STORTINGET

Innst. 78 L

(2023–2024)

Innstilling til Stortinget
fra justiskomiteen

Prop. 109 LS (2022–2023)

Innstilling fra justiskomiteen om Lov om digital sikkerhet (digitalsikkerhetsloven)

Til Stortinget

Sammendrag

Justis- og beredskapsdepartementet foreslår i proposisjonen en ny lov om digital sikkerhet. I tillegg bes det om Stortingets samtykke til godkjenning av to beslutninger i EØS-komiteen. Det vises til egen innstilling om samtykkesaken.

Loven bygger på Europaparlaments- og rådsdirektiv (EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen (NIS-direktivet). Direktivet og tilhørende gjennomføringsforordning 2018/151 om spesifisering av NIS-direktivet artikkel 16 nr. 1 og nr. 4 (gjennomføringsforordningen) ble besluttet tatt inn i EØS-avtalen 3. februar 2023.

Forslaget til lov om digital sikkerhet er ment å være i samsvar med NIS-direktivet og øvrige sammenlignbare lands nasjonale lovgivning på området.

Loven skal forplikte virksomheter som har en særlig viktig rolle for å opprettholde kritisk samfunnsmessig og økonomisk aktivitet, til å overholde digitale sikkerhetskrav og varsle om alvorlige digitale hendelser. Loven skal bidra med forebyggende sikkerhetstiltak som gjør en virksomhet bedre rustet til å stå imot angrep mot nettverks- og informasjonssystemer de er avhengige av. Videre skal loven sikre planer for håndtering av uønskede hendelser. Loven stiller overordnede krav til sikkerhet og varsling, og virkeområdet er kun angitt i form av hvilke sektorer den gjelder i. Dette forutsetter et underliggende regelverk med tydeligere avgrensinger og konkretiseringer. Loven inneholder derfor en vid adgang til å fastsette nærmere bestemmelser i forskrift.

Loven etablerer rammeverk for tilsyn med virksomhetene og åpner for ileggelse av pålegg og eventuelt overtredelsesgebyr ved manglende oppfyllelse av pliktene. Myndighetene skal også ta imot varsler om alvorlige digitale hendelser. Departementet legger opp til at eksisterende myndighetsstruktur benyttes i størst mulig grad for å begrense behovet for nye kontaktpunkter for virksomhetene som blir underlagt regelverket, og for at myndigheter som allerede utfører oppgaver som ligner oppgaver denne loven pålegger dem, skal kunne samkjøre disse så langt det er mulig. Departementet mener videre at eksisterende myndigheter også bør føre tilsyn med virksomheter som per i dag ikke er underlagt tilsyn.

De økonomiske og administrative kostnadene knyttet til lovforslaget er vanskelige å tallfeste. Loven legger opp til at det i forskrift vil bli utarbeidet både nærmere kriterier for identifisering av tilbydere av samfunnsviktige tjenester og også spesifisering av sikkerhets- og varslingskrav. Forslag til forskrift vil bli gjenstand for egen offentlig høring hvor det trolig vil komme noe mer konkret om eventuelle kostnader knyttet til blant annet sikkerhets- og varslingskrav.

Komiteens merknader

Komiteen, medlemmene fra Arbeiderpartiet, Odd Harald Hovland, Hadia Tajik og Maria Aasen-Svensrud, fra Høyre,

Ingunn Foss og Sveinung Stensland, fra Senterpartiet, Ivar B. Prestbakmo og Else Marie Rødby, fra Fremskrittspartiet, lederen Per-Willy Amundsen og Tor André Johnsen, fra Sosialistisk Venstreparti, Andreas Sjalg Unneland, og fra Venstre, Ingvild Wetrhus Thorsvik, viser til at Justis- og beredskapsdepartementet i proposisjonen foreslår en ny lov om digital sikkerhet. Komiteen viser til at loven bygger på NIS-direktivet, hvis formål er å forbedre det indre markedets funksjon gjennom å stille sikkerhetskrav til nettverks- og informasjonssystemer som er nødvendige for å opprettholde leveransen av samfunnsviktige tjenester.

Komiteen viser til at den omfattende digitaliseringen som preger samfunnsutviklingen, er et viktig premiss for effektivisering av samfunnet, verdiskaping og økonomisk vekst. Digitale systemer er sentrale for alle samfunnsfunksjoner. Digital sikkerhet er derfor helt avgjørende for å ivareta velferdssamfunnet, viktige samfunnsfunksjoner og nasjonale interesser. Den sikkerhetspolitiske situasjonen i verden er i endring, noe som påvirker det nasjonale trusselbildet og skaper sikkerhetsmessige utfordringer. Komplekse trusler og verdikjeder fordrer helhetlige sikkerhetstiltak og myndighetenes kontroll av disse.

Komiteen viser videre til at loven vil være et utgangspunkt for videre kravstilling og regulering innen digital sikkerhet. NIS-direktivet av 6. juli 2016 ble først besluttet tatt inn i EØS-avtalen 3. februar 2023. NIS2-direktivet (EU) 2022/2555 ble vedtatt i EU 14. desember 2022. Innen 24. oktober 2024 skal medlemsstatene ha gjennomført direktivet i nasjonal rett. Fra dette tidspunktet oppheves gjeldende NIS-direktiv. Dersom NIS2-direktivet blir en del av EØS-avtalen, vil dette medføre behov for lovendringer og endringer i tilhørende forskrifter. Det vil også bli behov for å kartlegge relevant sektorspesifikt regelverk og vurdere eventuelle behov for endringer eller tilpasninger som følge av NIS2-direktivet.

