



Bruxelles, den 19.2.2020
COM(2020) 65 final

HVIDBOG

om kunstig intelligens - en europæisk tilgang til ekspertise og tillid

Hvidbog om kunstig intelligens

En europæisk tilgang til ekspertise og tillid

Kunstig intelligens er i hastig udvikling. Det vil ændre vores tilværelse ved at forbedre sundhedsplejen (f.eks. med mere præcis diagnosticering og bedre forebyggelse af sygdomme), øge effektiviteten i landbruget, bidrage til afbødning af og tilpasning til klimaforandringer, forbedre effektiviteten af produktionssystemer ved hjælp af prædiktiv vedligeholdelse, øge sikkerheden for de europæiske borgere og på mange andre måder, som vi endnu ikke kan forestille os. Samtidig indebærer kunstig intelligens en række potentielle risici, f.eks. uigennemskuelige beslutningsprocesser, kønsbaseret eller andre former for diskrimination, krænkelse af privatlivets fred eller anvendelse til kriminelle formål.

På baggrund af den skarpe globale konkurrence er der behov for en solid europæisk tilgang, der bygger på den europæiske strategi for kunstig intelligens, der blev fremlagt i april 2018¹. For at tackle både mulighederne og udfordringerne ved kunstig intelligens må EU skride til værks som en enhed og fastsætte sin egen kurs på grundlag af europæiske værdier for at fremme udviklingen og udbredelsen af kunstig intelligens.

Kommissionen er fast besluttet på at bane vejen for videnskabelige gennembrud, bevare EU's teknologiske førerposition og sikre, at nye teknologier stilles til gavn for alle europæere for at forbedre deres tilværelse, samtidig med at deres rettigheder overholdes.

Kommissionens formand, Ursula von der Leyen, fremsatte i sine politiske retningslinjer² en koordineret europæisk tilgang til de menneskelige og etiske konsekvenser af kunstig intelligens samt overvejelser om bedre anvendelse af big data til innovation.

Kommissionen støtter således en lovgivnings- og investeringsorienteret tilgang, der har til formål både at fremme anvendelsen af kunstig intelligens og at håndtere de risici, der er forbundet med visse anvendelser af denne nye teknologi. Formålet med denne hvidbog er at opstille politiske løsningsmodeller for, hvordan disse mål skal nås. Den omhandler ikke udviklingen og anvendelsen af kunstig intelligens til militære formål. Kommissionen opfordrer medlemsstaterne, andre EU-institutioner og alle interessenter, herunder erhvervslivet, arbejdsmarkedets parter, civilsamfundsorganisationer, forskere, offentligheden generelt og alle interesserede parter, til at reagere på nedenstående valgmuligheder og bidrage til Kommissionens fremtidige beslutninger på dette område.

1. INDLEDNING

Den digitale teknologi bliver en stadig mere central del af menneskers liv på alle fronter, så derfor bør folk kunne stole på den. Pålidelighed er også en forudsætning for dens udbredelse. Her er Europa godt stillet i betragtning af dets stærke værdier, tilslutning til retsstatsprincippet og dets dokumenterede evne til at opbygge sikre, pålidelige og sofistikerede produkter og tjenesteydelser, lige fra luftfart til energi, biler og medicinsk udstyr.

EU's nuværende og fremtidige bæredygtige økonomiske vækst og samfundsmæssige velfærd bygger i stigende grad på den værdi, der skabes ved hjælp af data. Kunstig intelligens er en af dataøkonomiens vigtigste værktøjer. De fleste af nutidens data omhandler forbrugere og lagres i centrale cloudbaserede

¹ Kunstig intelligens for Europa (COM(2018) 237 final).

²https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_da.pdf.

infrastrukturer. I modsætning hertil vil en stor del af morgendagens langt mere omfattende data stamme fra industrien, erhvervslivet og den offentlige sektor og vil blive lagret på en række forskellige systemer, navnlig computersystemer i udkanten af netværket. Dette skaber nye muligheder for Europa, som er stærkt stillet inden for digitaliseret industri og anvendelser mellem virksomheder, men relativt svagt stillet med hensyn til forbrugerplatforme.

Kort sagt er kunstig intelligens en sammensætning af teknologier, der kombinerer data, algoritmer og computerkraft. Fremskridtene inden for databehandling og den stigende datatilgængelighed er derfor vigtige drivkræfter for den hastige udvikling inden for kunstig intelligens. Ved at kombinere sine teknologiske og industrielle styrker med en digital infrastruktur af høj kvalitet og en lovramme baseret på sine grundlæggende værdier kan Europa **blive førende på verdensplan inden for innovation i dataøkonomien og dens anvendelsesmuligheder** som fastsat i den europæiske datastrategi³. Derved kan Europa udvikle et økosystem for kunstig intelligens, som udbreder teknologiens fordele til hele Europas samfund og økonomi:

- for **borgerne**, der kan høste nye fordele ved f.eks. bedre sundhedspleje, mere holdbare husholdningsmaskiner, sikrere og renere transportsystemer og bedre offentlige tjenester
- for **virksomhederne**, der f.eks. kan udvikle nye generationer af produkter og tjenester på områder, hvor Europa er særlig stærkt (maskineri, transport, cybersikkerhed, grøn og cirkulær økonomi, sundhedspleje og sektorer med høj merværdi såsom mode og turisme)
- for **tjenester i offentlighedens interesse** ved f.eks. at mindske omkostningerne ved levering af tjenesteydelser (transport, uddannelse, energi og affaldsforvaltning), ved at forbedre produkters bæredygtighed⁴ og ved at udruste de retshåndhævende myndigheder med passende redskaber til at beskytte borgerne⁵ og passende sikkerhedsforanstaltninger, der skal sikre deres rettigheder og friheder.

I betragtning af den store indvirkning, som kunstig intelligens kan have på vores samfund, og behovet for at opbygge tillid, er det afgørende, at europæisk kunstig intelligens baseres på vores værdier og grundlæggende rettigheder, såsom beskyttelse af den menneskelige værdighed og privatlivets fred.

Derudover bør indvirkningen af systemer med kunstig intelligens ikke kun tages i betragtning fra et subjektivt perspektiv, men også fra et perspektiv, der ser samfundet som en helhed. Anvendelsen af systemer med kunstig intelligens kan spille en væsentlig rolle med hensyn til at nå målene for bæredygtig udvikling og støtte den demokratiske proces og de sociale rettigheder. Med sine seneste forslag om Europas grønne pagt⁶ står Europa i spidsen for håndteringen af klima- og miljørelaterede udfordringer. Digitale teknologier såsom kunstig intelligens er en afgørende forudsætning for at nå målene i den grønne pagt. I betragtning af den stigende betydning af kunstig intelligens skal den miljømæssige indvirkning af systemer med kunstig intelligens tages behørigt i betragtning i hele deres livscyklus og langs hele forsyningskæden, f.eks. med hensyn til anvendelse af ressourcer til tilpasning af algoritmer og lagring af data.

³ COM(2020) 66 final.

⁴ Kunstig intelligens og digitalisering generelt er afgørende forudsætninger for Europas ambitioner om en grøn pagt. IKT-sektorens nuværende miljøaftryk anslås imidlertid til at udgøre mere end 2 % af de samlede emissioner på verdensplan. I EU's digitale strategi, der ledsager denne hvidbog, foreslås der grønne omstillingsforanstaltninger for den digitale sektor.

⁵ Værktøjer baseret på kunstig intelligens giver mulighed for at beskytte EU-borgerne bedre mod kriminalitet og terrorhandlinger.

Sådanne værktøjer kan f.eks. bidrage til at identificere terrorrelateret indhold på nettet, opdage mistænkelige transaktioner i forbindelse med salg af farlige produkter, identificere farlige skjulte genstande eller ulovlige stoffer eller produkter, yde bistand til borgere i nødsituationer og vejlede retningsarbejdere.

⁶ COM(2019) 640 final.

En fælles europæisk tilgang til kunstig intelligens er nødvendig for at opnå en tilstrækkelig gennemslagskraft og undgå en opsplittning af det indre marked. Hvis der i stedet indføres nationale initiativer i de enkelte lande, kan det bringe retssikkerheden i fare, svække borgernes tillid og forhindre, at den europæiske industri udvikler sig dynamisk.

Denne hvidbog indeholder en række politiske valgmuligheder, som skal muliggøre en pålidelig og sikker udvikling af kunstig intelligens i Europa under fuld overholdelse af EU-borgernes værdier og rettigheder. De vigtigste bestanddele i denne hvidbog er:

- Den politiske ramme for foranstaltninger til at ensrette indsatsen på europæisk, nationalt og regionalt plan. Rammen har i partnerskab mellem den private og offentlige sektor til formål at mobilisere ressourcer til at oprette et "**ekspertisemiljø**" i hele værdikæden, der begynder med forskning og innovation, og skabe de rette incitamenter til at fremskynde ibrugtagningen af løsninger baseret på kunstig intelligens, herunder hos små og mellemstore virksomheder (SMV'er).
- De centrale elementer i en fremtidig lovramme for kunstig intelligens i Europa, der skal skabe et unikt "**tillidsmiljø**". Med henblik herpå skal rammen sikre overholdelse af EU-reglerne, herunder reglerne for beskyttelse af grundlæggende rettigheder og forbrugerrettigheder, navnlig for systemer med kunstig intelligens, der anvendes i EU, og som udgør en stor risiko⁷. At opbygge et tillidsmiljø er i sig selv en politisk målsætning, der skal give borgerne tillid til anvendelsen af kunstig intelligens og give virksomheder og offentlige organisationer den fornødne retssikkerhed til at innovere med kunstig intelligens. Kommissionen støtter i høj grad en menneskecentreret tilgang baseret på meddelelsen om opbygning af tillid til menneskecentreret kunstig intelligens⁸ og vil også tage hensyn til de input, der blev indsamlet i løbet af pilotfasen for de etiske retningslinjer, som Ekspertgruppen på Højt Niveau vedrørende Kunstig Intelligens har udarbejdet.

Den europæiske strategi for data, som ledsager denne hvidbog, har til formål at sætte Europa i stand til at blive den mest attraktive, sikre og dynamiske data-agile økonomi i verden — Europa skal bruge data til at forbedre sine beslutningsprocesser og tilværelsen for alle sine borgere. Strategien indeholder en række politiske tiltag, der er nødvendige for at nå dette mål, herunder mobilisering af private og offentlige investeringer. I Kommissionens rapport, der ledsager denne hvidbog, analyseres derudover konsekvenserne af kunstig intelligens, tingenes internet og andre digitale teknologier for lovgivningen om sikkerhed og ansvar.

2. UDNYTTELSE AF STYRKER PÅ INDUSTRI- OG ERHVERVSMARKEDERNE

Europa har gode forudsætninger for at drage fordel af kunstig intelligens, ikke blot som bruger, men også som udvikler og producent af denne teknologi. Det har fremragende forskningscentre, innovative opstartsvirksomheder, en førende position inden for robotteknologi samt konkurrencedygtige fremstillings- og servicesektorer, fra bilindustrien til sundhedspleje, energi, finansielle tjenesteydelser og landbrug. Europa har udviklet en stærk databehandlingsinfrastruktur (f.eks. højtydende computere), som er afgørende for, at kunstig intelligens kan fungere. Desuden råder Europa over store offentlige og industrielle data, hvis potentiale i øjeblikket ikke udnyttes fuldt ud. Det har velanerkendte industrielle

⁷ Selv om der kan blive behov for yderligere ordninger for at forebygge og modvirke misbrug af kunstig intelligens til kriminelle formål, falder dette uden for rammerne af denne hvidbog.

⁸ COM(2019) 168.

styrker inden for sikre digitale systemer med lavt strømforbrug, hvilke har afgørende betydning for videreudviklingen af kunstig intelligens.

Udnyttelse af EU's kapacitet til at investere i næstegenerationsteknologier og -infrastrukturer samt digitale kompetencer såsom datafærdigheder vil øge Europas teknologiske suverænitet inden for centrale støtteteknologier og -infrastrukturer i dataøkonomien. Infrastrukturerne bør understøtte oprettelsen af europæiske datapuljer, der muliggør pålidelig kunstig intelligens, f.eks. kunstig intelligens baseret på europæiske værdier og regler.

Europa bør udnytte sine styrker til at udvide sin indflydelse i økosystemerne og langs værdikæden, lige fra visse hardwarefremstillingssektorer gennem software og hele vejen til tjenesteydelser. Dette er allerede i et vist omfang ved at ske. Europa fremstiller over en fjerdedel af industriens og erhvervslivets servicerobotter (f.eks. til præcisionslandbrug, sikkerhed, sundhed og logistik) og spiller en vigtig rolle i udviklingen og udnyttelsen af softwareapplikationer til virksomheder og organisationer (applikationer til brug mellem virksomheder såsom software til virksomhedsstyring (ERP), design og konstruktion) samt applikationer til digital forvaltning og "intelligent virksomhed".

Europa baner vejen for udbredelsen af **kunstig intelligens inden for produktion**. Over halvdelen af de største producenter har indført kunstig intelligens i mindst én fase af deres produktionsforløb⁹.

