NITO

Kommunal- og distriktsdepartementet
digitaliseringsstrategi@kdd.dep.no 29.11.2023

Vår ref. Robert Nyheim-Jomisko

INNSPILL TIL NY NASJONAL DIGITALISERINGSSTRATEGI
I oktober sendte NITO skriftlig innspill om kunstig intelligens (KI) til ny nasjonal digitaliseringsstrategi. I det følgende vil vi gi et supplerende innspill om ytterligere drivkrefter og utviklingstrekk som vil påvirke samfunnet, hva vi anser som de viktigste digitaliseringsutfordringene framover, og hvordan regjeringen kan bidra til å løse disse utfordringene gjennom strategien.

Digitalisering og personvern
Personvernkommisjonens rapport gir en grundig analyse av hvordan personvernutfordringer påvirker samfunnet som følge av digitalisering.[1] Et tema som imidlertid ikke forfølges tilstrekkelig er personvern på arbeidsplassen. Selv om enkelte teknologier er godt regulert, både i lovverk og forskrifter, mener NITO det er behov for langsiktige og samordnende tiltak for å kontrollere og regulere digitale overvåkningsmidler. Her kan blant annet nevnes «bossware» - programvare for overvåkning av aktivitet på personlig datamaskin, GPS-sporing, RFID-brikker, biometriske systemer, «wearables», KI-drevne analyseverktøy og ansiktsgjenkjenningsteknologi. Teknologier som dette kan bidra til økt produktivitet og sikkerhet, men samtidig skape store personvernutfordringer og misnøye blant ansatte.

NITO arbeider for at norsk arbeidskultur skal forbli tillitsbasert, og mener beslutninger omkring digitalisering må skje i samarbeid mellom partene i arbeidslivet og offentlige myndigheter. Det er viktig at staten, sammen med partene i arbeidslivet, utformer og vurderer tiltak for å forhindre overvåking på arbeidsplassen.

Offentlig innsamling og behandling av data
Norge har innført regler og er i ferd med å innføre flere, som medfører økt innsamling av data fra både offentlige og private kilder.[2] Lovendringene har blitt begrunnet ut fra sikkerhets- og beredskapshensyn. Likevel har forarbeidene til lovendringene gitt en tydelig advarsel om at de har en nedkjølende effekt, som bidrar til å svekke ytringsfriheten. NITO med flere har i tillegg påpekt at det er stor fare for formålsutglidning.

Datamengdene som samles inn, er av en slik størrelse at det er urealistisk å basere databehandlingen på noe annet enn algoritmer. I og med at maskiner skal behandle dataene og gjøre vurderinger, er det helt sentralt å få på plass verktøy som sikrer at enkeltpersoner og grupper ikke urettmessig profileres, mistenkeliggjøres og siktes. Verktøyene må ikke under noen

[1] NOU 2022: 11 *Ditt personvern – vårt felles ansvar: Tid for en personvernpolitikk*
[2] Eksempler på lover som er endret eller der endring snart behandles i Stortinget er politiloven, politiregisterloven, etterretningstjenesteloven og ekomloven.

omstendigheter brukes på annen måte enn lovens intensjon tilsier. Skulle likevel en slik situasjon oppstå, må norske myndigheter bruke alle nødvendige midler for å motvirke utviklingen, inkludert vurdere en reversering av lovendringene.

IKT-sikkerhetslovgivning

Det er lagt ned betydelig tverrpolitisk arbeid med sikkerhetslovgivning gjennom årene.[3] Likevel er regelverk, som behandler IKT-sikkerhet, nokså fragmentert, idet sikkerhetsanliggender må håndteres på tvers av sektorer. Forskjellige sektortilsyn forholder seg ulikt til sikkerhetskrav og har i varierende grad nødvendig hjemmel til å foreta IKT-sikkerhetsrettet aktivitet.

Gjennom sikkerhetsloven har alle virksomhetseiere som forvalter «skjermingsverdige objekter og infrastruktur» et overordnet ansvar for forebyggende sikkerhetsarbeid. Loven har imidlertid svakheter som kan føre til ulik praksis og manglende forutsigbarhet. En vesentlig svakhet er mangelen på regelverk som angir hvordan tilstrekkelig objektsikkerhet skal oppnås. Samtidig gir loven betydelig rom for tolkning. NITO mener etableringen av ett sektorovergripende regelverk for IKT-sikkerhet vil gjøre regelverket mindre komplisert for den enkelte virksomhet, både i det offentlige og i det private. Vi håper investeringskontrollutvalgets pågående arbeid vil bidra til å gi bedre løsninger.[4]

Siden 2016 har NITO bedt om at IKT-infrastrukturen i helsevesenet underlegges sikkerhetsloven. Med lagring og drift av samfunnskritiske registre i Norge, herunder helseregistre, vil det bli enklere for norske myndigheter å holde kontroll med virksomheter som forvalter sensitive og samfunnskritiske data hvis de omfattes av loven.