Komiteen viser til at bakgrunnen for NIS2-direktivet er erkjennelsen av at selv om NIS-direktivet har vært en viktig start på reguleringen av sikkerhet i EU, har implementeringen avdekket flere mangler som forhindrer direktivet fra effektivt å adressere aktuelle og fremtidige utfordringer innen digital sikkerhet. Det har blant annet vært en fragmentert tilnærming i de ulike EU-landene til kravene i direktivet, noe som har medført økte kostnader for virksomheter som tilbyr tjenester på tvers av landegrenser. Det har også vært ulik praksis i utpekingen av virksomheter som er omfattet av NIS-direktivet.

Komiteen vil peke på at i NIS2-direktivet ønsker kommisjonen å redusere fragmenteringen og øke harmoniseringen gjennom mer effektivt samarbeid mellom kompetente myndigheter fra hver medlemsstat, gjennom underleggelse av flere sektorer og gjennom sanksjoner som kan brukes til effektiv håndheving.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet, Fremskrittspartiet og Venstre, viser til at det råder liten tvil om at det er et betydelig behov for økt fokus på sikkerhet og beredskap, også ved bruk av IT og IT-basert samfunnskritisk infrastruktur. Flertallet viser til at den skjerpede sikkerhetspolitiske situasjonen, spesielt med henblikk på Russland og Kina, fortsatt går mot en forverring.

Komiteens medlemmer fra Høyre, Fremskrittspartiet og Venstre viser til at det i NSMs rapport om digital sikkerhet av i år, «Nasjonalt digitalt risikobilde 2023», pekes på at beredskapen for å håndtere omfattende cyberangrep mot Norge har store mangler. Evnen til å oppdage digitale angrep i Norge er for dårlig, og det mangler helhetlig styring og koordinering av IT-sikkerhet på tvers av statlige etater.

Disse medlemmer merker seg at det i rapporten pekes på at ettersom stadig flere industrielle anlegg kobles fysisk til internett, øker faren for at cyberangrep også kan lamme fysisk infrastruktur. NSM mener at det trengs bedre koordinering, deteksjon og beredskap for å tette igjen disse hullene før de utnyttes av fiendtlige aktører. Samtidig må kritisk infrastruktur sikres bedre mot digitale trusler.

Disse medlemmer viser til at det i rapporten advares av NSM mot målrettede cyberangrep mot energi- og petroleumssektoren med potensial til å lamme kritisk infrastruktur i Norge og Europa. I kjølvannet av at Norge har blitt en svært viktig gassleverandør til kontinentet, trekkes cybertrusler mot gassforsyning spesielt frem. I rapporten påpekes det at vellykkede hackerangrep kan få store konsekvenser som strømbrudd og stans i gassleveransene til Europa.

Disse medlemmer viser også til at petroleumsbransjen nylig har blitt underlagt sikkerhetsloven ved at «kontroll med utvinning av petroleum på norsk sokkel» og «transport av gass i rør til Europa» har blitt definert som grunnleggende nasjonale funksjoner (GNF) som skal ivaretas. I petroleumsbransjen er imidlertid hovedprinsippet i sikkerhetsreguleringen at hvis man ikke har kontroll over situasjonen, skal man stenge ned produksjon og evakuere personell for å sikre liv og helse, verdier og miljø. Myndighetsreguleringen er derfor i mindre grad fokusert på å ivareta leveransesikkerhet i situasjoner som er utenfor det normale.

Disse medlemmer viser i den forbindelse til høringsinnspillet fra Det norske Veritas (DNV), hvor det fremholdes at sikkerhetsloven og digitalsikkerhetsloven

«på mange måter [har] et 'motsatt' fokus som den gjeldende sektorbaserte sikkerhetsreguleringen».

DNV anbefaler derfor at myndighetene ved implementeringen av digitalsikkerhetsloven vier særskilt oppmerksomhet til lovens forhold til den sektorbaserte sikkerhetsreguleringen i petroleumsnæringen, og at dette bør skje i nær dialog med både sektortilsyn og relevante næringsaktører, en anbefaling disse medlemmer støtter.

Disse medlemmer viser videre til at NSM i sin rapport peker på at man i løpet av det siste året har sett bølger av tjenestenektangrep fra pro-russiske aktører, som har truffet virksomheter i transport-, finans- og helsesektoren, sektorer som NSM tidligere ikke har sett på som mål for denne typen hendelser. Dataangrep rammer i økende grad flere mål samtidig, med en økende grad av profesjonalisering i alle ledd i angrepskjeden. Innbruddsmetoder endrer seg raskt på taktisk nivå, og flere nulldagssårbarheter kommer til syne.

Komiteens medlemmer fra Arbeiderpartiet og Senterpartiet vil understreke at regjeringen har kommet med en rekke kraftfulle satsinger for å møte den endrede sikkerhetspolitiske situasjonen. Disse medlemmer viser til at regjeringen våren 2022 foreslo å styrke den sivile beredskapen med en halv milliard.

Disse medlemmer bemerker at regjeringen har fremmet en stortingsmelding om nasjonal kontroll og digital motstandskraft, med flere sentrale tiltak for å styrke den digitale beredskapen, og at det nå fremmes et lovforslag om digital sikkerhet. Dette er den første loven om digital sikkerhet i Norge.