En af grundene til, at Europa har indtaget en stærk position inden for forskning, er EU's finansieringsprogram, der har spillet en afgørende rolle i at samle indsatsen, undgå dobbeltarbejde og opnå en løftestangseffekt med offentlige og private investeringer i medlemsstaterne. I løbet af de sidste tre år er EU-midlerne til forskning og innovation inden for kunstig intelligens steget til 1,5 mia. EUR, dvs. **en stigning på 70 % i forhold til den foregående periode**.

Investeringer i forskning og innovation i Europa er dog stadig kun en brøkdel af de offentlige og private investeringer i andre regioner i resten af verden. Der blev investeret ca. 3,2 mia. EUR i kunstig intelligens i Europa i 2016 sammenlignet med ca. 12,1 mia. EUR i Nordamerika og 6,5 mia. EUR i Asien¹⁰. Som modsvar er Europa nødt til at øge sit investeringsniveau betydeligt. Den koordinerede plan for kunstig intelligens¹¹, der er udviklet i samarbejde med medlemsstaterne, har vist sig at være et godt springbræt til at opbygge et stærkere samarbejde om kunstig intelligens i Europa og skabe synergier for at maksimere investeringerne i værdikæden for kunstig intelligens.

3. UDNYTTELSE AF FREMTIDIGE MULIGHEDER: DEN NÆSTE DATABØLGE

Europa har i øjeblikket en svagere stilling inden for forbrugerapplikationer og onlineplatforme, hvilket er en konkurrencemæssig ulempe i forbindelse med adgang til data, men der er vigtige ændringer på vej i samtlige sektorer med hensyn til datas værdi og genanvendelse. Den mængde data, der genereres i verden, stiger hurtigt: fra 33 zettabytes i 2018 til en forventet mængde på 175 zettabytes i 2025¹². Hver ny databølge medfører lige så mange muligheder for, at Europa kan placere sig fordelagtigt i den data-agile økonomi og blive førende i verden på dette område. Desuden vil måden, hvorpå data lagres og behandles ændre sig drastisk i løbet af de kommende fem år. I dag sker 80 % af den databehandling og -analyse, der finder sted i skyen, i datacentre og centraliserede databehandlingsfaciliteter og 20 % i intelligente forbundne objekter, såsom biler, husholdningsapparater eller produktionsrobotter, og i

⁹ Efterfulgt af Japan (30 %) og USA (28 %). Kilde: CapGemini (2019).

¹⁰ "10 imperatives for Europe in the age of AI and automation" ("10 imperativer for Europa i den kunstige intelligens' og automatiseringens tidsalder"), McKinsey, 2017.

¹¹ COM(2018) 795.

¹² IDC, 2019.

databehandlingsfaciliteter tæt på brugeren ("edge computing"). Inden 2025 vil dette forhold sandsynligvis have ændret sig markant¹³.

Europa er blandt de førende på verdensplan inden for elektronik med lavt strømforbrug, som er afgørende for den næste generation af specialiserede processorer til kunstig intelligens. Dette marked domineres i øjeblikket af aktører uden for EU. Dette kan ændres ved hjælp af initiativer som f.eks. det europæiske processor-initiativ, hvor der fokuseres på udviklingen af energibesparende computersystemer til både edge computing og den næste generation af højtydende databehandling, eller fællesforetagendet "Key Digital Technology Joint Undertaking", der foreslås påbegyndt i 2021. Europa er desuden førende inden for neuromorfiske løsninger¹⁴, der er velegnede til automatisering af industriprocesser (industri 4.0) og transport. Disse løsninger kan fordoble energieffektiviteten indtil flere gange.

Den seneste udvikling inden for kvantedatabehandling vil medføre eksponentielle stigninger i databehandlingskapaciteten¹⁵. Europa kan blive førende inden for denne teknologi takket være sine akademiske styrker inden for kvantedatabehandling samt den europæiske industris stærke position inden for kvantesimulatorer og programmeringsmiljøer for kvantedatabehandling. Europæiske initiativer, der har til formål at øge tilgængeligheden af test- og forsøgsfaciliteter til kvantedatabehandling, vil bidrage til anvendelsen af disse nye kvanteløsninger inden for en række industrielle og akademiske sektorer.

Sideløbende hermed vil Europa fortsat være på forkant med fremskridtet på algoritmegrundlaget for kunstig intelligens og bygge videre på sin egen videnskabelige ekspertise. Der er behov for at bygge bro mellem discipliner, der i øjeblikket benyttes separat, såsom maskinindlæring og dyb læring (karakteriseret ved at være vanskelige at fortolke, behovet for store mængder data til brug for modellerne og læring gennem korrelationer) og symbolske tilgange (hvor mennesker fastsætter regler direkte). Ved at kombinere symbolske tankeløse med dybe neurale net kan vi opnå kunstig intelligens med bedre forklarlighed.

4. ET VERDENSKLASSEMILJØ

For at opbygge et ekspertisemiljø, der kan støtte udviklingen og udbredelsen af kunstig intelligens i hele EU's økonomi og offentlige forvaltning, er der behov for at optrappe indsatsen på flere niveauer.

A. SAMARBEJDE MED MEDLEMSSTATERNE

Kommissionen fremlagde i december 2018 en koordineret plan, der er udarbejdet i samarbejde med medlemsstaterne, og som har til formål at fremme udviklingen og anvendelsen af kunstig intelligens i Europa¹⁶, og gennemfører dermed sin strategi for kunstig intelligens, der blev vedtaget i april 2018¹⁷.

Denne plan indeholder forslag til 70 fælles aktioner med henblik på et tættere og mere effektivt samarbejde mellem medlemsstaterne og Kommissionen på centrale områder såsom forskning, investering, markedsudbredelse, færdigheder og talenter, data og internationalt samarbejde. Planen forventes at vare frem til 2027 og vil blive overvåget og revideret regelmæssigt.

¹³ Gartner, 2017.

¹⁴ Ved neuromorfiske løsninger forstås meget store systemer af integrerede kredsløb, der efterligner nervesystemets neurobiologiske strukturer.

¹⁵ Kvantecomputere vil på kortere tid kunne behandle mange gange større datasæt, end de bedste computere kan i dag, hvilket vil gøre det muligt at udvikle nye anvendelsesmuligheder inden for kunstig intelligens på tværs af sektorer.

¹⁶ [Koordineret plan for kunstig intelligens, COM \(2018\) 795.](#)

¹⁷ [Kunstig intelligens for Europa, COM\(2018\) 237.](#)

Formålet er at maksimere virkningen af investeringer i forskning, innovation og udbredelse, vurdere de nationale strategier for kunstig intelligens og bygge på og udvide den koordinerede plan for kunstig intelligens sammen med medlemsstaterne:

- *Foranstaltning 1: Kommissionen vil under hensyntagen til resultaterne af den offentlige høring om hvidbogen foreslå medlemsstaterne en revision af den koordinerede plan, der skal vedtages senest ved udgangen af 2020.*

Finansiering på EU-plan af kunstig intelligens bør tiltrække og samle investeringerne på områder, hvor der kræves en indsats ud over, hvad en enkelt medlemsstat kan opnå. Målet er at tiltrække mere end 20 mia. EUR¹⁸ i samlede investeringer om året i kunstig intelligens i EU i løbet af det næste årti. For at stimulere private og offentlige investeringer vil EU stille midler til rådighed fra programmet for et digitalt Europa, Horisont Europa og de europæiske struktur- og investeringsfonde for at imødekomme landdistrikternes og de mindre udviklede regioners behov.

Den koordinerede plan kan også tage fat på samfundsmæssig og miljømæssig velfærd som et centralt princip for kunstig intelligens. Systemer med kunstig intelligens forventes at kunne hjælpe med at tackle de mest presserende problemer, herunder klimaændringer og miljøforringelse. Det er netop også vigtigt, at dette sker på en miljøvenlig måde. Kunstig intelligens kan og bør i sig selv foretage en kritisk undersøgelse af ressource- og energiforbruget og være tilpasset til at træffe valg, der er gavnlige for miljøet. Kommissionen vil sammen med medlemsstaterne overveje mulighederne for at tilskynde til og fremme løsninger med kunstig intelligens, der gør dette.

B. FOKUS PÅ FORSKNINGS- OG INNOVATIONSSAMFUNDETS INDSATS

Europa har ikke råd til at opretholde det nuværende landskab med spredte kompetencecentre, hvor ingen af dem har nået det omfang, der skal til for at konkurrere med de førende institutter på globalt plan. Det er bydende nødvendigt at skabe flere synergier og netværk mellem de forskellige europæiske forskningscentre, der beskæftiger sig med kunstig intelligens, og ensrette deres bestræbelser på at forbedre ekspertisen, fastholde og tiltrække de bedste forskere og udvikle den bedste teknologi. Europa har brug for et centrum for forskning, innovation og ekspertise, som skal koordinere denne indsats og udgøre et forbillede i verdensklasse inden for kunstig intelligens, og som kan tiltrække investeringer og de bedste talenter på området.

Centrene og netværkene bør fokusere på de sektorer, hvor Europa har potentialet til at blive verdens førende, såsom industri, sundhed, transport, finans, fødevarer-værdikæder, energi/miljø, skovbrug, jordobservation og rumfart. På alle disse områder er kapløbet om førstepladsen på verdensplan allerede skudt i gang, og Europa kan byde ind med et betydeligt potentiale samt stor viden og ekspertise¹⁹. Lige så vigtigt er det at oprette test- og forsøgsfaciliteter til at støtte udviklingen og den efterfølgende anvendelse af nye anvendelsesmuligheder inden for kunstig intelligens.

- *Foranstaltning 2: Kommissionen vil fremme oprettelsen af ekspertisecentre og testfaciliteter, der kan kombinere europæiske, nationale og private investeringer, eventuelt med et nyt retsinstrument. Som led i den flerårige finansielle ramme for 2021-2027 har Kommissionen fremsat forslag om at afsætte et ambitiøst beløb til støtte for europæiske testfaciliteter i*

¹⁸ COM(2018) 237.

¹⁹ Den kommende Europæiske Forsvarsfond og det permanente strukturerede samarbejde (PESCO) vil også skabe muligheder for forskning og udvikling inden for kunstig intelligens. Disse projekter bør synkroniseres med EU's bredere civile programmer om kunstig intelligens.

verdensklasse under programmet for et digitalt Europa, om nødvendigt suppleret af Horisont Europas forsknings- og innovationsforanstaltninger.

C. FÆRDIGHEDER

Den europæiske tilgang til kunstig intelligens skal understøttes af et stærkt fokus på færdigheder for at udfylde eventuelle kompetencemangler²⁰. Kommissionen vil snart fremlægge en optrapning af dagsordenen for færdigheder, som skal sikre, at alle i Europa kan drage fordel af de grønne og digitale omstillinger af EU's økonomi. De dertil hørende initiativer kan også omfatte støtte til sektorspecifikke tilsynsmyndigheder for at forbedre deres færdigheder inden for kunstig intelligens og dermed gennemføre de relevante regler på virkningsfuld og effektiv vis. Den ajourførte handlingsplan for digital uddannelse vil bidrage til at gøre bedre brug af data og teknologier inden for kunstig intelligens (såsom læring og prædiktive analyser) med henblik på at forbedre uddannelsessystemerne og gøre dem parate til den digitale tidsalder. Handlingsplanen vil også øge kendskabet til kunstig intelligens på alle uddannelsesniveauer, således at borgerne forberedes på informeret beslutningstagning, der i stigende grad vil blive påvirket af kunstig intelligens.

I den reviderede koordinerede plan for kunstig intelligens, der skal udvikles sammen med medlemsstaterne, prioriteres udviklingen af de færdigheder, der er nødvendige for at arbejde med kunstig intelligens, og opkvalificering af arbejdsstyrken, så den bliver tilpasset den digitale omstilling. Som led heri kunne evalueringslisten i de etiske retningslinjer omformes til et vejledende "pensum" for udviklere af kunstig intelligens, der så ville blive stillet til rådighed som en ressource for uddannelsesinstitutioner. Der bør gøres en særlig indsats for at øge antallet af kvinder, der er uddannet og beskæftiget på dette område.

Desuden vil et fyrtårn for forskning og innovation vedrørende kunstig intelligens i Europa tiltrække talenter fra hele verden som følge af de muligheder, der kan tilbydes. Det vil også bidrage til udviklingen og udbredelsen af ekspertfærdigheder i hele Europa.

- *Foranstaltning 3: Gennem søjlen for avancerede færdigheder i programmet for et digitalt Europa skal netværk af førende universiteter og højere uddannelsesinstitutioner etableres og understøttes for at tiltrække de bedste lærere og videnskabsfolk og tilbyde kandidatuddannelser inden for kunstig intelligens i verdensklasse.*

Ud over opkvalificering påvirkes både arbejdstagere og arbejdsgivere direkte af udformningen og anvendelsen af systemer med kunstig intelligens på arbejdspladsen. Inddragelsen af arbejdsmarkedets parter vil være en afgørende faktor i at sikre en menneskecentreret tilgang til kunstig intelligens på arbejdspladsen.

