FAGFORBUNDET

Forsvarsdepartementet
Postboks 8126 Dep.

0032 OSLO

Deres ref.	Vår ref / Saksbehandler	Dato:
2015/3139	18/5587-6 X21 &13 Mats Kvaløy-Bjørbekk / tlf.	01.10.2018

HØRING - FORSKRIFTER TIL NY SIKKERHETSLOV

Oppsummering

Fagforbundet mener myndighetsforskriften bør inneholde egne bestemmelser om identifisering og beskyttelse av skjermingsverdige informasjonssystemer. Videre mener Fagforbundet at regjerningen bør trekke konsekvensene av sikkerhetsbruddene i helseforetakene de sist årene, og at Helse- og omsorgsdepartementet som ansvarlig fagdepartement bør utpeke den delen av IKT-infrastrukturen i helseforetakene som utgjør skjermingsverdige informasjonssystemer. Fagforbundet etterspør en forskriftsfesting av departementenes ansvar med hjemmel i sikkerhetsloven kapittel 6.

Innledning

Fagforbundet mener myndighetsforskriften bør inneholde egne bestemmelser om identifisering og beskyttelse av skjermingsverdig informasjonssystemer jf. lov av 6. mars 2018 om nasjonal sikkerhet (heretter sikkerhetsloven) § 6-2 annet ledd jf. § 6-1 annet ledd. Fullmaktsbestemmelsene i § 6-1 annet ledd og § 6-2 annet ledd bør derfor benyttes til å gi departementene ansvar for å utpeke skjermingsverdige informasjonssystemer innenfor sitt ansvarsområde. I forarbeidene til ny sikkerhetslov framkommer det at man ønsker flere endringer i bestemmelsene om informasjonssystemsikkerhet for å sikre et tidsriktig regelverk i tråd med digitaliseringen av samfunnet. Både i NOU 2016:19 «Samhandling for sikkerhet» og Prop. 153 L «Lov om nasjonal sikkerhet», understrekes det spesielt at bestemmelsen i sikkerhetsloven § 6-2 er en viktig nyvinning. Det gir dessuten best sammenheng i regelverket om det gjelder like bestemmelser for identifisering av objekt- og infrastruktur etter sikkerhetsloven kapittel 7 og informasjonssystemer etter kapittel 6.

Videre framheves det i proposisjonen at forskriftsfesting av bestemmelser knyttet til informasjonsysstemstikkerhet er spesielt viktig: «En utfordring vil være at loven kan oppfattes som utydelig innenfor særlig sammensatte områder som informasjonssystemsikkerhet. Dette er en utydelighet som etter departementets syn er uunngåelig, samtidig som at dette også er hensiktsmessig for å gi rom for å møte den

fremtidige utviklingen. Konkretiseringen av hvilke konsekvenser loven får, vil skje gjennom forskriftsutvikling og praktisering av regelverket.» Det er etter vårt syn svært viktig at regelverket blir konkretisert gjennom at det gis forskrifter på området.

Vi mener videre det vil være klokt av regjerningen å trekke konsekvensene av sikkerhetsbruddene i helseforetakene de sist årene. Helse- og omsorgsdepartementet som ansvarlig fagdepartement bør utpeke den delen av IKT-infrastrukturen i helseforetakene som utgjør skjermingsverdige informasjonssystemer. Det er uholdbart at det stadig oppstår situasjoner hvor helseopplysninger fryktes å være på avveie og hvor disse kan falle i hendene på fremmede makter.

For det første tydeliggjør slike brudd på informasjonssikkerheten at IKT-systemene i helseforetakene utgjør en betydelig beredskapsrisiko. For å oppfylle sikkerhetslovens formål om å «å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser», bør disse IKT-systemene skjermes.

For det andre er slike brudd på informasjonssikkerhet i strid med grunnleggende hensyn til personvern og dermed også retten til privatliv for rikets borgere. Vi minner om at retten til privatliv er grunnlovsfestet i Grunnloven § 102, hvor statens myndigheter er forpliktet til å «sikre et vern om den personlige integritet». I tillegg er retten til privatliv vernet under Den europeiske menneskerettighetskonvensjon artikkel 8. Videre medfører «Forordning om beskyttelse av individer ved behandling av personopplysninger og om fri flyt av slike opplysninger» (Personvernforordningen) styrket personvern innenfor EU/EØS-området.