Disse medlemmer viser videre til at det etableres en nasjonal portal for digital sikkerhet for bedre å tilgjengeliggjøre nasjonale råd og veiledninger, samt et støtteverktøy for norske virksomheter for å forenkle arbeidet med å følge opp nasjonale råd.

Disse medlemmer merker seg også at arbeidet med å kartlegge verdier både innenfor og utenfor sikkerhetsloven er intensivert for å sikre bedre oversikt over den nasjonale sikkerhetstilstanden, i tillegg at det også blir arbeidet med en ny ekomlov med skjerpede sikkerhetskrav, bl.a. sikkerhetskrav til datasentre og en registreringsplikt for datasenteraktører. Disse medlemmer viser også til at det jobbes med å etablere en nasjonal skytjeneste.

Saklig virkeområde

Komiteen viser til at digitalsikkerhetsloven retter seg mot virksomheter som leverer tjenester som er viktige for et velfungerende samfunn og næringsliv. Virksomhetene er delt i to hovedkategorier: tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester.

Komiteen merker seg at en virksomhet skal anses som tilbyder av en «digital tjeneste» dersom den tilbyr nettbaserte markedsplasser, nettbaserte søkemotorer og skytjenester. På dette området er hensikten å få ensartede regler i hele EØS, hva gjelder både virkeområde og sikkerhets- og varslingsplikter. De aktuelle virksomhetene må dermed vurdere om de er omfattet, ut ifra lovforslagets bestemmelser.

Komiteen viser også til at en virksomhet skal anses som tilbyder av en «samfunnsviktig tjeneste» dersom tre kumulative vilkår er oppfylt. Det første kriteriet er at virksomheten må tilby en tjeneste som er viktig for opprettholdelsen av kritiske samfunnsmessige eller økonomiske aktiviteter innen samfunnssektorene energi, transport, helse, bank, finansmarkedsinfrastruktur, drikkevannsforsyning og -distribusjon og digital infrastruktur. Det er kun den delen av virksomheten som leverer den aktuelle tjenesten, som omfattes. Eksempelvis vil trafikkstyringen på en stor flyplass omfattes, mens butikkområdet ikke omfattes. Det andre kriteriet er at tjenesteleveransen må være avhengig av nettverks- og informasjonssystemer. Det tredje kriteriet er at en hendelse i virksomhetens nettverks- og informasjonssystemer ville hatt «betydelig forstyrrende virkning» på leveransen av den samfunnsviktige tjenesten. Vurderingstemaet knytter seg ikke til virksomhetens tjenesteleveranse isolert sett, men til tjenesteleveranse i en samfunnssammenheng. Det er altså spørsmål om i hvilken grad det går ut over samfunnets tilgang på en viss tjeneste at den aktuelle virksomheten ikke leverer sitt bidrag til totalen som normalt.

Komiteen viser til at ved identifisering av virksomheter underlagt loven vil det som utgangspunkt være to mulige tilnærminger, enten utpeking ved enkeltvedtak (ovenfra og ned) eller selvidentifisering basert på nærmere fastsatte kriterier og terskelverdier (nedenfra og opp). Ovenfra-og-ned-tilnærmingen er for eksempel valgt for utpeking av grunnleggende nasjonale funksjoner og virksomheter med avgjørende betydning for disse etter sikkerhetsloven. Fordelen med en slik tilnærming er at den gir sektormyndighetene god oversikt over verdikjedene og avhengighetene i sektoren. Ulempen er at en slik løsning blir svært tid- og ressurskrevende, da loven vil ha et vesentlig bredere nedslagsfelt enn sikkerhetsloven. På den andre siden vil en nedenfra-og-opp-tilnærming gi sektormyndighetene mindre kontroll.

Komiteen merker seg at en nedenfra-og-opp-tilnærming, der virksomhetene selv vil identifisere seg, etter departementets syn fremstår som den mest hensiktsmessige. For å sikre at virksomheter som ikke tilfredsstiller terskelverdiene, men som kan være i en særstilling og slik likevel har en rolle som gjør at de bør omfattes av loven, mener departementet at det vil være hensiktsmessig at sektormyndighet gis anledning til å

utpeke enkeltvirksomheter loven skal gjelde for. Dette vil gi sektormyndighetene nødvendig fleksibilitet og ligner på vedtakskompetansen som sikkerhetsmyndigheten har etter sikkerhetsloven.

Komiteen viser til at det etter NIS-direktivet i stor grad er opp til medlemsstatene å fastsette hvilke aktører som oppfyller kriteriene for å bli klassifisert som tilbyder av samfunnsviktige tjenester. Fordi virkeområdet etter gjeldende direktiv er snevert og ikke klart angitt i direktivet, medfører dette en krevende utpekingsprosess. I EU-landene har denne prosessen medført et stort sprik i hvordan medlemsstatene har definert virkeområdet nærmere, og medført at enkelte grenseoverskridende virksomheter ikke har blitt identifisert. Komiteen viser også til at Justis- og beredskapsdepartementet i et posisjonsnotat av 23. august 2023 skriver at

«det anses som positivt at dette tydeliggjøres i det nye direktivet, da et vil gi mer forutberegnelighet og være prosessbesparende».

Komiteen viser videre til at det i NIS2-direktivet er fastsatt mer enhetlige kriterier for hvilke aktører som skal omfattes av direktivet. NIS2-direktivet innlemmer flere sektorer som anses som kritiske for både økonomien og samfunnet. De nye sektorene er forvaltning av IKT-tjenester, post- og kurertjenester, avfallshåndtering, fremstilling, produksjon og distribusjon av kjemikalier og produksjon av visse typer utstyr og forskning.