D. FOKUS PÅ SMV'ER

Det vil også være vigtigt at sikre, at SMV'er kan få adgang til og anvende kunstig intelligens. Med henblik herpå bør de digitale innovationsknudepunkter²¹ og on-demand-plattformen²² for kunstig intelligens styrkes yderligere for at fremme samarbejdet mellem SMV'er. Programmet for et digitalt Europa vil være af afgørende betydning for at opnå dette. Selv om alle digitale innovationsknudepunkter bør yde støtte til SMV'er til at forstå og anvende kunstig intelligens, vil det

²⁰ <https://ec.europa.eu/jrc/en/publication/academic-offer-and-demand-advanced-profiles-eu>

²¹ ec.europa.eu/digital-single-market/en/news/digital-innovation-hubs-helping-companies-across-economy-make-most-digital-opportunities.

²² www.Ai4eu.eu.

være vigtigt at have mindst ét innovationsknudepunkt i hver medlemsstat med en høj grad af specialisering inden for kunstig intelligens.

SMV'er og nystartede virksomheder skal have adgang til finansiering med henblik på at tilpasse deres processer eller innovere ved hjælp af kunstig intelligens. Med udgangspunkt i den kommende pilotinvesteringsfond på 100 mio. EUR til kunstig intelligens og blockchain vil Kommissionen yderligere øge adgangen til finansiering af kunstig intelligens inden for rammerne af InvestEU²³. Kunstig intelligens nævnes udtrykkeligt blandt de områder, der er støtteberettigede i forbindelse med InvestEU-garantien.

- *Foranstaltning 4: Kommissionen vil samarbejde med medlemsstaterne for at sikre, at der er mindst ét digitalt innovationsknudepunkt i hver medlemsstat med en høj grad af specialisering inden for kunstig intelligens. Digitale innovationsknudepunkter kan støttes under programmet for et digitalt Europa.*
- *Kommissionen og Den Europæiske Investeringsfond vil iværksætte en pilotordning med 100 mio. EUR i første kvartal af 2020, der skal tilvejebringe egenkapitalfinansiering af innovativ udvikling inden for kunstig intelligens. Kommissionen har fra 2021 til hensigt at optrappe dette i betydelig grad gennem InvestEU under forudsætning af, at der kan opnås endelig enighed herom i den flerårige finansielle ramme.*

E. PRIVATSEKTOREN SOM PARTNER

Det er også afgørende at sikre, at den private sektor inddrages fuldt ud i fastlæggelsen af forsknings- og innovationsdagsordenen og bidrager med saminvesteringer i det nødvendige omfang. Dette vil kræve, at der etableres et stort offentligt-privat partnerskab, og at virksomhedernes øverste ledelse engagerer sig.

- *Foranstaltning 5: I forbindelse med Horisont Europa vil Kommissionen etablere et nyt offentlig-privat partnerskab inden for kunstig intelligens, data og robotteknologi med henblik på at kombinere indsatsen, sikre koordinering af forskning og innovation inden for kunstig intelligens og samarbejde med andre offentlig-private partnerskaber i Horisont Europa, de ovennævnte testfaciliteter og de digitale innovationsknudepunkter.*

F. FREMME AF ANVENDELSEN AF KUNSTIG INTELLIGENS I DEN OFFENTLIGE SEKTOR

Det er vigtigt, at offentlige forvaltninger, hospitaler, forsynings- og transporttjenester, finansielle tilsynsmyndigheder og andre områder af offentlig interesse hurtigt begynder at anvende produkter og tjenester, der benytter kunstig intelligens. Der vil især blive fokuseret på sundhedspleje og transport, hvor teknologien er moden til udbredelse i stor målestok.

- *Foranstaltning 6: Kommissionen vil indlede åbne og gennemsigtige sektordialoger, hvor sundhedstjenester, forvaltninger i landdistrikter og operatører af offentlige tjenester prioriteres, med henblik på at fremlægge en handlingsplan, der skal lette udvikling af, forsøg med og ibrugtagning af kunstig intelligens. Sektordialogerne vil blive brugt til at udarbejde et specifikt "brug kunstig intelligens"-program, der skal støtte offentlige organers anskaffelse af*

²³ Europe.eu/investeu.

systemer med kunstig intelligens og bidrage til at ændre selve procedurerne for offentlige udbud.

G. SIKRING AF ADGANG TIL DATA OG DATABEHANDLINGSINFRASTRUKTUR

De indsatsområder, der er beskrevet i denne hvidbog, supplerer den plan, der sideløbende fremlægges i forbindelse med den europæiske datastrategi. Det er afgørende at forbedre datastyringen og adgangen til data. Uden data er det ikke muligt at udvikle kunstig intelligens eller andre digitale applikationer. De enorme mængder af nye data, der vil blive genereret i fremtiden, vil gøre det muligt for Europa at indtage en førerposition inden for omstillingen til en datadreven økonomi med kunstig intelligens. Fremme af ansvarlig dataforvaltningspraksis og dataenes overensstemmelse med FAIR-principperne vil bidrage til at opbygge tillid og sikre, at data kan videreanvendes²⁴. Investeringer i centrale databehandlingsteknologier og -infrastrukturer er ligeledes vigtige.

Kommissionen har foreslået at afsætte over 4 mia. EUR under programmet for et digitalt Europa til støtte for højtydende databehandling og kvantedatabehandling, herunder edge computing og kunstig intelligens samt data- og cloudinfrastruktur. Den europæiske datastrategi videreudvikler disse prioriteter.

H. INTERNATIONALE ASPEKTER

Europa er godt rustet til at udvise globalt lederskab i forbindelse med opbygningen af alliancer omkring fælles værdier og fremme af etisk anvendelse af kunstig intelligens. EU's arbejde med kunstig intelligens har allerede haft indflydelse på den internationale debat. Med udarbejdelsen af sine etiske retningslinjer har ekspertgruppen på højt plan inddraget en række organisationer uden for EU og observatører fra en række regeringer. Sideløbende hermed var EU tæt involveret i udviklingen af OECD's etiske principper for kunstig intelligens²⁵. G20 godkendte efterfølgende disse principper i sin ministererklæring fra juni 2019 om handel og den digitale økonomi.

Sideløbende hermed anerkender EU, at der udføres vigtigt arbejde med kunstig intelligens i andre multilaterale fora, herunder Europarådet, De Forenede Nationers Organisation for Uddannelse, Videnskab og Kultur (UNESCO), Organisationen for Økonomisk Samarbejde og Udvikling (OECD), Verdenshandelsorganisationen (WTO) og Den Internationale Telekommunikationsunion (ITU). I FN er EU involveret i opfølgningen af rapporten fra højniveaupanelet om digitalt samarbejde, herunder henstillingen om kunstig intelligens.

EU vil fortsat samarbejde med ligesindede lande, men også med globale aktører, om kunstig intelligens med en tilgang baseret på EU's regler og værdier (f.eks. støtte til opadgående regelkonvergens, adgang til centrale ressourcer, herunder data, og lige konkurrencevilkår). Kommissionen vil nøje overvåge de politikker i tredjelande, der begrænser datastrømme, og vil behandle uberettigede begrænsninger i bilaterale handelsforhandlinger og gennem foranstaltninger inden for rammerne af Verdenshandelsorganisationen. Kommissionen er overbevist om, at det internationale samarbejde om kunstig intelligens skal baseres på en tilgang, der fremmer respekten for de grundlæggende rettigheder, herunder menneskelig værdighed, pluralisme, inklusion,

²⁴ "Findable, Accessible, Interoperable and Reusable" (data der kan findes og er tilgængelige, interoperable og videreanvendelige) som det fremgår af den endelige rapport og handlingsplan fra Kommissionens ekspertgruppe vedrørende FAIR data, 2018, https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf.

²⁵ <https://www.oecd.org/going-digital/ai/principles/>

ikkeforskelsbehandling og beskyttelse af privatlivets fred og personoplysninger²⁶, og den vil bestræbe sig på at eksportere sine værdier til hele verden²⁷. Det står også klart, at ansvarlig udvikling og anvendelse af kunstig intelligens kan være en drivkraft til at nå målene for bæredygtig udvikling og fremme 2030-dagsordenen.

5. ET TILLIDSMILJØ: LOVRAMMEN FOR KUNSTIG INTELLIGENS

Som med al ny teknologi er der både muligheder og risici forbundet med anvendelsen af kunstig intelligens. Borgerne frygter, at de bliver ude af stand til at forsvare deres rettigheder og sikkerhed, når de står over for informationsasymmetrierne forbundet med algoritmisk beslutningstagning, og virksomhederne er bekymrede over manglende retssikkerhed. Selv om kunstig intelligens kan bidrage til at beskytte borgernes sikkerhed og sætte dem i stand til at udøve deres grundlæggende rettigheder, er borgerne også bekymrede for, om kunstig intelligens kan få utilsigtede virkninger eller endda anvendes til ondsindede formål. Disse bekymringer bør der tages højde for. Ud over manglende investeringer og færdigheder er manglende tillid desuden en vigtig faktor, der bremser udbredelsen af kunstig intelligens.

Derfor har Kommissionen den 25. april 2018 udarbejdet en strategi for kunstig intelligens²⁸, som tager fat på de socioøkonomiske aspekter parallelt med en forøgelse af investeringerne i forskning, innovation og kapacitet for kunstig intelligens i hele EU. Den har vedtaget en koordineret plan²⁹ med medlemsstaterne for at ensrette strategierne og har også oprettet en ekspertgruppe på højt niveau, som i april 2019 offentliggjorde et sæt retningslinjer for pålidelig kunstig intelligens³⁰.

Kommissionen har offentliggjort en meddelelse³¹, hvori den bifalder de syv centrale krav i retningslinjerne fra ekspertgruppen på højt niveau:

- menneskelige aktiviteter og tilsyn udført af mennesker
- teknologisk robusthed og sikkerhed
- privatlivets fred og datastyring
- gennemsigtighed
- mangfoldighed, ikkediskrimination og retfærdighed
- social og miljømæssig velfærd, samt
- ansvarlighed.

Retningslinjerne indeholder desuden en evalueringsliste, der skal anvendes af virksomhederne i praksis. I andet halvår af 2019 har over 350 organisationer afprøvet denne evalueringsliste og indsendt feedback. Ekspertgruppen på højt niveau er i færd med at revidere sine retningslinjer i lyset af denne feedback og vil afslutte dette arbejde inden juni 2020. Et vigtigt resultat af feedback-processen er, at selv om en række af kravene allerede er afspejlet i eksisterende retlige eller lovgivningsmæssige ordninger, er dem, der vedrører gennemsigtighed, sporbarhed og menneskeligt tilsyn, ikke specifikt omfattet af den nuværende lovgivning i mange økonomiske sektorer.

²⁶ Inden for rammerne af partnerskabsinstrumentet vil Kommissionen finansiere et projekt til en værdi af 2,5 mio. EUR, som skal lette samarbejdet med ligesindede partnere med henblik på at fremme EU's etiske retningslinjer for kunstig intelligens og vedtage fælles principper og praktiske konklusioner.

²⁷ Kommissionsformand Ursula von der Leyen, En mere ambitiøs Union — Min dagsorden for Europa, side 17.

²⁸ COM(2018) 237.

²⁹ COM(2018) 795.

³⁰ <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top>

³¹ COM(2019) 168.

Ud over dette sæt ikkebindende retningslinjer fra ekspertgruppen på højt niveau og i overensstemmelse med formandens politiske retningslinjer vil en klar europæisk lovramme skabe tillid til kunstig intelligens blandt forbrugere og virksomheder og dermed fremskynde udbredelsen af teknologien. En sådan lovramme bør være i overensstemmelse med andre tiltag til fremme af Europas innovationskapacitet og konkurrenceevne på dette område. Derudover skal den sikre socialt, miljømæssigt og økonomisk optimale resultater og overholdelse af EU's lovgivning, principper og værdier. Dette er særlig relevant på områder, hvor borgernes rettigheder kan blive mest direkte berørt, f.eks. i forbindelse med anvendelse af kunstig intelligens til retshåndhævelse og retsvæsenet.

Udviklere og udbydere af kunstig intelligens er allerede omfattet af EU-lovgivningen om grundlæggende rettigheder (f.eks. databeskyttelse, privatlivets fred og ikkeforskelsbehandling), forbrugerbeskyttelse og produktsikkerheds- og ansvarsregler. Forbrugerne forventer samme sikkerhedsniveau og respekt for deres rettigheder, uanset om et produkt eller et system anvender kunstig intelligens eller ej. Visse særlige træk ved kunstig intelligens (f.eks. uigennemsiagtighed) kan imidlertid vanskeliggøre anvendelsen og håndhævelsen af denne lovgivning. Det er derfor nødvendigt at undersøge, om den nuværende lovgivning er i stand til at håndtere de risici, der er forbundet med kunstig intelligens, om den kan håndhæves effektivt, og om der er behov for tilpasninger af lovgivningen eller helt ny lovgivning.

I betragtning af, at kunstig intelligens er under hastig udvikling, bør lovrammen give plads til yderligere udvikling. Eventuelle ændringer bør begrænses til klart konstaterede problemer, som der findes gennemførlige løsninger på.

