EUROPA-
KOMMISSIONEN

Bruxelles, den 19.2.2020
COM(2020) 64 final

RAPPORT FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, RÅDET OG DET EUROPÆISKE ØKONOMISKE OG SOCIALE UDVALG

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

RAPPORT OM DE KONSEKVENSER, SOM KUNSTIG INTELLIGENS, TINGENES INTERNET OG ROBOTTEKNOLOGI VIL HAVE FOR SIKKERHED OG ERSTATNINGSANSVAR

1. Indledning

Kunstig intelligens[1], tingenes internet[2] og robotteknologi vil skabe nye muligheder og fordele for vores samfund. Kommissionen har erkendt disse teknologiers betydning og potentiale samt behovet for betydelige investeringer inden for disse områder[3], og er fast besluttet på at sikre Europa en global førerposition inden for kunstig intelligens, tingenes internet og robotteknologi. For at nå dette mål er det nødvendigt at skabe en klar og forudsigelig retlig ramme, der tager hensyn til de teknologiske udfordringer.

1.1. Den eksisterende ramme for sikkerhed og erstatningsansvar

Det overordnede formål med de retlige rammer for sikkerhed og erstatningsansvar er at sikre, at alle produkter og tjenester, herunder dem, der integrerer nye digitale teknologier, fungerer på en sikker, pålidelig og konsekvent måde, og at eventuelle skadevirkninger udbedres på effektiv vis. Høje sikkerhedsniveauer for produkter og systemer, der integrerer nye digitale teknologier, og robuste mekanismer, der udbedrer eventuelle skadevirkninger (dvs. rammen for erstatningsansvar), bidrager til at beskytte forbrugerne bedre. De skaber også tillid til disse teknologier, hvilket er en forudsætning for deres udbredelse i industrien og hos brugerne. Dette vil efterfølgende understøtte industriens konkurrenceevne og bidrage til EU's målsætninger[4]. En klar ramme for sikkerhed og erstatningsansvar er særlig vigtig, når der udvikles nye teknologier som kunstig intelligens, tingenes internet og robotteknologi, både med henblik på at sikre beskyttelse af forbrugerne og retssikkerhed for virksomhederne.

Unionen har en solid og pålidelig lovgivningsmæssig ramme for sikkerhed og erstatningsansvar og et solidt sæt sikkerhedsstandarder, der suppleres af national, ikke-harmoniseret produktansvarslovgivning. Sammen sikrer de, at vores borgere trives i det indre marked, og tilskynder til innovation og teknologisk udbredelse. Imidlertid ændrer kunstig intelligens, tingenes internet og robotteknologi mange produkters og tjenesteydelsers egenskaber.

I Kommissionens meddelelse om kunstig intelligens for Europa[5], der blev vedtaget den 25. april 2018, meddelte Kommissionen, at den ville forelægge en rapport med en vurdering af de nye digitale teknologiers indvirkning på de eksisterende rammer for sikkerhed og erstatningsansvar. Denne rapport har til formål at identificere og undersøge de mere vidtrækkende konsekvenser for og potentielle huller i rammerne for erstatningsansvar og

---

1 Den definition af kunstig intelligens, som Ekspertgruppen på Højt Niveau vedrørende Kunstig Intelligens har udarbejdet, kan findes på https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines

2 Den definition af tingenes internet, som findes i henstilling ITU-T Y.2060, kan findes på https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060.

3 SWD(2016) 110, COM(2017) 9, COM(2018) 237 og COM(2018) 795.

4 http://ec.europa.eu/growth/industry/policy_da

5 https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=COM%3A2018%3A237%3AFIN.
Det tilhørende arbejdsdokument, SWD (2018) 137 (https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137) indeholdt en første kortlægning af de ansvarsrelaterede udfordringer, som opstår på baggrund af nye digitale teknologier.

sikkerhed i forbindelse med kunstig intelligens, tingenes internet og robotteknologi. De retningslinjer, der udstikkes i denne rapport, og som ledsager hvidbogen om kunstig intelligens, udgør et oplæg til diskussion og indgår i en bredere høring af de berørte parter. Afsnittet om sikkerhed bygger på evalueringen[6] af maskindirektivet[7] og arbejdet med de relevante ekspertgrupper[8]. Afsnittet om erstatningsansvar bygger på evalueringen[9] af produktansvarsdirektivet[10], input fra de relevante ekspertgrupper[11] og kontakt med interessenter. Denne rapport har ikke til formål at give et udtømmende overblik over de eksisterende regler for sikkerhed og erstatningsansvar, men fokuserer på de centrale spørgsmål, der er blevet identificeret indtil nu.

1.2. Kendetegn ved teknologier inden for kunstig intelligens, tingenes internet og robotteknologi

Kunstig intelligens, tingenes internet og robotteknologi har mange kendetegn til fælles. De kan kombinere **konnektivitet**, **autonomi** og **dataafhængighed** med henblik på at udføre opgaver med begrænset eller slet ingen menneskelig kontrol eller overvågning. Systemer, der omfatter kunstig intelligens, kan også forbedre deres egne resultater ved at lære af deres erfaringer. Deres **kompleksitet** afspejles både i de mange økonomiske aktører, der er involveret i **forsyningskæden**, og de mange forskellige komponenter, dele, software, systemer eller tjenester, som tilsammen udgør de nye teknologiske økosystemer. Hertil kommer **åbenheden** over for opdateringer og opgraderinger, efter at de er kommet på markedet. De enorme mængder af data, der er involveret, afhængigheden af algoritmer og **uigennemsigtigheden** med hensyn til beslutningstagningen inden for kunstig intelligens gør det vanskeligere at forudsige, hvordan et produkt, der er baseret på kunstig intelligens, vil opføre sig, og forstå de potentielle årsager til en skade. Endelig kan konnektivitet og åbenhed også gøre produkter, der er baseret på kunstig intelligens og tingenes internet, sårbare overfor **cybertrusler**.

1.3. Muligheder som følge af kunstig intelligens, tingenes internet og robotteknologi

At øge brugernes tillid til og sociale accept af nye teknologier, forbedre produkter, processer og forretningsmodeller og hjælpe europæiske fabrikanter til at blive mere effektive er kun nogle af de muligheder, der opstår som følge af kunstig intelligens, tingenes internet og robotteknologi.

---

6 SWD(2018) 161 final.

7 Direktiv 2006/42/EF

8 Forbrugerbeskyttelsesnetværk som fastsat i direktiv 2001/95/EF om produktsikkerhed i almindelighed, direktiv 2006/42/EF om maskiner og direktiv 2014/53/EU om radioudstyr, ekspertgrupper bestående af medlemsstaterne, erhvervslivet og andre interessenter såsom forbrugerorganisationer.

9 COM(2018) 246 final.

10 Direktiv 85/374/EØF

11 Ekspertgruppen vedrørende ansvarsforhold og nye teknologier blev nedsat for at forsyne Kommissionen med ekspertise vedrørende produktansvarsdirektivets og nationale regler om civilretligt ansvars anvendelighed og med bistand i forbindelse med udvikling af vejledende principper for eventuelle tilpasninger af gældende lovgivning vedrørende nye teknologier. Gruppen består af to undergrupper vedrørende henholdsvis produktansvar og nye teknologier, jf. http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1.
For rapporten fra undergruppen vedrørende nye teknologier om ansvar i forbindelse med kunstig intelligens og andre nye teknologier, se https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

Ud over produktivitets- og effektivitetsgevinster har kunstig intelligens også potentiale til at gøre mennesker i stand til at udvikle intelligens på et hidtil uset niveau, muliggøre nye opdagelser og bidrage til at løse nogle af verdens største udfordringer: lige fra at behandle kroniske sygdomme, forudsige sygdomsudbrud eller nedbringe antallet af omkomne i trafikulykker til at bekæmpe klimaændringer eller forudse trusler mod cybersikkerheden.

Disse teknologier kan medføre mange fordele ved at forbedre produkternes sikkerhed, så de bliver mindre sårbare over for visse risici. F.eks. kan opkoblede og automatiserede køretøjer forbedre færdselssikkerheden, idet de fleste trafikulykker på nuværende tidspunkt skyldes menneskelige fejl[12]. Systemer inden for tingenes internet er desuden udformet med henblik på at modtage og behandle store mængder data fra forskellige kilder. Dette øgede informationsniveau kan bruges til at få produkter til at tilpasse sig selv og dermed blive mere sikre. Nye teknologier kan bidrage til en mere effektiv tilbagekaldelse af produkter, idet produkter f.eks. kan advare brugerne med henblik på at undgå et sikkerhedsproblem[13]. Hvis der opstår et sikkerhedsproblem i forbindelse med anvendelsen af et opkoblet produkt, kan producenterne kommunikere direkte med brugerne, dels for at advare dem om risiciene, dels for om muligt at løse problemet direkte ved f.eks. at gennemføre en sikkerhedsopdatering. F.eks. foretog en smartphoneproducent i forbindelse med tilbagekaldelsen af en af dens enheder i 2017 en softwareopdatering for at reducere de tilbagekaldte telefoners[14] batterikapacitet til nul for at få brugerne til at holde op med at bruge de farlige enheder.