Alle virksomheter av en viss størrelse og en viss type skal være omfattet. Også mindre virksomheter som anses for å ha en nøkkelrolle for samfunnet, økonomien eller en viss sektor, omfattes av direktivet. Dette kan være tilfelle for mindre virksomheter som er eneleverandør til et EU-land, eller som driver en særskilt utsatt virksomhet. Slike virksomheter skal identifiseres og jevnlig innmeldes til Kommisjonen (og eventuelt, for Norges del, EFTAs overvåkingsorgan). NIS2-direktivet skiller mellom vesentlige og viktige samfunnsviktige tjenester.

Komiteen viser til at Justis- og beredskapsdepartementet i et posisjonsnotat av 23. august 2023 skriver at departementet

«anser NIS2 som et positivt tilskudd for å høyne sikkerhetsnivået og forbedre samarbeidet om IKT-sikkerhet i Europa. Det anses som positivt at EU satser på digital sikkerhet, og det er viktig at Norge deltar på denne arenaen».

Krav om sikkerhet

Komiteen viser til at en rekke virksomheter per i dag er underlagt sikkerhetskrav av ulik art, men at det i mange tilfeller er uklart om disse kan tolkes slik at det stilles krav om digital sikkerhet. Departementet mener derfor at det er behov for bestemmelser som stiller krav til digital sikkerhet i virksomhetene som er omfattet av lovforslaget.

Komiteen merker seg at tilbydere av samfunnsviktige tjenester skal treffe tekniske og organisatoriske tiltak som er hensiktsmessige og står i et rimelig forhold til risikoen som knytter seg til nettverkene og informasjonssystemene. Det er departementets vurdering at hvis tilbydere følger «NSMs grunnprinsipper for IKT-sikkerhet», vil de ivareta kravene som fremgår av loven.

Hva tilbydere av digitale tjenester angår, viser komiteen til at det går tydelig frem av fortalen til NIS-direktivet at det skal stilles mindre strenge sikkerhetskrav til tilbydere av digitale tjenester, da de anses noe mindre viktige enn de samfunnsviktige tjenestene. Ut over den generelle føringen i direktivet om at det skal stilles noe mindre strenge krav til tilbydere av digitale tjenester, gis det ikke særlige føringer på hva dette betyr i praksis. På grunn av digitale tjenesters grensekryssende natur bør de være underlagt et regelverk som er harmonisert i hele EØS. Dette er ivaretatt gjennom gjennomføringsordningen, som etterlater lite rom for nasjonale tilpasninger. I tråd med direktivet er momenter som skal hensyntas, konkretisert i lovforslaget § 10 andre ledd bokstav a til e. Med unntak av dette er §§ 7 og 10 likelydende.

Komiteen viser til at kravene om sikkerhet reguleres nærmere i forskrift. Samtidig må nærhetsprinsippet og sektoransvaret tas i betraktning. Hvilke tiltak som bør iverksettes, kan variere avhengig av hvilken sektor det er tale om, og den enkelte tilbyders egenart. Kravene som stilles etter loven og direktivet, utgjør minimumskrav til digital sikkerhet, og de er ikke til hinder for at tilbyderne iverksetter strengere sikkerhetstiltak enn de som følger av direktivet og loven.

Komiteen merker seg at NIS2-direktivet styrker sikkerhetskravene som stilles til tilbydere, sammenlignet med NIS-direktivet. I NIS2-direktivet oppstilles det i tillegg en risikostyringsmetode med en minimumsliste over grunnleggende sikkerhetselementer som må legges til grunn for sikkerhetsarbeidet, blant annet krav om at tilbydere håndterer cybersikkerhetsrisiko i forsyningskjeder og hos leverandører, planer for vedlikehold, overvåkning og testing samt bruk av krypto.

Krav om varsling

Komiteen viser til at det i loven etableres likelydende varslingskrav for de to kategoriene av tilbydere, selv om det legges opp til en nyanseforskjell i varslingskravene i NIS-direktivet. Varsling skal skje ved hendelser som «virker betydelig inn på tjenesteleveransen», og varsling skal skje «uten unødig opphold». Dersom det er behov for å fange opp nyanseforskjellen direktivet legger opp til, kan dette gjøres i forskrift. Departementet legger videre opp til at tidspunktet for varsling presise-

res ytterligere i forskrift, og at fristen for å varsle vil kunne bero på blant annet hvilken sektor tilbyderen tilhører.

Komiteen merker seg at det i NIS2-direktivet innføres mer presise bestemmelser om prosessen for varsling av hendelser, hva det skal varsles om, og når. Etter artikkel 23 nr. 1 skal det varsles om hendelser som har en betydelig innvirkning på tjenesteleveransen, i nr. 3 står det beskrevet hva som utgjør en slik hendelse, og i nr. 4 er det angitt detaljerte bestemmelser om tidspunktene for varsling.

Tilsyn

Komiteen viser til at NIS-direktivet artikkel 8 og 9 bestemmer at statene skal utpeke eller etablere et nasjonalt kontaktpunkt, én eller flere kompetente myndigheter og ett eller flere hendelseshåndteringsmiljøer. Særlig fordi mange virksomheter per i dag ikke er underlagt tilsyn med digital sikkerhet, foreslår departementet bestemmelser om tilsyn og sanksjoner som er ment å dels tilsvare direktivets krav, med mulighet for å gi nærmere bestemmelser om tilsyn i forskrift.

