Høringsinnspill forslag til forskrift til lov 20. desember 2023 nr. 108 om digital sikkerhet (digitalsikkerhetsloven) fra Juristforbundet

Innledning

-Norge har alle forutsetninger for å bli verdens mest digitaliserte land. Nå kommer taktskiftet i digitaliseringen av Norge. Det betyr en enklere og tryggere hverdag for folk, et mer konkurransedyktig næringsliv og en mer moderne offentlig sektor.

Dette uttalte statsminister Støre ved fremleggelsen av den nye nasjonale digitaliseringsstrategien 26.09.2024. Dette er et ambisiøst mål som Juristforbundet deler. Og det er et mål og visjon som passer det tradisjonelt tillitsbaserte norske demokratiet og virkelighetsbildet godt.

Spørsmålet er om Norge ruster seg godt nok for en ny virkelighet. Som er her akkurat nå og hvor ulike aktører ønsker å bryte ned både demokratiet og tillitssamfunnet som vi har tatt for gitt. Vi befinner oss i en svært usikker sikkerhetspolitisk situasjon med et forhøyet konfliktnivå, økende ustabilitet og verdens maktsentra deltar i et teknologikappløp. Hvor demokratienes samlede evne til å identifisere og motstå uønsket informasjonsinnflytelse fra fremmede makter eller andre aktører settes på helt nye prøver.

Snart skal et nytt regjeringskvartal stå ferdig for over 54 milliarder, mens Forsvarets har fått en langtidsplan som i større grad er tilpasset en ny virkelighet. Med teknologi og digital infrastruktur som kritiske komponenter i de fleste samfunnsfunksjoner, har det digitale trusselbildet økt betraktelig. Når det gjelder justis- og beredskapssektorens evne til å agere basert på dette akselererende trusselbilde, er bildet dessverre at Norge over tid har ligget bakpå. Det gjelder myndighetene, virksomheter og organisasjoner.

Digital sikkerhet har derfor aldri vært viktigere. Den nye sikkerhetspolitiske situasjonen i Europa stiller andre krav til digital sikkerhet og beredskap. Ekstraordinære fremskritt innenfor kunstig intelligens (KI), særlig generativ KI, har stor betydning for vår samfunnssikkerhet innenfor områder som forebyggende sikkerhet, situasjonsforståelse og digital etterretning. Norge må derfor evne å utnytte denne nasjonale kapasiteten som finnes på både privat og offentlig side for å avdekke og håndtere digitale angrep i fellesskap. Sårbarheter ett sted kan få store konsekvenser for mange virksomheter.

Juristforbundet utfordrer derfor myndighetene til raskt å *forsere* innsatsen basert på trusselen mot tillitssamfunnet og demokratiet, basert på innspill som vi tidligere har gitt. Det er helt avgjørende at de grep som gjøres og de tiltak som settes inn er egnet til å ivareta og styrke rettsstaten vår, og at grunnleggende rettigheter alltid har en helt sentral plass i sikkerhetsarbeidet. For å sikre et liberalt demokrati og en sterk rettsstat.

Vi viser her til at:

- **Digitalsikkerhetsloven**, som implementerer NIS1-direktivet først trådte i kraft i Norge åtte år etter at direktivet ble vedtatt i EU.
- **Dokument 3:7 (2022–2023) Myndighetenes samordning av arbeidet med digital sikkerhet** i sivil sektor viste at Justis- og beredskapsdepartementet ikke har ivaretatt sitt pådriveransvar, ikke har lagt godt nok til rette for tverssektoriell hendelseshåndtering, få tilsyn med digital sikkerhet er gjennomført, og tilsynsmyndighetene generelt er lite samordnet.