For det tredje rammer brudd på informasjonssikkerheten tilliten til helsevesenet ved at pasienter ikke lenger kan føle seg trygge på at den informasjonen de oppgir til helsepersonell blir behandlet fortrolig. Pasienters tillit til helsevesenet er blant annet en viktig betingelse for at våre yrkesgrupper skal kunne utføre sitt arbeid på en tilfredsstillende måte.

Nærmere om informasjonssystemer

Informasjonssystemer er som nevnt behandlet i den nye sikkerhetsloven kapittel 6. § 6-1 første ledd gir to alternative vilkår for at et informasjonssystem skal anses som skjermingsverdig. Vi mener begge vilkårene er oppfylte når det gjelder skjerming av IKT-systemer i helseforetakene og vi ber departementet bruke sin myndighet til å ivareta skjerming jf. sikkerhetsloven § 6-1 annet ledd.

Første alternative vilkår er at systemet behandler «skjermingsverdig informasjon» jf. § 5-1. Ordlyden i bestemmelsen fremhever at informasjonen er skjermingsverdig dersom det kan «skade nasjonale sikkerhetsinteresser» at informasjonen blir «kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.» Nasjonale sikkerhetsinteresser er videre definert i lovens § 1-5 nr.1, hvor «forsvar, sikkerhet og beredskap» er nevnt i bokstav b).

Forarbeidene til bestemmelsen (prop. 153 L (2016-2017) punkt 19.5) fremhever at begrepet «skjermingsverdig informasjon» utvides sammenlignet med tidligere sikkerhetslov. I motsetning til tidligere lov, da det utelukkende var konfidensialitetsbehov som skulle vurderes, skal nå også integritets- og tilgjengelighetsbehov inngå som kriterier i

verdivurderingen av informasjonen. I proposisjonen nevnes under punkt 10.5.1 offentlige saksbehandlingssystemer, militære kampsystemer, kontorstøttesystemer og industrielle kontroll- og styringssystemer som eksempler.

Det kan få alvorlig konsekvenser når pasientinformasjon om norske borgere, herunder sentrale myndighetspersoner, kommer på avveie. For utenlandsk etterretning vil dette være av stor interesse og kan gi grunnlag for målrettede operasjoner både mot grupper av personer og mot enkeltpersoner. Videre kan sletting eller endring av slik informasjon lamme helseforetakenes evne til å ivareta befolkning i en krisesituasjon. Med tanke på at begrepet «skjermingsverdig informasjon» utvides i sammenligning med tidligere sikkerhetslov, medfører dette at IKT-systemer i helseforetakene behandler slik informasjon.

Annet alternativ er at systemet i seg selv har avgjørende betydning for «grunnleggende nasjonale funksjoner» jf. § 6-1. I forarbeidende uttales det under punkt 19.6 i proposisjonen: «Skjermingsverdige systemer kan defineres (…) ved å fastslå at systemet har en særlig viktig rolle i virksomhetens leveranse av sine kritiske tjenester.»

Under kriser og i krig er velfungerende helsesystemer avgjørende. Dersom systemer for journal og beslutningsstøtte blir slått ut av en fremmed makt, vil dette få alvorlige konsekvenser for operativ klinisk beredskap. Vi mener derfor at journalsystemer og systemer for beslutningstøtte i helseforetakene utgjør «kritiske tjenester». Sikkerhetsbruddet i Sykehuspartner 8. januar 2018, hvor noen til fordel for fremmed stat samlet inn opplysninger, viser at informasjonen har en strategisk viktig funksjon også i fredstid.

Vi imøteser derfor en forskriftsfesting av departementenes ansvar med hjemmel i sikkerhetsloven kapittel 6.

Med hilsen
FAGFORBUNDET

Jan-Tore Strandås
fagleder

Mats Kvaløy-Bjørbekk
rådgiver