Datasikkerhed

Udgiver
Morgenavisen Jyllands-Posten

Ansvarshavende chefredaktør
Jacob Nybroe

Magasinredaktør
Jakob Vestergaard

Redaktør
Mathias Gram og Lars Dalsgaard/ Media Movers

Layouter
Nini Nielsen/ Media Movers

Forsidefoto
Ivan Boll

Kontakt
temasektion@jp.dk

It-systemet Watson skulle forudsige den bedste behandling til cancerpatienter, men endte med at få en forkert forståelse af, hvad cancer er. Arkivfoto: Nikolai Linares

Patienter risikerer forkert behandling, når computeren misforstår, hvad de fejler

I intelligente it-systemer er udviklernes evner til at fortolke data korrekt alfa og omega, hvis systemerne skal bruges til sygdomsbehandling

DATALAB
ANNE HENRIKSEN
OG ANJA BECHMANN

Det er en udbredt antagelse at "big data is king". Hvis blot mængderne af data er store nok, så vil mønstrene i dem kunne tale for sig selv og f.eks. bidrage positivt til produktudviklingen i en virksomhed.

I de senere år har en række eksempler dog vist, at data alene ikke er nok. Skal fremtidens intelligente it-systemer være sikre og pålidelige, må de naturligvis fortsat baseres på solide målinger, men det er samtidig afgørende, at udviklerne har kompetencerne til at fortolke den virkelighed, de skal repræsentere og gengive i matematiske maskinlæringsmodeller.

Et eksempel er Google Flu Trend. Det blev designet til at forudsige influenzaepidemier i USA, men endte med at forudsige, at der i 2012 og 2013 ville komme dobbelt så mange influenzarelaterede besøg hos lægen, som der rent faktisk kom.

Forskere har siden vurderet, at systemet på daværende tidspunkt var bygget på en række fejlagtige antagelser om de data, der havde til formål at afspejle virkeligheden.

Et andet kendt eksempel er IBM's intelligente it-system Watson. Det var bl.a. programmeret til at analysere store mængder tekstdata fra elektroniske patientjournaler og medicinske forskningsartikler i USA.

Idéen var at forudsige de behandlinger, der mest sandsynligt ville gavne cancerpatienter. I praksis viste det sig imidlertid, at systemet opererede med en markant anderledes forståelse af både cancer, og hvad den mest rigtige behandlingsform var. It-systemet fortolkede simpelthen cancer forskelligt fra mange af de kulturer, som det blev anvendt i, mens behandlingsformerne blev fortolket på baggrund af statistiske beregninger alene og ikke ud fra lægemiddelstyrelsens anbefalinger.

Selv om intelligente systemer og maskiner har rødder tilbage i 1950'erne og derfor ikke er noget nyt fænomen, er det altså stadigvæk en stor udfordring for selv verdens største techvirksomheder at få dem til at tænke og handle ligesom læger og andre professionelle.

Det understøttes af delresultaterne af vores igangværende forskning i udviklingen af intelligente maskinlæringssystemer og af en stadig større mængde humanistisk og samfundsfaglig forskning indenfor it og automatisering.

De intelligente systemer udvikles ofte til at kunne "tænke" ligesom mennesker – eller vel nok anderledes eller bedre end mennesker – så de kan bidrage med at skabe en solid viden som baggrund for at udføre en bestemt arbejdsopgave.

Det gælder ikke kun den rigtige behandling af cancerpatienter, men også ansættelsen af den rigtige medarbejder eller forsyningen af den rigtige elevlæring.

Hvis den producerede viden er robust nok, kan maskinen enten selv udføre opgaven automatisk eller understøtte mennesker i at udføre den. Men ligesom med al anden viden så er den sandsynlighedsbaserede viden, som vi får med big data og maskinlæring, stærkt afhængig af klassiske spørgsmål om validitet og pålidelighed: Måler vi nu også på det, vi tror, vi måler på? Hvad måler vi som rigtigt og forkert? Hvordan måler vi, når flere svar kan være rigtige? Er målingerne stabile og sammenlignelige med andre målinger henover tid?

Det er vigtigt, fordi dataene, som de intelligente systemer lærer af, sjældent er komplette eller fuldstændige spejlbilleder af virkeligheden. Hvis udviklerne ikke er opmærksomme på det, risikerer vi, at livsvigtige beslutninger bliver taget på en forkert baggrund.

Grundlaget for at udvikle og anvende intelligente systemer er ofte baseret på mål om besparelser i tid og penge i virksomheder og institutioner.

Skal de intelligente systemer virke sikkert og pålideligt, er det dog vigtigt at anerkende systemerne som vidensproducerende værktøjer, hvis sikkerhed hviler på spørgsmål om menneskers evne til at fortolke data og måle præcist – ikke kun på spørgsmål om opbevaring eller anonymisering af data.

Anja Bechmann er professor på medievidenskab, Aarhus Universitet og leder af Datalab, der arbejder med anvendelse af personlige data og algoritmer i teknologi og samfund.
Anne Henriksen er ph.d.-studerende samme sted.