KANDIDATAFHANDLING

Kunstig intelligens & GDPR

- EFTERLEVELSE AF FORDNINGENS PRINCIPPER

Michael Sahl Daucke | 10. semester, HA Jura | 19. Maj 2021

Studienummer: 20115698

Vejleder: Niels Vase, advokat (H) HjulmandKaptain

Antal anslag: 136.479

AALBORG UNIVERSITY
DENMARK

Abstract

The following thesis is set out to investigate the consequences and difficulties the implementation of the General Data Protection Regulation has set for users and developers of artificial intelligence. The purpose of this thesis is to present the controller with guidelines to comply with the rules in the GDPR, whilst applying artificial intelligence models.
The thesis will present a brief introduction to the scope of artificial intelligence, followed by a technical description and review of the sphere of artificial intelligence in chapter 5. Chapter 6 introduces the analysis of this thesis, where the relevant provisions of the GDPR are examined. The thesis concludes with a presentation of the identified difficulties derived from the analysis, followed by a brief illumination of possible solutions.

The implementation of the GDPR challenges controllers use of complex and vast artificial intelligence, such as deep learning or online models. These techniques consist of many layers of decisions, which complicates the controller's ability to specify purpose or guarantee transparency, as are requirements in the GDPR. Due to complexity of the online models, controllers are not able to determine the result of the processing beforehand, and therefore not the specific purpose either. Transparency is one of the main issues concerning GDPR and the use of artificial intelligence. The ability to show and demonstrate how the model operates and processes the data is quite problematic, and requires technical solutions if compliance is to be reached.

The scale of the artificial intelligence models is essential in relation to how comprehensive complying with the regulations is. Deep learning or online models are of much greater complexity than for instance offline models. However, solutions are achievable when employing these models. Pseudonymization is explicitly mentioned several times in the GDPR as a solution, and this thesis find this to be a relevant measure. The GDPR does not impose impossible requirements unto the controllers altogether, however, many requirements seem impractical without technical solutions, which are not set forth in the GDPR.

Indholdsfortegnelse

1. Indledning

Scenariet hvori teknologien er mennesket overlegent, kommer efterhånden tættere og tættere på. Det er ingen hemmelighed, at vi mennesker altid har været fascineret af at udvikle og producere maskiner, hvilket kan spores så langt tilbage som til det 18. århundrede og den industrielle revolution, hvilken bragte store samfundsmæssige og socioøkonomiske forandringer med sig, og udviklingen er ingenlunde aftaget, nærmest tværtimod[1]. Biler der kører selv og maskiner der træffer automatiske afgørelser i den offentlige forvaltning, er blot eksempler på de teknologiske løsninger som unægtelig rummer et stort potentiale, og ambitions- og forventningsniveau må siges at være tårnhøjt[2].

I 2019 offentliggjorde regeringen en national strategi for brugen af kunstig intelligens, i hvilken der bliver lagt op til intensivering af udviklingen af kunstig intelligens, med det formål på sigt at kunne sidestille den kunstige intelligens med den menneskelige[3]. Set i lyset af den stigende tendens og tilsyneladende samfundsøkonomiske gevinst ved at udvikle teknologi og "robotter", der arbejder og varetager funktioner uafhængigt af menneskelig indblanding, er der et væsentlig behov for at stille skarpt på en række juridiske udfordringer. I takt med at anvendelsen af kunstig intelligens udbredes, vil de bagvedliggende teknologier og algoritmer ligeledes udvikle sig, og dermed kan udviklere og anvendere potentielt miste kontrollen med deres teknologi, og den mængde af data der bliver behandlet.

Med implementering af forordning 2016/679 om databeskyttelse (GDPR), synes det stigende behov og krav om ansvarlig databehandling for imødekommet – eller hvad? Anvendelsen af kunstig intelligens, og de uanede muligheder der findes i forbindelse hermed, udgør en vanskelig faktor i det retlige og etiske landskab i relation til GDPR. Når man betragter kravene til grundlæggende GDPR-principper som lovlighed, rimelighed og gennemsigtighed bliver man i høj grad fristet til at anspore, hvorvidt det er muligt for os at vide, hvorvidt en algoritme er i stand til for eksempel at træffe en korrekt og rimelig afgørelse. Er det overhovedet muligt med de rammer, som GDPR har sat for brugere af kunstig intelligens?

[1] https://faktalink.dk/titelliste/kunstig-intelligens (Artikel fra januar 2015. Senest Opdateret april 2018)
[2] https://www.horten.dk/viden/artikler-2018/kunstig-intelligens-gdpr-og-andre-juridiske-udfordringer (Artikel fra april 2020)
[3] https://digst.dk/media/19302/national_strategi_for_kunstig_intelligens_final.pdf (Artikel fra marts 2019)

1.1. Problemformulering

Denne afhandling vil, med afsæt i nedenstående problemformulering, analysere de gældende bestemmelser og principper indeholdt i EU-forordning 2016/679 om databeskyttelse, hvorledes rammerne for brugen af kunstig intelligens sættes, og dermed hvilke regler der skal iagttages for at sikre lovlig og ansvarlig databehandling.

> *"Hvilke konsekvenser har bestemmelserne i EU-forordning 2016/679 om databeskyttelse, for anvendere og udviklere af kunstig intelligens?"*

Det er en forudsætning for at besvare ovenstående problemformulering, at alle aspekter af problemformulering er berørt. Derfor er strukturen i afhandlingen bygget op således, at begrebet "kunstig intelligens" gennemgås i kapitel 4, hvorefter relevante persondataretlige principper i GDPR vil blive analyseret i relation til anvendelsen af kunstig intelligens, hvor udfordringer og problematikker vil blive belyst i kapitel 5. I kapitel 6 vil den etiske problemstilling i relation til anvendelsen af kunstig intelligens blive inddraget, hvilket vil fungere som afhandlingens perspektiverende vinkel.

2. Afgrænsning

Denne afhandling lægger til grund, at læseren har kendskab til persondataretten og GDPR, hvorved der vil blive taget udgangspunkt i de grundlæggende principper og bestemmelser i forordningen, der er relevante i besvarelsen af problemformuleringen. Der vil således ikke blive redegjort for samtlige bestemmelser i GDPR, på samme måde vil lovens baggrund, systematik og opbygning heller ikke blive gennemgået.

Nærværende afhandling er juridisk, hvorfor begrebet kunstig intelligens og de bagvedliggende teknologiske begreber kun vil blive redegjort for, og ikke blive indeholdt i en selvstændig analyseproces. For at kunne forstå kunstig intelligens, vil begreber som; "Machine Learning" og "Big data" blive inddraget på et overordnet niveau, da disse begreber er fundamentale, i forhold til forståelsen af hvad kunstig intelligens er. Teknologiske processer vil ikke blive gennemgået, da disse ikke er indenfor denne afhandlings scope og dermed ikke vil bidrage til besvarelsen af problemformuleringen.

Denne afhandling benytter sig ikke af en retspolitisk tilgang til problemstillingen. Den retspolitiske tilgang indebærer blandt andet, "udtalelser om retten, som den bør være"[4], hvilket ikke er formålet med denne afhandling. Afhandlingen er båret af den stigende anvendelse af kunstig intelligens, og de problematikker dette kan medføre i forbindelse med efterlevelse af kravene i persondataforordningen. Der vil således ikke blive udøvet retsskabende virksomhed, eller argumenteret for ændringer i retstilstanden.

Lovgrundlaget i denne afhandling vil for omfangets skyld, være begrænset til den danske indførsel af forordning 2016/679 om databeskyttelse. Det er således GDPR, der er i centrum, og ikke særlovgivning som for eksempel regnskabsloven eller den danske databeskyttelseslov.

[4] Evald, Jens (2020): "*Juridisk teori, metode og videnskab*", side 155.

3. Metodik og retskilder

Denne afhandlings metodiske struktur er bygget op således, at fundamentale emner, som kan bidrage til forståelsen af kunstig intelligens, vil blive redegjort og gennemgået på et overordnet niveau. Herefter vil relevante persondataretlige bestemmelser blive analyseret i relation til kunstig intelligens og anvendelsen hermed. Dette har til formål at identificere, hvilke udfordringer og problemstillinger anvendere og udviklere af kunstig intelligens står overfor, når de skal iagttage forordningens bestemmelser.

Herudover vil der blive perspektiveret til de etiske problemstillinger, som angår konstruktion og anvendelse af kunstig intelligens. Denne diskussion rækker udover de bestemmelser, som er indeholdt i lovgivningen (EU-forordning 2016/679), men kan ikke desto mindre vise sig at være betydningsfuld, idet både anvendere og brugere af kunstig intelligens har med enorme mængder data og kloge algoritmer at gøre. En diskussion om det etiske dilemma vil give afhandlingen og problemstillingen en retssociologisk og samfundsmæssig dimension, der kan betragtes som væsentlig i takt med anvendelsen af kunstig intelligens udbreder sig.

På trods af, at kunstig intelligens ikke er et nyt fænomen, så er retstilstanden på området fortsat ikke tydeligt klarlagt, da persondataforordningen er teknologineutral. Med persondataforordningens indførsel i 2018, blev kravene for dataansvarlige og databehandlere dog skærpet i forbindelse med ansvarlig og lovlig behandling af persondata, men kunstig intelligens er ikke direkte indeholdt i forordningen, hvorfor øget retlig regulering fortsat er EU-Kommissionens fokus. Af denne årsag, vil den metodiske tilgang til problemløsning i denne afhandling være *den retsdogmatiske metode*.

Den retsdogmatiske metode knytter sig til retsforskerens beskrivelse, analyse og fortolkning af et retsområde[5]. I dette tilfælde, udvalgte bestemmelser i persondataforordningen, i relation til anvendelsen af kunstig intelligens. Denne metodeanvendelse vil fungere som afhandlingens røde tråd, og sikre, at besvarelsen af den overordnede problemstilling vil være det altoverskyggende fokus fra start til slut.

[5] Munk-Hansen, Carsten (2018): "*retsvidenskabsteori*", side 193.

Der vil blive inddraget relevant litteratur af videnskabelig og teknologisk karakter, med henblik på at give læseren en forståelse af hvad kunstig intelligens nærmere bestemt er, og hvad det rummer. Denne litteratur vil hovedsaligt bestå af artikler, som er relevante i forhold til den overordnede besvarelse af problemformuleringen, og vil således blive anvendt metodisk.

