STORTINGET

Representantforslag 197 S

(2017–2018)

fra stortingsrepresentantene Kjersti Toppe, Emilie Enger Mehl, Per Olaf Lundteigen, Nicholas Wilkinson, Torgeir Knag Fylkesnes og Mona Fagerås

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

Til Stortinget

Bakgrunn

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-Øst sitt 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.

Nettverksinnbrudd og trusselvurdering

8. januar 2018 ble Sykehuspartner, Helse Sør-Øst, 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). På en felles pressekonferanse med helse- og omsorgsministeren og justis-, beredskaps- og innvandringsministeren uttalte politiadvokat i PST Line Nyvoll Nygaard om hendelsen:

> «Det er mistanke om at noen til fordel for en fremmed stat samler inn opplysninger som, hvis de blir kjent for en slik stat eller for øvrig avsløres, kan skade grunnleggende nasjonale interesser som gjelder samfunnets infrastruktur. Dette kan være opplysninger om helseberedskap.»

Da Etterretningstjenesten (E-tjenesten) 5. mars 2018 la fram sin trusselvurdering, uttalte sjef for Etterretningstjenesten, generalløytnant Morten Haga Lunde, om nettverksangrepet mot Helse Sør-Øst RHF at:

> «Saken illustrerer hvor komplekst og sammensatt dagens trusselbilde er, og hvor sårbar kritisk nasjonal infrastruktur er for angrep.»

Ifølge NRK la han til at angrepet kunne vært avverget dersom E-tjenesten hadde fått bruke sine kapabiliteter mot ytre trusler. Forslagsstillerne understreker at dette angrepet vurderes uavhengig av IKT-skandalen i Helse Sør-Øst RHF. Nettverksangrepet i Helse Sør-Øst RHF viser at IKT-infrastruktur i helsevesenet er samfunnskritisk infrastruktur som fremmede makter og andre som ikke skal ha tilgang til det, ønsker seg tilgang til. Saken viser også at det er svært sannsynlig at disse ikkelegitime aktørene forsøker å få tilgang til denne informasjonen, og at myndighetene må sørge for et lovverk som beskytter befolkningen mot slikt tyveri.

IKT-skandalen i Helse Sør-Øst

Forslagsstillerne mener at IKT-skandalen i Helse Sør-Øst RHF 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 del av kjerneoppgavene til helsevesenet.

Styret i Helse Sør-Øst gjorde et vedtak den 8. september 2016 om at videre modernisering av regionens IKT-infrastruktur skulle skje ved bruk av eksterne leverandører. Den 10. november 2016 sa helse- og omsorgsministeren fra Stortingets talerstol:

«Den eksterne leverandørens tjenester er som nevnt begrenset til IKT infrastruktur, altså ikke pasientjournalsystemer eller pasientadministrative systemer. Avtalen med tjenesteleverandøren stiller klare krav om at alle datasentre skal stå i Norge, inkludert all lagring av pasientdata (...).

Personell som drifter infrastrukturen, skal ikke ha tilgang til systemer (...) eller administrative systemer hvor personopplysninger behandles.

Driften av disse systemene skal fortsatt leveres av Sykehuspartner HF. Ifølge Helse Sør-Øst RHF vil alle personopplysninger forbli fysisk i Norge, og tilgangen til disse vil fremdeles skje fra Norge og være begrenset til Sykehuspartner og helseforetakene selv. Dette innebærer at personopplysningene ikke skal overføres til andre land eller noen form for skytjeneste.»

Forslagsstillerne viser til at kontroll- og konstitusjonskomiteen våren 2017 tok tak i saken, da de mente at opplysningene fra statsråden var villedende. Da svarte helse- og omsorgsministeren i brev tilbake:

«Mine svar i interpellasjonsdebatten omhandlet det sikkerhetsregimet som skal være på plass etter at driften er overført til ekstern leverandør.»

Statsrådens første svar omhandlet altså ikke hva som kunne skje i planleggings- og oppfølgingsfasen. Forslagsstillerne mener at norske myndigheter i fremtiden ikke kan forholde seg til styring av tilganger til sikkerhetskritisk informasjon på denne måten. For befolkningen har det ingen betydning hvilken fase statsråden snakker om, men at all samfunnskritisk infrastruktur er under forsvarlig kontroll.

