

Innspill til revisjon av Langtidsplan for forskning og høyere utdanning

Datatilsynet vil med dette gi sine innspill til revisjonen av Langtidsplan for forskning og høyere utdanning, med høringsfrist 16. september 2017.

Fremover vil data spille en helt avgjørende rolle i utviklingen av norsk økonomi og samfunn. Personopplysninger er byggesteinene i det nye data-drevne samfunnet. Når informasjonsteknologi benyttes i tilknytning til enkeltpersoner, er ivaretagelse av personvern en viktig faktor. Vi mener derfor at personvern må være et sentralt tema forskning som omhandler bruk av informasjon om enkeltpersoner, samt i IKT-utdanning. Dette er nødvendig for å bidra til et bedre personvern i morgendagens smarte samfunn, men også for å gi forskningen kredibilitet, finne muligheter for å anvende data som eller ikke ville vært akseptable, og for å sikre relevans i IKT-utdanningen. Vi ser også behov for at det forskes på den samfunnsetiske siden av morgendagens datadrevne samfunn, for eksempler konsekvenser av øket overvåkning.

Vi mener følgende temaer og perspektiver særlig bør reflekteres sterkere i den reviderte planen:

1. Bruk av stordata og kunstig intelligens krever forskning på personvern fremmende teknologi og etterprøvbare algoritmer

Vi ser et økende ønske om og påtrykk for gjenbruk av opplysninger til stordataanalyse i både offentlig og privat sektor. Gjenbruk av opplysninger, såkalt sekundærbruk av data, utfordrer personvernprinsippet om formålsbegrensning som er uttrykt i artikkel fem i den kommende personvernforordningen.

Det er enorme verdier å hente ut av innsamlede data, men det er ikke mulig å høste fordelene med *stordata* på bekostning av grunnleggende personvernrettigheter. Å lage løsninger som ivaretar personvernet vil være en fordel for både virksomheter, myndighetene og enkeltindividet.

Forskning på teknologi og metoder som muliggjør utnyttelse av stordata, samtidig som personvernulempene for enkeltindividet reduseres mest mulig, er derfor av stor betydning hvis man skal kunne hente ut verdiene som ligger i dataanalyse. Forskning på personvern fremmende teknologi må derfor reflekteres sterkere i Langtidsplanen. Eksempel på metoder det er interessant å forske på og tilgjengeliggjøre for allmenn bruk er differential privacy og ulike krypteringsteknologier som blockchain og homomorfisk kryptering.

Fremover vil stadig flere beslutninger automatiseres basert på kunstig intelligens. En utfordring ved mange av systemene som utvikles i dag er at de er så komplekse at mennesker ikke kan forklare hvordan de kom frem til resultatet. Hvis de som eier systemet ikke kan forklare hvordan det virker kan det påvirke tillitten vi har til beslutningene de treffer. Det er derfor viktig å forske på modeller og metoder som sikrer en etisk forsvarlig utvikling og bruk automatiserte beslutningssystemer basert på kunstig behandling. Etter vårt syn er det nødvendig at forskning på algoritmebaserte løsninger ledsages av forskning på hvordan en sikrer at algoritmene opptrer ansvarlig. Dette inkluderer, men er ikke begrenset til, ivaretagelse av personvern.

2. Behov for et kompetanseløft på sikkerhets- og risikovurderinger

Mange av dagens digitale tjenester og samfunnsfunksjoner er avhengig av lange og kompliserte verdikjeder, som gjerne involverer aktører i flere land.

Tjenesteutsetting er et område som krever kompetanse på risikovurderinger for at dette skal kunne gjøres med akseptabel risiko. Datatilsynet erfarer at kompetansen på risikovurderinger i private og offentlige virksomheter ikke er tilfredsstillende. Konsekvensen av mangelfulle risikovurderinger er i verste fall at det inntreffer hendelser som svekker brukernes tillitt til digitaliserte tjenester

Forbrukertester, blant annet foretatt av Forbrukerrådet¹, viser at smarte produkter har mangelfull sikkerhet. Selv om produktet har et visst nivå av sikkerhet når de kommer i salg, er det ofte ikke lagt til rette for at de oppdateres slik at sikkerheten ivaretas i hele produktets levetid. Dette fordrer bedre sikkerhetskompetanse og utvikling av modeller for å sikre tillit til at produktene sikres gjennom levetiden, på en måte som forbrukerne kan forholde seg til.

Det er behov for et kompetanseløft innen IKT-utdanningen på risiko- og sårbarhetsanalyser. Det er også behov for mer forskning på utvikling av gode systemer og metoder for risikoanalyse.

3. Innebygd personvern må inn i høyere utdanning

Innebygd personvern og personvern som standardinnstilling er et sentralt krav i personvernregelverket som gjelder fra mai 2018. Innebygd personvern betyr at det tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning. Det er både kostnadsbesparende og mer effektivt enn å endre et ferdig system. I dag er det stor mangel på kunnskap om og kompetanse på innebygd personvern blant teknologer og utviklere. **Det er derfor viktig at innebygd personvern tas inn som en sentral del av undervisningen i all høyere IKT-utdanning.** Dette er kompetanse det vil bli høy etterspørsel etter fremover. Et eksempel på et område hvor kompetanse på innebygd personvern er av stor betydning er innen velferdsteknologi. En vellykket utrulling og implementering av velferdsteknologi avhenger av systemene oppfyller dette kravet i regelverket.

Datatilsynet stiller gjerne til møte med departementet for å komme med utfyllende kommentarer til punktene over.

¹ <https://www.forbrukerradet.no/siste-nytt/forbrukerutfordringer-ved-tingenes-internett/>