Udviklingen og anvendelsen af kunstig intelligens skal efterleve kravene i persondataforordningen, men da der ingen retspraksis eksisterer på området, sammenholdt med det faktum, at persondataforordningen er teknologineutral, og dermed ikke konkretiserer hvordan kunstig intelligens kan eller skal opbygges for at efterleve reglerne, vil der i denne afhandling ikke blive præsenteret en fuldstændig løsning på denne problemstilling.
Der vil, ved hjælp af guidelines fra det Europæiske Databeskyttelsesråd, blive præsenteret mulige løsninger for, hvordan kunstig intelligens bør udvikles og anvendes ud fra et persondataretligt perspektiv, hvis bestemmelserne skal efterleves.

Persondataforordningen vil være den centrale retskilde i denne afhandling, og den vil samtidig være genstand for en gennemgående analyse af de grundlæggende principper og bestemmelser, som er vurderet centrale i forhold til besvarelsen af problemformuleringen i denne afhandling. Da persondataforordningen kun har været i effekt siden 2018 og kunstig intelligenssfæren fortsat er en ubekendt størrelse, er det begrænset hvor meget retspraksis der findes på området. Kunstig intelligens er ligeledes ikke indeholdt i forordningen, hvorfor analyser og betragtninger kan blive suppleret af retslitteratur og guidelines fra eksempelvis Artikel-29 gruppen og Det Europæiske Databeskyttelsesråd, hvis det vurderes relevant i forhold til besvarelsen af problemformuleringen. Her er det væsentligt at nævne, at litteratur kan være væsentligt for at give læseren et bedre overblik og en bedre forståelse af et emne, men litteratur et udtryk for en holdning til et emne, og udgør således ikke en retskilde[6].

[6] Von Eyben, William Edler (1991) "*Juridisk Grundbog Bind 1 – Retskilderne*", side 19.

4. Konklusion

Denne afhandling har søgt at determinere, hvilke konsekvenser indførslen af persondataforordningens bestemmelser og principper har i relation til anvendere og udviklere af kunstig intelligens. Ved dybdegående gennemgang af forordningens regler, fremgår det klart, at regelefterlevelsen i mange tilfælde beror på konkrete vurderinger, baseret på den enkelte bestemmelse og den faktiske databehandling. Denne afhandling har præsenteret dataansvarlige, samt anvendere og udviklere af kunstig intelligens for, hvilke persondataretlige udfordringer der er forbundet med anvendelse af kunstig intelligens. Dermed kan denne afhandling fungere som en dybdegående vejledning til dataansvarlige, samt anvendere og udvikleres brug af kunstig intelligens, idet det er blevet anskueliggjort, hvilke problemstillinger og udfordringer der kan opstå med anvendelse og udvikling af kunstig intelligens i relation til persondatabehandling.

Det er blevet afsøgt i denne afhandling, at kategoriseringen af de personoplysninger der behandles, samt hvilken type kunstig intelligens der anvendes, har stor betydning for omfanget af regelefterlevelsen i persondataforordningen. Som det fremgik af forordningens artikel 5, stk. 1, litra b kan personoplysninger viderebehandles uden de forbryder sig mod princippet om formålsbegrænsning, hvis der er tale om oplysninger, som skal bruges til statistiske, historiske eller videnskabelig formål. Ligeledes gør sig gældende i litra e, hvor personoplysningerne kan opbevares i længere tid, uden at forbryde sig mod princippet om opbevaringsbegrænsning, hvis oplysningerne skal bruges til statistiske, historiske eller videnskabelige formål.
Herudover blev en række forskellige former for anvendelse af kunstig intelligens præsenteret, og som tidligere beskrevet, er det ikke ubetydeligt hvilken type model man arbejder med. Er der tale om eksempelvis online læringsmodeller eller deep learning, bliver udfordringen med regelefterlevelsen større, da kompleksiteten af modellerne bliver større. Det er herudover ikke utænkeligt, at kunstig intelligens kan anvendes til statistiske, historiske eller videnskabelige formål, hvilket betyder, at kunstig intelligens under visse forudsætninger kan viderebehandle personoplysninger til et andet formål end det, som de var indsamlet til.

I relation til den konkrete databehandling har denne afhandling gennemgået en række essentielle principper i forordningen. Det overordnede princip i artikel 5, stk. 1, litra a, om lovlighed, rimelighed og gennemsigtighed blev indledningsvist gennemgået og det blev påvist, at overholdelse af disse 3

principper er forbundet med en del udfordringer for anvendere og udviklere af kunstig intelligens. Rimelighed relaterer sig primært til kravet i artikel 5, stk. 1, litra c om dataminimering, da den registrerede har krav på at vide, til hvilket formål personoplysningerne bliver behandlet og at de ikke bliver behandlet videre udover dette formål, og at der ikke bliver behandlet mere data end nødvendigt for at opfylde formålet. Dette princip kan for anvendere og udviklere være vanskeligt at overholde, da kompleksiteten i visse kunstig intelligens modeller gør, at det ikke altid er muligt at determinere hvilke oplysninger en online model skal bruge, da det ofte kræver et enormt datainput for modellen at nå frem til beslutninger eller resultater, hvilket er tilfældet i Big Data. En potentiel løsning på dette, som også er positivt listet i forordningen, er pseudonymisering.

Herudover er rimelighed også forbundet med princippet om ansvarlighed og kravet om dokumentation i artikel 5, stk. 2, men også princippet om rigtighed i artikel 5, stk. 1, litra d, særligt i relation til kunstig intelligens. Den dataansvarlige er forpligtet til at sikre, at den data der bliver behandlet, er korrekt, og hvis den er forkert, han den registrerede ret til at få dataen berigtiget. Dette kan ikke desto mindre vise sig som en stor udfordring, da det, afhængig af kompleksiteten af den kunstige intelligens, ikke altid er muligt at tilkomme den enkelte data og sikre hverken sletning eller berigtigelse. En løsning kan som tidligere nævnt være pseudonymisering, men hvorvidt denne løsning rent faktisk er tilstrækkelig, må bero på en konkret vurdering baseret på formålet med behandlingen.

Gennemsigtighedsprincippet relaterer sig særligt til kravet om formålsspecifikation i artikel 5, stk. 1, litra b, da udfordringen ved at give indsigt i, hvad den kunstige intelligens bruger dataen til, forstørres jo mere kompleks den kunstige intelligens er. Problematikken omkring den sorte boks gør ligeledes efterlevelse af dokumentationskravet yderst vanskeligt, da det ikke altid er muligt at opnå indsigt i hvilke databehandlinger der foregår i en kompleks online model.

4.1 Løsninger

Som kort beskrevet i afsnit 7.2 om ansvarlighed, kan implementering af tekniske softwareløsninger være en mulig løsning for iagttagelse af forordningens principper og regler. Persondataforordningen tager ikke stilling til hvordan kunstig intelligens kan udvikles og tilpasses de krav og forpligtelser som bestemmelserne i forordningen fremsætter. Udviklingen synes ikke desto mindre at pege i retning af, at løsningen ikke skal findes i lovgivning, men i udviklingen af teknologi. Der er i denne afhandling præsenteret en række principper, som i praksis er udfordrende at overholde i relation til

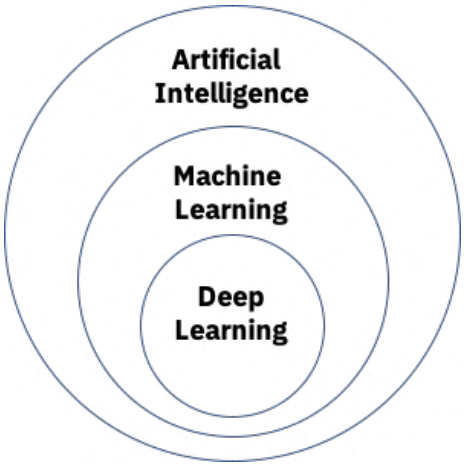
anvendelse af kunstig intelligens, da forordningen forholder sig teknologineutral. Af denne årsag forekommer det naturligt, at specialister på området skal udvikle og præsentere teknologiske løsninger til, hvordan disse grundlæggende persondataretlige principper kan efterleves i praksis.

Overordnet set har denne afhandlings gennemgang af de konsekvenser, som indførslen af persondataforordningen har for anvendere og udviklere af kunstig intelligens, påvist at der forelægger en række udfordringer på området. Dog er anvendelsen af kunstig intelligens, i forbindelse med behandling af personoplysninger, ikke entydigt forbundet med forbrydelse på persondataforordningens regler. Det afhænger af kompleksiteten af modellen der anvendes, hvilket stiller større krav til den dataansvarliges sikkerhedsforanstaltninger og kontinuerlige arbejde med efterlevelse af de principper som i forordningen er særligt relevante med henblik på anvendelse af kunstig intelligens i persondatabehandlingen.

5. Begrebet "Kunstig intelligens"

Indenfor computerteknologien refererer begrebet kunstig intelligens til en menneskelignende intelligens, som bliver udøvet af en robot, computer eller maskine[7]. Efter at være blevet forbundet med science fiction i årtier, er kunstig intelligens, eller AI, i dag blevet en stor del af vores hverdag. Den pludselige tilgængelighed af store mængder data og den dertilhørende udvikling af computerteknologi har gjort, at udviklingen og anvendelsen af kunstig intelligens har taget fart og giver stort set uanede muligheder på området.

På trods af, at kunstig intelligens i dag er blevet et almindeligt begreb, kan det ikke desto mindre være vanskeligt at få forstå hvad begrebet dækker over, da en række forskellige termer bliver anvendt indenfor begrebet kunstig intelligens. Hvad er eksempelvis forskellen på kunstig intelligens og machine learning? Eller hvad er forskellen på machine learning og deep learning?
Kunstig intelligens, machine learning og deep learning forvekslet let, men adskiller sig på den måde, at kunstig intelligens er et overordnet begreb, hvorunder machine learning er omfattet[8]. Begrebet machine learning kom efter begrebet kunstig intelligens, og er en række teknologiske løsninger til at opbygge kunstig intelligens. Deep learning er indeholdt under machine learning, og er en teknik der anvendes til at opbygge machine learning. Nedenstående figur 1 fungerer som en illustration af begreberne og deres relation til hinanden.



Figur 1 – Illustration af sammenhængen mellem begreberne "*Artificial Intelligence*", "*Machine Learning*" og "*Deep Learning*".
Kilde: IBM Cloud Education: https://www.ibm.com/cloud/learn/what-is-artificial-intelligence

[7] https://www.ibm.com/cloud/learn/what-is-artificial-intelligence (Artikel fra 3. juni 2020. Downloadet den 23. februar 2021).
[8] https://www.ibm.com/cloud/learn/what-is-artificial-intelligence (Artikel fra 3. juni 2020. Downloadet den 23. februar 2021).

