



Statsråden

Justiskomiteen
Stortinget
Postboks 1700 Sentrum
0026 OSLO

Deres ref

Vår ref

Dato

25/1394-4

8. mai 2025

Dok 8:227 S (2024-2025) Representantforslag fra Rasmus Hansson og Sigrid Zurbuchen Heiberg om bedre digital beredskap i urolige tider

Jeg viser til Justiskomiteens brev 4. april 2025 der dere ber om min uttalelse til Dokument 8:227 S (2024–2025) representantforslag fra stortingsrepresentantene Rasmus Hansson og Sigrid Zurbuchen Heiberg om bedre digital beredskap i urolige tider.

Dagens sammensatte trussel- og utfordringsbilde berører alle samfunnssektorer, og hybride angrep er en større del av trusselbildet enn før. Den skjerpede sikkerhetspolitiske situasjonen i verden gjør at arbeidet med digital sikkerhet og beredskap blir viktigere, og dette arbeidet er avgjørende for å ivareta kritiske samfunnsfunksjoner og grunnleggende nasjonale funksjoner. Det er behov for økt samarbeid og digital samhandling innenfor rammen av totalforsvaret og med allierte i NATO og EU.

Digitalisering er avgjørende for den nasjonale sikkerhets- og beredskapsevnen. Effekter som kan oppnås med digitalisering, er blant annet forbedret samhandling i totalforsvaret, og med allierte. Regjeringens strategiske retning, prioriteringer og tiltak for å ivareta digital sikkerhet er nedfelt i Meld. St. 9 (2022–2023) *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet* og Meld. St. 9 (2024–2025) *Totalberedskapsmeldingen - Forberedt på kriser og krig*. Skal vi opprettholde og styrke vår digitale motstandskraft, er det viktig å delta i internasjonale samarbeid. De senere årene har Norge prioritert tettere bånd og samarbeid med flere nære allierte. Vi har en særlig høy grad av gjensidige forpliktende samarbeid med USA og Storbritannia.

Regjeringen har nedlagt et betydelig arbeid for å styrke nasjonal sikkerhet de seneste årene. Dette gjenspeiles blant annet i Totalberedskapsmeldingen, som ble lagt frem for Stortinget i januar.

Nedenfor følger vurderinger av enkeltforslagene som er fremmet. Justisministeren har gitt innspill til vurderinger av forslagene 5, 6 og 9, forsvarsministeren har gitt innspill til vurderinger av forslag 6 og kultur- og likestillingsministeren har svart på forslag 10.

1. Stortinget ber regjeringen utarbeide en digital beredskapsplan som kan redusere Norges teknologiske avhengighet til USA og Kina, i samarbeid med sivilsamfunn, næringsliv og arbeidsliv.

Digitale tjenester og digital infrastruktur drives av internasjonale markeder. Norge har og må fortsette å ha, et tett samarbeid med mange land, også innenfor digitalisering.

Teknologidiversitet er viktig, og offentlige virksomheter vurderer behovet for sikkerhet og beredskap på selvstendig grunnlag. Meld. St. 9 (2022–2023) *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet* inneholder prioriteringer og tiltak for å ivareta digital sikkerhet og vektlegger offentlig-privat, sivil-militært og internasjonalt samarbeid.

Norske lover stiller strenge krav til sikkerhet og beredskap, til digital infrastruktur og digitale tjenester som er viktige og kritiske for samfunnet, bl.a. sikkerhetsloven og ulike sektorregelverk stiller slike krav. Jeg mener at regelverket dekker dagens behov for sikkerhet og beredskap.

2. Stortinget ber regjeringen gjennomføre en helhetlig sårbarhetsgjennomgang av Norges digitale infrastruktur, inkludert telekommunikasjon, programvarebruk og datalagring, med særlig vekt på avhengighet til aktører i USA, Kina og andre land med lav grad av rettssikkerhet og demokratisk kontroll.

Det stilles strenge krav til sikkerhet til digital infrastruktur i norske lover, blant annet i ekomloven og sikkerhetsloven. Regelverket stiller bl.a. krav til at ekomtilbyderne skal ha forsvarlig sikkerhet og at de gjennomfører risiko- og sårbarhetsanalyser (RoS-analyser). Nasjonal kommunikasjonsmyndighet (Nkom) fører tilsyn etter ekomloven og er sektormyndighet for ekomsektoren etter sikkerhetsloven. Nasjonal sikkerhetsmyndighet (NSM) har et overordnet ansvar for arbeidet med gjennomføring av sikkerhetsloven på tvers av sektorene. I arbeidet blir blant annet redundans og leverandørdiversitet vektlagt. I tillegg til tilbydernes egne RoS-analyser, gjennomfører Nkom regionale RoS-analyser, der de ser helhetlig på den digitale infrastrukturen uavhengig av hvem som eier den, peker på risiko og sårbarheter og identifiserer mulige tiltak for å styrke sikkerheten og beredskapen i hver region. Slike analyser er gjennomført for Finnmark, Troms, Nordland, Trøndelag, Innlandet og Buskerud, og regjeringen vil fortsette analysene i resten av landet.