Komiteen merker seg at departementet ser det som hensiktsmessig å gi hjemmel i lov til å gi forskrift om nasjonalt kontaktpunkt, samtidig som departementet utpeker Nasjonal sikkerhetsmyndighet (NSM) som en naturlig kandidat til rollen.

Komiteen viser videre til at departementet ser for seg en tilsynsmodell der myndigheter med sektoransvar fører tilsyn etter loven i den enkelte sektor. En forutsetning for en slik modell er at sektormyndighetene har tilstrekkelig kompetanse innenfor digital sikkerhet og gjennomføring av tilsyn. Der sektormyndighetene ikke allerede besitter nødvendig kompetanse innen digital sikkerhet, forutsettes det at loven vil kunne fungere som en pådriver for opparbeidelse av kompetanse på feltet.

Komiteen merker seg at det i tråd med NIS-direktivet legges til rette for forskjellige tilsynsregimer for henholdsvis tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester. Departementet ser det som mest hensiktsmessig at dette gjøres i forskrift. Der kan det eksempelvis reguleres at det bare føres tilsyn med en tilbyder av digitale tjenester dersom det foreligger informasjon om at tilbyderen ikke overholder kravene i direktivet, og at den ikke kan bli gjenstand for uanmeldt tilsyn.

Komiteen merker seg at NIS2-direktivets skille mellom vesentlige og viktige samfunnsviktige tjenester innebærer at de underlegges forskjellige tilsynsregimer. Tilbydere av samfunnsviktige tjenester skal underlegges et mindre strengt tilsynsregime enn tilbydere av vesentlige samfunnsviktige tjenester. Direktivet innfører mer detaljerte og strengere tiltak for nasjonale tilsynsmyndigheter og tar sikte på å harmonisere sanksjonsregimer i medlemslandene.

Pålegg, tvangsmulkt og overtredelsesgebyr

Komiteen viser til at det i mange sektorer er etablert sektorregelverk som har sanksjonsbestemmelser, samtidig som det for mange sektorer er uklart om sanksjonsbestemmelsene omfatter digital sikkerhet. I NIS-direktivet stilles det krav om at EØS-statene fastsetter regler om sanksjoner ved brudd på forpliktelsene etter direktivet. Sanksjonene skal være virkningsfulle, stå i et rimelig forhold til overtredelsen og virke avskrekkende. Det skilles ikke mellom tilbydere av samfunnsviktige og digitale tjenester i direktivets sanksjonsbestemmelse.

Komiteen viser til at det i loven foreslås å gi tilsynsmyndigheten kompetanse til å pålegge den som overtrer lovens bestemmelser, å bringe de ulovlige forholdene til opphør, og at pålegg kan gis i tilknytning til brudd på loven og forskrifter gitt i medhold av loven. Påleggskompetansen er ikke avgrenset til grove eller gjentatte brudd på loven og kan gis uavhengig av subjektiv skyld.

Komiteen viser videre til at det i loven foreslås å gi tilsynsmyndigheten hjemmel til å ilegge tvangsmulkt. Tvangsmulkt kan ilegges uavhengig av subjektiv skyld og uavhengig av omfanget av overtredelsen. Tvangsmulktens størrelse skal fastsettes under hensyn til hvor viktig det er at pålegget blir gjennomført, og hvilke kostnader det antas å medføre. Tvangsmulkt skal fungere som et pressmiddel, og utgangspunktet er at mulkten skal være så stor at den er effektiv uten å være urimelig.

Komiteen peker på at departementet videre foreslår en bestemmelse om overtredelsesgebyr som gjelder alle tilbydere som omfattes av loven. Det skal kunne reageres med overtredelsesgebyr ved brudd på plikten både til å sikre og til å varsle og der det er gitt uriktige eller ufullstendige opplysninger til tilsynsmyndigheten.

Komiteen merker seg at NIS2-direktivet i mye mer detalj regulerer hvordan overtredelser av direktivet skal sanksjoneres. Blant annet pålegges medlemsstatene å sørge for at tilsynsmyndigheten har mulighet til å ilegge administrativ sanksjon ved overtredelse av direktivet. I direktivet gis det nærmere bestemmelser om administrative sanksjoner, og det oppstilles størrelsestak ved overtredelsesgebyr.

Samarbeidsmekanismer på EU-nivå

Avslutningvis merker komiteen seg at NIS2-direktivet skal styrke sikkerheten i forsyningskjeden for viktige informasjons- og kommunikasjonsteknologier på europeisk nivå. Det legges opp til et tettere samarbeid mellom Kommisjonen og ENISA om å utføre koordinerte risikovurderinger av kritiske forsyningskjeder. Direktivet forplikter medlemsstatene til å sikre at myndighetene har anledning til å pålegge bøter av en nærmere angitt maksimalsats.

Komiteen merker seg også at NIS2-direktivet forbedrer NIS-samarbeidsgruppens rolle i utformingen av

øvrige strategiske politiske beslutninger om ny teknologi og nye trender. CSIRT-nettverket videreføres, men det opprettes også et nytt nettverk: European cyber crisis liaison organisation network (EU-CyCLONe). Sammen skal disse foraene øke informasjonsdeling og samarbeid mellom myndighetene i medlemsstatene og forbedre det operative samarbeidet, inkludert cyberkrisehåndtering. NIS2-direktivet etablerer også et grunnleggende rammeverk for koordinert offentliggjøring av sårbarheter for nylig oppdagede sårbarheter i hele EU. Det skal opprettes et register for sårbarheter, som skal forvaltes av ENISA.