Gjennom offentlige utredninger og lovendringer de senere årene, finnes det antakelig teoretisk beslutningsgrunnlag for det meste av sikkerhetshendelser som kan inntreffe. Verre er det med kompetanse og bevilgninger for å gripe an arbeidet.

NITO mener:

- Det er behov for et tydeligere nasjonalt regelverk for IKT-sikkerhet.
- Samfunnskritiske private virksomheter må underlegges restriksjoner på lik linje med de offentlige, som for eksempel olje- og gassvirksomheten.
- Samfunnskritisk IKT-infrastruktur må være under nasjonal kontroll.
- Alle offentlige registre som lagrer sensitive eller samfunnskritiske data må lagre data på servere i Norge, og registrene må driftes av ansatte i Norge.

---

[3] Siden NOU 2000: 24 *Et sårbart samfunn: Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet* har det kommet flere utredninger og lovendringer, blant annet NOU 2006: 6 *Når sikkerheten er viktigst — Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*, St.meld. nr. 22 (2007-2008) *Samfunnssikkerhet: Samvirke og samordning* og NOU 2016: 19 *Samhandling for sikkerhet: Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.* Sistnevnte førte til revisjon av Lov om nasjonal sikkerhet (sikkerhetsloven), Lov om særlige rådgjerder under krig, krigsfare og liknende forhold (beredskapsloven) og Svendsen-utvalgets rapport fra 2020 *Økt evne til å kombinere menneske og teknologi: Veier mot et høyteknologisk forsvar*.

[4] Regjeringen vil utrede behovet for nærmere sikkerhetsvurderinger av utenlandske investeringer https://www.regjeringen.no/no/aktuelt/regjeringen-vil-utrede-behovet-for-narmere-sikkerhetsvurderinger-av-utenlandske-investeringer/id2942007/

- Store sektorer som olje, helse, politi, elektronisk kommunikasjon, vann og kraft må defineres som kritisk infrastruktur og falle innunder sikkerhetsloven.
- Departementene må styrke sitt forebyggende arbeid i henhold til sikkerhetsloven.
- Det må gjøres enklere for teknologibedrifter å etterleve sikkerhetslovens bestemmelser slik at de kan levere oppdrag i sikkerhets- og beredskapsarbeidet.

Norske datasentre
Datasentre er avgjørende for det digitale samfunnet og vil bidra til å skape framtidige arbeidsplasser. NITO mener myndighetene må legge til rette for stabile rammevilkår for denne næringen.

Norge har betydelige konkurransefordeler, inkludert tilgang til areal, rimelig og miljøvennlig strøm, kaldt klima, overskudd av fornybar energi, digital infrastruktur, høy kompetanse, sikkerhetsmiljøer og stabile rammevilkår. For å styrke veksten i den bærekraftige dataindustrien, må konkurransefordelene opprettholdes. Norsk datasenterstrategi foreslår tiltak som markedsføring av Norge som datasenternasjon, økt datautveksling i næringslivet og fortsatt statlig støtte til bredbåndsutbygging, dette støttes av NITO.

Vi vil videre understreke behovet for forutsigbarhet i kraftnæringen, spesielt med tanke på de store energikravene til datasentre. Sammen med organisasjons- og næringslivet må regjeringen finne løsninger for rimelig, fornybar energi, økt kraftunderskudd og behovet for å bedre nettkapasiteten. Økte investeringer i sikkerhet for digital infrastruktur er også nødvendig å prioritere på grunn av endrede trusselbilder. NITO foreslår en felles organisering av norske datasentre for økt beredskap. Vi anbefaler også vurdering av nordisk samarbeid for storskala datasentre. NITO støtter regjeringens utredning av en nasjonal skyløsning og oppfordrer til vurdering av hvilke data som bør holdes på norsk jord. Krav om beredskap og robusthet bør innarbeides i offentlige anskaffelser, med søkelys på bygging av datasentre i eksisterende fjellhaller.

Med den teknologiske utviklingen kreves styrking av innkjøpskompetansen i offentlig sektor. NITO foreslår utvikling av regionale distribuerte skyløsninger for nasjonal og regional IKT-beredskap, samt kravspesifikasjoner for robuste leveranser ved offentlige anskaffelser.