For at kunne besvare den udvalgte problemformulering, er det nødvendigt at have relevant baggrundsviden og forståelse for, hvad begrebet kunstig intelligens nærmere indebærer. I det følgende vil relevante begreber indenfor kunstig intelligens således blive gennemgået ud fra et teknisk og juridisk udgangspunkt.

5.1. Paradigmer indenfor kunstig intelligens

Udviklingen indenfor kunstig intelligens kan i grove træk inddeles i 3 forskellige kategorier eller paradigmer: 1) det klassiske symbolparadigme 2) det konnektionistiske paradigme 3) kroppen i kunstig intelligens. Måden hvorpå kunstig intelligens, og brugen af denne, er tænkt igennem historien, er væsentlig for at forstå hvordan vi anvender kunstig intelligens i dag. De forskellige paradigmer vil derfor blive belyst i det følgende.

5.1.1. Det klassiske symbolparadigme

Den centrale tese indenfor det klassiske symbolparadigme er, at al tænkning er mekaniske operationer i et formelt system. Den generelle tankegang var, at computere var i stand til at foretage de samme formelle operationer som menneskehjernen, kravet var blot, at computeren var tilført tilstrækkelig regnekraft og udstyret med det rigtige program[9].

I 1967 præsterede trioen Allen Newell, Herbert Simon og J. Cliff Shaw et program kaldet "General Problem Solver", hvilket var i stand til at bevise logiske og matematiske sætninger, og gøre det på lignende måder som mennesker ville gøre det. Det klassiske symbolparadigmes tidlige succes med skabe systemer, der kunne spille eksempelvis skak på et rimelig niveau, blot dog aldrig overført til løsningen af realistiske problemstillinger[10].

Det klassiske symbolparadigme havde dog en række udfordringer, eksempelvis rammeproblemet. Der påpeges et principielt problem, der går ud på, at enhver handling i den virkelig verden har umådeligt mange konsekvenser. Der er således stor forskel på, at planlægge og forstå konsekvenser af handlinger i den virkelige verden, fremfor i et spil skak, hvor hver handling har et begrænset antal konsekvenser[11].

5.1.2. Det konnektionistiske paradigme

Den grundlæggende ide i konnektionismen er at opbygge systemer, der efterligner den menneskelige hjerne både i tankegang og opbygning. Da hjernen består af mange neuroner, som er sammensat i et

[9] https://www.etiskraad.dk/etiske-temaer/optimering-af-mennesket/homo-artefakt/leksikon/kunstig-intelligens (Artikel fra 1. september 2007. Downloadet den 16. februar 2021.)
[10] https://www.etiskraad.dk/etiske-temaer/optimering-af-mennesket/homo-artefakt/leksikon/kunstig-intelligens (Artikel fra 1. september 2007. Downloadet den 16. februar 2021.)
[11] https://www.etiskraad.dk/etiske-temaer/optimering-af-mennesket/homo-artefakt/leksikon/kunstig-intelligens (Artikel fra 1. september 2007. Downloadet den 16. februar 2021.)

meget komplekst netværk, er opgaven for udviklere af kunstig intelligens, indenfor den konnektionistiske tankegang, at vanskelig og stor. Det handler om, både at forstå hvordan et netværk af beregningsenheder fungerer, og at opbygge kunstige netværk, der kan efterligne de funktioner, som hjernens biologiske netværk har[12].

5.1.3. Kroppen i kunstig intelligens

Embodiment-filosofien knytter menneskets intelligens sammen med vores fysiske eksistens. Det er derfor heller ikke muligt at forstå menneskets evne til abstrakt tænkning, medmindre man først har forstået vores helt grundlæggende evne til at spille sammen med omgivne miljøer. Embodiment-filosofien slog igennem i midt 80'erne, og tog udgangspunkt i robotter og deres evne til at klare sig på egen hånd i dynamiske miljøer[13].

Denne typer robotter går under navnet 'autonome agenter', og forsøgene med denne typer robotter blev anerkendt i 1980'erne, da det klassiske symbolparadigme havde spillet fallit. Gennembruddet kom med subsumptions arkitekturen, der gjorde det muligt at udvikle robotter, der med en vis robusthed overfor den virkelige verdens uforudsigelighed var i stand til at løse simple opgaver, såsom at indsamle coladåser i et hektisk kontormiljø. Disse robotter fik et kommercielt gennembrug i starten af det nye årtusind, da deres evne til at begå sig i hektiske og uforudsigelig miljøer, gjorde de autonome agenter værdifulde indenfor industri-, underholdnings,- og plejesektoren. De blev dog aldrig udviklet udover det basale intelligensniveau[14].

5.1.4. Selvstrukturerende systemer

Opfattelsen af hvordan kunstig intelligens kan og bør skabes, har siden midten af 00'erne, stået overfor et fundamentalt skifte. Selvstrukturende systemer forekommer, når der opstår en overordnet orden eller struktur, hvis et system følger bestemte regler. I forskning af kunstig intelligens kan neurale netværk ses som et tidligt eksempel på brug af selvstrukturering, men det er særligt i forbindelse med

[12] https://www.etiskraad.dk/etiske-temaer/optimering-af-mennesket/homo-artefakt/leksikon/kunstig-intelligens (Artikel fra 1. september 2007. Downloadet den 16. februar 2021.)
[13] https://www.etiskraad.dk/etiske-temaer/optimering-af-mennesket/homo-artefakt/leksikon/kunstig-intelligens (Artikel fra 1. september 2007. Downloadet den 16. februar 2021.)
[14] https://www.etiskraad.dk/etiske-temaer/optimering-af-mennesket/homo-artefakt/leksikon/kunstig-intelligens (Artikel fra 1. september 2007. Downloadet den 16. februar 2021.)

det øgede fokus på biologiske realistiske systemer i den nye kunstig intelligens forskning, at man mere målrettet er begyndt at bruge selvstrukturering[15].

Hvorvidt der er tale om et egentlig paradigmeskift, skal forblive usagt, men forskere og udviklere ser ikke længere sig selv som urmagere, der skal designere og kontrollere alle systermerne ned til den mindste detalje. I stedet gælder det om at opbygge de rigtige betingelser og regler for et system, således den overordnede kompleksitet kan vokse af sig selv[16].

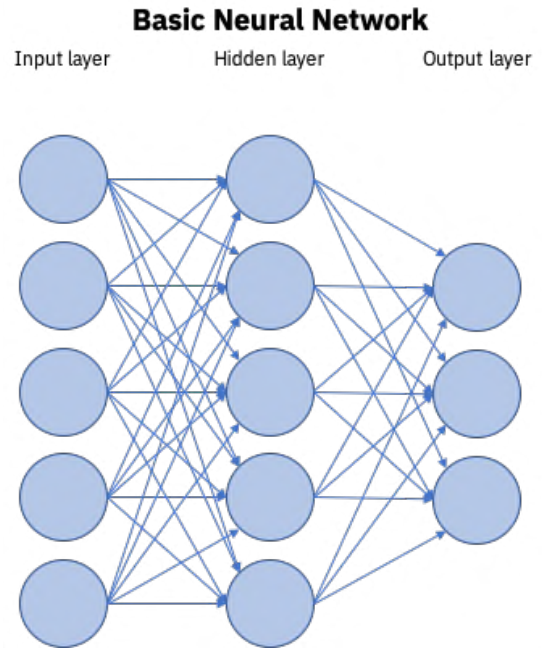
Denne nye og mere moderne tilgang til udvikling og arbejde med kunstig intelligens, har defineret rammerne for hvordan vi arbejder med og opbygger teknologien i dag. Kan man fastlægge de rette betingelser og regler for et system, så kan systemet lære af sig selv og vokse sig større og større.

[15] https://www.etiskraad.dk/etiske-temaer/optimering-af-mennesket/homo-artefakt/leksikon/kunstig-intelligens (Artikel fra 1. september 2007. Downloadet den 16. februar 2021.)
[16] https://www.etiskraad.dk/etiske-temaer/optimering-af-mennesket/homo-artefakt/leksikon/kunstig-intelligens (Artikel fra 1. september 2007. Downloadet den 16. februar 2021.)

5.2. Machine Learning

Som beskrevet kort i indledningen i afsnit 5., er begrebet machine learning en teknologisk løsning til at opbygge kunstig intelligens. Machine learning applikationer, eller modeller, er baseret på neurale netværk af matematiske algoritmer, som forsøger at imitere den menneskelige hjernes tankegang. Det basale neurale netværk er opbygget af 3 niveauer eller lag; et input niveau, et skjult niveau (abstraktionsniveau) og et output niveau. Input-niveauet er hvor dataen kommer ind i netværket. Det skjulte niveau er hvor algoritmerne bearbejder de datainput netværket bliver fodret med, hvilket også kaldes abstraktionsniveauet. Output-niveauet er hvor netværket træffer beslutninger og konklusioner, baseret på det datainput der kommer[17].

Nedenstående figur illustrer hvordan dataen bevæger sig fra niveau til niveau, på det basale neurale netværk indenfor machine learning.



Figur 2 – Illustration af sammenhæng mellem de 3 niveauer i det basale neurale netværk.
Kilde: IBM Cloud Education: https://www.ibm.com/cloud/learn/what-is-artificial-intelligence

Dette netværk, bliver således trænet til, uden menneskelig indvirkning, at kunne udføre opgaver eller løse problemer, ud fra det enorme datainput modellen modtager. Machine learning modeller, som

[17] https://www.ibm.com/cloud/learn/what-is-artificial-intelligence (Artikel fra 3. juni 2020. Downloadet den 23. februar 2021.)

ikke er baseret på deep learning modeller, er neurale netværk med kun ét skjult niveau. Disse modeller er fodret med data, som er mærket med en eller flere etiketter. Disse etiketter indeholder karakteristika eller specifikationer, som er værdifulde for modellen i forståelsen og identificeringen af dataen. Ved at fodre en computer eller maskine med en algoritme som indeholder specifikke regler, kan man blive i stand til at lære en maskine en specifik opgave eller løsning, som for eksempel at kunne spille skak. Dette kaldes "supervised learning" og det kræver en menneskelig overvågning og et specifikt data-input[18]. Begrebet "unsupervised learning" vil blive gennemgået i kap. 5.3 om deep learning.

5.2.1. Hvordan opbygges kunstig intelligens?

Som allerede beskrevet er kunstig intelligens opbygget omkring én eller flere algoritmer. Disse algoritmer er bygget op af software, som udvikleren har valgt, skal indeholde specifikke funktioner. Kunstig intelligens er således opbygget af algoritmer, som er baseret på software hvis formål er af kognitiv karakter. Algoritmerne kræver fodring af træningsdata for at kunne lære af sig selv. Denne læring starter med et udvalg af oplysninger, som indeholder en eller flere etiketter, som nævnt i kap. 5.2. Ved hjælp af machine learning afdækkes indholdet af disse etiketter, og der vil således blive dannet en model, som kan genkende etiketterne når det nye data bliver bearbejdet af modellen[19].