Desuden kan nye teknologier bidrage til at gøre produkter mere sporbare. F.eks. kan konnektivitetsfunktioner ved tingenes internet gøre virksomheder og markedsovervågningsmyndigheder i stand til at spore farlige produkter og identificere risici på tværs af forsyningskæder[15].

Ud over de muligheder, som kunstig intelligens, tingenes internet og robotteknologi kan skabe for økonomien og vores samfund, kan de også skabe en risiko for skade på retligt beskyttede interesser, både materielle og immaterielle. Risikoen for, at en sådan skade indtræder, stiger, efterhånden som anvendelsesområdet bliver større. Det er derfor vigtigt at undersøge om og i hvilket omfang de nuværende retlige rammer for sikkerhed og erstatningsansvar stadig er egnede til at beskytte brugerne.

2. Sikkerhed

I Kommissionens meddelelse om "opbygning af tillid til menneskecentreret kunstig intelligens" slås det fast, at ***systemer baseret på kunstig intelligens bør integrere***

[12] Det anslås, at omkring 90 % af alle trafikulykker skyldes menneskelige fejl. Se Kommissionens rapport om redning af liv: forbedret sikkerhed i biler i EU, COM(2016) 0787 final.

[13] F.eks. er det muligt at anmode føreren af en bil om at sænke farten, hvis vedkommende nærmer sig et ulykkessted.

[14] OECD (2018), "Measuring and maximising the impact of product recalls globally: OECD workshop-rapport", *OECD Science, Technology and Industry Policy Papers*, nr. 56, OECD Publishing, Paris, https://doi.org/10.1787/ab757416-en.

[15] OECD (2018), "Enhancing product recall effectiveness globally: OECD background report", *OECD Science, Technology and Industry Policy Papers*, No. 58, OECD Publishing, Paris, https://doi.org/10.1787/ef71935c-en.

mekanismer for beskyttelse og indbygget sikkerhed for at garantere, at de er beviseligt sikre på alle trin**, idet der tages hensyn til alle berørte parters **fysiske og mentale sikkerhed[16].

I forbindelse med vurderingen af EU's produktsikkerhedslovgivning i dette afsnit udarbejdes der en analyse af, om den nuværende EU-lovgivning indeholder de relevante elementer for at sikre, at nye teknologier og navnlig systemer baseret på kunstig intelligens integrerer beskyttelse og indbygget sikkerhed.

Denne rapport behandler hovedsagelig direktivet om produktsikkerhed i almindelighed[17] og den harmoniserede produktlovgivning, som følger de horisontale regler i "den nye tilgang"[18] og/eller "den nye lovgivningsmæssige ramme" (i det følgende benævnt "EU's lovgivning om eller ramme for produktsikkerhed")[19]. De horisontale regler sikrer sammenhængen mellem de sektorspecifikke regler om produktsikkerhed.

Unionens produktsikkerhedslovgivning har til formål at sikre, at produkter, der bringes i omsætning på EU-markedet, opfylder høje krav til sundhed, sikkerhed og miljø, og at sådanne produkter kan cirkulere frit i hele Unionen. Den sektorspecifikke lovgivning[20] suppleres af direktivet om produktsikkerhed i almindelighed[21], som kræver, at alle forbrugerprodukter skal være sikre, selv hvis de ikke reguleres af EU's sektorspecifikke lovgivning. Sikkerhedsreglerne suppleres af markedsovervågning og de beføjelser, der er tildelt de nationale myndigheder i henhold til forordningen om markedsovervågning[22] og direktivet om produktsikkerhed i almindelighed[23]. Inden for transportområdet er der supplerende regler på EU-plan og nationalt plan for, hvordan et motorkøretøj[24], et fly eller et skib tages i drift, og klare regler om sikkerhed under driften, herunder klare opgaver for operatørerne samt overvågningsopgaver for myndighederne.

Europæisk standardisering er også et væsentligt element i EU-lovgivningen om produktsikkerhed. I betragtning af digitaliseringens og de nye digitale teknologiers globale karakter er det internationale standardiseringssamarbejde særlig relevant for den europæiske industris konkurrenceevne.

En stor del af EU-rammen for produktsikkerhed blev skabt inden digitale teknologier såsom kunstig intelligens, tingenes internet eller robotteknologi dukkede op. Den indeholder derfor

---

[16] Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget om opbygning af tillid til menneskecentreret kunstig intelligens, Bruxelles, 8.4.2019, (COM(2019) 168 final).

[17] Europa-Parlamentets og Rådets direktiv 2001/95/EF af 3. december 2001 om produktsikkerhed i almindelighed (EFT L 11 af 15.1.2002, s. 4).

[18] EFT C 136 af 4.6.1985, s. 1.

[19] Forordning (EF) nr. 2008/765 og afgørelse nr. 2008/768/EF

[20] Dette skema omfatter ikke EU's lovgivning om transport og biler.

[21] Europa-Parlamentets og Rådets direktiv 2001/95/EF af 3. december 2001 om produktsikkerhed i almindelighed (EFT L 11 af 15.1.2002, s. 4).

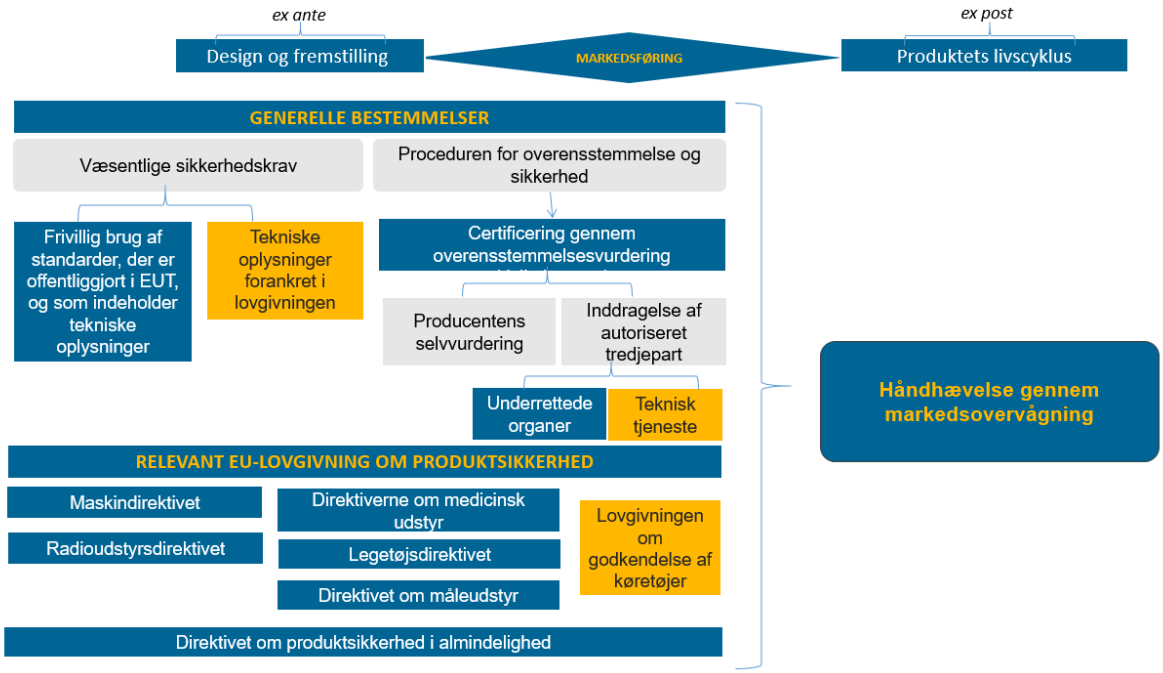
[22] Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 af 9. juli 2008 om kravene til akkreditering og markedsovervågning i forbindelse med markedsføring af produkter og om ophævelse af Rådets forordning (EØF) nr. 339/93, EUT L 218 af 13.8.2008, s. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj, og, fra 2021, Europa-Parlamentets og Rådets forordning (EU) 2019/1020 af 20. juni 2019 om markedsovervågning og produktoverensstemmelse og om ændring af direktiv 2004/42/EF og forordning (EF) nr. 765/2008 og (EU) nr. 305/201,1, EUT L 169 af 25.6.2019, s. 1, ELI: http://data.europa.eu/eli/reg/2019/1020/oj

[23] Artikel 8, stk. 1, litra b), nr. 3, i direktivet om produktsikkerhed i almindelighed.