Komiteen registrerer at departementet i posisjonsnotatet av 23. august 2023 skriver at det

«anser det som viktig at Norge gis adgang til å delta i samarbeidet som videreføres fra gjeldende direktiv, blant annet CSIRT-nettverket, NIS-samarbeidsgruppen og EU-CyCLONe, men også andre nyetablerte samarbeidsfora som følger av dette forslaget og ny strategi om cybersikkerhet».

Komiteens medlemmer fra Høyre, Fremskrittspartiet og Venstre viser til at et av hovedformålene med NIS2-direktivet er å rette opp i flere mangler i NIS-direktivet som forhindrer det fra å effektivt adressere aktuelle og fremtidige utfordringer innen digital sikkerhet. Den fragmenterte tilnærmingen i de ulike landene til kravene i direktivet har eksempelvis medført økte kostnader for virksomheter som tilbyr tjenester på tvers av landegrenser. Med NIS2-direktivet ønsker kommisjonen å redusere fragmentering og øke harmonisering, blant annet gjennom underleggelse av flere sektorer og mer effektivt samarbeid mellom kompetente myndigheter fra hver medlemsstat.

Disse medlemmer merker seg i den forbindelse at DNV i sitt høringssvar peker på at mange norske virksomheter opererer i EU og derfor allerede nå må forberede seg på krav for å etterleve NIS2-direktivet og CER-direktivet, og at disse direktivene dekker et bredere spekter av trusler enn digitale angrep. For norske selskaper som opererer internasjonalt, vil det derfor være viktig at digitalsikkerhetsloven

«så langt som mulig 'harmoniseres' og tilrettelegger for senere tilpasninger av forventede krav etter både NIS2 og CER».

Disse medlemmer viser til at departementet er positive til NIS2-direktivet, og at deres «foreløpige vurdering er at direktivet er EØS-relevant og akseptabelt for Norges del». Disse medlemmer viser videre til at regjeringen kan vedta nasjonalt regelverk i tråd med EU-regelverk selv om det foreløpig ikke er fattet EØS-komitévedtak. Disse medlemmer spør seg om NIS-direktivet og NIS2-direktivet ikke er et slikt tilfelle, gitt at NIS2-direktivet ble vedtatt allerede før NIS-direktivet ble tatt inn i EØS-avtalen, og at regjeringen er positiv til endringene som ligger i NIS2-direktivet. Disse medlemmer mener det er hensiktsmessig å vurdere hvilke tilpasninger som kan gjøres allerede nå for å tilfredsstille kravene i NIS2-direktivet, uavhengig av prosessen med å ta NIS2-direktivet inn i EØS-avtalen.

På denne bakgrunn fremmer komiteens medlemmer fra Høyre og Venstre følgende forslag:

«Stortinget ber regjeringen vurdere hvilke tilpasninger som må gjøres i lov om digital sikkerhet for å tilfredsstille kravene i NIS2-direktivet, og sende forslag til endringer på høring uavhengig av prosessen med å ta NIS2-direktivet inn i EØS-avtalen.»

Når det gjelder forslaget fra Høyre og Venstre, viser komiteens medlemmer fra Arbeiderpartiet og Senterpartiet til at regjeringen er i gang med å utrede gjennomføringen av NIS2. Dette vurderes i sammenheng med CER-direktivet, og regjeringen vurderer det som svært viktig å se disse to tingene i sammenheng. Disse medlemmer mener at forslaget fra Høyre og Venstre ikke vil bringe oss raskere til målet, og vil derfor ikke støtte det.

Forslag fra mindretall

Forslag fra Høyre og Venstre:

Forslag 1

Stortinget ber regjeringen vurdere hvilke tilpasninger som må gjøres i lov om digital sikkerhet for å tilfredsstille kravene i NIS2-direktivet, og sende forslag til endringer på høring uavhengig av prosessen med å ta NIS2-direktivet inn i EØS-avtalen.

Komiteens tilråding

Komiteens tilråding fremmes av en samlet komité.

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

vedtak til lov

om digital sikkerhet (digitalsikkerhetsloven)

Kapittel 1. Innledende bestemmelser

§ 1 *Formål*

Loven skal bidra til å sikre grunnleggende krav til digital sikkerhet i virksomheter med særlig betydning for samfunnet ved å forebygge, avdekke og motvirke uønskede hendelser i nettverks- og informasjonssystemer som brukes for å levere samfunnsviktige tjenester og di-

gitale tjenester. Loven skal også legge til rette for sikkerhet i IKT-produkter, IKT-tjenester og IKT-prosesser.

§ 2 *Saklig virkeområde*

Loven gjelder for

a. tilbydere av samfunnsviktige tjenester etter § 6 i sektorene energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur
b. tilbydere av digitale tjenester etter § 9.

Loven gjelder ikke for virksomheter som er omfattet av lov om elektroniske tillitstjenester.

Kongen kan gi forskrift med nærmere bestemmelser om og unntak fra lovens virkeområde.

§ 3 *Geografisk virkeområde*

Loven gjelder for

a. tilbydere av samfunnsviktige tjenester som er etablert i Norge
b. tilbydere av digitale tjenester som har sitt hovedkontor i Norge, eller som har eller skal ha en representant i Norge etter § 12.

