kravene kan ikke tildeles kontrakt. I denne vurderingen kan eventuelle forhold i det landet tjenesten leveres fra tas i betraktning.

Jeg forventer at det er høy ledelsesoppmerksomhet på gjennomføring og oppfølging av risikovurderinger ved eventuelle spørsmål om tjenesteutflytting av virksomhetskritisk IKT, særlig dersom deler av en slik tjeneste er av kritisk betydning for helseforetakenes evne til å understøtte grunnleggende nasjonale funksjoner, jf. ny sikkerhetslov. Jeg vil presisere at dette gjelder både til private leverandører som er etablert i Norge og ved bruk av internasjonale leverandører.

Når det gjelder det konkrete representantforslaget mener jeg at denne problemstillingen må sees i lys av det arbeidet som nå pågår i samarbeid med NSM, de regionale helseforetakene, Direktoratet for e-helse, Helsedirektoratet, Sykehusbygg HF og Norsk Helsenett SF. Vurderingen som skal gjøres er om hele eller deler av IKT-infrastrukturen i helseforetakene er av avgjørende betydning for grunnleggende nasjonale funksjoner, og om disse må objektsikres. Når dette er klart, er det naturlig å vurdere organiseringen av disse tjenestene.

Forslag 3:

Stortinget ber regjeringen sikre at outsourcing av utvikling og drift av kritiske nasjonale IKT-tjenester og systemer i helsesektoren avsluttes og at nye avtaler ikke kan inngås.

Svar:

Jeg vil også her vise til min redegjørelse i Stortinget den 30. januar i år om tilgangsstyring og informasjonssikkerhet i Helse Sør-Øst og til mitt svar under spørsmål nr 2 ovenfor.

Jeg vil også vise til at Regjeringen har oppnevnt et IKT-sikkerhetsutvalg høsten 2017, som skal utrede rettslig regulering på IKT-sikkerhetsområdet og organisering av ansvar. Dette arbeidet vil også bidra med nyttig kunnskap til vurderinger omkring outsourcing av IKT-infrastruktur og sikkerhet.

Svanemerketrykksak, 2041 0654 Trykk og layout: Stortingets grafiske seksjon