Digitalt utenforskap
Som følge av økt digitaliseringstakt, blir digital kompetanse stadig viktigere og konsekvensene av å ikke henge med større. Selv om digitalisering av offentlig sektor har til hensikt gjøre det enklere for innbyggere og næringsliv, anslår Digdir at om lag 20 prosent av befolkningen er sårbare i møte med offentlige digitale tjenester. Når digitaliseringen i privat sektor går i et enda raskere tempo, er det enkelt å forstå at kompetansebarrierer oppstår.

Problemet rammer ikke bare den eldre befolkningen. Selv kyndige fagfolk melder om at digitale systemer som benyttes er lite brukervennlige. Dette reiser spørsmål omkring hvor tilgjengelige teknologiene er for gjennomsnittsbrukeren. Digital sårbarhet fører til at flere helt eller delvis faller utenfor arbeidslivet. Mange arbeidstakere har også vanskeligheter med å møte digitale krav som arbeidsgivere stiller. I det utfordringer med å ta i bruk digitale verktøy blir større, øker faren for at eksisterende samfunnsskiller forsterkes.

Under pandemien ble det tydelig at manglende tilgang til internett og utdatert teknologi vanskeliggjorde fjernundervisning for mange skoleelever. Uten nettilgang og digitale enheter, blir det vanskelig å delta i det digitale samfunnet. Dette påvirker alt fra utdanning til tilgang på offentlige tjenester.

NITO mener vi trenger flere tiltak for digital inkludering. Med økt bruk av generativ KI i samfunnet er det høyst relevant å snakke om «KI-gapet» som er i ferd med å utvikle seg.[5] Av den grunn er det avgjørende at regjeringen innfører et bredt spekter av utdannings- og opplæringstilbud som bidrar til å redusere KI-gapet i befolkningen. Læreplaner i hele utdanningssystemet bør inneholde kompetansemål som legger til rette for å øke befolkningens digitale kompetanse. Bransjeprogram for informasjonssikkerhet og IKT er et godt tiltak som kan bidra til å redusere digitale gap, men det er langt fra nok for hindre digital sårbarhet i befolkningen.

Sikring av åpne API og datadeling
Bruk av åpne programmeringsgrensesnitt (API) er ventet å øke som følge av at Norge og EU legger til rette for mer datadeling. Det anslås at 90 prosent av nettbaserte applikasjoner vil ha eksponert API innen få år. API-er er svært sårbare for dataangrep og alt tilsier at angrep mot disse vil bli stadig vanligere.

Mye av teknologiutviklingen foregår på premissene til store flernasjonale selskaper. Disse selskapene har gjerne hovedsete i land som skiller seg fra Norge både gjennom politisk kultur, regelverk og næringsstruktur. Hvor dataene våre blir av og hvem som har tilgang til dem, er ikke alltid like tydelig. I 2017 advarte og varslet NITOs tillitsvalgte om utflagging av IKT-drift i Helse Sør-Øst. Bakgrunnen for dette var faren for at norske pasientdata havnet på avveie. Det er ikke utenkelig at lignende situasjoner kan oppstå igjen.

API som skal eksponeres for offentligheten må beskyttes. Hvis offentlige virksomheter skal lage et stort «hull i muren» mot samfunnets mest sensitive dataregistre, må dette hullet ha en dør som er godt bevoktet.

NITO vil advare mot å pålegge offentlige etater å dele data. Dersom etatene presses til datadeling før det foretas konsekvensvurderinger av eventuelle skader, kan følgene bli katastrofale. Hvis datadeling skal lovfestes, må flere forhold avveies mot hverandre og interessemotsetninger avklares. Vi må blant annet sikre at de største selskapene ikke styrker sin stilling på bekostning av de mindre og samtidig påse at norsk regelverk følges. Overtredelser må kunne sanksjoneres mot.

NITO mener det er behov for å utvikle et godt offentlig digitalt tjenestetilbud for å unngå at private aktører får monopol på norske tjenester. Videre er det behov for å regulere teknologigiganter og kommersielle aktører innen sosiale medier, slik at brukere ikke kan utestenges fra plattformene. Handlinger som dette representerer en trussel mot demokratiet og våre verdier. En slik regulering bør utvikles på europeisk nivå. Dette for å sikre at maktmisbruk utøvd av teknologigiganter kan slås ned på og at aktører stilles til ansvar.

Med vennlig hilsen

Trond Markussen
President

Egil Thompson
Generalsekretær

[5] Kitsara, I. (2022). Artificial Intelligence and the Digital Divide: From an Innovation Perspective. In: Bounfour, A. (eds) Platforms and Artificial Intelligence. Progress in IS. Springer, Cham. https://doi.org/10.1007/978-3-030-90192-9_12