En model er en samlet betegnelse for slutproduktet af læringen, og en model vil altid blive resultatet, uafhængig af hvilke algoritmer der benyttes i machine learning processen. Denne model kan så benyttes sammen med ny data og producere et givent resultat, for eksempelvis en kategorisering. Det bør bemærkes, at modellen ikke altid indeholder den kildedata, som den blev fodret med. Den vil typisk indeholde en aggregeret version af den kildedata, der er brugt til at lære systemet op. Undtagelsen til disse aggregerede data, er beslutningstræet, hvor kildedataen vil kunne findes i varierende grad. Begrænsningerne til beslutningstræet forekommer ved, hvordan man vælger at beskære træet efter oplæringen, eller om man sætter niveaubegrænsninger på, inden oplæringen. På denne måde sikrer man, at dataen forbliver general, og modellen ikke tilpasser dataen til et scenarie. Dataen skal forblive objektiv. I deep learning modeller vil dataen være repræsenteret som talværdier i det neurale netværk, og det skal derfor ikke være muligt at trække data ud, når den data der er brugt som

[18] https://www.ibm.com/cloud/learn/what-is-artificial-intelligence (Artikel fra 3. juni 2020. Downloadet den 23. februar 2021.)
[19] Det Norske Datatilsyn (2018): *"Kunstig Intelligens og personvern"*, side 6.

oplæringsdata, er eksempelvis personoplysninger. Dette vil blive diskuteret yderligere i afsnit 5.4. om den sorte boks[20].

5.2.2. Statiske modeller

En kunstig intelligens-model kan opdeles i 2 forskellige typer; en statisk model og en dynamisk model. Den første model er den statiske eller også kaldet den offline, hvor modellen aldrig ændrer sig, og altid vil opføre sig på samme måde og give samme resultat. Når den statiske model er i brug, så lærer den ikke og den ændrer sig ikke. Al ny oplæring kommer fra træningsdata i et træningsmiljø, og ny læring forudsætter, at man skifter modellen ud med en ny. Da den statiske model ikke lærer af sine resultater, vil der altid være fuld kontrol med den[21].

5.2.3. Dynamiske modeller

Den anden type kaldes den dynamiske model, og den tages i brug på samme måde som den statiske model. Forskellen på de 2 modeller er, at den dynamiske model lærer i takt med de bliver brugt. Den dynamiske model har, via datainput, mulighed for at forbedre sig og tilpasse sig ændringer. Dette kunne eksempelvis være relevant ved kreditkortovervågning i forbindelse med afsløring af svindel. Kreditkorttransaktionerne kan ændre sig ud fra brugerens adfærd og brugsmønstre, for eksempel ved størrelsen af transaktionerne og hvor de bliver foretaget. Den statiske model vil blot kunne kategorisere dataen, men da den ikke lærer af de datainputs den kontinuerligt får, vil den være mindre nøjagtig[22].

I langt de fleste sammenhænge kræver kunstig intelligens-maskiner et meget større datagrundlag i forbindelse med oplæring, end mennesker kræver for at lære det samme. Dette gør, at maskinerne skal fodres med betydelige mængder data, og her er det i særdeleshed vigtigt, at kvaliteten af dataen er sikret, samt at dataens egenskaber er korrekt. I forbindelse med oplæring af en model, er det af afgørende betydning, at udvalget af dataen, som bruges til oplæring, er repræsentativt for den opgave der ønskes løst. Det er essentielt, at der ved vejledet læring er foretaget korrekt kategorisering af træningsdataen. Det kan påvirke resultatet negativt, hvis dette ikke er gjort korrekt, og effektiviteten

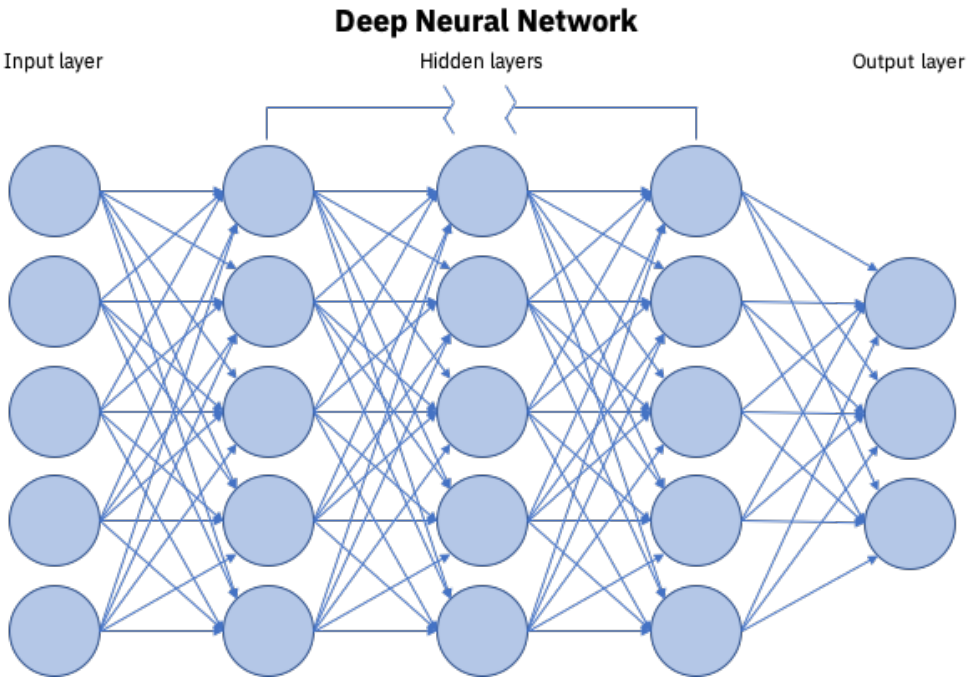
[20] Det Norske Datatilsyn (2018): *"Kunstig Intelligens og personvern"*, side 9.
[21] Det Norske Datatilsyn (2018): *"Kunstig Intelligens og personvern"*, side 9.
[22] Det Norske Datatilsyn (2018): *"Kunstig Intelligens og personvern"*, side 9.

af machine learning-udarbejdelsen kan blive stærkt påvirket af, hvordan kildedataen er blevet præsenteret for algoritmerne, som udarbejder modellerne[23].

5.3. Deep Learning

Deep learning-modeller er baseret på dybe neurale netværk, der, modsat de basale neurale netværk indenfor machine learning, indeholder mange skjulte abstraktionsniveauer (hidden layers), hvilke gør det muligt at kortlægge dataen mere præcist. De mange abstraktionsniveauer er blevet inspireret af det menneskelige neurale netværk[24].

Figur 1 nedenfor, illustrerer hvordan dataen bevæger sig og indenfor det dybe neurale netværk.



Figur 3 – Illustration af sammenhæng mellem niveauerne i det dybe neurale netværk.
Kilde: IBM Cloud Education: https://www.ibm.com/cloud/learn/what-is-artificial-intelligence

Nogle deep learning-modeller arbejder med data, som er mærket med en eller flere etiketter, hvilket resulterer i den såkaldte "Supervised learning". Andre deep learning-modeller derimod, arbejder med data, som er fri for mærker og etiketter, og som er designet til at identificere tendenser og mønstre uden menneskelig overvågning, hvilket kaldes "Unsupervised learning". Ved brugen af denne type

[23] Det Norske Datatilsyn (2018): *"Kunstig Intelligens og personvern"*, side 10.
[24] https://www.ibm.com/cloud/learn/what-is-artificial-intelligence (Artikel fra 3. juni 2020. Downloadet den 23. februar 2021.)

læring, ønsker man således at systemet selv skal kunne kategorisere data, som er ens. Et eksempel kunne være billeder af mennesker og dyr, hvor man ønsker at systemet skal kunne inddele billederne korrekt i de 2 kategorier – én med billeder af mennesker og én med billeder af dyr. Én af de helt åbenlyse udfordringer ved denne læringstype er, at modellen ikke er i stand til at kategorisere dataen i andre grupper, end dem som blev identificeret under oplæringsprocessen. Derfor er det afgørende, at dataen er repræsentativ[25] [26].

5.3.1 Svag og stærk kunstig intelligens

Svag kunstig intelligens, også kaldet smal kunstig intelligens, er betegnelsen for den kunstige intelligens-model, når den er trænet målrettet imod at kunne foretage specifikke opgaver. Det er således en begrænset kunstig intelligens-model, men er ikke desto mindre den type modeller, som driver størstedelen af kunstig intelligens landskabet i dag. Betegnelsen 'svag' betyder langt fra, at modellen rent faktisk er svag, hvorfor betegnelsen 'smal' er mere korrekt. Modellen er tværtimod i stand til at aktivere nogle imponerende applikationer, som eksempelvis 'Siri' eller 'Alexa, som kendes fra henholdsvis Apple og Amazon[27].

Stærk kunstig intelligens er betegnelsen for den udvidede form for kunstig intelligens, som til fulde forsøger at imitere den menneskelige biologiske hjerne. Denne type kunstig intelligens kan løse mange forskellige typer problemer, og kan sågar vælge hvilket problem den vil løse, uden nogen form for menneskelig overvågning eller indblanding. Denne form for stærk kunstig intelligens, og tanken om at opbygge modeller af denne type, er fortsat blot teoretisk, og er ikke udviklet i praksis endnu. Dette betyder imidlertid ikke, at udviklere ikke undersøger muligheden for denne type kunstig intelligens, på samme måde som de undersøger muligheden for udvikling af kunstig super intelligens, som menes at være den menneskelige intelligens og evne overlegen[28].

[25] https://www.ibm.com/cloud/learn/what-is-artificial-intelligence (Artikel fra 3. juni 2020. Downloadet den 23. februar 2021.)
[26] Det Norske Datatilsyn (2018): *"Kunstig Intelligens og personvern"*, side 8.
[27] https://www.ibm.com/cloud/learn/what-is-artificial-intelligence (Artikel fra 3. juni 2020. Downloadet den 23. februar 2021.)
[28] https://www.ibm.com/cloud/learn/what-is-artificial-intelligence (Artikel fra 3. juni 2020. Downloadet den 23. februar 2021.)