Medlemsstaterne peger på den nuværende mangel på en fælles europæisk ramme. Tysklands kommission for dataetik har opfordret til et risikobaseret system med fem niveauer, der går fra ingen regulering af de mest tilforladelige systemer med kunstig intelligens til et fuldstændigt forbud mod de farligste systemer. Danmark har netop lanceret prototypen til en mærkningsordning for dataetik. Malta har indført et frivilligt system til certificering af kunstig intelligens. Hvis EU ikke bringer en EU-dækkende tilgang på banen, er der en reel risiko for fragmentering i det indre marked, hvilket vil undergrave målsætningerne for tillid, retssikkerhed og markedsudbredelse.

En solid europæisk lovramme for pålidelig kunstig intelligens vil beskytte alle europæiske borgere og bidrage til at skabe et gnidningsløst indre marked for den videre udvikling og udbredelse af kunstig intelligens samt styrke Europas industrielle grundlag inden for kunstig intelligens.

A. PROBLEMFORMULERING

Kunstig intelligens kan skabe mange fordele, herunder ved at føre til sikrere produkter og processer, men kan også gøre skade. Skaderne kan både være fysiske (enkeltpersoners sikkerhed og sundhed, tab af menneskeliv eller tingsskade) og immaterielle (brud på privatlivets fred, begrænsning af ytringsfriheden, tab af menneskelig værdighed eller forskelsbehandling inden for f.eks. adgang til beskæftigelse) og kan stamme fra en lang række risici. Lovrammen bør være fokuseret på, hvordan man kan minimere de forskellige risici for eventuelle skader, især de mest betydelige risici.

De største risici i forbindelse med anvendelsen af kunstig intelligens vedrører anvendelsen af regler, der har til formål at beskytte grundlæggende rettigheder (herunder beskyttelse af personoplysninger og privatlivets fred og ikkeforskelsbehandling), samt sikkerheds- og ansvarsrelaterede spørgsmål³².

³² Dette omfatter spørgsmål om cybersikkerhed, spørgsmål om anvendelsesmuligheder for kunstig intelligens i kritiske infrastrukturer og spørgsmål om ondsindet brug af kunstig intelligens.

Risici for grundlæggende rettigheder, herunder beskyttelse af personoplysninger og privatlivets fred og ikkeforskelsbehandling

Brugen af kunstig intelligens kan påvirke de værdier, som EU bygger på, og føre til krænkelse af de grundlæggende rettigheder³³, herunder ytringsfriheden, forsamlingsfriheden, menneskelig værdighed, ikkeforskelsbehandling på grundlag af køn, race eller etnisk oprindelse, religion eller tro, handicap, alder eller seksuel orientering, alt efter hvad der er relevant på visse områder, beskyttelse af personoplysninger og privatlivets fred³⁴, retten til effektive retsmidler og en retfærdig rettergang samt forbrugerbeskyttelse. Disse risici kan opstå som følge af mangler i den overordnede udformning af systemer med kunstig intelligens (herunder med hensyn til menneskeligt tilsyn) eller ved anvendelse af data uden udbedring af eventuelle skævheder (f.eks. hvis systemet kun er oplært med data fra mænd, hvilket dermed fører til suboptimale resultater for kvinder).

Kunstig intelligens kan udføre mange funktioner, som tidligere kun kunne varetages af mennesker. Som følge heraf vil borgere og juridiske personer i stadig højere grad blive påvirket af handlinger og beslutninger truffet af eller med bistand fra systemer med kunstig intelligens, som undertiden kan være vanskelige at forstå og om nødvendigt anfægte. Desuden øger kunstig intelligens mulighederne for at spore og analysere folks daglige vaner. Der er f.eks. en potentiel risiko for, at kunstig intelligens i strid med EU's regler om databeskyttelse og andre regler anvendes af statslige myndigheder eller andre enheder til masseovervågning og af arbejdsgivere til at observere deres ansattes adfærd. Ved at analysere store mængder data og konstatere forbindelser mellem dem kan kunstig intelligens også anvendes til at opspore og deanonymisere data om personer, hvorved der opstår nye risici for beskyttelsen af personoplysninger, selv med hensyn til datasæt, der ikke som sådan indeholder personoplysninger. Kunstig intelligens bruges også af onlineformidlere til at prioritere information til deres brugere og til at moderere indhold. De behandlede data, udformningen af anvendelsesmetoderne og mulighederne for menneskelig indgriben kan påvirke retten til ytringsfrihed, beskyttelse af personoplysninger, privatlivets fred og politiske frihedsrettigheder.

Forudindtagethed og diskrimination udgør iboende risici for enhver samfundsmæssig eller økonomisk aktivitet. Fejl og forudindtagethed kan stadig forekomme, når det er mennesker, der træffer beslutningerne. Når samme forudindtagethed forekommer i kunstig intelligens, kan den dog have en

Visse algoritmer kan, når de benyttes til at forudsige tilbagefald til kriminel adfærd, være påvirket af forudindtagethed i forbindelse med køn og race og dermed udvise forskellige sandsynligheder for tilbagefald for kvinder i forhold til mænd eller for statsborgere i forhold til udlændinge. Kilde: Tolan S., Miron M., Gomez E. og Castillo C. "Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia" (*Hvorfor maskinindlæring kan føre til uretfærdighed: Dokumentation fra risikovurdering i ungdomsretten i Catalonien*), pris for bedste artikel, *International Conference on AI and Law*, 2019.

Visse programmer med kunstig intelligens til ansigtsanalyse udviser forudindtagethed med hensyn til køn og race, idet de udviser en lav fejlprocent i bestemmelsen af køn på mænd med lys hud, men udviser en høj fejlprocent i bestemmelsen af køn på kvinder med mørk hud. Kilde: Joy Buolamwini, Timnit Gebru, *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR bind 81, s. 77-91, 2018.

langt større virkning, som kan føre til diskrimination mod mange mennesker uden de sociale kontrolmekanismer, der styrer menneskets adfærd³⁵. Dette kan også ske, når systemet med kunstig intelligens "lærer", mens det er i drift. I sådanne tilfælde, hvor resultatet ikke kunne være blevet forhindret eller forudset i planlægningsfasen, skyldes risiciene ikke fejl i systemets oprindelige udformning, men opstår snarere af de praktiske konsekvenser af de korrelationer eller mønstre, som systemet konstaterer i et stort datasæt.

De særlige karakteristika ved mange teknologier inden for kunstig intelligens, herunder uigennemsigthed ("sort boks"-effekten), kompleksitet, uforudsigelighed og en delvis autonom adfærd, kan gøre det vanskeligt at kontrollere, om reglerne overholdes, og de kan lægge hindringer i vejen for en effektiv håndhævelse af gældende EU-lovgivning, der har til formål at beskytte de grundlæggende rettigheder. Håndhævende myndigheder og berørte personer kan mangle midler til at kontrollere et givent beslutningsforløb, hvori kunstig intelligens blev benyttet, og dermed om de relevante regler blev overholdt. Enkeltpersoner og juridiske personer kan have svært ved at få effektiv adgang til domstolsprøvelse i situationer, hvor sådanne afgørelser påvirker dem negativt.

Risici for sikkerheden og for erstatningsordningers effektivitet

Når teknologier inden for kunstig intelligens indgår i produkter og tjenester, kan de udgøre nye sikkerhedsrisici for brugerne. Eksempelvis kan en selvkørende bil som følge af en eventuel fejl i billedteknologien fejlagtigt identificere en genstand på vejen og forårsage en ulykke med personskade og tingsskade til følge. Som i forbindelse med risiciene for de grundlæggende rettigheder kan disse risici være forbundet med problemer med teknologiens udformning, med tilgængeligheden og kvaliteten af data eller med andre problemer i forbindelse med maskinindlæring. Visse af disse risici er ikke begrænset til produkter og tjenesteydelser, der er afhængige af kunstig intelligens, men anvendelsen af kunstig intelligens kan øge eller forværre risiciene.

Manglen på klare sikkerhedsbestemmelser, der imødegår disse risici, kan ud over risiciene for de berørte enkeltpersoner skabe usikkerhed om retstilstanden for virksomheder, der markedsfører deres produkter med kunstig intelligens i EU. Markedsovervågnings- og håndhævelsesmyndighederne kan komme i en situation, hvor de er usikre, om hvorvidt de kan gribe ind, fordi de måske ikke har de rette beføjelser eller ikke har tilstrækkelig teknisk kapacitet til at inspicere systemerne³⁶. Usikkerhed om retstilstanden kan derfor mindske det generelle sikkerhedsniveau og underminere konkurrenceevnen hos europæiske virksomheder.

³⁵ Kommissionens Rådgivende Udvalg for Ligestilling mellem Kvinder og Mænd er i færd med at udarbejde en udtalelse om kunstig intelligens, hvori det bl.a. analyserer følgevirkningerne af kunstig intelligens for ligestillingen mellem kønnene, og som forventes at blive vedtaget af udvalget i begyndelsen af 2020. EU's ligestillingsstrategi for 2020-2024 omhandler også forbindelsen mellem kunstig intelligens og ligestilling mellem kønnene. Det europæiske netværk af ligestillingsorganer (Equinet) vil offentliggøre en rapport (af Robin Allen og Dee Masters) med titlen "Regulating AI: the new role for Equality Bodies – Meeting the new challenges to equality and non-discrimination from increased digitalisation and the use of AI" (Regulering af kunstig intelligens: Ligestillingsorganernes nye rolle — De nye udfordringer for lighed og ikkeforskelsbehandling ved den stigende digitalisering og anvendelse af kunstig intelligens), som forventes fremlagt i begyndelsen af 2020.

³⁶ Smarture til børn er et eksempel på dette. Dette produkt vil sandsynligvis ikke være til direkte skade for det barn, der bærer det, men hvis uret ikke har indbygget basale sikkerhedsfunktioner, kan det nemt bruges som et redskab til at få adgang til barnet. Markedsovervågningsmyndighederne kan få svært ved at gribe i tilfælde, hvor risikoen ikke er knyttet til selve produktet.

Hvis sikkerhedsrisiciene manifesterer sig, vil manglen på klare krav og de karakteristika ved teknologier med kunstig intelligens, der er nævnt ovenfor, gøre det vanskeligt at spore potentielt problematiske beslutninger i forbindelse med anvendelsen af systemer med kunstig intelligens. Dette kan dermed gøre det vanskeligt for personer, der har lidt skade, at opnå erstatning i henhold til EU's gældende lovgivning om erstatningsansvar³⁷.

I henhold til produktansvarsdirektivet er en fabrikant ansvarlig for skader forårsaget af et defekt produkt. I forbindelse med et system baseret på kunstig intelligens, f.eks. selvkørende biler, kan det være vanskeligt at bevise, at produktet er defekt, at der er sket en skade, og at der er en årsagssammenhæng mellem de to. Desuden er der en vis usikkerhed med hensyn til, hvordan og i hvilket omfang produktansvarsdirektivet gælder for visse typer defekter, f.eks. hvis disse skyldes svagheder i produktets cybersikkerhed.

Derfor gælder det også for sikkerheds- og ansvarsmæssige anliggender, at det er vanskeligt at spore potentielt problematiske beslutninger, der er blevet truffet af systemer med kunstig intelligens, som nævnt ovenfor i forbindelse med grundlæggende rettigheder. Det kan være, at skadelidte f.eks. ikke har effektiv adgang til de beviser, der er nødvendige for at indbringe et søgsmål for domstolen, og har mindre effektive klagemuligheder i forhold til situationer, hvor skaden er forårsaget af traditionelle teknologier. Disse risici vil stige, efterhånden som anvendelsen af kunstig intelligens bliver mere udbredt.

B. MULIGE TILPASNINGER AF EU'S EKSISTERENDE LOVRAMME VEDRØRENDE KUNSTIG INTELLIGENS

Meget af den eksisterende EU-lovgivning om produktsikkerhed og produktansvar³⁸, herunder sektorspecifikke regler, der yderligere suppleres af national lovgivning, er relevant for og muligvis anvendelig på en række nye anvendelser af kunstig intelligens.

For så vidt angår beskyttelsen af grundlæggende rettigheder og forbrugerrettigheder, omfatter EU's lovramme bl.a. direktivet om racelighed³⁹, direktivet om ligebehandling med hensyn til beskæftigelse og erhverv⁴⁰, direktiverne om ligebehandling af mænd og kvinder i forbindelse med beskæftigelse og adgang til varer og tjenesteydelser⁴¹ samt en række retsakter om forbrugerbeskyttelse⁴² og beskyttelse af personoplysninger og privatlivets fred, herunder navnlig den generelle forordning om databeskyttelse og anden sektorspecifik lovgivning vedrørende beskyttelse af personoplysninger såsom direktivet om databeskyttelse på retshåndhævelsesområdet⁴³. Desuden vil reglerne om

³⁷ I Kommissionens rapport, der ledsager denne hvidbog, analyseres konsekvenserne af kunstig intelligens, tingenes internet og andre digitale teknologier for sikkerheds- og ansvarslovgivningen.

³⁸ EU's lovramme for produktsikkerhed består af direktivet om produktsikkerhed i almindelighed (direktiv 2001/95/EF) som sikkerhedsnet sammen med en række sektorspecifikke regler for forskellige kategorier af produkter, fra maskiner, fly og biler til legetøj og medicinsk udstyr, der har til formål at sikre et højt sundheds- og sikkerhedsniveau. Produktansvarslovgivningen suppleres af forskellige ordninger for civilretligt ansvar for skader forårsaget af produkter eller tjenester.