Regjeringen jobber nå også med en sikkerhetsplan for digitale kommunikasjonsinfrastruktur, som samler og styrker arbeidet med sikkerhet og beredskap for å styrke motstandsdyktigheten til mobil- og bredbåndsnett i krise og krig. Jeg mener at forslaget dekkes av dette arbeidet.

På generelt grunnlag er det viktig å kjenne til digitale verdikjeder for viktige og kritiske tjenester og infrastrukturer for det norske samfunnet. Det er også viktig å vurdere tiltak for redundans og leverandørdiversitet, for å hindre at kritiske tjenester kun har ett bein å stå på.

Sikkerhetsloven stiller krav til leverandører som skal benyttes i verdikjeder som er utpekt etter sikkerhetsloven. Det betyr at leverandører fra land som Norge ikke har sikkerhetsavtale med, ikke kan levere utstyr til slike verdikjeder. For mobilnettene betyr det at utstyr til mobil kjernenett kun kan leveres fra leverandører fra land som Norge har sikkerhetsavtale med. Det er i tillegg tydeliggjort at minst 50% av utstyr til basestasjoner skal leveres fra leverandører fra land som Norge har sikkerhetsavtale med.

Norge har sikkerhetsavtale med, og tett sikkerhetssamarbeid med USA. Jeg mener derfor at dette er godt regulert i sikkerhetsloven.

3. Stortinget ber regjeringen utarbeide en strategi for gradvis løsrivelse fra digitale løsninger som overfører norske persondata til USA, med mål om å stanse all overføring av norske persondata til USA innen 1. januar 2026, med mindre USA igjen kan garantere rettssikker personvernbehandling.

Ulike virksomheter behandler ulike typer persondata og har ulike behov. Dette er noe av grunnen til at ansvarsprinsippet står sterkt i personvernforordningen. Prinsippet innebærer at alle virksomheter selv er ansvarlige for å etterleve kravene i regelverket, uavhengig av hvor dataene lagres. Personvernforordningen krever at all overføring av persondata ut av EØS-området har et rettslig grunnlag. Regelverket oppstiller ulike typer overføringsgrunnlag, blant annet såkalte adekvansbeslutninger. Dette er beslutninger EU-kommisjonen har fattet, om at bestemte land har tilstrekkelig beskyttelsesnivå for personopplysninger. Slike beslutninger finnes blant annet for England, Canada, Japan og USA. Adekvansbeslutningen for USA er basert på Personvernrammeavtalen (Data Privacy Framework). Dette er en avtale mellom EU og USA, som Norge har sluttet seg til. Personvernrammeavtalen gjør det mulig å overføre personopplysninger til virksomheter i USA som har forpliktet seg til å opptre i tråd med avtalen. Overføring i tråd med Personvernrammeavtalen, vil være i samsvar med personvernforordningens krav.

Jeg mener at vi har gode regler for overføring av personopplysninger til land utenfor EØS-området, og at det derfor verken er behov for, eller hensiktsmessig, å utarbeide en strategi slik forslaget innebærer.

4. Stortinget ber regjeringen legge en plan for å gjøre sivil infrastruktur i offentlig sektor uavhengig av programvare fra USA og Kina, med mål om at denne erstattes av norske eller europeiske alternativer.

Regjeringen mener at gjeldende regelverk bl.a. sikkerhetsloven og relevante sektorregelverk, dekker behov for å ivareta nasjonale sikkerhetsinteresser. Det stilles krav til sikkerhet og

beredskap i offentlige anskaffelser i dag. I Totalberedskapsmeldingen har regjeringen varslet at den styrke disse kravene for å ivareta beredskapshensyn og nasjonale sikkerhetsinteresser. I tillegg vil regjeringen bidra til god veiledning om sikkerhet og beredskap i offentlige anskaffelser.

5. Stortinget ber regjeringen stanse offentlig sektors bruk av programvare fra selskaper med nære bånd til myndigheter eller etterretningstjenester i land hvor det finnes dokumenterte inngrep mot borgerrettigheter, rettssikkerhet eller personvern. Det skal særlig prioriteres å stanse bruken av slike løsninger der de brukes til behandling og analyse av personopplysninger.