5.3.2 Neurale netværk

Som beskrevet i afsnit 5.2 om machine learning, er opbygningen af kunstig intelligens applikationer baseret på neurale netværk af matematiske algoritmer. Disse neural netværk kan karakteriseres som en serie af forbundne enheder, der alle sammen indeholder indbyggede muligheder for at lære, udvikle og ændre sig, i takt med at de bliver fodret med data. De matematiske algoritmer indbygget i de neurale netværk har til opgave at identificere mønstre i dataen, som ville være enormt vanskeligt for et menneske. Grundlæggende kan det beskrives således, at den kunstige intelligens-maskine (eks. en computer) bliver fodret med data, som den skal behandle. Baseret på mængden, kvaliteten og repræsentativiteten af de datainput, bliver computeren i stand til at identificere mønstre og tendenser. Figur 3 på side 17 illustrerer hvordan dataen bevæger sig imellem niveauerne. Hvert niveau i figuren tillægger dataen en vægtning, og denne vægtning medfører en beslutning, hvor ud fra den kunstige intelligens er i stand til at producere en række udfald, som så tillægges ny vægt. Alle disse udfald er derudover også baseret på, hvad den kunstige intelligens tidligere har lært. Som det fremgår af figur 3 på side 17, så forekommer der en stor mængde data og udfald, som bliver bearbejdet indtil modellen når frem til et resultat eller en løsning. Idet der bliver foretaget så mange udfald, baseret på så stor en mængde data, bliver der automatisk opbygget et beslutningstræ, hvori der er indeholdt millioner af små beslutninger[29].

Da det neurale netværk er en imitation af den menneskelige kognition, burde man tro, at de indeholdt den samme grad af transparens. Når kunstig intelligens opbygges af denne form for deep learning, så foregår databehandling og beslutningsprocesserne på et langt højere og hurtigere niveau, end hvad et menneske ville være i stand til. Dette medfører de åbenbare konsekvenser, transparensen og gennemsigtighed bliver langt lavere, da beslutningstræet bliver mere komplekst og meget større, da det fremtidige resultat er drevet af potentielt millioner af små beslutninger. Således kan det være en stor udfordring at holde styr på alle processerne og beslutningerne som foregår inde i modellen – og hvordan sikrer man så gennemsigtighed i databehandlingen i henhold til persondataforordningens artikel 5, stk. 1, litra a? Ved udfordringen om den manglende gennemsigtighed opstår problematikken om den sorte boks, hvilket vil blive gennemgået yderligere i det følgende afsnit.

[29] Det Norske Datatilsyn (2018): *"Kunstig Intelligens og personvern"*, side 9.

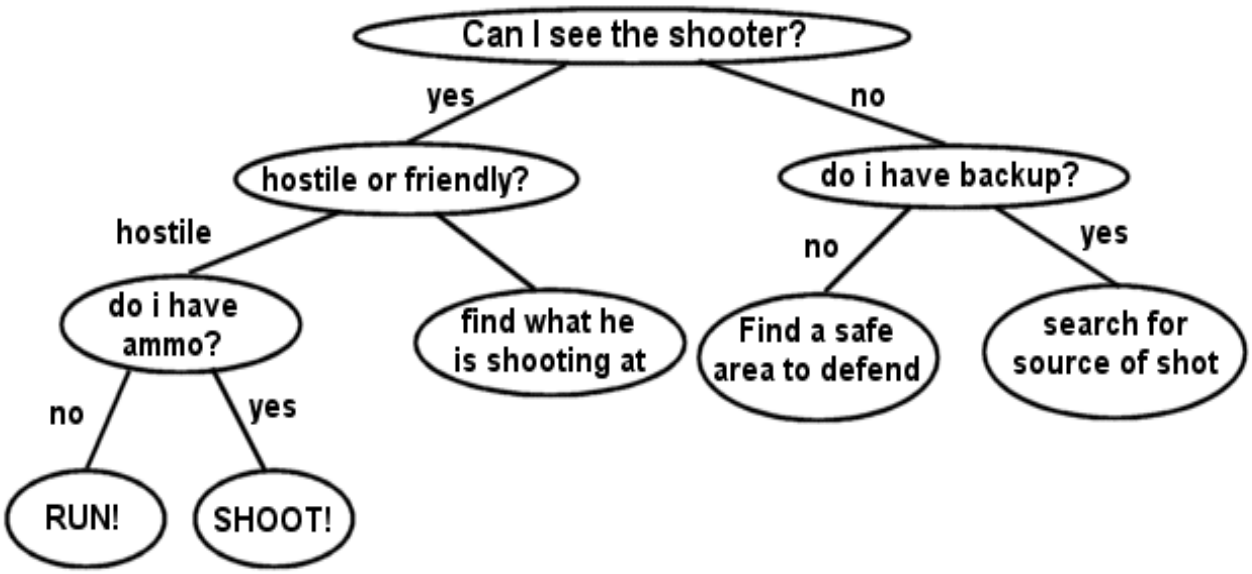
5.4. "Black Box" problematikken

Den store udfordring ved anvendelse af kunstig intelligens modeller er, at det ikke altid er let at identificere, hvordan et resultat eller en løsning er opnået. Denne problematik opstår i særlig grad i deep learning modeller, hvor databehandlingen og beslutningsprocesserne i det skjulte niveau er enormt komplekse. Modellen er i stand til at producere et tydeligt svar, men beslutningerne inde bag ved den kunstig intelligens, får man ingen indsigt i. Heri opstår udfordringen med den sorte boks.

Problematikken om den sorte boks bliver ofte forbundet med deep learning og neurale netværk, da der, i denne type kunstig intelligens, ingen indsigt gives i hvorledes beslutningerne bliver truffet. Deep learning er så komplekst, at brugen af denne type online kunstig intelligens, vil få den sorte boks til at vokse sig større og større, i takt med det stigende datainput. Dette er en stor udfordring, da tilliden til den kunstige intelligens nødvendigvis vil være lav, når der ikke er gennemsigtighed med hvordan dataen er blevet behandlet og hvordan løsningerne er nået. Konkret opstår problemet ved, at modellen er i stand til at lære af sig selv og på den måde danne nye lag, som udviklerne ikke kender til. Udviklerne kender i stor udstrækning de regler, som modellen er bygget op omkring, men den manglende kontrol med udviklingen i modellen er en udfordring, hvis der ikke er foretaget foranstaltninger eller taget forholdsregler på forhånd[30].

Der findes imidlertid modeller som er langt mere transparente i beslutningsprocessen, som for eksempel beslutningstræer, hvilke er enkle og nemmere at forklare. Et beslutningstræ kan godt være komplekst og avanceret, men hvis det indeholder overskuelige mængder data, så er træet, grundet dets opbygning, den simpleste model at gennemskue. Et beslutningstræ er bygget således op, at man starter på toppen og, baseret på egenskaberne, vil man herefter på hvert niveau vælge en gren. Dette gøres indtil man kommer ned til bunden af træet, hvorefter der vil være opnået et resultat. Se figur nedenfor:

[30] Det Norske Datatilsyn (2018): *"Kunstig Intelligens og personvern"*, side 12.



Figur 4 – Illustration af et beslutningstræ.
Kilde: https://corydesmondai.wordpress.com/2014/10/01/the-island-genre-and-implementation-of-ai/

Gennemsigtigheden for denne type model er langt større, da det er muligt at bevæge sig over grenene, og se hvilke betragtninger der ligger til grund for resultatet. Denne type model kaldes for en "hvid boks", da udvikleren har kontrol med, og indsigt i, beslutningsprocesserne. Den hvide boks kan imidlertid hurtigt blive sort, hvis man øger datamængden til det punkt, hvor det ikke længere er muligt for et menneske at have oversigt og kontrol[31].

[31] https://videnskab.dk/teknologi-innovation/black-box-problemet-naar-vi-ikke-forstaar-den-kunstige-intelligens (Artikel fra 25. november 2017. Downloadet den 27. februar 2021)

5.5. Big Data

Big data er en betegnelse for den enorme mængde data, som florerer i vores informations-drevne samfund. Tilbage i 2001, beskrev en forskergruppe kaldet "Gartner-gruppen", at de stigende data-udfordringer og muligheder er 3-dimensionelle og bliver betegnet som de 3 V'er (Volume, Velocity og Variety). De beskrev Big Data som værende: "*high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization*"[32]. Ud fra denne betragtning er Big Data et udtryk for en enorm mængde data, der behandles ved enorm fart og har enorm stor varians[33].

Big data er et udtryk for en datamængde så stor, at den er stort set umuligt for et menneske at skulle analysere og fortolke. IT professionelle og computer forskere fandt hurtigt ud af, at processen med at behandle al den data og konvertere det til et format man kunne forstå, er umulig uden kunstig intelligens. De komplekse modeller og algoritmer er designet til at læse opgaven om, at skabe indsigt ud af kaos, og derfor kan Big Data drage enorm fordel af kunstig intelligens[34].

5.5.1 Hvordan bruges kunstig intelligens i Big Data?

Som det fremgår af ovenstående, så er Big Data ikke en del af kunstig intelligens, men sammenkoblingen er ikke desto mindre åbenbar, da kunstig intelligens har den tekniske formåen til at analysere og udtrykke betydningen af de store mængder data, som Big Data bringer med sig. Ligeledes bidrager Big Data med den mængde data, der gør, at den kunstige intelligens er i stand til at udvikle sig og lære af sig selv[35].

Vigtigheden af kunstig intelligens ses især i markedsføringsarbejde i relation til "customer experience". Virksomheder har adgang til tonsvis af data relaterende til customer experience, hvilket er god mulighed for virksomheder til at lære om deres kunder, forbedre deres oplevelser og skaffe nye kunder. Problemet er blot, at den store mængde data kan være uoverskuelig at administrere og analysere, da det kommer fra mange forskellige kilder, men da kunstig intelligens er i stand til at analysere og lære, langt ud over hvad en almindelig computer kan, kan dette betragtes som revolutionerende indenfor markedsføring-sfæren. Evnen til at kunne anbefale et produkt, som præcist matcher det behov

[32] ENISA (2016): "*Big Data Threat Landscape and Good Practice guide*", side 9.
[33] https://online.maryville.edu/blog/big-data-is-too-big-without-ai/ (Artikel downloadet den 12. februar)
[34] https://online.maryville.edu/blog/big-data-is-too-big-without-ai/ (Artikel downloadet den 12. februar)
[35] UMBEL (2015): "*AI meets Big Data*", side 5.

kunden måtte have. Ved at samle data fra en masse forskellige kilder, er kunstig intelligens i stand til at opbygge et lager af viden, som ultimativt vil kunne give præcise forudsigelser på, hvad man som forbruger køber, hvor mange penge man bruger, hvor lang tid man er i forretningen, hvad man kigger på, men ikke køber osv. På denne måde er virksomheden i stand til at lære sine kunder at kende, hvis en kunde eksempelvis køber en kjole, så kan man fortælle kunden hvilke sko kunden kunne købe dertil, baseret på tidligere købsadfærd[36].