³⁹ Direktiv 2000/43/EF.

⁴⁰ Direktiv 2000/78/EF.

⁴¹ Direktiv 2004/113/EF, Direktiv 2006/54/EF.

⁴² F.eks. direktivet om urimelig handelspraksis (direktiv 2005/29/EF) og direktivet om forbrugerrettigheder (direktiv 2011/83/EF).

⁴³ Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger.

tilgængelighedskrav for produkter og tjenester, der er fastsat i den europæiske retsakt om tilgængelighed⁴⁴, finde anvendelse fra 2025. De grundlæggende rettigheder skal desuden respekteres i forbindelse med gennemførelsen af anden EU-lovgivning, herunder inden for finansielle tjenesteydelser, migration eller ansvar hos onlineformidlere.

Selv om EU-lovgivningen i princippet fortsat finder fuld anvendelse, uanset om kunstig intelligens er involveret eller ej, er det vigtigt at vurdere, om den kan håndhæves tilstrækkeligt for at imødegå de risici, som systemer med kunstig intelligens medfører, eller om der er behov for tilpasninger af specifikke retlige instrumenter.

For eksempel er økonomiske aktører fortsat fuldt ansvarlige for, at deres systemer med kunstig intelligens overholder de eksisterende regler om forbrugerbeskyttelse. Enhver form for algoritmisk udnyttelse af forbrugeradfærd i strid med de gældende regler er forbudt og straffes derefter.

Kommissionen er af den opfattelse, at lovrampen kan forbedres med henblik på at tage højde for følgende risici og situationer:

- *Effektiv anvendelse og håndhævelse af eksisterende EU-lovgivning og national lovgivning:* De centrale egenskaber ved kunstig intelligens skaber udfordringer med hensyn til at sikre korrekt anvendelse og håndhævelse af EU-lovgivning og national lovgivning. Den manglende gennemsigtighed (ved uigennemsigtig kunstig intelligens) gør det vanskeligt at konstatere og påvise mulige lovovertrædelser (herunder af retlige bestemmelser, der beskytter de grundlæggende rettigheder), pålægge ansvar og opfylde betingelserne for at kræve erstatning. For at sikre effektiv anvendelse og håndhævelse kan det derfor være nødvendigt at tilpasse eller præcisere eksisterende lovgivning på visse områder, f.eks. om ansvar som nærmere beskrevet i den rapport, der ledsager denne hvidbog.
- *Begrænsninger af anvendelsesområdet for eksisterende EU-lovgivning:* Et væsentligt fokusområde i EU's produktsikkerhedslovgivning er, når produkter bringes i omsætning. Når software indgår i et endeligt produkt, skal det i henhold til EU's produktsikkerhedslovgivning overholde de relevante produktsikkerhedsregler, men det er et åbent spørgsmål, om enkeltstående software uden for visse sektorer med udtrykkelige regler⁴⁵ er omfattet af EU's produktsikkerhedslovgivning. EU's gældende generelle sikkerhedslovgivning finder anvendelse på produkter og ikke på tjenesteydelser og derfor i princippet ikke på tjenester baseret på kunstig intelligens (f.eks. sundhedstjenester, finansielle tjenester, transporttjenester).
- *Funktionsændringer i systemer med kunstig intelligens:* Integration af software, herunder kunstig intelligens, i produkter kan ændre funktionen af sådanne produkter og systemer i løbet af deres livscyklus. Dette gælder især systemer, der kræver hyppige softwareopdateringer, eller som bygger på maskinindlæring. Disse egenskaber kan give anledning til nye risici, som ikke var til stede, da systemet i første omgang blev bragt i omsætning. Disse risici behandles ikke i tilstrækkelig grad i den eksisterende lovgivning, som hovedsagelig fokuserer på de sikkerhedsrisici, der er til stede på det tidspunkt, hvor systemet blev bragt i omsætning.

⁴⁴ Direktiv (EU) 2019/882 om tilgængelighedskrav for produkter og tjenester.

⁴⁵ F.eks. betragtes software, som af fabrikanten er beregnet til medicinske formål, som medicinsk udstyr i henhold til forordningen om medicinsk udstyr (forordning (EU) 2017/745) .

- *Usikkerhed med hensyn til ansvarsfordelingen mellem forskellige økonomiske aktører i forsyningskæden:* I henhold til EU's produktsikkerhedslovgivning er det almindeligvis producenten, der pålægges ansvaret for det produkt, der bringes i omsætning, herunder alle dets komponenter såsom systemer med kunstig intelligens. Men reglerne kan f.eks. blive uklare, hvis der tilføjes kunstig intelligens, efter produktet er blevet bragt i omsætning af en anden part end producenten. Derudover fastsætter EU's produktansvarslovgivning producenternes ansvar og overlader det til de nationale regler om erstatningsansvar at regulere det ansvar, som andre i forsyningskæden har.
- *Ændringer af begrebet sikkerhed:* Anvendelsen af kunstig intelligens i produkter og tjenesteydelser kan give anledning til risici, som EU-lovgivningen på nuværende tidspunkt ikke udtrykkeligt omhandler. Disse risici kan være forbundet med cybertrusler, risici for den personlige sikkerhed (f.eks. i forbindelse med nye anvendelser af kunstig intelligens såsom i husholdningsapparater), risici som følge af manglende forbindelse osv. Disse risici kan forekomme på det tidspunkt, hvor et givent produkt blev bragt i omsætning, eller opstå som følge af softwareopdateringer eller selvoplæring, når produktet anvendes. EU bør gøre fuld brug af sine til rådighed stående redskaber for at øge sit evidensgrundlag for potentielle risici i forbindelse med anvendelser af kunstig intelligens, herunder ved at udnytte erfaringerne fra EU's Agentur for Cybersikkerhed (ENISA) til at vurdere trusselsbilledet vedrørende kunstig intelligens.

Som tidligere nævnt er flere medlemsstater allerede i færd med at undersøge mulighederne for national lovgivning for at imødegå udfordringerne forbundet med kunstig intelligens. Dette øger risikoen for, at det indre marked fragmenteres. Forskelligartede nationale regler vil sandsynligvis skabe hindringer for virksomheder, der ønsker at sælge og anvende systemer med kunstig intelligens i det indre marked. En fælles tilgang på EU-plan vil give europæiske virksomheder uhindret adgang til det indre marked og støtte deres konkurrenceevne på de globale markeder.

Rapport om de konsekvenser, som kunstig intelligens, tingenes internet og robotteknologi vil have for sikkerhed og erstatningsansvar

I rapporten, der ledsager denne hvidbog, analyseres den relevante lovramme. Der konstateres usikkerhed med hensyn til anvendelsen af denne ramme med hensyn til de specifikke risici, der er forbundet med systemer med kunstig intelligens og andre digitale teknologier.

Det konkluderes, at den nuværende produktsikkerhedslovgivning allerede støtter et udvidet sikkerhedsbegreb, der værner mod alle former for risici i forbindelse med produkters anvendelse. Der vil dog kunne indføres bestemmelser, der udtrykkeligt omfatter nye risici i forbindelse med nye digitale teknologier, for at skabe større retssikkerhed.

- Visse systemer med kunstig intelligens kan i løbet af deres livscyklus udvise autonom adfærd, der kan medføre vigtige produktændringer med indvirkning på sikkerheden, hvilket kan kræve en ny risikovurdering. Desuden kan det være nødvendigt med en sikkerhedsforanstaltning i form af menneskeligt tilsyn med produkter og systemer med kunstig intelligens lige fra produktets udformning og frem gennem hele dets livscyklus.
- Producenternes udtrykkelige forpligtelser kan også overvejes i forbindelse med mentale sikkerhedsrisici for brugere, når dette er hensigtsmæssigt (f.eks. samarbejde med menneskelignende robotter).
- EU's produktsikkerhedslovgivning kan udvides til at omfatte specifikke krav, der har til formål at håndtere de sikkerhedsrisici, som følger af mangelfulde data i udformningsfasen, samt mekanismer til at sikre, at datakvaliteten opretholdes i hele det tidsrum, hvor produkter og systemer med kunstig intelligens anvendes.
- Ugennemsigtigheden af systemer, der er baseret på algoritmer, kan afhjælpes med krav om gennemsigtighed.
- Eksisterende regler kan eventuelt tilpasses og præciseres i tilfælde, der påvirker sikkerheden i forbindelse med enkeltstående software, der bringes i omsætning, eller software, der downloades til et produkt, efter at dette er bragt i omsætning.
- I betragtning af forsyningskædernes stigende kompleksitet, for så vidt angår nye teknologier, kan retssikkerheden øges via bestemmelser, der specifikt omhandler samarbejde mellem forsyningskædens økonomiske aktører og brugere.

Egenskaberne ved nye digitale teknologier såsom kunstig intelligens, tingenes internet og robotteknologi kan skabe udfordringer for forskellige aspekter af rammerne for erstatningsansvar og har potentialet til at mindske deres effektivitet. Nogle af disse egenskaber kan gøre det svært at koble skaden til en person, hvilket er påkrævet med henblik på culpa-baserede krav i henhold til de fleste nationale lovgivninger. Dette kan øge skadelidtes omkostninger betydeligt og medføre, at erstatningskrav mod andre end producenter kan være vanskelige at fremføre eller bevise.

- Personer, der har lidt skade som følge af inddragelsen af systemer med kunstig intelligens, skal have samme beskyttelsesniveau som personer, der har lidt skade som følge af andre teknologier, mens den teknologiske innovation fortsat bør have mulighed for at udvikle sig.
- Samtlige muligheder for at nå dette mål bør vurderes nøje, herunder mulige ændringer af produktansvarsdirektivet og eventuel yderligere målrettet harmonisering af nationale regler om erstatningsansvar. Kommissionen er f.eks. interesseret i synspunkter angående hvor vidt og i hvilket omfang det kan blive nødvendigt at afbøde konsekvenserne af kompleksitet ved at tilpasse den bevisbyrde, der kræves i henhold til nationale regler om erstatningsansvar i forbindelse med skader forårsaget af anvendelse af kunstig intelligens.

På grundlag af ovenstående overvejelser konkluderer Kommissionen, at der ud over eventuelle tilpasninger af eksisterende lovgivning kan være behov for en ny lovgivning, der specifikt vedrører kunstig intelligens, for at tilpasse EU's lovramme til den aktuelle og forventede teknologiske og kommercielle udvikling.

C. ANVENDELSESOMRÅDE FOR EN FREMTIDIG EU-LOVGIVNINGSRAMME

Et centralt spørgsmål i forbindelse med den fremtidige specifikke lovramme for kunstig intelligens er at fastlægge anvendelsesområdet. Det er en arbejdshypotese, at lovrammen vil gælde for produkter og tjenester, der er afhængige af kunstig intelligens. Kunstig intelligens bør derfor defineres klart i denne hvidbog og i ethvert fremtidigt initiativ med henblik på fastsættelse af politikken på området.

Kommissionen gav i sin meddelelse om kunstig intelligens for Europa en første definition af kunstig intelligens⁴⁶. Denne definition blev yderligere præciseret af ekspertgruppen på højt niveau⁴⁷.

I ethvert nyt retligt instrument skal definitionen af kunstig intelligens være tilstrækkelig fleksibel til, at den kan tage hensyn til den tekniske udvikling, samtidig med at den er tilstrækkelig præcis til at tilvejebringe den nødvendige retssikkerhed.

I forbindelse med denne hvidbog og eventuelle fremtidige drøftelser vedrørende politiktiltag synes det vigtigt at skabe klarhed om hovedbestanddelene i kunstig intelligens, som er "data" og "algoritmer". Kunstig intelligens kan integreres i hardware.

Hvad angår maskinlæringsteknikker, som er en form for kunstig intelligens, oplæres algoritmer til at udlede visse mønstre på grundlag af et datasæt med henblik på at fastlægge, hvilke handlinger der kræves for at nå et bestemt mål. Algoritmer kan fortsætte med at lære, når de anvendes. Mens produkter baseret på kunstig intelligens kan handle selvstændigt ved at observere deres miljø og uden at følge et på forhånd fastlagt sæt instrukser, defineres og begrænses deres adfærd i vid udstrækning af produktudviklerne. Mennesker fastlægger og programmerer de mål, som et system baseret på kunstig intelligens bør optimeres til at nå.

Ved autonom kørsel f.eks. anvender algoritmen i realtid dataene fra bilen (hastighed, motorforbrug, støddæmpere osv.) og fra sensorerne, der scanner alle bilens omgivelser (vej, skilte, andre køretøjer, fodgængere osv.), for deraf at udlede, hvilken retning, acceleration og hastighed bilen skal have for at nå en bestemt destination. På grundlag af de observerede data tilpasser algoritmen sig til køreforholdene og de omkringliggende forhold, herunder andre chaufførers adfærd, med henblik på deraf at udlede den mest komfortable og sikre kørsel.

