Datatilsynet

Digitaliseringsminister Nikolai Astrup
Kommunal- og moderniseringsdepartementet

Deres referanse	Vår referanse	Dato
	19/01858-1/CNE	20.06.2019

Datatilsynets innspill til regjeringens KI-strategi

Datatilsynet synes det er svært positivt at regjeringen vil lage nasjonal strategi for kunstig intelligens (KI). Hvordan vi skal sørge for at kunstig intelligens utvikles og tas i bruk på en måte som er til det beste for mennesket og samfunnet er en stor og viktig oppgave.

Nesten all bruk av kunstig intelligens forutsetter store mengder data, i mange tilfeller personopplysninger, for å kunne lære og ta intelligente avgjørelser. Potensialet for radikalt bedre tjenester, forskningsmessige gjennombrudd og økonomisk gevinst, setter KI høyt på agendaen i de fleste sektorer.

Vi kommer til å se stadig flere juridiske og etiske dilemmaer hvor potensialet for betydelig samfunnsgevinst må veies opp mot grunnleggende personvernhensyn. Datatilsynet mener debatt og kunnskap om personvernimplikasjonene ved kunstig intelligens er nødvendig – både for å ivareta enkeltmenneskers personvernrettigheter, og for å ivareta samfunnsbehov utover personvernet.

En vellykket utvikling og implementering av systemer basert på kunstig intelligens er avhengig av at befolkningen har tillit til at systemene håndterer opplysningene om dem på en sikker og rettferdig måte. Hvis folk ikke har tillit, vil de være mer forsiktige med å dele opplysningene sine. Dårlig ivaretatt personvern i utviklingen av KI kan derfor hemme graden av innovasjon og utvikling på dette feltet. I Europa har vi fått en oppdatert personvernlovgivning, GDPR. Oppdateringen kom i grevens tid. Personvernforordningen er, så langt, den første i verden som regulerer utvikling og bruk av kunstig intelligens.

Vi er i startgropen på noe som uomtvistelig vil ha en betydelig effekt på samfunnet. Det er derfor viktig at regjeringen lager en nasjonal strategi som trekker opp rammene for hvordan vi kan realisere mulighetene som kunstig intelligens innebærer på en sikker og rettferdig måte. Datatilsynet vil gjerne gi følgende innspill til den nasjonale strategien:

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr:	Hjemmeside:
Postboks 458 Sentrum 0105 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no

1. Etisk og personvernvennlig KI bygger tillit

Ansvarlig KI er kunstig intelligens som ivaretar menneskets grunnleggende rettigheter og friheter, herunder retten til personvern. Å utvikle KI i samsvar med personvernregelverket, vil bidra til å oppnå den tilliten som kreves for at teknologien kan nå sitt potensiale. Ett av personvernforordningens formål er å skape tillit ved bruk av personopplysninger.

Personvernforordningen gjelder både når KI utvikles ved hjelp av personopplysninger, og når KI brukes for å analysere eller ta avgjørelser om enkeltpersoner.

Datatilsynet mener at den nasjonale strategien må bidra til at utvikling og bruk av KI skjer i samsvar med personvernprinsippene i personvernforordningen:

- **Prinsippet om rettferdighet**
  KI må utvikles og brukes på en måte som har respekt for enkeltindividets interesser. Det vil si at den må utvikles og brukes på en måte som ikke bryter med folks forventninger til hvordan data som er samlet inn om dem, blir brukt.

  Videre må KI utvikles og brukes på en måte som hindrer at algoritmene trenes opp til å ta fordomsfulle og diskriminerende beslutninger. Dette kan blant annet gjøres ved å være oppmerksom på viktigheten av å ha oppdaterte, korrekte og representative data.

- **Prinsippet om åpenhet og gjennomsiktighet**
  Løsninger basert på KI må være åpne og gjennomsiktige. En bekymring knyttet til KI er at man ikke alltid vet hvordan beslutningene blir produsert. Ofte vil systemene produsere et svar uten noen forklaring. Dette gjør det vanskelig for enkeltindivider å imøtegå, og eventuelt klage på, beslutningene som systemene tar.

- **Prinsippet om retten til informasjon**
  KI må utvikles og brukes på en måte som bygger opp om individets rettigheter. Folk skal blant annet ha rett til innsyn i hvilke data som samles inn om dem og til informasjon om hvordan opplysningene brukes. Folk skal ha rett til en forklaring på beslutningene maskinene tar og til å klage på dem.

- **Prinsippet om formålsbestemthet**
  Mange av modellene som utvikles med kunstig intelligens skal brukes til gode formål, slik som for eksempel diagnostisering av kreft. Er det fritt fram for gjenbruk av personopplysninger så lenge det gjøres for et godt formål? Prinsippet om formålsbegrensning innebærer at formålet for behandlingen av personopplysninger må være tydelig angitt og fastsatt når personopplysningene samles inn. Dette er helt grunnleggende for at enkeltpersoner skal kunne ha kontroll over opplysningene sine.

- **Prinsippet om dataminimering**
  Prinsippet om dataminimering må ha en sentral rolle i utviklingen av KI slik at rettighetene til enkeltindividet og tilliten til løsningene ivaretas. Dette prinsippet utfordres av at presset på bruken av personopplysninger øker i takt med at analyser basert på KI kan bidra til effektivisering og bedre tjenester. Prinsippet om dataminimering kan ivaretas ved å begrense graden av identifisering av individene som inngår i datagrunnlaget. Graden av

identifisering begrenses både av mengden opplysninger og av hvilke opplysninger som brukes. Bruk av pseudonymiserings- eller krypteringsteknikker kan også bidra til å begrense inngrepet.