Det følger av sikkerhetsloven § 1-2 at loven gjelder for alle statlige, fylkeskommunale og kommunale organer. Alle virksomheter som er omfattet av loven, er pålagt å gjennomføre risikovurderinger for å fastsette hva som er å anse som forsvarlig sikkerhetsnivå for deres skjermingsverdige verdier. Virksomhetene skal gjennomføre sikkerhetstiltak på bakgrunn av risikovurderingen, for å opprettholde forsvarlig sikkerhetsnivå, også i forbindelse med anskaffelser. Det påhviler virksomhetene som er omfattet av loven en plikt til å risikovurdere anskaffelser som gir leverandører tilgang til skjermingsverdige verdier, eller mulighet til å påvirke disse verdiene. Sikkerhetsloven stiller krav til leverandører som leverer utstyr til informasjon, informasjonssystemer, objekter eller infrastruktur som har et skjermingsbehov etter sikkerhetsloven.

Bruk av programvare fra selskaper i tredjeland kan innebære overføring av persondata ut av EØS-området. Personvernforordningen oppstiller ulike typer overføringsgrunnlag, blant annet adekvansbeslutninger. Dette er beslutninger EU-kommisjonen har fattet, om at bestemte land har tilstrekkelig beskyttelsesnivå for personopplysninger. Hvis det ikke finnes en adekvansbeslutning for et gitt land, må virksomheten vurdere om det er adgang til å overføre persondata basert på et annet rettslig grunnlag i personvernforordningen. I slike tilfeller må det ses hen til tredjelandets personvernlovgivning og hvordan lovgivningen praktiseres. Ansvar for å etterleve kravene i personvernforordningen, herunder sikre at eventuell overføring til tredjeland er i tråd med regelverket, ligger hos den enkelte virksomheten. Dette gjelder både for offentlige og private virksomheter.

Gjeldende regelverk, som sikkerhetsloven og personopplysningsloven, oppstiller tilstrekkelige rammer for offentlig sektors bruk av programvare. Jeg mener derfor at det ikke er behov for å vedta dette forslaget.

6. Stortinget ber regjeringen fremme forslag til endringer av politiregisterloven og etterretningstjenesteloven som styrker personvernet og landets sikkerhet gjennom redusert datainnhenting og klarere krav til kontroll og åpenhet rundt verktøyene som brukes til å overvåke norske borgere.

Politiregisterloven ivaretar både hensynet til personvernet og hensynet til kriminalitetsbekjempelse og rikets sikkerhet, og reflekterer den avveining som er foretatt av disse hensynene opp mot hverandre. Loven og tilhørende forskrift gir klare og til dels detaljerte rammer for hvilke opplysninger politiet, herunder Politiets sikkerhetstjeneste (PST), kan behandle. Denne reguleringsformen gir god forutberegnelighet for borgerne. Den klare hovedregelen er at behandling av opplysninger skal være nødvendig og forholdsmessig for formålet med behandlingen. Det vil ikke være mulig å gi regler om «redusert datainnhenting». Dersom lovgiveren ønsker å innskrenke muligheten til å behandle opplysninger gjennom å redusere datainnhenting, vil det etter regjeringens oppfatning svekke politiets og PSTs mulighet til å bekjempe kriminalitet og ivareta rikets sikkerhet.

Politiregisterloven inneholder videre en rekke bestemmelser som sikrer kontroll med behandlingen av opplysninger. Datatilsynet har tilgang til alle opplysninger som politiet behandler og skal føre tilsyn med at behandlingen er i samsvar med loven. For PSTs vedkommende er det EOS-utvalget som har tilsynsfunksjonen.

Etterretningstjenesteloven bidrar til å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser. Loven bidrar dessuten til å trygge tilliten til og sikre grunnlaget for kontroll med Etterretningstjenestens virksomhet og sørge for at virksomheten utøves i samsvar med menneskerettighetene og andre grunnleggende verdier i et demokratisk samfunn. Loven reflekterer avveiningen mellom inngripen i den enkeltes privatliv og ivaretagelse av nasjonal sikkerhet. Loven ivaretar norske borgeres sikkerhetsgarantier, blant annet gjennom kontroll. Herunder fører EOS-utvalget løpende kontroll med Etterretningstjenestens operative bruk og etterlevelsen av reglene om tilrettelagt innhenting av grenseoverskridende kommunikasjon. I EOS-utvalgets årsmelding for 2024 trekkes det frem at denne typen kontroll forventes å bli mer omfattende i 2025.