Sikkerhetsloven

Forslagsstillerne viser til utenriks- og forsvarskomiteens innstilling om sikkerhetsloven (Innst. 103 L (2017–2018)). Ifølge regjeringens forslag til ny sikkerhetslov er ansvaret for å definere grunnleggende nasjonale funksjoner lagt til fagdepartementene, og Stortinget har i hovedsak sluttet seg til dette ved behandlingen av innstillingen. Forslagsstillerne viser til følgende merknad i innstillingen:

«Komiteens medlemmer fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti viser til at loven legger opp til at det primære ansvaret for forebyggende sikkerhet i de ulike samfunnssektorene blir lagt til det enkelte fagdepartement. Begrunnelsen er at det er det enkelte departement som kjenner sin sektor best.

Disse medlemmer viser til at utvalget i NOU 2016:19, Samhandling for sikkerhet-beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid, foreslo å lovfeste en systematikk for hvordan de ulike departementene skal identifisere grunnleggende nasjonale funksjoner innenfor sine egne myndighetsområder. Det samme gjelder for de virksomheter som har en kritisk rolle i understøttelse av slike funksjoner. Disse medlemmer støtter dette.

Disse medlemmer forutsetter at de ulike departementene følger opp loven og merknader og legger fram for Stortinget resultatet av sitt arbeid med å identifisere grunnleggende nasjonale funksjoner.

Disse medlemmer legger til grunn at de ulike fagdepartementene definerer grunnleggende IKT-infrastruktur i store sektorer som eksempelvis helse, Nav, politi, kraftforsyning og ekom som kritisk infrastruktur som da faller inn under sikkerhetsloven. Disse medlemmer merker seg at det etter § 1-3 i første omgang er opp til det enkelte departement å fatte vedtak om hvilke typer virksomheter loven helt eller delvis skal gjelde for. Dersom departementet ikke fatter vedtak i samsvar med sikkerhetsmyndighetens anbefaling, kan sikkerhetsmyndigheten bringe saken inn for endelig avgjørelse hos det departementet som har overordnet ansvar for forebyggende sikkerhetsarbeid. Disse medlemmer mener at lovens ambisjon må være at IKT-systemer i helse, Nav, politi, kraftforsyning og ekom defineres som kritisk infrastruktur når loven skal konkretiseres i bl.a. forskriftsarbeid og strategier.

Disse medlemmer mener at informasjon knyttet til nasjonale sikkerhetsinteresser må pålegges å bli driftet og lagret i Norge. Disse medlemmer vil understreke at outsourcing av utvikling og drift av kritiske nasjonale IKT-tjenester og system ikke må aksepteres, og at det må innføres klare nasjonale krav til vurdering av sikkerhet og sårbarhet.

Disse medlemmer viser til IKT-skandalen i Helse Sør-Øst som angår IKT-drift i Sykehuspartner. Konsekvensen av denne avtalen var at uvedkommende kunne få tilgang til pasientdata om 2,8 millioner nordmenn. Derved kunne sensitiv personinformasjon komme på avveie, og dessuten kunne uvedkommende kartlegge en infrastruktur som kunne brukes til sabotasje som kunne lamme Norge. Denne saken viser at lovverk og departementets praksis i dag ikke er betryggende.

Disse medlemmer vil understreke behovet for at Nasjonal sikkerhetsmyndighet får tilstrekkelig med ressurser, kompetanse og myndighet til å følge opp sitt lovpålagte ansvar.»

Forslagsstillerne viser også til at regjeringen har fremmet en stortingsmelding om IKT-sikkerhet (Meld. St. 38 (2016–2017)), som nå ligger til behandling i Stortinget, jf. Innst. 187 S (2017–2018).

Vil IKT i helse bli definert som kritisk samfunnsinfrastruktur som faller inn under sikkerhetsloven?