EU har indført en streng retlig ramme, der bl.a. skal sikre forbrugerbeskyttelse, bekæmpe urimelig handelspraksis og beskytte personoplysninger og privatlivets fred. Desuden indeholder EU-retten særlige regler for visse sektorer (f.eks. sundhedspleje og transport). Disse eksisterende bestemmelser i EU-retten vil fortsat gælde for kunstig intelligens, selv om visse ajourføringer af denne ramme kan

⁴⁶ COM(2018) 237 final, s. 1: "Med kunstig intelligens menes der systemer, der udviser intelligent adfærd ved at analysere omgivelserne og handle — med en vis grad af autonomi — for at opnå specifikke mål.

AI-systemer kan være rent softwarebaserede og agere i den virtuelle verden (f.eks. taleassistenter, billedanalyseprogrammer, søgemaskiner, tale- og ansigtsgenkendelsessystemer), eller AI kan indlejres i hardwareudstyr (f.eks. avancerede robotter, autonome biler, droner eller applikationer til tingenes internet)".

⁴⁷ Ekspertgruppen på højt niveau, En definition af AI, s. 8: "AI-systemer er softwaresystemer (og evt. også hardwaresystemer), der er designet af mennesker, som ud fra et komplekst mål fungerer i den fysiske eller digitale dimension, hvor de opfatter deres miljø ved at indhente data, fortolker de indsamlede strukturerede eller ustrukturerede data, ræsonnerer ud fra forholdene eller behandler de oplysninger, der er udledt af disse data, og vælger den handling, der bedst kan opfylde det angivne mål. AI-systemer kan enten bruge symbolske regler eller lære en numerisk model, og de kan tilpasse deres adfærd ved at analysere, hvordan miljøet blev påvirket af deres tidligere handlinger."

være nødvendige for at tage hensyn til den digitale omstilling og anvendelsen af kunstig intelligens (se afsnit B). Som følge heraf vil aspekter, der allerede er omfattet af eksisterende horisontal eller sektorspecifik lovgivning (f.eks. om medicinsk udstyr⁴⁸ og transportsystemer), fortsat være omfattet af denne lovgivning.

Principielt bør den nye lovramme for kunstig intelligens effektivt kunne nå sine mål uden at være alt for præskriptiv, så den kan medføre en uforholdsmæssig stor byrde, især for SMV'er. For at nå den rette balance er Kommissionen af den opfattelse, at den bør følge en risikobaseret tilgang.

En risikobaseret tilgang er vigtig for at sikre, at reguleringen står i et rimeligt forhold til målet. Det forudsætter imidlertid klare kriterier at skelne mellem de forskellige anvendelser af kunstig intelligens, navnlig med hensyn til spørgsmålet om, hvorvidt de indebærer "høj risiko"⁴⁹. Fastlæggelsen af, hvornår en anvendelse indebærer høj risiko, bør være tydelig og let forståelig og kunne anvendes af alle berørte parter. Selv hvis en anvendelse af kunstig intelligens ikke karakteriseres som indebærende høj risiko, er den ikke desto mindre fuldt ud underlagt gældende EU-regler.

Kommissionen er af den opfattelse, at vurderingen af, om en given anvendelse af kunstig intelligens bør betragtes som indebærende høj risiko, afhænger af, hvad der er på spil, under hensyntagen til om både sektoren og den tiltænkte anvendelse indebærer betydelige risici, navnlig med hensyn til beskyttelse af sikkerhed, forbrugerrettigheder og grundlæggende rettigheder. Mere specifikt bør en anvendelse af kunstig intelligens betragtes som indebærende en høj risiko, hvis den opfylder følgende to kumulative kriterier:

- For det første at anvendelsen af kunstig intelligens finder sted i en sektor, hvor der på grund af de typiske aktiviteter karakteristika kan forventes betydelige risici. Dette første kriterium sikrer, at reguleringsindsatsen målrettes de områder, hvor risici generelt betragtes som havende størst sandsynlighed for at opstå. De omfattede sektorer bør være specifikt og udtømmende opført i den nye lovramme. F.eks. sundhedspleje, transport, energi og dele af den offentlige sektor⁵⁰. Listen bør revideres regelmæssigt og ændres, hvor det er nødvendigt, afhængigt af den relevante udvikling i praksis.
- For det andet at anvendelsen af kunstig intelligens i den pågældende sektor desuden finder sted på en sådan måde, at der sandsynligvis vil opstå betydelige risici. Dette andet kriterium afspejler en erkendelse af, at det ikke er enhver anvendelse af kunstig intelligens i de udvalgte sektorer, der nødvendigvis indebærer betydelige risici. Selv om sundhedspleje generelt godt kan være en relevant sektor, vil en fejl i tidsbestillingssystemet på et hospital normalt ikke indebære risici af en sådan betydning, at et lovgivningsmæssigt indgreb er berettiget. Vurderingen af risikoniveauet for en given anvendelse kan baseres på konsekvenserne for de berørte parter. F.eks. anvendelser af kunstig intelligens, der medfører juridiske eller tilsvarende væsentlige virkninger for en persons eller et selskabs rettigheder, der udgør en risiko for personskade, død eller væsentlig materiel eller immateriel skade, eller som har virkninger, der ikke med rimelighed kan undgås af fysiske eller juridiske personer.

⁴⁸ F.eks. er der forskellige overvejelser om sikkerhed og retlige konsekvenser vedrørende systemer baseret på kunstig intelligens, der benyttes til indsamling af specialiserede sundhedsoplysninger til læger, ligesom der er systemer, der benyttes til indsamling af sundhedsoplysninger direkte til patienten, eller som selv udfører lægelige opgaver direkte på patienter. Kommissionen er i færd med at undersøge disse udfordringer vedrørende sikkerhed og ansvar, som er særlige for sundhedsområdet.

⁴⁹ I EU-lovgivningen kan "risici" være kategoriseret på en anden måde end den her beskrevne, alt efter hvilket område der er tale om, f.eks. produktsikkerhed.

⁵⁰ Den offentlige sektor kan omfatte områder som asyl, migration, grænsekontrol og retsvæsen, social sikring og arbejdsformidling.

Anvendelsen af de to kumulative kriterier vil sikre, at anvendelsesområdet for lovrammerne er målrettet og giver retssikkerhed. De obligatoriske krav i de nye rammebestemmelser for kunstig intelligens (se afsnit D) vil i princippet kun gælde for de anvendelser, der er identificeret som indebærende høj risiko, i overensstemmelse med disse to kumulative kriterier.

Uanset ovenstående kan der også være helt særlige tilfælde, hvor anvendelsen af kunstig intelligens til visse formål på grund af de risici, der er tale om, i sig selv skal betragtes som indebærende høj risiko — dvs., uanset hvilken sektor der er tale om, og hvor nedenstående krav stadig vil være gældende⁵¹. Som eksempel kan navnlig nævnes følgende:

- I betragtning af dens betydning for enkeltpersoner og gældende EU-ret vedrørende ligestilling på beskæftigelsesområdet vil brugen af kunstig intelligens i forbindelse med ansættelsesprocedurer og i situationer, der påvirker arbejdstagernes rettigheder, altid blive betragtet som indebærende høj risiko, og derfor vil nedenstående krav til enhver tid finde anvendelse. Yderligere specifikke anvendelser, der påvirker forbrugernes rettigheder, kan overvejes.
- Anvendelser af kunstig intelligens til biometrisk fjernidentificering⁵² og andre indgribende overvågningsteknologier vil altid blive betragtet som indebærende "høj risiko", og derfor vil nedenstående krav altid gælde.

D. TYPER AF KRAV

Ved udformningen af den fremtidige lovramme for kunstig intelligens vil det være nødvendigt at træffe afgørelse om, hvilke typer obligatoriske lovkrav der skal pålægges de relevante aktører. Disse krav kan præciseres nærmere ved hjælp af standarder. Som anført i afsnit C og ud over allerede eksisterende lovgivning vil disse krav kun finde anvendelse på anvendelser af kunstig intelligens indebærende høj risiko, og således sikres det, at regulerende indgreb er målrettede og står i et rimeligt forhold til målet.

Under hensyntagen til retningslinjerne fra ekspertgruppen på højt plan, og hvad der er blevet redegjort for i det foregående, kan kravene til anvendelser af kunstig intelligens indebærende høj risiko bestå af følgende centrale elementer, som behandles nærmere i nedenstående underafsnit:

- oplæringsdata
- data og registrering
- oplysninger, der skal udleveres
- robusthed og nøjagtighed
- menneskeligt tilsyn
- specifikke krav til visse særlige anvendelser af kunstig intelligens, såsom dem, der bruges til biometrisk fjernidentificering.

⁵¹ Det er vigtigt at understrege, at andre EU-retsakter også kan finde anvendelse. Når en anvendelse af kunstig intelligens f.eks. indgår i et forbrugerprodukt, kan direktivet om produktsikkerhed finde anvendelse på denne anvendelses sikkerhed.

⁵² Der bør skelnes mellem biometrisk fjernidentificering og biometrisk autentificering (sidstnævnte er en sikkerhedsproces, der med udgangspunkt i en persons unikke biologiske karakteristika benyttes til at kontrollere, at vedkommende er den, vedkommende siger at være). Biometrisk fjernidentificering består i at flere personer på afstand identificeres ved hjælp af biometriske identifikatorer (fingeraftryk, ansigtsbillede, iris, åremønstre osv.), i et offentligt rum og kontinuerligt eller løbende ved at sammenligne de indsamlede data med data lagret i en database.

For at sikre retssikkerheden vil disse krav blive yderligere præciseret, så de er klare for alle de aktører, der skal leve op til dem.

a) Oplæringsdata

Det er vigtigere end nogensinde at fremme, styrke og forsvare EU's værdier og regler og navnlig de rettigheder, som borgerne har i henhold til EU-retten. Disse bestræbelser omfatter utvivlsomt også de anvendelser af kunstig intelligens, der indebærer høj risiko, som markedsføres og anvendes i EU, og som er omhandlet i dette dokument.

Som fremhævet ovenfor er der ingen kunstig intelligens uden data. Funktionsmåden for mange systemer, der bygger på kunstig intelligens, og de handlinger og beslutninger, som de kan medføre, afhænger i høj grad af de datasæt, som systemerne er blevet oplært ved hjælp af. Der bør derfor træffes de nødvendige foranstaltninger for at sikre, at de data, der anvendes til at oplære systemer, der bygger på kunstig intelligens, lever op til og overholder EU's værdier og regler, navnlig med hensyn til sikkerhed og eksisterende lovgivningsmæssige bestemmelser om beskyttelse af grundlæggende rettigheder. Man kunne forestille sig følgende krav til de datasæt, der anvendes til oplæring af systemer, der bygger på kunstig intelligens:

- Krav, der har til formål at give rimelig sikkerhed for, at den efterfølgende anvendelse af de produkter eller tjenester, som systemet, der bygger på kunstig intelligens, muliggør, er sikker, idet den lever op til de standarder, der er fastsat i de gældende EU-regler om sikkerhed (eksisterende og eventuelle supplerende regler). F.eks. krav, der sikrer, at systemer, der bygger på kunstig intelligens, er oplært ved brug af datasæt, der er tilstrækkeligt favnende og omfatter alle relevante scenarier, der er nødvendige for at undgå farlige situationer.
- Krav om at træffe rimelige foranstaltninger med henblik på at sikre, at en sådan efterfølgende anvendelse af systemer, der bygger på kunstig intelligens, ikke medfører forbudt forskelsbehandling. Disse krav kan navnlig medføre forpligtelser til at anvende datasæt, der er tilstrækkeligt repræsentative, navnlig til at sikre, at alle relevante aspekter af køn, etnisk oprindelse og andre mulige grunde til forbudt forskelsbehandling afspejles på passende vis i disse datasæt.
- Krav, der har til formål at sikre, at privatlivets fred og personoplysninger beskyttes på passende vis under brugen af produkter og tjenester, der kan benytte kunstig intelligens. Forhold, der falder ind under anvendelsesområdet for henholdsvis den generelle forordning om databeskyttelse og retshåndhævelsesdirektivet, reguleres efter disse.

b) Registrering og data

Grundet bl.a. kompleksiteten og uigennemsigtheden af mange systemer, der bygger på kunstig intelligens, og de dertil knyttede problemer, der kan være med effektivt at kontrollere overholdelsen og håndhævelsen af gældende regler, er der behov for krav vedrørende registrering i forbindelse med programmeringen af algoritmen, de data, der anvendes til at oplære systemer, der bygger på kunstig intelligens, og som indebærer høj risiko, og i visse tilfælde selve opbevaringen af data. Disse krav gør det samlet set muligt at spore og kontrollere potentielt problematiske tiltag eller beslutninger foretaget af systemer, der bygger på kunstig intelligens. Dette bør ikke kun lette tilsyn og håndhævelse; det kan også øge incitamentet for de berørte økonomiske aktører til på et tidligt tidspunkt at tage hensyn til behovet for at overholde disse regler.

Med henblik herpå kunne lovrammen indeholde bestemmelser om, at følgende skal bevares:

- nøjagtige optegnelser om de datasæt, der anvendes til at oplære og teste systemer, der bygger på kunstig intelligens, herunder en beskrivelse af de væsentlige karakteristika og af, hvordan datasættet er udvalgt
- i visse begrundede tilfælde selve datasættene
- Dokumentation for programmerings⁵³- og uddannelsesmetoder, processer og teknikker, der anvendes til at opbygge, teste og validere systemerne, der bygger på kunstig intelligens, herunder i givet fald for så vidt angår sikkerhed og undgåelse af forudindtaget, der kan medføre forbudt forskelsbehandling.