I henhold til Stortingets anmodningsvedtak B pkt. 1 i Innstilling 357 L (2019-2020) har regjeringen våren 2025 oppnevnt et uavhengig utvalg som skal evaluere lov om Etterretningstjenesten. Utvalget har mandat til å evaluere etterretningstjenestelovens virke og muligheten for kontroll av dens bestemmelser. Utvalget skal særlig evaluere hvorvidt rettssikkerhetsmekanismene i loven fungerer i henhold til lovgivers intensjon. Herunder lovens bestemmelser om tilrettelagt innhenting, og hvorvidt disse lar seg kontrollere i henhold til Stortingets forutsetninger. Utvalgets rapport skal offentliggjøres september 2026.

7. Stortinget ber regjeringen sørge for at bevilgningene til overgang til fri og åpen programvare i offentlig sektor økes, og etablere et nasjonalt program for å utvikle og ta i bruk europeiske og åpne alternativer til programvare fra Microsoft og lignende amerikanske selskaper.

Fri og åpen programvare brukes av mange offentlige virksomheter i dag der dette er hensiktsmessig. Jeg mener at den enkelte virksomheten må vurdere dette selv og bruke den programvaren som best løser deres behov, og at lover og regler knyttet til personvern og lagring av data må være ivare tatt uavhengig av type løsning.

Norge har siden 2018 vært ledende på å fremme deling av trygge, digitale løsninger gjennom Alliansen for digitale fellesgoder. Norge leder alliansen sammen med FNs barnefond (Unicef) og Sierra Leone. Alliansen bidrar til økt koordinering, samarbeid, utvikling og deling av digitale løsninger. Digitaliseringsdirektoratet samarbeider med Europa gjennom Alliansen for digitale fellesgoder. digitale fellesgoder vil også være på programmet til Internet Governance Forum 2025 som arrangeres i Norge i juni.

Norge har i flere år støttet digitale fellesgoder i flere sektorer, spesielt helse og utdanning gjennom vår støtte til DHIS2, Global Digital Library og EduApp4Syria. Det er også offentlige virksomheter som tilbyr fri og åpen programvare. Helseinformasjonssystemet (DHIS2), som er utviklet av Universitetet i Oslo i samarbeid med deres internasjonale partnere, er nå i bruk i over 100 land. Altinn og værtjenester fra Meteorologisk institutt er andre eksempler på digitale fellesgoder som Norge deler med andre.

I de senere år har Norge vært en pioner og støttet arbeidet med digital offentlig infrastruktur og digitale offentlige goder. I 2023 forpliktet Norge seg til 50-in-5-kampanjen som et "first mover" land. Målet med kampanjen er at 50 land skal designe, lansere og skalere deler av sin digitale offentlige infrastruktur innen 2028.

Jeg mener Norge kommet langt på mange områder knyttet til bruk av fri og åpen programvare og at bruk og utvikling av disse løsningene ikke avhenger av økning i bevilgninger eller etablering av et nasjonalt program. Jeg mener følgelig at det ikke er behov for at forslaget vedtas.

8. Stortinget ber regjeringen delta aktivt i EU-initiativer for digital suverenitet, inkludert finansiering av europeisk skytjenestekapasitet og regnekraft, og sikre norsk deltakelse i et felleseuropeisk rammeverk for digital grunninfrastruktur.

Vi er i løpende dialog med EU og EUs medlemsland om hvordan vi kan samarbeide og delta i ulike EU-initiativer. Kjernen i vårt forhold til EU er EØS-avtalen. Gjennom EØS-avtalen deltar vi i en rekke initiativer fra EU som tar sikte på å utvikle kritiske europeiske verdikjeder på en sikker, motstandsdyktig og bærekraftig måte.

Norge deltar på flere arenaer i EU, blant annet i regi av ENISA (det europeiske byrået for nettverks- og informasjonssikkerhet) og NIS cooperation group (Samarbeid om sikkerhet i det digitale rom). Regjeringen prioriterer dette arbeidet, og ser behovet for videre samarbeid med allierte i den sikkerhetspolitiske situasjonen som verden nå står i.

Norge er fullverdig medlem i Programmet for et digitalt Europa (DIGITAL) 2021-2027, som er EUs investerings- og kapasitetsbyggingsprogram for digital omstilling og bruk av innovative digitale teknologier i samfunn og næringsliv. Programmet har en budsjetttramme på ca. 75 mrd. kroner i perioden 2021–2027, og fokuserer på å styrke Europas digitale kapasitet og suverenitet, inkludert tungregning, kunstig intelligens og skytjenestekapasitet.