[24] F.eks. direktiv 2007/46/EF — godkendelse af motorkøretøjer og påhængskøretøjer dertil samt af systemer, komponenter og separate tekniske enheder til sådanne køretøjer og Europa-Parlamentets og Rådets forordning (EU) 2018/858 af 30. maj 2018 om godkendelse og markedsovervågning af motorkøretøjer og påhængskøretøjer dertil samt af systemer, komponenter og separate tekniske enheder til sådanne køretøjer, om ændring af forordning (EF) nr. 715/2007 og (EF) nr. 595/2009 og om ophævelse af direktiv 2007/46/EF.

ikke altid bestemmelser, der udtrykkeligt omhandler de nye udfordringer og risici ved disse nye teknologier. Da den eksisterende produktsikkerhedsramme er teknologineutral, betyder dette imidlertid ikke, at den ikke finder anvendelse på produkter, der inkorporerer disse teknologier. Endvidere har efterfølgende lovgivningsmæssige retsakter, som er en del af denne ramme, f.eks. i bilsektoren eller sektoren for medicinsk udstyr, allerede udtrykkeligt taget hensyn til visse aspekter af fremkomsten af digitale teknologier, f.eks. automatiske afgørelser, software som et særskilt produkt og konnektivitet.

Den underliggende logik bag EU's gældende produktsikkerhedslovgivning[25]



De udfordringer, som de nye digitale teknologier medfører for EU's ramme for produktsikkerhed, fremlægges nedenfor.

Konnektivitet er et centralt element i et stadig større antal produkter og tjenester. Dette element udfordrer det traditionelle sikkerhedsbegreb, både direkte, fordi konnektivitet kan bringe produktets sikkerhed i fare, og indirekte, hvis produktet kan hackes, hvilket fører til sikkerhedstrusler og påvirker brugernes sikkerhed.

Et eksempel herpå er en meddelelse fra Island via EU's hurtige varslingssystem vedrørende et smartur til børn[26]. Dette produkt vil ikke være til direkte skade for det barn, der bærer det, men da uret end ikke har indbygget basale sikkerhedsfunktioner, kan det nemt bruges som et redskab til at få adgang til barnet. Da et af produktets formål er at beskytte børn gennem lokalisering, vil en forbruger forvente, at det ikke udgør en sikkerhedsrisiko for børn, der kan påvirke deres sikkerhed ved at de potentielt bliver sporet og/eller kontaktet af nogen.

Et andet eksempel fremgår af en meddelelse indgivet af Tyskland vedrørende en personbil[27]. Radioen i køretøjet kan have visse sikkerhedshuller i softwaren, som gør det muligt for uautoriserede tredjeparter at få adgang til de sammenkoblede kontrolsystemer i køretøjet.

[25] Dette billede omfatter ikke kravene til produkters livscyklus, dvs. anvendelse og vedligeholdelse, og vises kun til illustration.
[26] RAPEX-meddelelse fra Island offentliggjort på EU's "Safety Gate"-website (A12/0157/19)
[27] RAPEX-meddelelse fra Tyskland offentliggjort på EU's "Safety Gate"-website (A12/1671/15)

Hvis disse sikkerhedshuller i softwaren blev udnyttet af en tredjepart til ondsindede formål, kunne det føre til en trafikulykke.

Industrielle applikationer kan også være sårbare over for cybertrusler, der påvirker sikkerheden for personer i større målestok, når sådanne applikationer ikke har det nødvendige sikkerhedsniveau. Dette kan f.eks. være tilfældet ved cyberangreb mod et kontrolsystem med afgørende betydning for et industrielt anlæg, som har til formål at udløse en eksplosion, der kan koste menneskeliv.

EU-lovgivningen om produktsikkerhed omfatter generelt ikke specifikke obligatoriske centrale krav vedrørende cybertrusler, der påvirker brugernes sikkerhed. Der er dog bestemmelser vedrørende sikkerhedsaspekter i forordningen om medicinsk udstyr[28], direktivet om måleinstrumenter[29], direktivet om radioudstyr[30] eller lovgivningen om typegodkendelse af køretøjer[31]. Forordningen om cybersikkerhed[32] opretter en ramme for frivillig cybersikkerhedscertificering for IKT-produkter, -tjenester og -processer, mens den relevante EU-lovgivning om produktsikkerhed fastsætter obligatoriske krav.

Desuden kan den risiko for tab af konnektivitet, der er knyttet til nye digitale teknologier, også indebære sikkerhedsrelaterede risici. Hvis en opkoblet brandalarm eksempelvis mister konnektivitet, så advarer den måske ikke brugeren i tilfælde af brand.

I EU's nuværende produktsikkerhedslovgivning er sikkerhed et samfundspolitisk mål. Sikkerhedsbegrebet er knyttet til produktets anvendelse og de risici, f.eks. mekaniske, elektriske osv., der skal tages hånd om for at gøre produktet sikkert. Det skal bemærkes, at anvendelsen af produktet, afhængigt af EU's lovgivning om produktsikkerhed, ikke kun omfatter den påtænkte anvendelse, men også den forventede anvendelse og i visse tilfælde, som f.eks. i maskindirektivet[33], selv den misbrug , der med rimelighed kan forudses.

Sikkerhedsbegrebet i EU's nuværende produktsikkerhedslovgivning er i overensstemmelse med et udvidet sikkerhedsbegreb med det formål at beskytte forbrugere og brugere. Produktsikkerhedsbegrebet omfatter derfor beskyttelse mod alle former for risici i forbindelse med produktet, herunder ikke kun mekaniske, kemiske og elektriske risici, men også cyberrisici og risici i forbindelse med enheders tab af konnektivitet.

Udtrykkelige bestemmelser i denne henseende kan overvejes for de relevante EU-retsakters anvendelsesområde med henblik på at sikre en bedre beskyttelse af brugerne og skabe større retssikkerhed.

[28] Forordning (EU) 2017/745 om medicinsk udstyr

[29] Europa-Parlamentets og Rådets direktiv 2014/32/EU om harmonisering af medlemsstaternes love om tilgængeliggørelse på markedet af måleinstrumenter

[30] Direktiv 2014/53/EU om radioudstyr

[31] Europa-Parlamentets og Rådets direktiv 2007/46/EF om fastlæggelse af en ramme for godkendelse af motorkøretøjer og påhængskøretøjer dertil samt af systemer, komponenter og separate tekniske enheder til sådanne køretøjer Direktivet erstattes af forordning (EU) 2018/858 om godkendelse af motorkøretøjer og påhængskøretøjer dertil samt af systemer, komponenter og separate tekniske enheder til sådanne køretøjer, om ændring af forordning (EF) nr. 715/2007 og (EF) nr. 595/2009 og om ophævelse af direktiv 2007/46/EF med virkning fra 1. september 2020.

[32] Forordning (EU) 2019/881

[33] Direktiv 2006/42/EF om maskiner

Autonomi[34] er en af de vigtigste egenskaber ved kunstig intelligens. Utilsigtede resultater på grundlag af kunstig intelligens kan skade brugerne og udsatte personer.

I det omfang "adfærden" hos produkter baseret på kunstig intelligens kan fastslås på forhånd ved hjælp af den risikovurdering, der foretages af fabrikanten, inden produkterne bringes i omsætning, fastsætter EU-rammebestemmelserne for produktsikkerhed allerede forpligtelser for producenterne til i forbindelse med risikovurderingen at tage hensyn til produkternes "brug"[35] i hele deres levetid. Den indeholder også bestemmelser om, at fabrikanterne skal sørge for en brugsanvisning, sikkerhedsinformation eller advarsler[36] til brugerne. I denne forbindelse kræver direktivet om radioudstyr[37] f.eks., at fabrikanten vedlægger en brugsanvisning med oplysninger om, hvordan man anvender radioudstyret til det formål, det er beregnet til.

Der kan også opstå situationer i fremtiden, hvor kunstig intelligens-systemernes resultater ikke kan forudsiges fuldt ud på forhånd. I sådanne tilfælde afspejler den risikovurdering, der blev foretaget, før produktet blev bragt i omsætning, muligvis ikke længere produktets anvendelse, funktion eller adfærd. I disse tilfælde kan det overvejes at kræve en ny og samlet revurdering af det selvlærende produkt[38], hvis den af fabrikanten påtænkte anvendelse ændres[39] som følge af den autonome adfærd og overholdelsen af sikkerhedskravene påvirkes.