5.5.2. Trussels-landskabet

Denne form for databehandling kommer med betragtelige risici, da det er store og personlige mængder data der behandles. Generelt kan trusler, såsom system, - eller netværksfejl, påvirke Big Data betydeligt. Da Big Data træffer millioner af små mikrobeslutninger, som er baseret på enorme mængder data, som kan være placeret på forskellige fysiske lokationer, så er kravene til infrastruktur og forbindelse mellem servere i disse systemer kritiske[37].

Overordnet set er en trussel som "*Big Data Breach*" og "*Big Data Leak*"[38] de mest interessante, når det kommer til digital persondatabehandling. Generelt forekommer et databrud, når digital information bliver stjålet af angribere, som bryder ind i et system eller netværk, hvor informationen er tilgængelig. Dermed kan vi definere et "Big Data Breach", som et brud hvor der, gennem et indbrud i systemet eller netværket, er blevet stjålet et Big Data aktiv. Modsat, er et "Big Data Leak" den totale eller delvise offentliggørelse af et Big Data aktiv. Et "Big Data Leak" kan forekomme som konsekvens af forskellige årsager, for eksempel utilstrækkeligt design eller procedurefejl. "Big Data Breach" kræver onde hensigter, hvorimod "Big Data Leak" kan udnyttes af godsindede og ærlige mennesker[39].

Grundet de enorme mængder data der bliver behandlet i disse avancerede og komplekse systemer, og den stigende trussel disse systemer står overfor, er kravet om høj IT-sikkerhed skærpet. Generelt, da Big Data er en avanceret samling af datainput fra forskellige kanaler fra forskellige systemer og netværk, og dataoutput til forskellige brugere, er ansvaret for IT-sikkerheden delt. De forskellige parter bør, på baggrund af deres involvering, tage stilling til infrastruktur og sikkerhed, og hvordan man kan

[36] UMBEL (2015): "*AI meets Big Data*", side 7-9.
[37] ENISA (2016): "*Big Data Threat Landscape and Good Practice guide*", side 18
[38] ENISA (2016): "*Big Data Threat Landscape and Good Practice guide*", side 18
[39] ENISA (2016): "*Big Data Threat Landscape and Good Practice guide*", side 18.

sikre, at alle involverede parters interesser er beskyttet. Der eksisterer flere "best practice" kontrolsystemer på IT-sikkerhedsområdet, som for eksempel ISO og COBIT, udover en række andre foranstaltninger, som kan træffes for at sikre sig mod trusler. Disse foranstaltninger vil blive belyst yderligere i afsnit 6.6 om "sikkerhed"[40].

[40] ENISA (2016): "*Big Data Threat Landscape and Good Practice guide*", side 32.

5.6. Juridisk anvendelse af kunstig intelligens

I kapitel 4 er kunstig intelligens blevet beskrevet og defineret ud fra en teknisk betragtning. Det har modsat ikke været muligt at finde en bindende juridisk definition af kunstig intelligens. Som tidligere beskrevet er persondataforordningen teknologineutral, jf. præambelbetragtning 15[41]. Der eksisterer således ikke en lovgivning, der helt konkret regulerer anvendelsen af kunstig intelligens, eller definerer hvordan kunstig intelligens bør anvendes ud fra et retligt synspunkt.

På baggrund af dette, vil kunstig intelligens i det følgende blive anvendt som værende udelukkende et teknologisk koncept, som ikke er defineret ud fra et retligt perspektiv.

[41] EU forordning 2016/679, præambel 15.

6. De grundlæggende principper i artikel 5

Et af de helt grundlæggende persondataretlige principper og omdrejningspunkter i persondataforordningen er ansvarlighed ("accountability"), hvilket forudsætter, at den dataansvarlige skal være loyal overfor forordningen og efterleve dette krav. Persondataforordningens artikel 5 indeholder en række bestemmelser, som skaber det grundlæggende fundament for persondatabehandlingers lovlighed, og dermed angiver de generelle rammer for dataansvarliges virksomhed[42]. Med afsæt i kapitel 5, som definerede kunstig intelligens ud fra en teknisk betragtning, står anvendere og udviklere overfor en svær øvelse ved implementeringen af persondataforordningen. Det er ikke længere nok at have styr på hvornår man har ret til at behandle personoplysninger, nu skal virksomheder også kunne dokumentere, at oplysninger bliver behandlet med integritet og ansvarlighed. Disse krav er nye og omfattende, og betyder for udviklere og anvendere af kunstig intelligens, at man skal have styr på regelefterlevelsen, da den skal tænkes ind i systemerne og netværkene fra udviklingsfasen.

I det følgende vil princippet om lovlighed, rimelighed og gennemsigtighed indledningsvist blive gennemgået, herefter følgeder de yderligere principper i persondataforordningens artikel 5.

6.1. God databehandlingsskik

Det fremgår af persondataforordningens artikel 5, stk. 1, litra a, at persondatabehandlingen skal være lovlig, rimelig og gennemsigtig, hvilket tidligere blev kategoriseret som god databehandlingsskik.

At en persondatabehandling skal være lovlig, betyder at der i lovgivningen skal være hjemlet en ret til at behandle personoplysninger. Forordningen muliggør således ikke persondatabehandling, hvis behandlingen strider i mod en præceptiv regel i anden lovgivning – national eller international[43]. Med kravet om lovlighed henvises der direkte til forordningens regler i artikel 5 og 6, hvilke danner det retlige fundament for lovlig persondatabehandling.

Reglen om, at al persondatabehandling skal være rimelig, indebærer en overensstemmelse med den "ånd", der udtrykker forordningens beskyttelsesinteresse. På trods af, at en persondatabehandling er

[42] Blume, Peter (2018) "*Den nye Persondataret*", side 85.
[43] Blume, Peter (2018) "*Den nye Persondataret*", side 85.

i overensstemmelse med forordningens øvrige regler, så udgør bestemmelsen om rimelighed en generalklausul, hvilket gør det muligt for tilsynet at afvise denne persondatabehandling[44].
Der er således tale om en skønsafvejning, hvori det er fremgår, at en persondatabehandling ikke nødvendigvis er rimelig, selvom den efterlever forordningens øvrige bestemmelser. Herudover fremgår det af forordningens præambelbetragtning 39, at de registreredes rettigheder og interesser bør iagttages, for at princippet om lovlighed og rimelighed kan være overholdt[45]. Eksempelvis at der ud fra en rimelighedsvurdering, skal laves en formålsspecifikation, således den dataansvarlige og/eller databehandleren har iagttaget sin oplysningspligt, og den registrerede dermed ved, med hvilket formål oplysningerne bliver brugt.

Når dataansvarlige og/eller databehandlere anvender kunstig intelligens i forbindelse med behandling af persondata, er det således helt fundamentalt, at den registrerede kan få oplyst, hvilke data der bliver behandlet og med hvilket formål. I et så komplekst værktøj som kunstig intelligens, der har evnen til at blive klogere og klogere jo mere datainput den får, kan det være en udfordring at iagttage disse principper. Der opstår en praktisk udfordring i, at det er den dataansvarlige og/eller databehandleren, som har pligten til at oplyse den registrerede, men det er den kunstige intelligens som udfører selve persondatabehandlingen. I takt med at den kunstige intelligens får flere og flere datainput og bliver klogere, opstår chancen for at forskellige datasæt vil blive anvendt til forskellige formål, hvilket i sagens natur er et problem og ikke i tråd med forordningens principper. Dette vil blive uddybet yderligere i afsnit 6.3 om "Formålsbestemthed".

Betragter man herudover andet afsnit i forordningens præambel 71, så fremgår det, at "*for at sikre rimelig behandling, bør den dataansvarlige anvende passende matematiske eller statistiske procedurer… der tager højde for de potentielle risici for den registreredes rettigheder og interesser, og som hindrer blandt andet forskelsbehandling af fysiske personer på grund af race eller etnisk oprindelse, politisk, religiøst…*[46]". Det er afgørende, at den dataansvarlige har indrettet sig tilstrækkeligt sikkert, således der ikke bliver truffet diskriminerende og ukorrekte automatiske afgørelser. Dette stiller yderligere krav til hvordan man indretter sin kunstig intelligens, og hvilket output man forventer at få, baseret på de datainputs man giver sin kunstig intelligens. Det er således en forudsætning for at den

[44] Blume, Peter (2018) "*Den nye Persondataret*", side 85.
[45] EU-forordning 2016/679, præambel 39.
[46] EU-forordning 2016/679, præambel 71.

kunstige intelligens ikke kommer med diskriminerende og usaglige outputs, at den er bygget op på et rimeligt datagrundlag. Dette vil blive uddybet yderligere i afsnit 7.3.3 om "Retfærdighed".

Gennemsigtighed fremstår som et centralt element i artikel 5, stk. 1, litra a. Kravet om gennemsigtig skal gøre det muligt for den registrerede at overskue den persondatabehandling som finder sted[47]. Det følger af henholdsvis præambelbetragtning 39 og artikel 12, stk. 1, at enhver meddelelse eller oplysning om behandlingen skal være i en "*kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og enkelt sprog*[48]". Det er klart, at hvis man har med en højt avanceret og meget kompleks kunstig intelligens at gøre, så kan det være problematisk at sikre gennemsigtighed i sin oplysning til den registrerede. Der er ikke faste rammer for, hvordan en sådan kommunikation skal ske. Det er op til den enkelte dataansvarlig at tilrettelægge en formidlingsstrategi, og her er det af afgørende betydning for anvendere af kunstig intelligens, at man har indrettet sin model således, at man har mulighed for at spore daten, og at datakvaliteten ligeledes er sikret. Dette vil blive uddybet yderligere i afsnit 7.3.2 om "Gennemsigtighed".

Princippet om lovlighed, rimelighed og gennemsigtighed kan betragtes som et overordnet princip der skal iagttages, og som de øvrige principper, som fx formålsbestemthed og datakvalitet, understøtter og konkretiserer. Derfor vil princippet lovlighed, rimelighed og gennemsigtighed også nødvendigvis være indeholdt i den følgende analyse, da de er yderst relevante og uomtvistelige.

[47] Blume, Peter (2018) "*Den nye Persondataret*", side 86.
[48] Blume, Peter (2018) "*Den nye Persondataret*", side 86.