Optegnelserne, dokumentationen og, hvor det er relevant, datasættene skal opbevares i et begrænset, rimeligt tidsrum for at sikre effektiv håndhævelse af den relevante lovgivning. Der bør træffes foranstaltninger for at sikre, at de stilles til rådighed efter anmodning, navnlig med henblik på test eller inspektion foretaget af de kompetente myndigheder. Om nødvendigt bør der træffes foranstaltninger til at sikre, at fortrolige oplysninger såsom forretningshemmeligheder beskyttes.

c) Udlevering af oplysninger

Der kræves gennemsigtighed, også ud over de registreringskrav, der behandles i punkt c) ovenfor. For at nå de efterstræbte mål – navnlig fremme af en ansvarlig anvendelse af kunstig intelligens, tillidsopbygning og lettet klageadgang, hvor det er nødvendigt – er det vigtigt, at der på en proaktiv måde gives fyldestgørende oplysninger om brugen af systemer, der bygger på kunstig intelligens, som indebærer høj risiko.

Derfor kunne følgende krav overvejes:

- Sikre klare oplysninger om systemet, der bygger på kunstig intelligens, hvad angår dets muligheder og begrænsninger, navnlig det formål, som det er beregnet til, de betingelser, under hvilke de kan forventes at fungere efter hensigten, og den forventede nøjagtighed med hensyn til det angivne formål. Disse oplysninger er især vigtige for dem, der udbreder systemerne, men kan også være relevante for kompetente myndigheder og berørte parter.
- Borgerne bør særskilt informeres tydeligt, når de interagerer med et system, der bygger på kunstig intelligens, og ikke et menneske. Selv om EU's databeskyttelseslovgivning allerede indeholder visse regler af denne art⁵⁴, kan der være behov for yderligere krav for at nå ovennævnte mål. Unødvendige byrder bør i så fald undgås. Derfor er det f.eks. ikke nødvendigt at give sådanne oplysninger i situationer, hvor det umiddelbart er indlysende for borgerne, at de interagerer med systemer, der bygger på kunstig intelligens. Det er desuden vigtigt, at oplysningerne er objektive, kortfattede og let forståelige. Den måde, hvorpå oplysningerne skal gives, bør tilpasses den specifikke situation.

d) Robusthed og nøjagtighed

Systemer, der bygger på kunstig intelligens, skal være teknisk robuste og nøjagtige for at være pålidelige, og dette gælder afgjort anvendelser af kunstig intelligens indebærende høj risiko. Det

⁵³ F.eks. dokumentation vedrørende algoritmen, herunder om modellens optimeringsmål, hvilke vægte der som udgangspunkt er udformet til visse parametre osv.

⁵⁴ De dataansvarlige skal i medfør af artikel 13, stk. 2, litra f), i GDPR på det tidspunkt, hvor personoplysningerne indhentes, give de registrerede yderligere oplysninger, der er nødvendige for at sikre en retfærdig og gennemsigtig behandling, om eventuel automatiseret beslutningstagning og visse yderligere oplysninger.

betyder, at sådanne systemer skal udvikles på en ansvarlig måde og under forudgående behørig hensyntagen til de risici, de kan medføre. Deres udvikling og funktion skal være af en sådan art, at der er sikkerhed for, at systemer, der bygger på kunstig intelligens, fungerer pålideligt efter hensigten. Der bør træffes alle rimelige foranstaltninger for at minimere risikoen for, at der forvoldes skade.

Derfor kunne følgende forhold overvejes:

- Krav, der sikrer, at systemer, der bygger på kunstig intelligens, er robuste og nøjagtige eller i det mindste korrekt viser deres nøjagtighedsgrad i alle faser af livscyklusen
- Krav, der sikrer, at resultaterne er reproducerbare
- Krav, der sikrer, at systemer, der bygger på kunstig intelligens, på passende vis kan håndtere fejl eller uoverensstemmelser i alle faser af livscyklusen.
- Krav, der sikrer, at systemer, der bygger på kunstig intelligens, er modstandsdygtige over for både åbenlyse angreb og mere subtile forsøg på at manipulere de enkelte data eller algoritmer, og at der træffes afhjælpende foranstaltninger i sådanne tilfælde.

e) Menneskeligt tilsyn

Menneskeligt tilsyn hjælper med at sikre, at et system, der bygger på kunstig intelligens, ikke undergraver menneskers autonomi eller har andre negative virkninger. Målet om pålidelig, etisk og menneskecentreret kunstig intelligens kan kun nås ved at sikre en passende inddragelse af mennesker i forbindelse med anvendelser af kunstig intelligens indebærende høj risiko.

Selv om alle de anvendelser af kunstig intelligens, der omhandles i denne hvidbog med henblik på en særlig retlig ordning, anses for at indebære høj risiko, kan den passende type og grad af menneskeligt tilsyn variere fra sag til sag. Den afhænger navnlig af den påtænkte anvendelse af systemerne og af de virkninger, som anvendelsen kan have for berørte borgere og juridiske enheder. Den berører heller ikke de juridiske rettigheder, der er fastsat i GDPR, når systemet, der bygger på kunstig intelligens, behandler personoplysninger. F.eks. kan menneskeligt tilsyn foregå på følgende ikke-udtømmende måder:

- De resultater, som systemet, der bygger på kunstig intelligens, genererer, bruges ikke, medmindre de forudgående er blevet gennemset og valideret af et menneske (f.eks. kan en beslutning om afslag på en ansøgning om social sikring kun træffes af et menneske)
- De resultater, som systemet, der bygger på kunstig intelligens, genererer, bruges umiddelbart, men der sikres efterfølgende menneskelig indgriben (f.eks. kan et system, der bygger på kunstig intelligens, generere et afslag på en ansøgning om et kreditkort, men det skal være muligt, at et menneske efterfølgende gennemgår beslutningen)
- Overvågning af systemet, der bygger på kunstig intelligens, mens det er i drift, og evnen til at gribe ind i realtid og deaktivere (f.eks. findes der en stopknap eller -procedure i en førerløs bil, når et menneske afgør, at bilens kørsel ikke er sikker)
- I designfasen ved at indføre operationelle begrænsninger for systemet, der bygger på kunstig intelligens (f.eks. skal en førerløs bil standse under visse forhold med lav sigtbarhed, når

sensorerne være mindre pålidelige, eller til enhver tid opretholde en vis afstand fra det foran kørende køretøj).

f) Særlige krav vedrørende biometrisk fjernidentificering

Indsamling og brug af biometriske data⁵⁵ til biometrisk fjernidentificering⁵⁶, f.eks. gennem udbredelse af ansigtsgenkendelse i det offentlige rum, medfører særlige risici, hvad angår grundlæggende rettigheder⁵⁷. Konsekvenserne for fundamentale rettigheder af at bruge systemer til biometrisk fjernidentificering, der bygger på kunstig intelligens, kan variere betydeligt afhængigt af formålet, konteksten og brugens omfang.

EU's databeskyttelsesregler indeholder i princippet forbud mod behandling af biometriske data med det formål entydigt at identificere en fysisk person, undtagen på særlige betingelser⁵⁸. Nærmere bestemt kan en sådan behandling i henhold til GDPR kun finde sted med henvisning til et begrænset antal grunde, hvoraf den vigtigste er hensynet til væsentlige samfundsinteresser. Foreligger en sådan situation, skal behandlingen finde sted på grundlag af EU-retten eller national ret, under forbehold af kravene om proportionalitet, respekt for det væsentligste indhold af retten til databeskyttelse og passende sikkerhedsforanstaltninger. Efter retshåndhævelsesdirektivet skal der være forhold, der gør det strengt nødvendigt med en sådan behandling, i princippet en tilladelse i henhold til EU-retten eller national ret samt passende sikkerhedsforanstaltninger. Da behandling af biometriske data med det formål entydigt at identificere en fysisk person falder ind under en undtagelse fra et forbud i EU-retten, er den omfattet af EU's charter om grundlæggende rettigheder.

Det følger heraf, at kunstig intelligens i overensstemmelse med EU's nuværende databeskyttelsesregler og chartret om grundlæggende rettigheder kun kan anvendes til biometrisk fjernidentificering, hvis en sådan anvendelse er behørigt begrundet, står i et rimeligt forhold til formålet og er omfattet af passende sikkerhedsforanstaltninger.

For at imødegå eventuelle samfundsmæssige betænkeligheder i forbindelse med anvendelsen af kunstig intelligens til sådanne formål på offentlige steder og for at undgå fragmentering af det indre marked vil Kommissionen lancere en bred europæisk debat om eventuelle særlige omstændigheder, der kan berettige en sådan anvendelse, og om fælles sikkerhedsforanstaltninger.

⁵⁵ Biometriske data defineres som "personoplysninger, der som følge af specifik teknisk behandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika muliggør eller bekræfter en entydig identifikation af vedkommende, f.eks. ansigtsbillede eller fingeraftryksoplysninger."

(Retshåndhævelsesdirektivet, artikel 3, stk. 13, GDPR, artikel 4, stk. 14, forordning (EU) 2018/1725, artikel 3, stk. 18).

⁵⁶ I forbindelse med ansigtsgenkendelse forstås der ved identificering, at skabelonen for en persons ansigtsbillede sammenlignes med mange andre skabeloner, der er lagret i en database, for at finde ud af, om vedkommendes billede er lagret dér. Autentificering (eller verifikation) omtales derimod ofte som én-til-én-matchning. Den gør det muligt at sammenligne to biometriske skabeloner, der normalt antages at høre til samme person. Der foretages en sammenligning af to biometriske skabeloner for at fastslå, om den person, der vises på de to billeder, er den samme person. En sådan fremgangsmåde benyttes f.eks. ved automatiserede grænsekontrolposter til grænsekontrol i lufthavne.

⁵⁷ F.eks. med hensyn til menneskers værdighed. Tilsvarende står retten til respekt for privatliv og beskyttelse af personoplysninger centralt i bekymringerne for de grundlæggende rettigheder i forbindelse med ansigtsgenkendelsesteknologi. Ikke-diskrimination og rettighederne for særlige grupper, såsom børn, ældre og personer med handicap, kan potentielt også blive påvirket. Desuden må yrings-, forenings- og forsamlingsfriheden ikke undermineres af brugen af teknologi. Se Facial recognition technology: fundamental rights considerations in the context of law enforcement (Ansigtsgenkendelsesteknologi: fundamentale rettigheder i retshåndhævelsessammenhæng),

<https://fra.europa.eu/en/publication/2019/facial-recognition>.

⁵⁸ Artikel 9 i GDPR, artikel 10 i retshåndhævelsesdirektivet. Se også artikel 10 i forordning (EU) 2018/1725 (gælder for EU's institutioner og organer).

E. HVEM ER OMFATTET?

Med hensyn til de aktører, der vil være omfattet af de retlige krav, der skal gælde i forbindelse med de ovennævnte anvendelser af kunstig intelligens, der indebærer høj risiko, er der to vigtige spørgsmål, der skal behandles.

For det første er der spørgsmålet om, hvordan forpligtelserne skal fordeles mellem de berørte økonomiske aktører. Der er mange aktører involveret i et livscyklus for et system, der bygger på kunstig intelligens. Disse omfatter udvikleren, udbrederen (den person, der bruger et produkt eller en tjenesteydelse, der er udstyret med kunstig intelligens) og potentielt andre (producent, distributør eller importør, tjenesteyder, professionel eller privat bruger).

Kommissionen er af den holdning, at hver forpligtelse i en fremtidig lovramme bør pålægges den eller de aktører, der er bedst i stand til at imødegå potentielle risici. F.eks. kan udviklere af kunstig intelligens være bedst placeret til at håndtere risici i udviklingsfasen, men deres evne til at kontrollere risici i brugsfasen kan være mere begrænset. I så fald bør udbrederen være omfattet af den relevante forpligtelse. Dette berører ikke spørgsmålet om, hvad enten det angår ansvar over for slutbrugere eller andre parter, der lider skade, og for at sikre effektiv adgang til domstolene, hvilken part der skal være ansvarlig for eventuelle skader. I henhold til EU's bestemmelser om produktansvar gives producenten ansvar for defekte produkter, med mindre andet er fastsat i nationale love, som også kan give mulighed for inddrivelse hos andre parter.

For det andet er der spørgsmålet om det geografiske anvendelsesområde af den lovgivningsmæssige indgriben. Efter Kommissionens opfattelse er det af afgørende betydning, at kravene finder anvendelse på alle relevante økonomiske aktører, der leverer produkter eller tjenesteydelser, som kan benytte kunstig intelligens, i EU, uanset om de er etableret i EU eller ej. Ellers kan målene med den tidligere nævnte lovgivningsmæssige indgriben ikke opfyldes fuldt ud.

F. OVERHOLDELSE OG HÅNDHÆVELSE

For at sikre, at kunstig intelligens er pålidelig, sikker og i overensstemmelse med europæiske værdier og regler, skal de gældende lovkrav overholdes i praksis og håndhæves effektivt af både de kompetente nationale og europæiske myndigheder og de berørte parter. De kompetente myndigheder bør være i stand til at undersøge individuelle sager, men også til at vurdere indvirkningen på samfundet.