Inden for den nuværende ramme skal en producent straks underrette de kompetente myndigheder og træffe foranstaltninger til at forebygge de risici, som brugerne udsættes for[40], hvis vedkommende bliver klar over, at et produkt i løbet af dets livscyklus udgør en risiko for sikkerheden.

Ud over den risikovurdering, der er foretaget, inden et produkt bringes i omsætning, kan der eventuelt indføres en ny risikovurderingsprocedure, hvis produktet undergår væsentlige ændringer i sin levetid, som hvis det f.eks. overgår til en anden produktfunktion end den, som fabrikanten påtænkte i forbindelse med den oprindelige risikovurdering. I denne procedure bør der fokuseres på den autonome adfærds indvirkning på sikkerheden i løbet af produktets levetid. Risikovurderingen bør foretages af den relevante økonomiske aktør. Derudover kan

---

[34] Selv om produkter, der er baseret på kunstig intelligens, kan handle uafhængigt ved at opfatte deres omgivelser og uden at følge et sæt på forhånd fastlagte instrukser, begrænses deres adfærd af det mål, de gives, og andre relevante designvalg, som deres udviklere træffer. "

[35] I EU's produktsikkerhedslovgivning foretager producenterne en risikovurdering på grundlag af den påtænkte anvendelse af produktet, den forventede anvendelse og/eller det misbrug, der med rimelighed kan forventes.

[36] Europa-Parlamentets og Rådets afgørelse nr. 768/2008/EF af 9. juli 2008 om fælles rammer for markedsføring af produkter og om ophævelse af Rådets afgørelse 93/465/EØF (EUT L 218 af 13.8.2008, s. 82). Artikel R2.7 i bilag I har følgende ordlyd: "*Fabrikanten sikrer, at produktet ledsages af en brugsanvisning og sikkerhedsinformation på et for forbrugerne og andre slutbrugere letforståeligt sprog fastsat af den pågældende medlemsstat*."

[37] Artikel 10, stk. 8, der henviser til brugsanvisningen til slutbrugeren og bilag VI, der henviser til EU-overensstemmelseserklæringen

[38] Dette er i overensstemmelse med afsnit 2.1 i den blå vejledning om gennemførelsen af EU's produktregler 2016."

[39] Indtil videre anvendes "selvlæring" i forbindelse med kunstig intelligens primært for at angive, at maskiner er i stand til at lære i løbet af deres uddannelse; det er endnu ikke et krav, at maskiner baseret på kunstig intelligens skal fortsætte med at lære, efter at de er taget i brug; tværtimod holder maskiner baseret på kunstig intelligens normalt op med at lære, efter at deres uddannelse er afsluttet med et positivt resultat, navnlig inden for sundhedsvæsenet. På nuværende tidspunkt betyder den autonome adfærd som følge af kunstig intelligens-systemer derfor ikke, at produktet udfører opgaver, som udviklerne ikke har forudset.

[40] Artikel 5 i Europa-Parlamentets og Rådets direktiv 2001/95/EF af 3. december 2001 om produktsikkerhed i almindelighed

de relevante EU-retsakter omfatte skærpede krav til fabrikanterne angående brugsanvisninger og advarsler til brugerne.

Der stilles allerede krav om lignende risikovurderinger i transportlovgivningen[41]; når et jernbanekøretøj ændres efter certificeringen, pålægges ophavsmanden til ændringen i henhold til lovgivningen om jernbanetransport f.eks. en særlig procedure, og der opstilles klare kriterier med henblik på at afgøre, om myndigheden skal inddrages eller ej.

AI-produkternes og -systemernes selvlærende funktion kan gøre maskinen i stand til at træffe beslutninger, der afviger fra det, der oprindeligt var producenternes hensigt, og dermed, hvad brugerne forventer. Dette rejser spørgsmål om menneskelig kontrol, som gør mennesker i stand til at vælge, hvordan og om en beslutning skal uddelegeres til AI-produkter og -systemer med henblik på at opfylde mål, der er fastsat af mennesker[42]. Den eksisterende EU-lovgivning om produktsikkerhed adresserer ikke eksplicit menneskelig overvågning i forbindelse med selvlærende AI-produkter og systemer[43].

De relevante EU-retsakter kan indeholde en sikkerhedsforanstaltning i form af specifikke krav til menneskelig overvågning lige fra KI-produkterne og -systemerne udformes og i hele deres livscyklus.

AI-applikationers fremtidige "adfærd" kan medføre **mentale sundhedsrisici**[44] for brugerne, f.eks. som følge af deres samarbejde med menneskelignende robotter og systemer baseret på kunstig intelligens, enten hjemme eller i arbejdsmiljøer. I den forbindelse henviser sikkerhed i dag generelt til den af brugeren opfattede trussel om fysisk skade, der kan stamme fra nye digitale teknologier. Samtidig defineres sikre produkter i EU's retlige ramme som produkter, der ikke udgør nogen risiko eller kun minimale risici for personers sikkerhed og sundhed. Der er almindelig enighed om, at definitionen af sundhed omfatter både fysisk og psykisk velvære. Psykiske sundhedsrisici bør dog udtrykkeligt være omfattet af produktsikkerhedsbegrebet under den lovgivningsmæssige ramme.

For eksempel bør autonomi ikke medføre ovedreven stress og ubehag i længere perioder og skade den mentale sundhed. I denne forbindelse anses de faktorer, der har en positiv indvirkning på ældres[45] følelse af sikkerhed, for at være at: have sikre relationer til

---

41 I tilfælde af ændringer af jernbanesystemet, som kan påvirke sikkerheden (f.eks. tekniske og operationelle ændringer eller organisatoriske ændringer, der kan påvirke drifts- eller vedligeholdelsesprocessen), beskrives den procedure, der skal følges, i bilag I til Kommissionens gennemførelsesforordning (EU) 2015/1136 (EUT L 185 af 14.7.2015, s. 6).
I tilfælde af "væsentlig ændring" bør den, der står bag forslaget om ændringen, modtage en sikkerhedsvurderingsrapport udarbejdet af et uafhængigt vurderingsorgan (f.eks. den nationale sikkerhedsmyndighed eller en anden teknisk kompetent myndighed).
Efter risikoanalyseprocessen vil den, der står bag forslaget om ændringen, træffe de relevante foranstaltninger med henblik på at afbøde risici (hvis forslagsstilleren er en jernbanevirksomhed eller infrastrukturforvalter, er anvendelsen af forordningen en del af forslagsstillerens sikkerhedsstyringssystem, hvis anvendelse overvåges af den nationale sikkerhedsmyndighed).

42 "Policy and investment recommendations for trustworthy artificial intelligence" (Politiske og investeringsmæssige henstillinger vedrørende pålidelig kunstig intelligens), ekspertgruppen på højt plan vedrørende kunstig intelligens, juni 2019.

43 Dette udelukker dog ikke, at overvågning kan være nødvendig i en given situation som følge af nogle af de eksisterende mere generelle forpligtelser vedrørende markedsføring af produktet.

44 WHO's forfatning, første led: "sundhed er en tilstand af fuldstændig fysisk, psykisk og socialt velbefindende og ikke blot fravær af sygdom eller svækkelse". (https://www.who.int/about/who-we-are/constitution)

45 Sociale robotter: Technological, Societal and Ethical Aspects of Human-Robot Interaction, s.237-264, Research, Neziha Akalin, Annica Kristoff ersson og Amy Loutfi, juli 2019.

sundhedspersonale, have kontrol over de daglige rutiner og blive informeret om dem. Producenter af robotter, der interagerer med ældre, bør tage hensyn til disse faktorer med henblik på at forebygge psykiske sundhedsrisici.

Man kan eventuelt overveje som en del af den relevante EU-lovgivning at pålægge producenter af bl.a. menneskelignende robotter baseret på kunstig intelligens eksplicitte forpligtelser til udtrykkeligt at overveje den immaterielle skade, som deres produkter kan påføre navnlig sårbare brugere såsom ældre i plejemiljøer.

En anden væsentlig egenskab ved produkter og systemer, der er baseret på kunstig intelligens, er **dataafhængighed**. Datanøjagtighed og -relevans er afgørende for at sikre, at systemer og produkter baseret på kunstig intelligens træffer de beslutninger, producenten har haft til hensigt.

EU-lovgivningen om produktsikkerhed adresserer ikke udtrykkeligt sikkerhedsrelaterede risici som følge af mangelfulde data. På baggrund af produktets "brug" bør producenterne imidlertid i konstruktions- og testfasen forudse, at datanøjagtigheden er relevant for sikkerhedsfunktionerne.