- **Dokument 3:18 (2023–2024) – Riksrevisjonens undersøkelse av bruk av kunstig intelligens i staten** ble på sin side nylig behandlet i Stortinget. Denne avdekket på sin side mangelfull og fragmentert oppfølging av den forrige nasjonale digitaliseringsstrategien.
- Nettverks- og informasjonssikkerhetsdirektivet 2 (NIS2) som avløser NIS1, innfører strengere krav til cybersikkerhetsrutiner og forsvar innen sektorer som energi, helse, transport, finans, offentlige tjenester, romfart, næringsmiddelindustri og digital infrastruktur.
- Bank- og finanssektoren forbereder seg på å etterleve **Dora-reglene (Digital Operational Resilience Act)**, som skal tre i kraft i midten av januar 2025. Diskusjonene om implementeringen av KI-forordningen (AI Act) pågår også for fullt, med særlig fokus på regulering av sikkerhet, personvern og autonomi.
- **Nordic Cyber Resilience Report** utarbeidet av Tietoevry og som undersøker cybersikkerhetstilstanden i organisasjoner, viser at 30 prosent mangler en plan for hvordan håndtere et mulig digitalt angrep. Det betyr i praksis at de heller ikke er forberedt på de nye lovene og reglene som EU enten har vedtatt eller varslet
- **Kommunesektoren** understøtter flere kritiske samfunnsfunksjoner, og er spesielt sårbar for tjenestebortfall. Dette krever særskilt beredskap og oppmerksomhet.
- Totalberedskapskommisjonen peker i **NOU 2023:17** videre på at Norges beredskap mot *desinformasjon og påvirkningsoperasjoner* er fragmentert og mangler en samlet nasjonal funksjon i møte med disse sammensatte truslene
- **Hele** justissektoren trenger en langtidsplan. Totalberedskapskommisjonen fremhevet behovet for bedre samordning og koordinering på tvers av sektorer for å håndtere det stadig mer komplekse trusselbildet. **«Innenriksforsvaret»,** dvs. justissektoren mangler helhetlig planlegging og mulighet til å budsjettere langsiktig. Det foreligger imidlertid to anmodningsvedtak fra Stortinget hvor det bes om henholdsvis en langtidsplan for «politiet» (vedtak 755) og en langtidsplan for «sivil beredskap» (vedtak 729).

Implementeringen av EUs NIS1-direktiv- en god start på overtid

Implementeringen av EUs NIS1-direktiv i norsk lov er et viktig og helt nødvendig skritt i møte med et endret trusselbilde. Juristforbundet mener digital sikkerhet best kan oppnås gjennom grunnleggende krav til styringssystemer og risikovurderinger under god veiledning fra tilsynsmyndighetene. Samtidig ser vi en utfordring med at gjennomføringen av NIS1 i norsk rett allerede er utdatert, idet EUs Nettverks- og informasjonssikkerhetsdirektivet 2 (NIS2) har utvidet det opprinnelige grunnlaget for tiltak for håndtering av cybersikkerhetsrisiko og rapporteringsforpliktelser til å inkludere flere sektorer og kritiske organisasjoner.

Juristforbundet har følgende hovedanbefalinger til forslaget til ny digitalsikkerhetsforskrift:

1. Behovet for harmonisering med overlappende regelverk for å unngå dobbeltregulering og sikre en effektiv implementering av digitalsikkerhetsloven.
2. Utvikling av tekniske krav i tråd med NIS ved bruk av internasjonale risikobaserte standarder: Juristforbundet anbefaler bruk av internasjonale standarder som NIST CSF 2.0 og ISO/IEC 27001 for å utvikle tekniske krav i tråd med NIS1.

3. Tydeliggjøring av tilsynets veiledningsplikt med behov for å utarbeide en omfattende veileder som inkluderer risikovurderinger, håndtering av risiko, og beste praksis for å oppfylle NIS1- og NIS2-kravene, med referanser til relevante EU- og sektorspesifikke standarder.

Særskilt om krav til styringssystem og risikovurderinger

Juristforbundet er positive til de viktigste endringene i forskriften til digitalsikkerhetsloven når det gjelder krav til styringssystem basert på anerkjente standarder, og tydelighet rundt at tilbydere av samfunnsviktige tjenester må etablere og vedlikeholde et styringssystem som dekker digitale, fysiske og personelle sikkerhetstiltak. Juristforbundet støtter også minimumskravet til at tilbydere utarbeider risikovurderinger og planer for å håndtere risiko.

Særskilt om varsling

Juristforbundet anerkjenner viktigheten av de mer presise bestemmelsene om varsling av hendelser. Dette inkluderer spesifikasjoner om hva som skal varsles og når det skal varsles, noe som bidrar til økt ansvarlighet og bedre håndtering av sikkerhetshendelser.