6.2. Saglighed

I persondataforordningens artikel 5, stk. 1, litra b fremgår det, at personoplysninger kun må indsamles til fastslåede og legitime (saglige) formål. Det skal således være klart for den registrerede, hvorfor hans eller hendes oplysninger er blevet indsamlet og formålet skal være sagligt begrundet. Artikel 5, stk. 1, litra b har til formål at skabe transparens ved behandlingen af data, og herved opstår den omstændighed, at formålet skal være eksplicit formuleret til den registrerede, hvilket også følger af oplysningspligten i artikel 13 og 14. Dette krav fungerer som en sikring, således den registrerede er i stand til at påberåbe sig sine rettigheder, i tilfælde af, at kravet ikke overholdes[49].

6.2.1 Formålsbestemthedsprincippet

Ved fastsættelsen af formålsbestemthedsprincippet, sikrer artikel 5, stk. 1, litra b, at indsamlede oplysninger, på et senere tidspunkt efter indsamlingen, ikke må anvendes til andre formål, end det der var indsamlingsformålet. Betragter man ordlyden i artikel 5, stk. 1, litra b, så fremgår det at, der ikke opstilles krav om, at formålet med en ny anvendelse af oplysningerne skal være foreneligt med indsamlingsformålet. Kravet ligger derimod i, at formålet med en ny anvendelse ikke må være uforeneligt med indsamlingsformålet, hvilket alt andet lige, pålægger den dataansvarlige et mindre restriktivt bånd. I forbindelse med den teknologiske udvikling og praksissen omkring Big Data, som tidligere beskrevet, forekommer dette at medføre en smidig praksis i relation til databehandling. Princippet kan dog fortsat vise sig, at være vanskeligt at benytte i praksis, da det fortsat pålægges den dataansvarlige klart at udtrykke overfor den registrerede, at formålet ikke er uforeneligt med indsamlingsformålet[50].

I det følgende vil der blive kigget dybere ned i lovgivningen, idet udvalgte elementer fra bestemmelsen i artikel 5, stk. 1, litra b vil blive nærmere analyseret. Der søges at tilvejebringe en forståelse af de enkelte led i bestemmelsen, som er indeholdt i det overordnede princip om formålsbestemthed.

6.2.1.1 Udtrykkeligt angivne formål

Artikel 5, stk. 1, litra b lyder: "[*Personoplysninger skal]indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling*

[49] Blume, Peter (2018) "*Den nye Persondataret*", side 86.
[50] Blume, Peter (2018) "*Den nye Persondataret*", side 87.

til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål[51]". Ved at bruge betegnelsen "*udtrykkelig*" fastslås det, at formålet med behandlingen skal være klar og tydelig, og klart og tydeligt formuleret til den registrerede, som beskrevet i kapitel 6.2. Udtrykkelighedsbetragtningen er et centralt element persondataforordningen i forbindelse med persondatabehandling, og det er afgørende, at den dataansvarlige kun indsamler data, som er nødvendigt, tilstrækkeligt og relevant for formålet[52].

Formålet med databehandlingen skal være 'udtrykkeligt angivet' til den registrerede, inden selve databehandlingen finder sted. Det skal være klart, tydeligt og detaljeret nok til, at den registrerede kan identificere, hvilken form for databehandling der er, og ikke er, indeholdt i formålet. Udtryk som "marketingsformål" eller "IT-sikkerhedsmæssige formål" betragtes ikke som værende detaljeret nok, da de ikke udtrykkeligt angiver med hvilket formål databehandlingen finder sted, og den registrerede når således ikke indsigt i, hvilke data der behandles og i hvilket omfang. Som tidligere beskrevet, er gennemsigtighed et afgørende princip i persondataforordningen. Gennemsigtighed og forudsigelighed er nøgleprincipperne bag kravet om de 'udtrykkeligt angivne formål'. Det tillader utvetydig identifikation af databehandlingen og grænserne for, hvad dataansvarlige må anvende registreredes data til. Dette krav fungerer som et sikkerhedsnet for, at de registrerede kan træffe beslutninger på et oplyste grundlag, og ikke får deres oplysninger krænket eller misbrugt[53].

Kravet om det 'udtrykkeligt angivne formål' kan vise sig problematisk for anvendere og udviklere af kunstig intelligens. Med afsæt i kapitel 5.3, hvor det beskrives hvordan avancerede kunstig intelligens modeller og algoritmer kan opbygges, står dataansvarlige overfor en potentiel umulig opgave, da det er deres opgave som dataansvarlige 'udtrykkeligt at angive formålet' med databehandlingen, men hvor det er den kunstige intelligens som rent faktisk behandler og bruger dataen. problematikken afhænger af valget af kunstig intelligens form. Som beskrevet i afsnit 5.3 om "deep learning" og afsnit 5.3.2 om "neurale netværk", så indeholder disse modeller ofte enorme og komplekse mængder af beslutningslag, hvilket besværliggør muligheden for transparens for den registrerede. Som tidligere beskrevet er kunstig intelligens af denne karakter også i stand til at lære selv, i takt med at den

[51] EU-forordning 2016/679, artikel 5, stk. 1, litra b.
[52] Article 29 Data Protection Working Party (2013): "*Opinion 03/2013 on purpose limitation*", side 15.
[53] Article 29 Data Protection Working Party (2013): "*Opinion 03/2013 on purpose limitation*", side 16-17.

anvender dataen i sine beslutningsprocesser. Dette gør muligheden for transparens endnu vanskeligere, da den kunstige intelligens model i disse tilfælde vil kunne anvende dataen til forskellige formål, da den konstruerer nye regler og beslutninger baseret på datainput og anvendelse.

Som præsenteret længere oppe, står formuleringer som "marketingsformål" eller "IT-sikkerhedsmæssige formål" ikke mål med forordningens krav til udtrykkelighed. Det samme vil gøre sig gældende for formuleringer som "kunstig intelligens-relaterede formål". Formålsspecifikationen skal være skarp og tydelig, da det overordnede princip om gennemsigtighed skal iagttages i henhold til artikel 5, stk. 1, litra a. Det afgørende er, at den dataansvarlige er i stand til at formulere et formål med databehandlingen, der er tilstrækkeligt præcist, så den registrerede kan gennemskue hvilken behandling der vil finde sted på baggrund af det formål. Derudover fremgår det af side 17 i "*opinon 03/2013 on limitation purpose*" præsenteret af Article 29 Data Protection Working Party, at formålet skal være formuleret således, at den dataansvarlige og den registrerede opnår en fælles forståelse af, hvad dataen skal bruges til[54]. Ud fra denne betragtning må det kunne udledes, at udtrykkeligheden af formålsspecifikationen må bero på en konkret vurdering af den enkelte situation. Som udgangspunkt må det forventes, at den dataansvarlige er i stand til udtrykkeligt at angive med hvilket formål en kunstig intelligens model behandler persondata og, hvis relevant, hvad modellen forventes at lære eller hvordan den forventes at udvikle sig. Derimod synes det meget sandsynligt, at dataansvarlige og anvendere af komplekse kunstig intelligens modeller på tidligere stadier i udviklingsfasen, ikke nødvendigvis er i stand til at forudse, hvilke beslutninger eller resultater en algoritme vil nå frem til.

6.2.1.2 Legitime formål

Uddrag af artikel 5, stk. 1, litra b lyder: "[*Personoplysninger skal] indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; …*[55]". Betegnelsen "*legitim*" må betragtes som værende en bred formulering af krav. Legitimitetskravet relaterer sig til artikel 6 i persondataforordningen, som lister 6 kriterier for legitim behandling af personoplysninger, og for overholdelse af legitimitetskravet, skal et formål således være baseret på mindst ét af de 6 kriterier. Kravet om legitimitet strækker sig længere end blot bestemmelserne i artikel 6. Det er således indeholdt i bestemmelsen i artikel 5, stk. 1, litra b, at formål skal være i overensstemmelse med reglerne i GDPR og anden relevant lovgivning. Legitimitetskravet betyder

[54] Article 29 Data Protection Working Party (2013): "*Opinion 03/2013 on purpose limitation*", side 17.
[55] EU forordning 2016/679, artikel 5, stk. 1, litra b.

derfor, at formål skal være i overensstemmelse med lovgivningen, hvilket fortolkes bredt, da der udover anden relevant lovgivning, også refereres til retspraksis, bekendtgørelser, guidelines, best practice og lignende. Betegnelsen "legitim" indeholder således en, ikke kun lovlig, men også saglig og velbegrundet redegørelse for hvad formålet med databehandlingen er[56].

6.2.1.3 Uforenelige formål

Uddrag af artikel 5, stk. 1, litra b lyder: *"[Personoplysninger skal] indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; …*[57]". Betegnelsen "*uforenelige*" henviser til den formålsbegrænsning der er indbygget i litra b. Denne betragtning udføres på baggrund af en vurdering af formålenes forenelighed. Som tidligere beskrevet eksisterer der ikke et eksplicit krav om, at viderebehandling af data skal følge de samme forenelige formål, de må blot ikke være uforenelige. Indledningsvist vil betegnelsen "*viderebehandling*", for forståelighedens skyld, blive belyst yderligere i det følgende.
Ved forordningens indførsel af kravet om formålsbegrænsning, refereres der ikke specifikt til databehandlingen til det 'oprindeligt udtrykte formål' og databehandlingen til 'formål defineret efterfølgende'. Kravet om formålsbegrænsning differentierer mellem den første databehandling, som er dataindsamling, og alle efterfølgende behandlinger, som eksempelvis opbevaring[58].

Som tidligere beskrevet, er formålsbegrænsningen i artikel 5, stk.1, litra b udtrykt således, at der ikke eksisterer et eksplicit krav om forenelighed. Lovgiver har i stedet valgt at udtrykke kravet således, at viderebehandlingsformålet ikke må være uforeneligt med indsamlingsformålet. Ved på denne måde at hjemle viderebehandling, så længe det ikke er uforeneligt med indsamlingsformålet, og i øvrigt ikke forbryder sig med anden lovgivning eller retspraksis, har lovgiver indarbejdet ekstra fleksibilitet ind i bestemmelsen. Viderebehandling kan i disse tilfælde være tæt forbundet med det oprindelige formål, eller det kan være et helt andet. Med denne formulering af kravet i bestemmelsen, er det ikke entydigt, at et helt nyt formål på forhånd antages at være uforeneligt. Dette må i stedet bero på en konkret vurdering. Denne fleksibilitet kan imidlertid vise sig relevant, da den tillader ændring et fokus i forbindelse med databehandlingen i tilfælde af situationer, hvor forventninger til hvad dataen skal anvendes til, har ændret sig. Som databehandlingen udvikler sig, er det ikke utænkeligt, at

[56] Article 29 Data Protection Working Party (2013): "*Opinion 03/2013 on purpose limitation*", side 19-20.
[57] EU-forordning 2016/679, artikel 5, stk. 1, litra b.
[58] Article 29 Data Protection Working Party (2013): "*Opinion 03/2013 on purpose limitation*", side 21.

formålsbetragtningen kan skifte og bevæge sig i en retning, hvor hverken den dataansvarlige eller den registrerede havde forventet at behandlingen skulle bevæge sig hen. Det kan tværtimod ofte vise sig relevant, for det forventede dataoutput, at databehandlingen skifter fokus eller retning. I sådanne situationer skal der foretages en konkret forenelighedsvurdering af formålene[59].