Forslagsstillerne viser til at helse- og omsorgsministeren uttalte i redegjørelsen i Stortinget 30. januar

2018 om IKT-skandalen og senere i media at helseforetakene var underlagt sikkerhetsloven. I svar på skriftlig spørsmål, jf. Dokument nr. 15:902 (2017–2018), blir dette utdypet:

«Helse- og omsorgsdepartementet har innenfor sin sektor ansvar for forebyggende sikkerhetstjeneste etter sikkerhetsloven. På grunnlag av erfaringer fra arbeidet knyttet til objektsikkerhetsforskriften i 2013-2014 og gjennomgang av gradert kommunikasjon i helse- og omsorgssektoren, gjennomførte departementet 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 at de regionale helseforetakene, helseforetakene og Norsk Helsenett SF er omfattet av sikkerhetsloven, jf. sikkerhetsloven § 2 første ledd. Dette innebar at virksomhetene nevnt over ble omfattet av sikkerhetsloven og tilhørende forskrifter, med ansvar for å iverksette og utøve forebyggende sikkerhetstjeneste fra desember 2014.

Helse- og omsorgsdepartementet har det overordnede ansvar for forebyggende sikkerhetstjeneste i sin sektor, jf. sikkerhetsloven § 4. Dette begrenser likevel ikke den enkeltes ansvar og plikter etter bestemmelsene i eller i medhold av denne loven. Videre har Helse- og omsorgsdepartementet ansvaret for å utpeke skjermingsverdige objekter innen sitt myndighetsområde, jf. sikkerhetsloven § 17.

Helseforetakene og de regionale helseforetakene plikter å utøve forebyggende sikkerhetstjeneste i henhold til bestemmelsene gitt i eller i medhold av sikkerhetsloven, jf. sikkerhetslovens § 5. Videre pålegger loven de som er objekteier en plikt til å foreslå hvilke objekter som er skjermingsverdige overfor departementet. Utvelgelse av skjermingsverdig objekt skal skje på grunnlag av en 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.

Den nye sikkerhetsloven som skal behandles i Stortinget i februar i år har et utvidet virkeområde særlig knyttet til grunnleggende nasjonale funksjoner og de virksomheter som har vesentlig betydning for disse funksjonene. Virksomhetene skal sørge for et forsvarlig sikkerhetsnivå for skjermingsverdig informasjon, skjermingsverdige informasjonssystemer og skjermingsverdige objekter og infrastruktur når dette har betydning for nasjonale sikkerhetsinteresser, samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet. Virksomheter som har råderett over informasjon, informasjonssystemer, objekter eller kritisk infrastruktur av avgjørende betydning for understøttelsen av grunnleggende nasjonale funksjoner må gjennomføre nye risikovurderinger. Dette innebærer både verdi- og skadevurderinger for å avklare sikkerhetsnivå og behov for forebyggende sikkerhetstiltak.

Helseministeren har i foretaksmøte med de regionale helseforetakene i januar i år stilt krav om at de skal gjennomføre tiltak som gjør at de regionale helseforetakene og regionens helseforetak er klar for å implementere ny sikkerhetslov når den trer i kraft. Som ledd i dette arbeidet har departementet etablert et samarbeid med Nasjonal sikkerhetsmyndighet (NSM) hvor de regionale helseforetakene, Norsk Helsenett SF, Helsedirektoratet, Direktoratet for e-helse og Sykehusbygg HF deltar. Målsettingen er å gjennomføre vurderinger av om hele eller deler av deres informasjonssystemer, objekter eller kritisk infrastruktur kan ha avgjørende betydning for understøttelsen av grunnleggende nasjonale funksjoner. Videre skal arbeidet avklare eventuelt sikkerhetsnivå og behov for forebyggende sikkerhetstiltak.

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 både helseforetakene, de regionale helseforetakene og Helse- og omsorgsdepartementet arbeider med i samarbeid med Nasjonal sikkerhetsmyndighet (NSM).»

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.

Forslag

På denne bakgrunn 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.

10. april 2018

Kjersti Toppe **Emilie Enger Mehl** **Per Olaf Lundteigen**

Nicholas Wilkinson **Torgeir Knag Fylkesnes** **Mona Fagerås**

Svanemerketrykksak, 2041 0654 Trykk og layout: Stortingets grafiske seksjon