F.eks. kan et system baseret på kunstig intelligens, der er udformet med henblik på at opdage specifikke objekter, have vanskeligt ved at genkende genstande under dårlige lysforhold, og derfor bør designerne medtage data, der kommer fra produktprøvninger i både typiske og dårligt belyste miljøer.

Et andet eksempel vedrører landbrugsrobotter, såsom frugtplukkende robotter, som har til formål at opdage og lokalisere modne frugter på træer eller på jorden. Selv om de relevante algoritmer allerede viser succesrater med hensyn til klassificering på over 90 %, kan en mangel i de datasæt, som disse algoritmer fodres med, føre til, at sådanne robotter træffer en dårlig beslutning og i forlængelse heraf skader et dyr eller en person.

Dette giver anledning til spørgsmålet om, hvorvidt EU's produktsikkerhedslovgivning bør indeholde specifikke krav, der har til formål at adressere de sikkerhedsrisici, som følger af mangelfulde data i udformningsfasen, samt mekanismer til at sikre, at datakvaliteten opretholdes i hele det tidsrum, hvor AI-produkter og -systemer anvendes.

Uigennemsigtighed er en anden vigtig egenskab hos nogle af de produkter og systemer, der er baseret på kunstig intelligens, og som kan blive resultatet af deres evne til at forbedre deres resultater ved at lære af deres erfaringer. Afhængigt af den metodiske tilgang kan produkter og systemer baseret på kunstig intelligens være kendetegnet ved forskellige grader af uigennemsigtighed. Dette kan føre til en beslutningsproces i systemet, der er vanskelig at følge ("black box-effect"). Mennesker behøver muligvis ikke at forstå hvert eneste trin i beslutningsprocessen, men efterhånden som AI-algoritmer bliver mere avancerede og tages i anvendelse inden for kritiske områder, er det afgørende, at mennesker kan forstå, hvordan systemets algoritmiske beslutninger er blevet truffet. Dette vil være særlig vigtigt for den efterfølgende håndhævelsesmekanisme, da det vil give håndhævelsesmyndighederne mulighed for at spore ansvaret for kunstig intelligens-systemers adfærd og valg. Dette anerkendes også i Kommissionens meddelelse om opbygning af tillid til menneskecentreret kunstig intelligens[46].

[46] https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top

Unionens produktsikkerhedslovgivning adresserer ikke eksplicit de øgede risici, som er forbundet med uigennemsigtighed af systemer, der er baseret på algoritmer. Det er derfor nødvendigt at overveje krav til algoritmers gennemsigtighed samt til robusthed, ansvarlighed og, hvor det er relevant, menneskeligt tilsyn og objektive resultater[47], hvilket er særligt vigtigt for den efterfølgende håndhævelsesmekanisme og for at opbygge tillid til anvendelsen af disse teknologier. En måde at tackle denne udfordring på kunne være at pålægge algoritmernes udviklere at offentliggøre konstruktionsparametre og metadata for datasæt i tilfælde af uheld.

Yderligere risici, der kan have indvirkning på sikkerheden, udpringer af **produkternes og systemernes kompleksitet**, idet forskellige komponenter, apparater og produkter kan integreres med hinanden og påvirke hinandens funktionsmåde (f.eks. produkter, som er en del af et smart home-økosystem).

Denne kompleksitet adresseres allerede af EU's retlige sikkerhedsramme, jf. begyndelsen af dette afsnit[48]. Når producenten foretager risikovurderingen, skal vedkommende navnlig tage hensyn til den påtænkte anvendelse, den forventede anvendelse og, hvor det er relevant, det misbrug, der med rimelighed kan forventes.

På denne baggrund vil det være sådan, at **hvis en producent forestiller sig, at vedkommendes apparat skal kobles sammen og interagere med andre apparater, så bør der tages hensyn hertil i forbindelse med risikovurderingen.** Om der er tale om brug eller misbrug afgøres på grundlag af f.eks. erfaringer med tidligere brug af samme slags produkt, undersøgelser af ulykker eller menneskelig adfærd.

Systemernes kompleksitet adresseres også mere specifikt af sektorspecifik lovgivning såsom forordningen om medicinsk udstyr og i et vist omfang i lovgivningen om produktsikkerhed i almindelighed[49]. Eksempelvis bør producenten af et opkoblet apparat, som er beregnet til at være en del af et smart home-økosystem, være i stand til at forudse, at deres produkt vil have indvirkning på andre produkters sikkerhed.

Derudover adresserer transportlovgivningen denne kompleksitet på systemniveau. For biler, tog og fly gennemføres typegodkendelse og certificering i lige så høj grad for hver enkelt komponent som for hele køretøjet eller flyet. Vej- og luftdygtighed samt jernbaneinteroperabilitet er en del af sikkerhedsvurderingen. På transportområdet skal "systemer" godkendes af en myndighed, enten på grundlag af en tredjepartsvurdering af konformiteten på grundlag af klare tekniske krav, elle efter en demonstration af, hvordan risici håndteres. Løsningen er overordnet set en kombination af "produktniveau" og "systemniveau".

EU's produktsikkerhedslovgivning, herunder transportlovgivningen, tager allerede til en vis grad hensyn til produkters eller systemers kompleksitet med henblik på at tackle de risici, der kan have indvirkning på brugernes sikkerhed.

---

[47] Baseret på de vigtigste krav, som ekspertgruppen på højt plan har foreslået i "Ethics Guidelines for Trustworthy AI" (Etiske retningslinjer vedrørende pålidelig kunstig intelligens): https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines

[48] Forordning (EF) nr. 2008/765 og afgørelse (EF) nr. 2008/768 og harmoniseret sektorspecifik produktsikkerhedslovgivning f.eks. direktiv 2006/42/EF om maskiner.

[49] Artikel 2 i direktivet om produktsikkerhed i almindelighed slår fast, at et sikkert produkt skal tage hensyn til "produktets virkning på andre produkter, såfremt det med rimelighed kan forudses anvendt sammen med andre produkter".

Komplekse systemer omfatter ofte **software,** som er en vigtig del af et system, der er baseret på kunstig intelligens. Generelt har fabrikanten af det endelige produkt som led i den indledende risikovurdering pligt til at forudse de risici, der er forbundet med software, der er integreret i produktet på det tidspunkt, hvor produktet bringes i omsætning.

Visse dele af EU's produktsikkerhedslovgivning henviser eksplicit til den software, der er integreret i produktet. I direktivet om maskiner[50] kræves det eksempelvis, at en fejl i kontrolsystemets software ikke må medføre farlige situationer.

I EU's produktsikkerhedslovgivning kan softwareopdateringer sammenlignes med vedligeholdelsesoperationer af sikkerhedshensyn under forudsætning af, at de ikke i væsentlig grad ændrer et produkt, der allerede er bragt i omsætning, og at de ikke medfører nye risici, som ikke var forudset i den indledende risikovurdering. Hvis en softwareopdatering i væsentlig grad ændrer det produkt, som den downloades til, kan hele produktet dog betragtes som et nyt produkt, hvorfor det, når ændringen udføres, er nødvendigt at foretage en ny vurdering af, om den relevante produktsikkerhedslovgivning overholdes[51].

Når der er tale om stand-alone software, der bringes i omsætning som det er eller uploades, efter at produktet er bragt i omsætning, indeholder EU's sektorspecifikke harmoniserede produktsikkerhedslovgivning generelt ingen specifikke bestemmelser. Visse dele af EU's produktsikkerhedslovgivning adresserer dog stand-alone software, f.eks. forordningen om medicinsk udstyr. Derudover kan stand-alone software, som er uploadet til opkoblede produkter, der kommunikerer via bestemte radiomoduler[52], også reguleres af direktivet om radioudstyr via delegerede retsakter. Dette direktiv kræver, at specifikke klasser eller kategorier af radioudstyr understøtter funktioner, der sikrer, at produktet stadig overholder reglerne, når softwaren er uploadet[53].

Selv om EU's produktsikkerhedslovgivning tager hensyn til de sikkerhedsrisici, der udgøres af software, som er integreret i produkter, når disse bringes i omsætning, og af eventuelle senere opdateringer fra producenten, kan der være behov for specifikke og/eller eksplicitte krav til stand alone-software (f.eks. en "app", der downloades). Der bør særligt være fokus på den stand-alone software, som sikrer sikkerhedsfunktionerne i AI-produkter og -systemer.

Det kan være nødvendigt at pålægge fabrikanterne supplerende forpligtelser for at sikre, at de sørger for funktioner, der er i stand til at forhindre download af software, som har indvirkning på sikkerheden i hele AI-produkternes levetid.