- **Prinsippet om ansvarlighet**
  Virksomheter som utvikler og bruker KI må evaluerer effekten systemene har. De må sikre at systemene ikke produserer beslutninger som fører til usaklig forskjellsbehandling av enkeltpersoner. Prinsippet om ansvarlighet innebærer også at virksomheter som bygger systemer for KI må gjøre dette etter prinsippene for innebygd personvern. Det vil si at systemene teknisk og organisatorisk må være bygd opp på en måte som ivaretar individets interesser.

2. Økt satsning på personvernfremmende teknologi viktig for å hente ut potensialet i KI

Skal vi utnytte potensialet i KI og samtidig ivareta enkeltmenneskets grunnleggende friheter og rettigheter, må vi utvikle løsninger som er åpne og gjennomsiktige, som fatter beslutninger som lar seg forklare og som er rettferdige og ikke-diskriminerende. Vi må utvikle metoder og teknologi som støtter opp under personvernprinsippene. Den nasjonale strategien må bidra til å styrke forsking på metoder som gjør utnyttelse av store datamengder mulig samtidig som personvernet ivaretas. Datatilsynet mener at den nasjonale strategien for kunstig intelligens må bidra til å:

- Styrke forskningen på, og bruken av, personvernfremmende teknologi. Vi trenger økt forskning på metoder for å:
  - redusere behovet for treningsdata
  - ivareta personvernet uten at datagrunnlaget reduseres
  - unngå svart boks-problematikken
- Fremme bruken av innebygd personvern i utviklingen av systemer basert på kunstig intelligens.
- Øke kompetansen om personvernkonsekvensvurderinger i offentlig og privat sektor.
- Heve bestillingskompetansen på systemer basert på KI i offentlig og privat sektor
- Få personvern innarbeidet i relevante utdanning på universitet og høgskoler

3. Effektiv håndheving ivaretar tillit – krever kompetente og kraftfulle tilsynsorgan

I tiden fremover vil vi oppleve at flere og flere av beslutningene om oss blir tatt ved hjelp av kunstig intelligens. Kraftfull håndheving av personvernforordningens prinsipper er viktig for å ivareta folks tillit til at beslutningene som treffes om dem er korrekte og rettferdige.

Undersøkelser av systemer med kunstig intelligens vil være teknisk komplekse og by på nye utfordringer for Datatilsynet. En utfordring vil være hvordan tilsynet skal gå frem for å undersøke om systemene tar rettferdige avgjørelser. Mange av systemene er karakterisert som «svarte bokser». I disse systemene er det ikke mulig å vite hvordan modellen kommer frem til resultatet, noe som gjør det vanskelig å undersøke hvordan personopplysningene behandles. **Undersøkelse av KI-systemer krever derfor medarbeidere med teknisk kompetanse på maskinlæring og data science og utvikling av tilsynsmetodikk for kontroll av slike systemer.**

Tilsyn av systemer med KI vil sannsynligvis kreve nye og utvidede lovhjemler. I dag har Datatilsynet ikke hjemmel til å ta beslag eller en kopi av systemet som undersøkes, slik at det kan gjøres grundigere tester etter at de stedlige undersøkelsene er avsluttet. Vi antar at det ved KI-tilsyn vil være behov for å verifisere funn som fremkommer i skriftlig dokumentasjon og samtaler, blant annet for å kontrollere om systemet tar rettferdige avgjørelser. Vi kan heller ikke se bort fra at aktører kan ønske å skjule forhold som kan være brudd på personvernforordningen fordi det ofte er store verdier involvert i teknologien.

Flere andre norske tilsynsmyndigheter har særregler om bevissikring, herunder regler om å gjøre beslag. Et eksempel er konkurranseloven § 25, som gir Konkurransetilsynet adgang til «å ta med ting som kan ha betydning som bevis for nærmere granskning». I tillegg finnes det EU-/EØS-land som har egne nasjonale regler om bevissikring for datatilsynsmyndigheten. Et eksempel er Storbritannia hvor det britiske datatilsynet har rett til å gjøre beslag i bevisgjenstander. Bevissikring krever forutgående domstolskontroll. Vi mener at Datatilsynet bør få lignende eller tilsvarende hjemler som det britiske datatilsynet. **Lovendring vil være svært nyttig, og nærmest avgjørende, når Datatilsynet skal bygge opp et fagmiljø for bevissikring i forbindelse med tilsyn med systemer basert på KI.**

Det er ikke bare Datatilsynet som vil føre tilsyn med beslutningssystemer basert på KI. Også andre statlige myndigheter som Forbrukertilsynet, Arbeidstilsynet, Konkurransetilsynet, Helsetilsynet og Likestillings- og diskrimineringsombudet vil føre kontroll med systemer basert på kunstig intelligens som er rettet mot enkeltindivider. **Den nasjonale strategien for kunstig intelligens må se på hvordan statlige myndigheters kontroll av kunstig intelligens skal håndheves og koordineres slik at den fungerer mest mulig effektivt og enhetlig. Enhetlig og effektiv håndheving av relevant regelverk er viktig for at folk skal ha tillit til systemene.**

Datatilsynet mener at den nasjonale strategien bør bidra til å:

- Bygge opp og ivareta effektive og kompetente tilsynsorgan på kunstig intelligens. Tilsyn med systemer basert på KI er teknisk komplekse og arbeidskrevende. Dette krever en opprustning av tilsynsmyndighetene i form av ny kompetanse og økte ressurser. Det er også viktig å diskutere behovet for en lovendring for å gjøre det er mulig for Datatilsynet å ta beslag av utstyr i forbindelse med gjennomføring av stedlig tilsyn.
- Koordinere tilsynsmyndigheter som har ansvar for å føre kontroll med systemer basert på kunstig intelligens. Dette for å sikre enhetlig og effektiv håndheving av relevant regelverk.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Catharina Nes
fagdirektør