Lista må legges i tråd med NIST2-direktivet

NIS2-direktivet er en videreføring og utvidelse av det tidligere cybersikkerhetsdirektivet NIS1 fra EU introdusert tilbake i 2016. Med NIS2 har EU allerede utvidet det opprinnelige grunnlaget for tiltak for håndtering av cybersikkerhetsrisiko og rapporteringsforpliktelser til å inkludere flere sektorer og kritiske organisasjoner. Juristforbundet understreker at formålet med å etablere et grunnlag av sikkerhetstiltak for digitale tjenesteleverandører og operatører av samfunnsviktige tjenester, er å redusere risikoen for cybertrusler og forbedre det generelle nivået av cybersikkerhet i EU.

Juristforbundet mener derfor at lista må legges i tråd med NIS2-direktivet. I møte med et galopperende digitalt trusselbilde, der statlige aktører i økende grad spiller på lag med kriminelle[1] , er det nødvendig å gjennomføre tiltak som sikrer robust risikostyring innen cybersikkerhet. Dette innebærer igjen at:

- ***NIS1 bør harmoniseres med andre EU-reguleringer***

Implementeringen av NIS1 bør harmoniseres med andre EU-reguleringer som «NIS2», Digital Operational Resilience Act» og «Cyber Resilience Act».

- ***Bruk av internasjonale risikobaserte standarder***

Juristforbundet støtter at forslaget anerkjenner behovet for utvikling av tekniske krav i tråd med internasjonale risikobaserte standarder, generelle eller sektorspesifikke retningslinjer eller prinsipper for digital sikkerhet.

Vi vil understreke behovet for en presisering av bruk av internasjonale standarder som NIST CSF 2.0 og ISO/IEC 27001 for å utvikle tekniske krav i tråd med NIS1. Internasjonale standarder og beste praksiser former cybersikkerhetsstrategier verden over, og flere land inntar disse standardene i sine rammeverk. Bruken av disse standardene vil gi økt sikkerhet, kostnadsbesparelser og økonomiske fordeler, og fremmer interoperabilitet og tillit. Juristforbundet viser til at NIS2-direktivet allerede dekker områder som cybersikkerhetsstyring, risikostyring i forsyningskjeden, tredjeparts risikostyring, og håndtering og avdekking av sårbarheter.

- ***Utvikling av en beste praksis veileder***

Juristforbundet ser det som positivt at veiledningsplikten til tilsynet er tydeliggjort i forslaget, og anbefaler at det utarbeides en veileder som ikke kun omfatter risikovurderinger og håndtering av risiko, men som også viser til beste praksis for å overholde både NIS1- og NIS2-kravene. Veiledningen bør derfor inkludere informative referanser og kartlegginger til EU- og sektorspesifikke standarder. NIST har vist til "Public Draft: Implementation Examples for the NIST Cybersecurity Framework 2.0", som kan brukes som en viktig kilde til informasjon for å utvikle NIS1/NIS2-veileder.

Avslutning

Å gjennomføre EUs NIS1-direktiv i norsk lov, er et viktig og helt nødvendig skritt i møte med et endret trusselbilde. Juristforbundet håper at dette innebærer et klart signal om at myndighetene *forserer* innsatsen for å sikre vår samfunnssikkerhet innenfor områder som forebyggende sikkerhet, situasjonsforståelse og digital etterretning. For å sørge for at vi i Norge bevarer det tillitssamfunnet og demokratiet som vi er stolte av, og som gjort Norge til et av de rikeste og mest likestilte landene i verden.

Med vennlig hilsen

Sverre Bromander-president Juristforbundet

Kristine Beitland-medlem Juristforbundets Tech Forum

Frode P. Ettesvold- medlem Juristforbundets Tech Forum

André Oktay Dahl-politisk seniorrådgiver Juristforbundet

[1] Microsoft Digital Defense Report 2024: Tre hovedfunn er 1. Økende cybertrusler: betydelig økning i cyberangrep, med over 600 millioner angrep daglig fra både cyberkriminelle og statlige aktører 2. Kunstig intelligens (KI) og sikkerhet: KI spiller en stadig større rolle i både angrep og forsvar mot trusler der trussel aktører bruker KI for mer sofistikerte angrep, og 3. Global innsikt: Microsofts globale digitale infrastruktur gir unik innsikt i trusselbildet, med data fra 78 trillioner sikkerhetssignaler daglig.