Kongen kan gi forskrift om lovens anvendelse for Svalbard, Jan Mayen og bilandene og fastsette særlige regler som er nødvendige av hensyn til de stedlige forholdene.

§ 4 *Definisjoner*

I denne loven menes med

1. nettverks- og informasjonssystemer:
   a. elektronisk kommunikasjonsnett som nevnt i ekomloven § 1-5 nr. 2
   b. en enhet eller en gruppe av sammenkoblede eller beslektede enheter som behandler digitale data automatisk ved hjelp av et program
   c. digitale data som lagres, behandles, innhentes eller overføres ved hjelp av elementer som nevnt i bokstav a eller b for at dataene skal kunne driftes, vernes, beskyttes eller vedlikeholdes.
2. sikkerheten i nettverks- og informasjonssystemer: evnen nettverk eller informasjonssystemer har til å tåle, på et gitt tillitsnivå, enhver handling som går ut over tilgjengeligheten, autentisiteten, integriteten eller tilliten til lagrede, overførte eller behandlede data eller tilknyttede tjenester som tilbys eller er tilgjengelige via slike nettverks- og informasjonssystemer
3. hendelse: enhver hendelse med negativ virkning på sikkerheten i nettverks- og informasjonssystemer.

§ 5 *Forholdet til andre lover som stiller krav om sikkerhet og varsling*

Kravene om sikkerhet og varsling i §§ 7, 8, 10 og 11 gjelder så langt det ikke er fastsatt tilsvarende eller strengere krav i eller i medhold av annen lov.

Kapittel 2. Krav til tilbydere av samfunnsviktige tjenester

§ 6 *Tilbydere av samfunnsviktige tjenester*

Som tilbyder av en samfunnsviktig tjeneste regnes virksomheter som

a. leverer en tjeneste som er viktig for å opprettholde kritiske samfunnsmessige eller økonomiske aktiviteter
b. er avhengig av nettverks- og informasjonssystemer for å levere tjenesten, og
c. kan få tjenesteleveransen betydelig forstyrret av en hendelse.

Ved vurderingen av om en hendelse kan betydelig forstyrre en tjenesteleveranse, skal det særlig legges vekt på

a. antallet brukere som er avhengig av tjenesten
b. i hvilken grad andre samfunnssektorer som er nevnt i § 2, er avhengig av tjenesten
c. hvilken virkning en hendelse kan ha i form av omfang og varighet for økonomiske og samfunnsmessige aktiviteter eller samfunnssikkerheten
d. virksomhetens markedsandel
e. størrelsen på det geografiske området som kan bli påvirket av en hendelse
f. den berørte virksomhetens betydning for at det er tilstrekkelig tilgang på tjenesten, tatt i betraktning hvilke alternativer som finnes
g. særlige sektorspesifikke forhold.

Kongen kan gi forskrift om hvilke virksomheter som skal regnes som tilbydere av samfunnsviktige tjenester.

§ 7 *Krav om sikkerhet for tilbydere av samfunnsviktige tjenester*

En tilbyder av en samfunnsviktig tjeneste skal gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenesten.

Tilbyderen skal iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak som samlet skal sørge for et sikkerhetsnivå som er tilpasset risikoen. Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, skal det blant annet ses hen til den teknologiske utviklingen.

Tilbyderen skal iverksette proporsjonale tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser, slik at tjenesteleveransen kan opprettholdes.

§ 8 *Krav om varsling for tilbydere av samfunnsviktige tjenester*

En tilbyder av en samfunnsviktig tjeneste skal uten unødig opphold og uten hinder av taushetsplikt varsle det organet Kongen utpeker, om hendelser som virker betydelig inn på tjenesteleveransen. Ved vurderingen av om innvirkningen er betydelig, skal det blant annet legges vekt på antallet brukere som påvirkes, hendelsens varighet og størrelsen på det geografiske området som berøres.

Kapittel 3. Krav til tilbydere av digitale tjenester

§ 9 *Tilbydere av digitale tjenester*

Som tilbyder av en digital tjeneste regnes virksomheter som tilbyr tjenester som definert i ehandelsloven § 1 andre ledd bokstav a og b i form av nettbaserte markedsplasser, nettbaserte søkemotorer eller skytjenester.

Med nettbasert markedsplass menes en tjeneste som gjør det mulig for forbrukere og næringsdrivende å inngå nettbaserte salgs- eller tjenesteavtaler med næringsdrivende, enten på nettstedet til den nettbaserte markedsplassen eller på nettstedet til en næringsdrivende som bruker datatjenester som leveres av den nettbaserte markedsplassen.

Med nettbasert søkemotor menes en tjeneste som gjør det mulig for brukere å foreta søk på i prinsippet alle nettsteder eller nettsteder på et bestemt språk, på grunnlag av et nøkkelord, en setning eller andre inndata, og som viser lenker hvor det er mulig å finne informasjon om det forespurte innholdet.

Med skytjeneste menes en tjeneste som gir tilgang til en skalerbar og fleksibel samling av delbare databehandlingsressurser.

Kongen kan gi forskrift om hvilke virksomheter som skal regnes som tilbydere av digitale tjenester.

§ 10 *Krav om sikkerhet for tilbydere av digitale tjenester*

En tilbyder av en digital tjeneste skal gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenesten.