I betragtning af den høje risiko, som visse anvendelser af kunstig intelligens indebærer for borgerne og vores samfund (se afsnit A), finder Kommissionen på nuværende tidspunkt, at det er nødvendigt at foretage en objektiv, forudgående overensstemmelsesvurdering for at kontrollere og sikre, at visse af de ovennævnte obligatoriske krav til anvendelser, der indebærer høj risiko (se afsnit D), overholdes. Den forudgående overensstemmelsesvurdering kunne omfatte procedurer for testning, inspektion eller certificering⁵⁹. Den kunne omfatte kontrol af algoritmerne og af de datasæt, der anvendes i udviklingsfasen.

Overensstemmelsesvurderinger for anvendelser af kunstig intelligens, der indebærer høj risiko, bør indgå i de overensstemmelsesvurderingsmekanismer, der allerede findes for et stort antal produkter, der bringes i omsætning på EU's indre marked. Hvis ingen sådanne eksisterende mekanismer kan

⁵⁹ Systemet ville skulle baseres på overensstemmelsesvurderingsprocedurer i EU, se afgørelse 768/2008/EF eller forordning (EU) 2019/881 (forordningen om cybersikkerhed) under hensyntagen til de særlige forhold, der gør sig gældende for kunstig intelligens. Se den blå vejledning om gennemførelsen af EU's produktregler fra 2014.

benyttes, kan det være nødvendigt at indføre lignende mekanismer på grundlag af bedste praksis og eventuelle bidrag fra interessenter og europæiske standardiseringsorganisationer. En sådan ny mekanisme bør stå i et rimeligt forhold til målet og være ikke-diskriminerende og gøre brug af gennemsigtige og objektive kriterier i overensstemmelse med internationale forpligtelser.

Ved udformningen og gennemførelsen af et system, der bygger på forudgående overensstemmelsesvurdering, bør der navnlig tages hensyn til følgende:

- Alle de krav, der er beskrevet ovenfor, er ikke nødvendigvis egnede til verificering ved en forudgående overensstemmelsesvurdering. F.eks. er kravet om, at oplysninger skal stilles til rådighed, generelt ikke godt egnet til verificering ved en sådan vurdering.
- Der bør tages særligt hensyn til muligheden for, at visse systemer, der bygger på kunstig intelligens, udvikler sig og lærer af erfaringer, hvilket kan medføre, at det er nødvendigt at gentage vurderingen i de pågældende systemers levetid.
- Behovet for at kontrollere de data, der anvendes til oplæring, og de relevante programmerings- og oplæringsmetoder, processer og teknikker, der anvendes til at opbygge, teste og validere systemer, der bygger på kunstig intelligens.
- Hvis overensstemmelsesvurderingen viser, at et system, der bygger på kunstig intelligens, ikke opfylder kravene til f.eks. de data, der anvendes til at oplære det, skal de konstaterede mangler afhjælpes, f.eks. ved at genoplære systemet i EU på en sådan måde, at det sikres, at alle gældende krav opfyldes.

Overensstemmelsesvurderingerne vil være obligatoriske for alle økonomiske aktører, der er omfattet af kravene, uanset hvor de er etableret⁶⁰. For at begrænse byrden for SMV'er kan det overvejes at etablere en støttestruktur, herunder gennem digitale innovationsknudepunkter. Desuden kan standarder og særlige onlineværktøjer fremme overholdelsen.

Enhver forudgående overensstemmelsesvurdering bør ikke berøre de kompetente nationale myndigheders overholdelse af overvågningsforpligtelser og efterfølgende håndhævelse. Dette gælder for anvendelser af kunstig intelligens, der indebærer høj risiko, men også for andre anvendelser af kunstig intelligens, der er underlagt lovkrav, også selv om den høje risiko, som de pågældende anvendelser måtte indebære, kan være årsag for de kompetente nationale myndigheder til i særlig grad at være opmærksomme på de førstnævnte. Det bør være muligt at gennemføre efterfølgende kontrol ved hjælp af passende dokumentation vedrørende den relevante anvendelse af kunstig intelligens (se afsnit E) og, hvor det er relevant, bør det være muligt for tredjeparter såsom kompetente myndigheder at teste sådanne anvendelser. Dette kan især være vigtigt, hvis der opstår risici for grundlæggende rettigheder, som er kontekstafhængige. En sådan overvågning af overholdelsen bør indgå i en kontinuerlig markedsovervågningsordning. Forvaltningsrelaterede aspekter behandles yderligere i afsnit H.

Desuden bør der sikres en effektiv domstolsprøvelse for parter, der påvirkes negativt, både for anvendelser, der indebærer høj risiko, og for andre anvendelser af kunstig intelligens. Spørgsmål vedrørende ansvar drøftes yderligere i rapporten om rammerne for sikkerhed og ansvar, der ledsager denne hvidbog.

⁶⁰ Hvad angår den relevante forvaltningsstruktur, herunder organer til udførelse af overensstemmelsesvurderingerne, se afsnit H.

G. FRIVILLIG MÆRKNING AF ANVENDELSER AF KUNSTIG INTELLIGENS, DER IKKE INDEBÆRER HØJ RISIKO

For anvendelser af kunstig intelligens, der ikke kan betegnes som indebærende høj risiko (se afsnit C), og som derfor ikke er omfattet af de ovenfor omhandlede obligatoriske krav (se afsnit D, E og F), vil en valgmulighed ud over den gældende lovgivning være at indføre en frivillig mærkningsordning.

Under ordningen kunne interesserede økonomiske aktører, der ikke er omfattet af de obligatoriske krav, beslutte på frivillig basis enten at underkaste sig disse krav eller et specifikt sæt af lignende krav, der er fastsat med særligt henblik på den frivillige ordning. De berørte økonomiske operatører ville så blive tildelt et kvalitetsmærke for deres anvendelser, der bygger på kunstig intelligens.

Den frivillige mærkning ville gøre det muligt for de berørte økonomiske aktører at signalere, at deres produkter og tjenester, der kan benytte kunstig intelligens, er pålidelige. En sådan ordning ville gøre det let for brugerne at se, at de pågældende produkter og tjenester er i overensstemmelse med bestemte mål og standardiserede EU-dækkende benchmarks, der går ud over de normalt gældende retlige forpligtelser. Dette ville bidrage til at øge brugernes tillid til AI-systemer og fremme den generelle udbredelse af teknologien.

Til brug for mærkningsordningen ville der skulle skabes et nyt retligt instrument, hvori rammerne for den frivillige mærkning af systemer, der bygger på kunstig intelligens, som ikke indebærer høj risiko, ville skulle fastlægges for systemernes udviklere og/eller udbredere. Mens det ville være frivilligt at deltage i mærkningsordningen, ville kravene være bindende, når udvikleren eller udbrederen først har valgt at anvende mærket. Kombinationen af forudgående og efterfølgende håndhævelse ville skulle sikre, at alle krav overholdes.

H. FORVALTNING

Det er nødvendigt med en europæisk forvaltningsstruktur for kunstig intelligens i form af en ramme for samarbejde mellem nationale kompetente myndigheder for at undgå en opsplnitning af ansvaret, øge kapaciteten i medlemsstaterne og sikre, at Europa giver sig selv den kapacitet, der er nødvendig for at teste og certificere produkter og tjenester, der kan benytte kunstig intelligens. I den forbindelse vil det være nyttigt at støtte de kompetente nationale myndigheder for at sætte dem i stand til at opfylde deres mandat, hvor kunstig intelligens anvendes.

En europæisk forvaltningsstruktur kan have en række forskellige opgaver og fungere som et forum for regelmæssig udveksling af oplysninger og bedste praksis, hvor nye tendenser identificeres, og der gives råd om standardisering og certificering. Den bør også spille en central rolle med hensyn til at lette gennemførelsen af de retlige rammer, f.eks. gennem udformning af retningslinjer, udtalelser og ekspertise. Med henblik herpå bør den bygge på et netværk af nationale myndigheder samt sektornetværk og regulerende myndigheder på nationalt plan og EU-plan. Desuden kunne et ekspertudvalg yde Kommissionen bistand.

Forvaltningsstrukturen bør sikre maksimal deltagelse af interessenter. Interessenter – forbrugerorganisationer og arbejdsmarkedets parter, virksomheder, forskere og civilsamfundsorganisationer – bør høres om rammens gennemførelse og videreudvikling.

Der findes allerede strukturer, f.eks. inden for finansiering, lægemidler, luftfart, medicinsk udstyr, forbrugerbeskyttelse og databeskyttelse, og den foreslåede forvaltningsstruktur bør ikke overlape med eksisterende funktioner. I stedet bør der etableres tætte forbindelser med andre kompetente EU-myndigheder og nationale myndigheder i de forskellige sektorer for at supplere den eksisterende ekspertise og hjælpe eksisterende myndigheder med overvågning og tilsyn med de aktiviteter, der

udføres af økonomiske aktører, og som omfatter systemer, produkter og tjenester, der bygger på kunstig intelligens.

Hvis det besluttes at gå videre med dette, kan det desuden betros bemyndigede organer, der er udpeget af medlemsstaterne, at udføre overensstemmelsesvurderinger. Testcentre bør muliggøre uafhængig revision og vurdering af systemer, der bygger på kunstig intelligens, i overensstemmelse med ovenstående krav. Uafhængig vurdering vil øge tilliden og sikre objektivitet. Relevante kompetente myndigheders arbejde ville også nyde godt heraf.

EU har fremragende test- og vurderingscentre og bør også udvikle sin kapacitet inden for kunstig intelligens. Økonomiske aktører, der er etableret i tredjelande, og som ønsker at komme ind på det indre marked, ville enten kunne gøre brug af udpegede organer, der er etableret i EU, eller, hvis de er omfattet af aftaler om gensidig anerkendelse med tredjelande, benytte tredjelandes organer, der er udpeget til at foretage en sådan vurdering.

Forvaltningsstrukturen vedrørende kunstig intelligens og de her omhandlede mulige overensstemmelsesvurderinger ville ikke berøre de relevante kompetente myndigheders beføjelser og ansvar under eksisterende EU-lovgivning inden for specifikke sektorer eller problemstillinger (finansiering, lægemidler, luftfart, medicinsk udstyr, forbrugerbeskyttelse, databeskyttelse osv.).

6. KONKLUSION

Kunstig intelligens er en strategisk teknologi, der medfører mange fordele for borgere, virksomheder og samfundet som helhed, forudsat at den er menneskecentreret, etisk, bæredygtig og anvendt under overholdelse af og med respekt for de grundlæggende rettigheder og værdier. Kunstig intelligens giver mulighed for store effektivitets- og produktivitetsgevinster, som kan styrke det europæiske erhvervslivs konkurrenceevne og forbedre borgernes velfærd. Kunstig intelligens kan også bidrage til at finde løsninger på nogle af de mest presserende samfundsudfordringer, herunder bekæmpelse af klimaændringer og miljøforringelser, udfordringer i forbindelse med bæredygtighed og demografiske ændringer samt beskyttelse af vores demokratier og, hvor det er nødvendigt og står i et rimeligt forhold til målet, bekæmpelse af kriminalitet.

For fuldt ud at kunne udnytte de muligheder, som kunstig intelligens giver, skal Europa udvikle og styrke den nødvendige industrielle og teknologiske kapacitet. Som det fremgår af den ledsagende europæiske strategi for data, kræver dette også foranstaltninger, der kan give EU mulighed for at blive et globalt dataknudepunkt.

Den europæiske tilgang til kunstig intelligens har til formål at fremme Europas innovationskapacitet inden for kunstig intelligens og samtidig støtte udviklingen og udbredelsen af etisk og pålidelig kunstig intelligens i hele EU's økonomi. Kunstig intelligens bør tjene mennesker og udgøre en positiv kraft i samfundet.

Med denne hvidbog og den ledsagende rapport om rammerne for sikkerhed og ansvar iværksætter Kommissionen en bred høring af medlemsstaternes civilsamfund, erhvervslivet og forskningsmiljø om konkrete forslag til en europæisk tilgang til kunstig intelligens. Disse omfatter både politiske midler til

Kommissionen opfordrer til at fremsætte bemærkninger til forslagene i hvidbogen gennem en åben offentlig høring på https://ec.europa.eu/info/consultations_en. Der kan indgives bemærkninger i forbindelse med høringen frem til den 19. maj 2020.

Det er Kommissionens faste praksis at offentliggøre de bemærkninger, den modtager som led i en offentlig høring. Der er imidlertid mulighed for at anmode om, at bemærkningerne eller dele heraf forbliver fortrolige. Skulle De være interesserede heri, bedes De på forsiden af bemærkningerne klart angive, at de ikke må offentliggøres, og også fremsende en ikke-fortrolig version af Deres bemærkninger til Kommissionen til offentliggørelse.

at sætte skub i investeringer i forskning og innovation, fremme udviklingen af færdigheder og støtte SMV'ers brug af kunstig intelligens samt forslag til centrale elementer i en fremtidig lovramme. Denne høring vil give mulighed for en omfattende dialog med alle berørte parter, som vil danne grundlag for Kommissionens næste skridt.