Norge deltar også i EuroHPC Joint Undertaking, som er et felleseuropeisk initiativ for å utvikle og anskaffe superdatamaskiner. Norske aktører som Sigma2 og UNINETT er involvert i samarbeidsprosjekter.

Gjennom deltakelse i DIGITAL og EuroHPC har Norge mulighet til å søke støtte til utvikling og bruke europeiske fellestjenester og kapasitet på linje med EUs medlemsland.

Regjeringen har også lagt fram en nasjonal digitaliseringsstrategi som speiler og støtter EUs arbeid for digital suverenitet.

9. Stortinget ber regjeringen styrke Datatilsynets mandat og finansiering, samt utrede etablering av et uavhengig nasjonalt digitalt kriseråd med ansvar for å gi strategiske råd knyttet til digital sikkerhet, suverenitet og personvern.

Datatilsynet er et uavhengig organ som ikke kan instrueres om behandlingen av enkeltsaker eller den faglige virksomheten for øvrig. Tilsynets mandat følger av personopplysningsloven og personvernforordningen. Mandatet favner svært bredt, og tilsynet har en rekke virkemidler til disposisjon for å håndheve personvernregelverket. Siden personvernforordningen ble gjennomført i norsk rett i 2018, har Datatilsynet blitt styrket betydelig. Dette er blant annet gjort for at tilsynet skal kunne bidra aktivt i det felleseuropeiske personvernarbeidet. Styrkingen de siste årene har også satt Datatilsynet i stand til å drifte den regulatoriske sandkassen for personvernvennlig digitalisering og innovasjon, og styrket arbeidet deres for å trygge barns personvern. Jeg er generelt opptatt av at Datatilsynet har tilstrekkelige ressurser til å utføre samfunnsoppdraget sitt på en god måte. Samtidig mener jeg at det ikke er behov for å iverksette særskilte tiltak knyttet til Datatilsynets mandat eller ressursituasjon, basert på tematikken som stortingsrepresentantene Hansson og Heiberg har reist.

10. Stortinget ber regjeringen styrke innsatsen mot digital desinformasjon gjennom å utvikle og iverksette et nasjonalt folkeopplysningsprogram om digitale trusler, kildekritikk, algoritmisk manipulasjon og fremmede aktørers påvirkningsoperasjoner.

Regjeringen arbeider med en strategi for å styrke motstandskraften mot desinformasjon. Strategien vil blant annet inkludere omtale av virkemidler og tiltak for å styrke befolkningens kritiske medieforståelse og oppfølging av sosiale mediers påvirkning på den offentlige samtalen. Strategien skal etter planen legges frem før sommeren.

Jeg mener derfor at det ikke er behov for å vedta forslaget.

Overordnet vurdering av representantforslaget

Jeg deler i all hovedsak forslagsstillernes synspunkter på behovet for å styrke den digitale sikkerheten og beredskapen. Dette jobber vi aktivt med. Regjeringen la frem en ny nasjonal

digitaliseringsstrategi i september 2024. Digitaliseringsstrategien peker på at regjeringen vil frem mot 2030 styrke nasjonal digital sikkerhet og beredskap slik at kritiske samfunnsfunksjoner og grunnleggende nasjonale funksjoner blir ivaretatt. Strategien har en rekke tiltak som skal bidra til å nå dette målet.

I januar i år ble Totalberedskapmeldingen lagt frem. Meldingen har flere strategiske prioriteringer, bl.a. å styrke digital motstandskraft og nasjonal kontroll over kritisk infrastruktur og strategisk viktige virksomheter, naturressurser, eiendom og verdier, hvor økt kompetanse innenfor digital sikkerhet er et foreslått tiltak. I Totalberedskapsmeldingen har regjeringen også varslet at den vil klargjøre muligheten for å stille krav til sikkerhet og beredskap i offentlige anskaffelser for å ivareta beredskapshensyn og nasjonale sikkerhetsinteresser. I tillegg vil regjeringen bidra til god veiledning om sikkerhet og beredskap i offentlige anskaffelser, som blant annet identifiserer hvilke kategorier av anskaffelser der det er særlig viktig å stille krav til sikkerhet og beredskap. Sikkerhet er høyt prioritert i offentlige digitale løsninger og tjenester. Jeg ser derfor ikke behov for særskilte tiltak slik forslagsstillerne foreslår, og mener forslagene ikke bør vedtas.

Med hilsen



Karianne Oldernes Tung