Endelig påvirkes nye digitale teknologier af **komplekse værdikæder**. Denne kompleksitet er dog hverken ny eller udelukkende et spørgsmål, som skyldes nye digitale teknologier såsom KI og tingenes internet. Dette er eksempelvis tilfældet for produkter såsom computere, servicerobotter eller transportsystemer.

I henhold til EU-rammen for produktsikkerhed ligger ansvaret for produktsikkerheden fortsat hos den producent, som bringer produktet i omsætning, uanset hvor kompleks værdikæden er. Producenter er ansvarlige for sikkerheden i forbindelse med det endelige produkt, herunder de dele, der er integreret i produktet, som f.eks. softwaren i en computer.

---

50 Afsnit 1.2.1 i bilag I til direktivet om maskiner

51 Den blå vejledning om gennemførelsen af EU's produktregler 2016

52 Radiomoduler er elektroniske apparater, som udsender og/eller modtager radiosignaler (WIFI, Bluetooth) mellem to apparater

53 Artikel 3, stk. 3, litra i), i direktivet om radioudstyr

Nogle dele af EU's produktsikkerhedslovgivning indeholder allerede bestemmelser, som eksplicit omhandler situationer, hvor flere økonomiske aktører griber ind over for et givet produkt, før dette produkt bringes i omsætning. Eksempelvis kræver direktivet om elevatorer[54], at den økonomiske aktør, som udformer og fremstiller elevatoren, skal forsyne installatøren[55] med "*al den nødvendige dokumentation og information, for at sidstnævnte kan installere og afprøve elevatoren korrekt og sikkert*". Direktivet om maskiner kræver, at fabrikanter af udstyr forsyner operatøren med oplysninger om, hvordan udstyret bygges sammen med andre maskiner[56].

EU's produktsikkerhedslovgivning tager hensyn til værdikædernes kompleksitet og pålægger adskillige økonomiske aktører forpligtelser efter princippet om "fælles ansvar".

Selv om producentens ansvar for den endelige produktsikkerhed har vist sig at være tilstrækkelig til aktuelle komplekse værdikæder, kan eksplicitte bestemmelser, der specifikt anmoder økonomiske aktører i forsyningskæden og brugerne om at samarbejde, skabe retssikkerhed i forbindelse med værdikæder, der muligvis er endnu mere komplekse. Navnlig ville hver enkelt aktør i værdikæden, som har indvirkning på produktsikkerheden (f.eks. softwareproducenter) og brugerne (ved at ændre produktet) påtage sig deres ansvar og give den næste aktør i kæden de nødvendige oplysninger og foranstaltninger.

3. Erstatningsansvar

EU's bestemmelser om produktsikkerhed og produktansvar er to supplerende mekanismer til at forfølge det samme politiske mål, nemlig målet om et velfungerende og sikkert indre marked for varer, hvor risikoen for at forbrugerne lider skade er minimal, og hvor der ydes erstatning for skader som følge af defekte varer.

Medlemsstaternes ikkeharmoniserede regler for civilretligt erstatningsansvar supplerer EU-reglerne ved at sikre erstatning for skader som følge af forskellige årsager (f.eks. produkter og tjenesteydelser) og ved at tage kontakt til forskellige ansvarlige personer (f.eks. ejere, operatører eller tjenesteydere).

Optimering af EU's sikkerhedsregler for kunstig intelligens kan bidrage til at undgå skader og ulykker, men de kan alligevel forekomme. Det er her, det civilretlige erstatningsansvar bliver aktuelt. Reglerne om civilretligt erstatningsansvar spiller en dobbelt rolle i vores samfund: på den ene side sikrer de, at ofre for skader forårsaget af andre får erstatning, og på den anden side giver de den ansvarlige part økonomiske incitamenter til at undgå at forårsage en sådan skade. Reglerne om erstatningsansvar skal altid finde en balance mellem at beskytte borgerne mod skade og samtidig give virksomhederne rum til at innovere.

De retlige rammer for erstatningsansvar i EU har fungeret godt. De er baseret på parallel anvendelse af produktansvarsdirektivet (direktiv 85/374/EØF), som harmoniserede producentens erstatningsansvar for defekte produkter, og andre ikkeharmoniserede nationale produktansvarsordninger.

---

[54] I henhold til artikel 16, stk. 2, i direktiv 2014/33/EU

[55] I direktiv 2014/33/EU om elevatorer svarer installatøren til fabrikanten og skal derfor overtage ansvaret for udformning, fremstilling, installation og markedsføring af elevatoren.

[56] Artikel 1.7.4.2 i bilag I til direktivet om maskiner har følgende ordlyd: *"Alle brugsanvisninger skal, hvor det er relevant, mindst indeholde følgende oplysninger"* i) *" instruktioner for montering, opstilling og tilslutning, herunder tegninger, diagrammer og fastgørelsesanordninger, og angivelse af den ramme eller installation, som maskinen skal monteres på;"*

Produktansvarsdirektivet skaber et beskyttelseslag, som nationalt culpaansvar ikke giver alene. Det indfører et system med objektivt erstatningsansvar, hvor producenter er ansvarlige for skader forårsaget af en defekt i deres produkt. I tilfælde af fysisk eller materiel skade har skadelidte ret til erstatning, hvis han eller hun kan bevise, at der er lidt skade, at produktet er defekt (dvs. at det ikke levede op til den sikkerhed, som offentligheden med rette bør kunne forvente), og at der er årsagssammenhæng mellem det defekte produkt og skaden.

De nationale ikkeharmoniserede erstatningsordninger for culpaansvar omfatter regler, hvor den skadelidte skal påvise den ansvarlige persons skyld, skaden og årsagssammenhængen mellem skylden og skaden med henblik på at fastslå et erstatningskrav. De indeholder også ordninger for objektivt ansvar, hvor man i den nationale lovgivning har tilskrevet ansvaret for en risiko til en bestemt person, uden at der er behov for et offer for at påvise skyld/defekt eller årsagssammenhængen mellem skyld/defekt og skaden.

De nationale erstatningsordninger sikrer ofre for skader, der er forårsaget af produkter og tjenester, flere parallelle erstatningskrav baseret på skyld eller objektivt ansvar. Disse krav er ofte rettet mod forskellige ansvarlige personer og har forskellige betingelser.

F.eks. kan offeret i en bilulykke i henhold til national civilret typisk fremsætte et erstatningskrav om objektivt ansvar mod bilens ejer (dvs. den person, der har tegnet ansvarsforsikring for køretøjet) og et erstatningskrav om culpaansvar mod føreren, og derudover kan der i henhold til direktivet om produktansvar fremsættes et erstatningskrav mod producenten, hvis bilen havde en defekt.

I overensstemmelse med de harmoniserede bestemmelser om motorkøretøjsforsikring skal brugen af et køretøj være forsikret[57], og forsikringsselskabet er i praksis de første, der modtager et erstatningskrav for personskade eller materiel skade. I henhold til disse regler kompenserer den obligatoriske forsikring offeret og beskytter den forsikrede person, som i henhold til nationale civilretlige regler[58] er forpligtet til at betale erstatning for den ulykke, som motorkøretøjet har været indblandet i. Producenter er ikke underlagt obligatorisk forsikring i henhold til produktansvarsdirektivet. I EU's lovgivning behandles selvkørende køretøjer ikke anderledes end ikkeselvkørende køretøjer med hensyn til motorkøretøjforsikring. Sådanne køretøjer skal som alle køretøjer være dækket af en ansvarsforsikring for motorkøretøjer, hvilket er den letteste måde, hvorpå skadelidte kan opnå erstatning.

Tegning af en passende forsikring kan mindske ulykkers negative konsekvenser ved at gøre det lettere for offeret at opnå erstatning. Klare regler om erstatningsansvar gør det lettere for forsikringsselskaberne at beregne deres risici og kræve refusion fra den part, der i sidste ende har erstatningsansvaret. Hvis en ulykke eksempelvis skyldes en defekt, kan bilforsikringsselskabet efter at have givet offeret erstatning kræve refusion fra fabrikanten.

Egenskaberne ved nye digitale teknologier såsom kunstig intelligens, tingenes internet og robotteknologi udfordrer forskellige aspekter af rammerne for erstatningsansvar på nationalt plan og EU-plan og har potentialet til at mindske deres effektivitet. Nogle af disse egenskaber kan gøre det svært at koble skaden til menneskelig adfærd, hvilket kan danne grundlag for et culpa-baseret krav i henhold til nationale regler. Dette betyder, at erstatningskrav baseret på national erstatningsret kan være svære eller uforholdsmæssigt dyre at underbygge, og at

[57] Harmoniseret for motorkøretøjer ved direktiv 2009/103/EF om ansvarsforsikring for motorkøretøjer og kontrollen med forsikringspligtens overholdelse.

