Rådet for
Digital Sikkerhed

3. oktober 2024

Lad os få konkretiseret udfordringerne ved kunstig intelligens

Rådet for Digital Sikkerhed har gennem mange år arbejdet for et trygt og frit digitalt samfund. Med udviklingen inden for kunstig intelligens er det helt centralt, at vi får indfanget de særlige udfordringer, som implementeringen af AI kan medføre. Både når det gælder nye former for cyberangreb, potentiel destabilisering af demokrati og samfund samt pres på individets rettigheder og de menneskelige konsekvenser det i øvrigt kan have, at algoritmer i stigende grad former vores liv. Rådets undersøgelse er et bidrag til at konkretisere de områder, vi skal være opmærksomme på, når vi drøfter, hvordan vi bedst kan udnytte de oplagte potentialer ved kunstig intelligens.

Anne Dorte Bach, næstformand for Rådet for Digital Sikkerhed

Innovation med et kritisk blik. Sådan kan man sammenfatte budskabet i Rådet for Digital Sikkerheds medlemsundersøgelse om kunstig intelligens (AI), der blev gennemført i foråret 2024.

Undersøgelsen indikerer, at de meget store teknologispring inden for kunstig intelligens lader vente på sig, og at vi derfor har et godt fundament for en innovativ, men kritisk tilgang til teknologierne i både privat og offentligt regi.

Medlemskredsen forventer, at kunstig intelligens ikke vil slå igennem med samme styrke overalt. De mest gennemgribende forandringer ventes inden for udvalgte sektorer så som sundhed, finans, kultur og kommunikation, it-teknologi og -sikkerhed samt forsvar, mens forventningen er mindre udtalt inden for energi- og vandforsyning, transport, landbrug og offentlig forvaltning.

Undersøgelsen udpeger flere kritiske udfordringer, der bør have stor opmærksomhed i den fortsatte udvikling:

- 'Gennemsigtighed og legitimitet' ved anvendelse af persondata. Det handler fx om gennemsigtighed i forhold til, hvilke persondata, der indgår i AI-træningsmodellerne, og i forhold til det digitale output, der indgår i afgørelser i forhold til borgere og kunder. Opmærksomheden samler sig også om algoritmebaseret bias, det vil sige risikoen for, at AI-systemer giver 'stigmatiserende' output i forhold til bestemte befolkningsgrupper.
- 'Cybersikkerhed' står tilsvarende højt på temalisten i kølvandet på kunstig intelligens. Risikoen for 'dataforurening', der handler om udnyttelse af svagheder i de anvendte datasæt og træningsmodeller, blev fremhævet som et væsentligt tema i undersøgelsen. Deciderede 'input-angreb', hvor fejlbehæftede instruktioner til et AI-system kan have ødelæggende konsekvenser for modellen, blev også fremhævet. Det samme blev sikringen mod såkaldte 'AI hallucinationer', hvor AI-systemet leverer selvopfundne og ukorrekte svar på forespørgsler.
- 'Det generelle tillidsniveau' i samfundet bør ifølge undersøgelsen være et vigtigt fokusområde i den fortsatte udbygning af det digitale samfund. Det handler om dagligdagens samspil mellem borgere, virksomheder og den offentlig forvaltning, hvor AI-udviklingen rummer risiko for erosion af den menneskelige kontakt og tillid. Det handler også om AI-teknologiens betydning i forhold til udbredelsen og gennemslagskraften af misinformation i det digitale miljø.

Rådets undersøgelse er selvsagt et øjebliksbillede, og ingen kender fremtidens innovationer. Så udviklingen inden for kunstig intelligens bør følges tæt. Rådets medlemsundersøgelse præsenterer vigtige pejlemærker og vil forhåbentlig bidrage til såvel den fortsatte samfundsdebat som forsvarlig digital udvikling i privat og offentligt regi.

For yderligere information kontakt venligst

Anne Dorte Bach, næstformand Rådet for Digital Sikkerhed og Head of Governance and Data Privacy Nykredit (anne.bach@digitalsikkerhed.dk)

Claus Hjorth, sekretariatschef Rådet for Digital Sikkerhed (claus.hjorth@digitalsikkerhed.dk, 5334 2522)