Tilbyderen skal iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak som samlet skal sørge for et sikkerhetsnivå som er tilpasset risikoen. Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, skal det blant annet ses hen til den teknologiske utviklingen og tas hensyn til

a. sikkerheten i systemer, utstyr og anlegg
b. hendelseshåndtering
c. styring av opprettholdelse av tjenesteleveransen
d. overvåking, revisjon og testing
e. anerkjente internasjonale standarder.

Tilbyderen skal iverksette proporsjonale tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser, slik at tjenesteleveransen kan opprettholdes.

§ 11 *Krav om varsling for tilbydere av digitale tjenester*

En tilbyder av en digital tjeneste skal uten unødig opphold og uten hinder av taushetsplikt varsle det organ Kongen utpeker, om hendelser som virker betydelig inn på tjenesteleveransen. Ved vurderingen av om innvirkningen er betydelig, skal det legges vekt på antall brukere som påvirkes, hendelsens varighet, størrelsen på det geografiske området som berøres, omfanget av funksjonalitetssvikten i tjenesten og omfanget av innvirkningen på økonomisk og samfunnsmessig aktivitet.

§ 12 *Plikt til å utpeke en representant i Norge*

En tilbyder av digitale tjenester som ikke har sitt hovedkontor i Norge eller en annen EØS-stat, og som tilbyr digitale tjenester i Norge, skal utpeke en representant i Norge, med mindre tilbyderen har utpekt en representant i en annen EØS-stat hvor tjenestene tilbys.

Kapittel 4. Tilsyn og administrative reaksjoner

§ 13 *Tilsyn*

Kongen utpeker én eller flere tilsynsmyndigheter som skal føre tilsyn med tilbydere som omfattes av loven.

§ 14 *Opplysningsplikt og tilgang til lokaler og utstyr*

Tilbydere og de som handler på vegne av en tilbyder, har plikt til å gi de opplysningene som tilsynsmyndigheten krever for å utføre sine oppgaver, og gi tilsynsmyndigheten tilgang til virksomhetens lokaler og utstyr og yte nødvendig bistand ved tilsynsmyndighetens undersøkelser.

Første ledd gjelder uten hinder av lovbestemt taushetsplikt.

§ 15 *Pålegg om retting*

Ved overtredelse av bestemmelser gitt i eller i medhold av denne loven kan tilsynsmyndigheten gi tilbydere pålegg om at forholdet skal bringes i orden. Når det gis pålegg, skal det settes en frist for oppfyllelse.

§ 16 *Tvangsmulkt*

Tilsynsmyndigheten kan treffe vedtak om tvangsmulkt for å sikre at pålegg etter § 15 blir oppfylt. Tvangsmulkten kan fastsettes som en løpende mulkt eller som et engangsbeløp.

Tilsynsmyndigheten kan i særlige tilfeller frafalle påløpt tvangsmulkt.

§ 17 *Overtredelsesgebyr*

Tilsynsmyndigheten kan ilegge overtredelsesgebyr dersom en tilbyder eller noen som handler på dennes vegne, forsettlig eller uaktsomt overtrer §§ 7, 8, 10, 11 eller 14.

Dersom den ansvarlige for overtredelsesgebyret er et foretak som inngår i et konsern, hefter foretakets morselskap og morselskapet i det konsern selskapet er en del av, subsidiært for beløpet.

Adgangen til å ilegge overtredelsesgebyr foreldes fem år etter at overtredelsen er opphørt. Fristen avbrytes ved at myndigheten gir forhåndsvarsel om eller fatter vedtak om overtredelsesgebyr.

Kapittel 5. Utfyllende regler mv.

§ 18 *Forskrifter*

Kongen kan gi forskrift om

a. krav til sikkerhet og varsling i samsvar med §§ 7, 8, 10 og 11, herunder hva som regnes som tilsvarende krav etter § 5
b. gjennomføring av tilsyn med tilbydere underlagt loven
c. opplysningsplikt og tilgang til lokaler og utstyr etter § 14
d. ileggelse og utmåling av tvangsmulkt og overtredelsesgebyr
e. at den som forsettlig eller uaktsomt overtrer forskrift gitt i medhold av bokstav a, kan ilegges overtredelsesgebyr
f. gjennomføring av forpliktelser som følger av EØS-avtalen og andre internasjonale avtaler, og som understøtter lovens regler eller formål
g. behandling av personopplysninger, blant annet om formålet med behandlingen, behandlingsansvar, hvilke personopplysninger som kan behandles, viderebehandling, utlevering og sletting
h. nasjonalt kontaktpunkt for sikkerhet i nettverks- og informasjonssystemer.

Kapittel 6. Sikkerhetssertifisering

§ 19 *Sikkerhetssertifisering av informasjons- og kommunikasjonsteknologi*

Kongen kan gi forskrift om sikkerhetssertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser for å gjennomføre forpliktelser etter EØS-avtalen. Dette omfatter også

a. utpeking av sertifiseringsmyndighet
b. tilsyn med sertifiseringsorganer som tilbyr sikkerhetssertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser
c. pålegg om retting, tvangsmulkt og overtredelsesgebyr ved overtredelse av krav til sikkerhetssertifisering.

Kapittel 7. Sluttbestemmelser

§ 20 *Ikrafttredelse*

Loven trer i kraft fra den tiden Kongen bestemmer. De enkelte bestemmelsene kan settes i kraft til ulik tid.

Oslo, i justiskomiteen, den 21. november 2023

Per-Willy Amundsen
leder

Ingvild Wetrhus Thorsvik
ordfører

Svanemerketrykksak, 2041 0654 Trykk og layout: Stortingets administrasjon