[58] I de fleste medlemsstater ligger det objektive ansvar hos den person, i hvis navn motorkøretøjet er registreret.

ofrene som følge heraf muligvis ikke modtager passende erstatning. Det er vigtigt, at ofre i forbindelse med ulykker, der omfatter produkter og tjenester, herunder nye digitale teknologier såsom kunstig intelligens, ikke oplever et lavere beskyttelsesniveau sammenlignet med andre produkter og tjenester, hvor de ville modtage erstatning i henhold til national erstatningsret. Dette kan mindske den sociale accept af disse nye teknologier og føre til tilbageholdenhed med hensyn til at bruge dem.

Det vil være nødvendigt at foretage en vurdering af, om de udfordringer, som de nye teknologier udgør i forhold til de eksisterende rammer, også kan skabe juridisk usikkerhed med hensyn til, hvordan eksisterende lovgivning gælder (f.eks. hvordan begrebet "fejl" skal anvendes i forhold til skader forårsaget af kunstig intelligens). Disse kan lægge en dæmper på investeringerne og øge omkostningerne til information og forsikring for producenter og andre virksomheder i forsyningskæden, navnlig små og mellemstore europæiske virksomheder. Hvis medlemsstaterne med tiden adresserer de udfordringer, som de nationale rammer for erstatningsansvar står over for, kan dette derudover føre til yderligere fragmentering og således øge omkostningerne ved at indføre innovative AI-løsninger og nedbringe handlen på tværs af grænserne i det indre marked. Det er vigtigt, at virksomhederne kender de risici, som er forbundet med deres erstatningsansvar, i hele værdikæden, og at de kan mindske eller forebygge dem og forsikre sig effektivt mod disse risici.

I dette kapitel forklares, hvordan nye teknologier udfordrer de eksisterende rammer, og hvordan disse udfordringer kan håndteres. Derudover kan særlige områder i nogle sektorer, f.eks. sundhedspleje, kræve ekstra opmærksomhed.

Produkters, tjenesters og værdikædens kompleksitet: Teknologi og industri har udviklet sig drastisk i løbet af de seneste årtier. Særligt skillelinjen mellem produkter og tjenester er ikke længere så skarp som tidligere. Produkter og ydelsen af tjenester bliver stadig mere flettet ind i hinanden. Selv om komplekse produkter og værdikæder ikke er nye for den europæiske industri eller dennes reguleringsmæssige model, så er der grund til at sætte ekstra fokus på software og kunstig intelligens med hensyn til produktansvar. Software er af afgørende betydning for, at en lang række produkter fungerer, og kan have indvirkning på deres sikkerhed. Det er integreret i produkter, men kan også leveres separat for at gøre brugeren i stand til at anvende produktet som påtænkt. Hverken en computer eller en smartphone ville være til nogen nytte uden software. Dette betyder, at software kan gøre et håndgribeligt produkt defekt og medføre fysisk beskadigelse (jf. boksen om software i afsnittet om sikkerhed). Dette kan i sidste ende resultere i, at producenten af produktet bliver erstatningsansvarlig i henhold til direktivet om produktansvar.

Da der findes mange typer af og former for software, er løsningerne på spørgsmålet om klassificering af software som en tjeneste eller et produkt dog ikke altid så lige til. Så selv om den software, der styrer et håndgribeligt produkts funktion, kan betragtes som en del eller komponent af dette produkt, så er det sværere at klassificere nogle former for stand-alone software.

Selv om definitionen af et produkt i direktivet om produktansvar er bred, kan rækkevidden dog tydeliggøres yderligere, så den bedre afspejler nye teknologiers kompleksitet og sikrer, at det altid er muligt at få erstatning for skader forårsaget af produkter, der er defekte pga. software eller andre digitale funktioner. Dette ville gøre økonomiske aktører såsom softwareudviklere bedre i stand til at vurdere, om de kan betragtes som producenter i henhold til direktivet om produktansvar.

Applikationer baseret på kunstig intelligens er ofte integreret i **komplekse miljøer i tilknytning til tingenes internet**, hvor mange forskellige forbundne apparater og tjenester

interagerer. Kombinationen af forskellige digitale komponenter i et komplekst økosystem og mangfoldigheden af involverede aktører kan gøre det svært at vurdere, hvor en potentiel skade har sit udspring, og hvilken person der har erstatningsansvaret for den. På grund af disse teknologiers kompleksitet kan det være meget svært for ofre at identificere den erstatningsansvarlige person og bevise alle de forhold, der er nødvendige for at få erstatning, og som kræves i henhold til national lovgivning. Omkostningerne for at få adgang til denne ekspertise kan være økonomisk uoverkommelige og afholde ofre fra at kræve erstatning.

Derudover vil produkter og tjenester, som er baseret på kunstig intelligens, interagere med traditionelle teknologier, hvilket også medfører yderligere kompleksitet hvad angår erstatningsansvar. Eksempelvis vil selvkørende biler dele vejene med traditionelle biler i en periode. Der vil opstå lignende kompleksitet i forbindelse med interagerende aktører i nogle servicesektorer (såsom trafikstyring og sundhedspleje), hvor delvist automatiserede systemer baseret på kunstig intelligens vil understøtte menneskelig beslutningstagning.

Ifølge rapporten[59] fra undergruppen vedrørende nye teknologier under ekspertgruppen vedrørende ansvarsforhold og nye teknologier kan man overveje at tilpasse den nationale lovgivning med henblik på at lette bevisbyrden for ofrene til skader med tilknytning til kunstig intelligens. Eksempelvis kan bevisbyrden knyttes sammen med (den relevante operatørs) overholdelse af specifikke lovbestemte sikkerhedsforpligtelser vedrørende cybersikkerhed. Hvis disse regler ikke overholdes, kan en ændring af bevisbyrden med hensyn til skyld og årsag finde anvendelse.

Kommissionen er interesseret i synspunkter angående hvor vidt og i hvilket omfang det kan blive nødvendigt gennem et passende EU-initiativ at afbøde konsekvenserne af kompleksitet ved at lette/bytte om på den bevisbyrde, der kræves i henhold til nationale regler om erstatningsansvar i forbindelse med skader forårsaget af betjening af applikationer baseret på kunstig intelligens.

Hvad angår EU-lovgivningen, så betragtes et produkt, som ikke opfylder de obligatoriske sikkerhedsregler, i henhold til direktivet om produktansvar for defekt, uanset om det er producentens skyld. Der kan dog også være grunde til at overveje måder, hvorpå man kan lette bevisbyrden for ofre i henhold til direktivet: Direktivet hviler på nationale regler om bevismateriale og etablering af årsagssammenhæng.

Konnektivitet og åbenhed: Det er på nuværende tidspunkt ikke helt klart, hvordan forventningerne bliver med hensyn til sikkerhed i forbindelse med skader, som skyldes brud på cybersikkerheden i produktet, og om denne type skader vil blive godtgjort i tilstrækkelig grad inden for rammerne af direktivet om produktansvar.

Der kan findes cybersikkerhedsmæssige svagheder fra starten, når et produkt bringes i omsætning, men de kan også dukke op på et senere tidspunkt, længe efter at produktet blev bragt i omsætning.

I culpabaserede rammer for erstatningsansvar giver fastsættelsen af klare cybersikkerhedsmæssige forpligtelser operatørerne mulighed for at finde ud af, hvad de skal gøre for at undgå erstatningsansvarets konsekvenser.

Inden for rammerne af direktivet om produktsikkerhed kan spørgsmålet om, hvor vidt en producent under hensyntagen til et produkts med rimelighed forventede anvendelse kunne

[59] Rapporten "Liability for Artificial Intelligence and other emerging technologies", https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

have forudset visse ændringer, blive mere fremtrædende. Eksempelvis vil man muligvis opleve en stigning i anvendelsen af "forsvaret i forbindelse med senere opståede defekter", ifølge hvilket en producent ikke er erstatningsansvarlig, hvis defekten ikke eksisterede, da produktet blev bragt i omsætning, eller "forsvaret i forbindelse med udviklingsrisici" (at man med den bedste tilgængelige viden på tidspunktet ikke kunne have forudset defekten). Derudover kan erstatningsansvaret blive mindsket i tilfælde, hvor skadelidte ikke foretager de sikkerhedsrelevante opdateringer. Dette kan potentielt betragtes som skadelidtes egen skyld og derfor mindske producentens erstatningsansvar. Da forestillingen om "med rimelighed forventet anvendelse" og spørgsmål vedrørende "egen skyld" såsom undladelse af at downloade en sikkerhedsopdatering kan blive mere fremtrædende, vil skadelidte personer muligvis opleve, at det er sværere af få erstatning for skader forårsaget af en defekt i et produkt.

Autonomi og uigennemsigtighed: I tilfælde, hvor applikationer baseret på kunstig intelligens kan agere autonomt, udfører de en opgave, uden at hvert eneste skridt er fastlagt på forhånd, og med mindre, eller i sidste ende helt uden, umiddelbart menneskeligt tilsyn. Algoritmer baseret på maskinlæring kan være svære, hvis ikke umulige, at forstå (den såkaldte "black-box effekt").

Ud over den kompleksitet, som blev drøftet ovenfor, kan det pga. black-box effekten i nogle former for kunstig intelligens blive svært at få erstatning for skader forårsaget af autonome applikationer baseret på kunstig intelligens. Behovet for at forstå algoritmen og de data, som den kunstige intelligens anvender, kræver analytisk kapacitet og teknisk ekspertise, som kan være økonomisk uoverkommelige for ofre. Derudover kan det vise sig umuligt at få adgang til algoritmen, uden at den potentielt erstatningspligtige part samarbejder. I praksis vil ofre således muligvis ikke være i stand til at kræve erstatning Derudover vil det være uklart, hvordan man dokumenterer fejl begået af en autonom kunstig intelligens, og hvad der vil blive betragtet som en fejl begået af en person, som benytter sig af kunstig intelligens.

I national lovgivning er der allerede udviklet en række løsninger med henblik på at lette bevisbyrden for ofre i lignende situationer.

Et vejledende princip for EU's produktsikkerhed og produktansvar er fortsat, at producenten skal sikre, at alle produkter, som bringes i omsætning, er sikre i hele deres levetid og ved den anvendelse af produktet, som med rimelighed kan forventes. Dette betyder, at en fabrikant vil skulle sikre, at et produkt, der anvender kunstig intelligens, overholder visse sikkerhedsparametre. Egenskaberne ved kunstig intelligens udelukker ikke, at man med rette kan have sikkerhedsmæssige forventninger til produkterne, uanset om der er tale om automatiske plæneklippere eller robotter, der udfører kirurgi.

Autonomi kan påvirke produktets sikkerhed, fordi det kan ændre produktets egenskaber væsentligt, herunder dets sikkerhedsfunktioner. Spørgsmålet er, på hvilke betingelser selvlærende funktioner udvider producentens erstatningsansvar, og i hvilket omfang producenten burde have forudset visse ændringer.

Man kan nøje koordineret med tilsvarende ændringer af EU's sikkerhedsramme eventuelt revidere begrebet "at bringe i omsætning", som på nuværende tidspunkt anvendes i direktivet om produktansvar, med henblik på at tage hensyn til, at produkter kan ændre sig og blive ændret. Dette kan også være med til at tydeliggøre, hvem der er erstatningspligtig for eventuelle ændringer af produktet.

Ifølge rapporten[60] fra undergruppen vedrørende nye teknologier under ekspertgruppen vedrørende ansvarsforhold og nye teknologier kan benyttelse af nogle apparater og tjenester, der er baseret på kunstig Intelligens, have en særlig risikoprofil hvad angår erstatningsansvar, fordi de kan forårsage betydelige skader på vigtige retlige interesser såsom liv, helbred og ejendom og udsætte den brede offentlig hed for risici. Dette kan først og fremmest berøre apparater baseret på kunstig intelligens, der bevæger sig rundt i det offentlige rum (f.eks. helt selvkørende køretøjer, droner[61] og robotter, der leverer pakker), eller tjenester baseret på kunstig intelligens, som indebærer de samme risici (f.eks. trafikforvaltningstjenester, der vejleder eller kontrollerer køretøjer, eller forvaltning af eldistribution). De udfordringer, som autonomi og uigennemsigtighed udgør for national erstatningsret, kan adresseres ved at følge en risikobaseret tilgang. Ordninger for objektivt ansvar kan sikre, at offeret i tilfælde, hvor denne risiko realiseres, modtager erstatning uanset skyldsspørgsmålet. Man bør nøje vurdere virkningen af valget af, hvem der har det objektive ansvar for sådanne operationer vedrørende udvikling og udbredelse af kunstig intelligens, og overveje en risikobaseret tilgang.

I forbindelse med betjening af applikationer baseret på kunstig intelligens med en specifik risikoprofil ønsker Kommissionen at indhente synspunkter angående hvor vidt og i hvilket omfang der med henblik på at opnå effektiv erstatning til eventuelle ofre er behov for objektivt ansvar, som det findes i national lovgivning vedrørende lignende risici, som offentligheden udsættes for (f.eks. angående betjening af motorkøretøjer, flyvemaskiner eller atomkraftværk). Kommissionen ønsker også at indhente synspunkter angående en sammenkobling af objektivt ansvar og en eventuel forpligtelse til at tegne en af de tilgængelige forsikringer og dermed følge eksemplet i direktivet om forsikring af motorkøretøjer med henblik på at sikre erstatning, uanset om den erstatningspligtige person er solvent, og for at bidrage til at nedbringe omkostningerne i forbindelse med skader.

I forbindelse med betjening af alle andre applikationer baseret på kunstig intelligens, hvilket omfatter hovedparten af disse applikationer, overvejer Kommissionen, om der er behov for at tilpasse bevisbyrden i forbindelse med årsag og skyld. I denne henseende er et af de spørgsmål, der er markeret i rapporten[62] fra undergruppen vedrørende nye teknologier under ekspertgruppen vedrørende ansvarsforhold og nye teknologier, den situation, der opstår, når den potentielt erstatningspligtige part ikke har registreret de data, der er relevante for at vurdere erstatningsansvaret, eller ikke er villig til at dele dem med offeret.

4. Konklusion

Fremkomsten af nye digitale teknologier som kunstig intelligens, tingenes internet og robotteknologi skaber nye udfordringer med hensyn til produktsikkerhed og erstatningsansvar såsom konnektivitet, autonomi, dataafhængighed, uigennemsigtighed, produkters og systemers kompleksitet, softwareopdateringer og mere kompleks sikkerhedsforvaltning og værdikæder.

[60] Rapporten "Liability for Artificial Intelligence and other emerging technologies", https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

[61] Jf. ubemandede luftfartøjssystemer omhandlet i Kommissionens gennemførelsesforordning (EU) 2019/947 af 24. maj 2019 om regler og procedurer for operation af ubemandede luftfartøjer.

[62] Rapporten "Liability for Artificial Intelligence and other emerging technologies", https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

Den aktuelle produktsikkerhedslovgivning har en række huller, som skal adresseres, navnlig direktivet om produktsikkerhed i almindelighed, direktivet om maskiner, direktivet om radioudstyr og den nye lovgivningsmæssige ramme. Det fremtidige arbejde med tilpasning af forskellige retsakter inden for denne ramme vil blive gennemført på en konsekvent og harmoniseret måde.

De nye udfordringer på sikkerhedsområdet skaber også nye udfordringer med hensyn til erstatningsansvar. Disse udfordringer vedrørende erstatningsansvar skal adresseres med henblik på at sikre det samme beskyttelsesniveau, som ofre nyder i forbindelse med traditionelle teknologier, samtidig med, at balancen med behovet for teknologisk innovation opretholdes. Dette vil bidrage til at skabe tillid til disse nye digitale teknologier og sørge for investeringsstabilitet.

Selv om den eksisterende lovgivning om erstatningsansvar på EU- og nationalt plan er i stand til at håndtere nye teknologier, kan dimensionen og den samlede effekt af de udfordringer, der er knyttet til kunstig intelligens, gøre det sværere at tilbyde ofre erstatning i alle de tilfælde, hvor dette ville være berettiget[63]. Derfor bliver fordelingen af omkostningerne i tilfælde af en skade muligvis urimelig eller ineffektiv efter de nuværende regler. For at rette op på dette og adressere potentielle usikkerheder i den nuværende ramme kan man overveje at foretage visse justeringer af produktansvarsdirektivet og de nationale erstatningsordninger gennem passende EU-initiativer via en målrettet risikobaseret tilgang, dvs. under hensyntagen til, at forskellige applikationer baseret på kunstig intelligens udgør forskellige risici.

[63] Se rapporten fra undergruppen vedrørende nye teknologier, s. 3, og politikhenstilling 27.2 fra Ekspertgruppen på Højt Niveau om Kunstig Intelligens.