Baseres en databehandling på samtykke eller på lovhjemmel i enten EU,- eller national ret er det ikke muligt at behandle dataen til andre formål, end det der udtrykkeligt er givet lov til, enten via samtykke eller lovgivning. Afviges der fra det oprindelige formål, skal viderebehandling af dataen være baseret på et nyt indsamlet samtykke eller på et nyt retligt grundlag. På samme måde kan fravigelse af uforenelighedskravet også ske ved indhentning af samtykke eller hvis baseret på et retligt grundlag. Disse undtagelser forekommer ret vidtgående. Sammenholdt med reglerne i persondataforordningens præambelbetragtning 50, hvor der ved indhentelse af nyt samtykke i forbindelse med viderebehandling, ikke er krav om forenelighed med tidligere formål, kan det diskuteres, hvorvidt princippet om formålsbestemthed elimineres[60] [61].

I tilfælde hvor personoplysninger viderebehandles i forbindelse med udvikling af kunstig intelligens, vil det ikke altid være på baggrund af det det oprindelige indsamlingsformål og således være i strid med princippet om formålsbegrænsning. Ofte er opgaven for anvendere og udviklere af kunstig intelligens, at automatisere en allerede eksisterende proces, og i disse tilfælde er det sikkert at antage, at tidligere indsamlet data vil blive anvendt. For at foretage en viderebehandling, hvis formål ikke er foreneligt med det oprindelige, og hvor det retlige grundlag ikke er baseret på samtykke eller EU, - eller national ret, skal persondataforordningens artikel 6, stk. 4 iagttages. Der er ligeledes indbygget en undtagelse til princippet om formålsbestemthed i artikel 5, stk. 1, litra b, hvilken gennemgås i kapitel 6.2.1.4. Artikel 6, stk. 4 fremstiller en række vurderingskriterier, der gør det muligt for anvendere af kunstig intelligens at foretage en viderebehandling baseret på et nyt formål. Der er tale om 5 kriterier i artikel 6, stk. 4, litra a - e, som skal betragtes ud fra en helhed. Det kan vise sig yderst vanskeligt for anvendere af kunstig intelligens, at skulle påvise tæt forbindelse mellem indsamlingsformålet og det nye formål, som er kravet i litra a. Ikke desto mindre kan det lade sig gøre, hvis anvenderne har brugt mindre komplekse modeller, som bruges indenfor blandt andet machine

[59] Article 29 Data Protection Working Party (2013): "*Opinion 03/2013 on purpose limitation*", side 21.
[60] Blume, Peter (2018) "*Den nye Persondataret*", side 88.
[61] EU-forordning 2016/679, præambel 50.

learning teknologier. Her er det således muligt at kende den data, som maskinen eller modellen er blevet fodret med, og som den skal lære af og træffe beslutninger ud fra. Omvendt kan efterlevelse af kriterierne i litra a – e vise sig vanskeligt, hvis der anvendes modeller og algoritmer, som er baseret på deep learning teknologier[62].

Kriterierne i litra d og e omhandler potentielle konsekvenser for den registrerede, og de foranstaltninger som den dataansvarlige bør træffe i forbindelse med databehandlingen, de kan således betragtes i fællesskab. Indledningsvist må det antages, at 'viderebehandlingens mulige konsekvenser for den registrerede' skal fortolkes bredt, da det må bero på en konkret vurdering af den enkelte situation, hvorvidt der kan være tale om mulige konsekvenser. Afhængig af hvor komplicerede modeller og teknologier anvendere af kunstig intelligens gør brug af, kan der imidlertid opstå konsekvenser, som har kompromitterer den registreredes retssikkerhed. Kan behandlingen af personoplysninger eksempelvis karakteriseres som automatisk, finder artikel 22 i persondataforordningen anvendelse. Automatiske afgørelser vil blive yderligere behandlet i afsnit 7.1. Ligeledes har princippet om gennemsigtighed og transparens afgørende betydning for valget af teknologi. Anvendes deep learning modeller, er langt fra tænkeligt, at den registrerede kan få indsigt i, hvorledes dataen bliver brugt[63].

I litra e er kryptering og pseudonymisering nævnt som potentielle sikkerhedsforanstaltninger, men som med de mulige konsekvenser for den registrerede, må dette også bero på konkrette vurderinger, hvorvidt disse foranstaltninger er anvendelige i den givne databehandling. I relation til kunstig intelligens og med hvilket fokus disse modeller anvendes og udvikles, er foranstaltninger, som kryptering og i særdeleshed pseudonymisering, oplagte værktøjer at anvende. Afhængig af valget af model, er det ofte irrelevant for det output eller resultat, der forventes at opnå, hvorvidt dataen er pseudonymiseret eller ej. Navne eller CPR-numre har ingen betydning for en model eller algoritme som træffer beslutninger og når frem til resultater på baggrund af mønstre og variabler. Ud fra disse betragtninger må det antages, at en undladelse af pseudonymisering kraftigt peger i retning af en tilsidesættelse af bestemmelsen i litra e, og dermed også tilsidesætter kravet om forenelighed mellem indsamlingsformålet og viderebehandlingsformålet. Persondataforordningens artikel 6, stk. 4 præsenter således en række viderebehandlingsmuligheder for kunstig intelligens anvendere, da formål, som oplæring af

[62] EU-forordning 2016/679, artikel 6, stk. 4, litra a – e.
[63] EU-forordning 2016/679, artikel 6, stk. 4, litra d – e.

kunstig intelligens modeller, ikke, ud fra disse betragtninger, nødvendigvis er uforenelige med indsamlingsformålet[64].

Databeskyttelsesloven er ikke indeholdt i omfanget af dette speciale, dog findes det relevante i denne sammenhæng at referere til lovens § 5, stk. 3, hvor i der præsenteres en mulighed for at offentlige dataansvarlige må viderebehandle personoplysninger til formål, som er uforenelige med indsamlingsformålet. Offentlige dataansvarlige er via § 5, stk. 3 i databeskyttelsesloven, således ikke pålagt at iagttage princippet om formålsbegrænsning i artikel 13 og 14. Dette er relevant at inddrage, da dette åbner for myndighedernes mulighed for fri opbevaring af persondata og automatisering af persondatabehandlingen[65].

6.2.1.4 Undtagelser til formålsbegrænsningen

Artikel 5, stk. 1, litra b lyder: [*Personoplysninger skal] indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål*[66]". Som beskrevet i kapitel 5.2.13, er der indbygget en undtagelse til reglen om formålsbestemthed direkte i bestemmelsen, og denne præsenterer 4 formål, som ikke skal iagttage dette krav. Denne adgang til at behandle oplysninger til andet formål end oprindelige, gælder således for formål i (1) samfundets interesse, (2) til videnskabelige forskningsformål, (3) historiske forskningsformål, og (4) statistiske formål. Denne bestemmelse tilvejebringer større fleksibilitet, især med henblik på datadeling i den offentlige forvaltning. I relation til kunstig intelligens er arkivformål i samfundets interesse og historiske forskningsformål, ikke af nær tilknytning, hvorfor der vil blive fokuseret på de videnskabelige og statiske formål. Denne del af artikel 5, stk. 1, litra b, skal sammenholdes med relevante præambelbetragtninger[67].

Det fremgår af præambelbetragtning 157, at: " *For at fremme videnskabelig forskning kan personoplysninger behandles til videnskabelige forskningsformål under iagttagelse af passende betingelser og*

[64] EU-forordning 2016/679, artikel 6, stk. 4, litra e.
[65] Blume, Peter (2018) "*Den nye Persondataret*", side 89.
[66] EU-forordning 2016/679, artikel 5, stk. 1, litra b.
[67] Article 29 Data Protection Working Party (2013): "*Opinion 03/2013 on purpose limitation*", side 28.

garantier i EU-retten eller medlemsstaternes nationale ret[68]". Hvorvidt kunstig intelligens og udvikling af modeller og teknologi kan betegnes som 'videnskabelig forskning', fremgår ikke entydigt persondataforordningen, og det må i stedet bero på konkrete vurderinger. Det fremgår imidlertid af præambelbetragtning 159, at: "*Behandlingen af personoplysninger til videnskabelige forskningsformål bør med henblik på denne forordning fortolkes bredt og f.eks. omfatte teknologisk udvikling og demonstration, grundforskning, anvendt forskning og privat finansieret forskning*[69]". Anvendere og udviklere af kunstig intelligens vil argumentere for, at deres innovative tilgang til læring og databrug, vil kunne betegnes som værende videnskabelig forskning. I forlængelse af dette, lyder præambelbetragtning 33 som følgende: "*Det er ofte ikke muligt fuldt ud at fastlægge formålet med behandling af personoplysninger til videnskabelige forskningsformål, når oplysninger indsamles. De registrerede bør derfor kunne give deres samtykke til bestemte videnskabelige forskningsområder, når dette er i overensstemmelse med anerkendte etiske standarder for videnskabelig forskning. Registrerede bør have mulighed for kun at give deres samtykke til bestemte forskningsområder eller dele af forskningsprojekter i det omfang, det tilsigtede formål tillader det*[70]". Betragtes denne udvikling af kunstig intelligens som værende videnskabelig forskning, fremgår det således af præambelbetragtning 33, at der hersker en relativt stor frihed til at angive formål i forbindelse med viderebehandling af personoplysninger.[71]

Det andet formål til viderebehandling, som i artikel 5, stk. 1, litra b er undtaget kravet om foreneliged, og som har tilknytning til kunstig intelligens, er viderebehandling anvendt til statistiske formål. En definition af statistiske formål fremgår af præambelbetragtning 162, at: "*Ved statistiske formål forstås enhver indsamling og behandlingen af personoplysninger, der er nødvendig for statistiske undersøgelser eller frembringelse af statistiske resultater*[72]". Derudover fremgår det af præambelbetragtningen, at de resultater som opnås kan viderebehandles til forskellige formål. Dog må de statistiske data, som skaber resultaterne ikke være personoplysninger, men derimod skal være aggregerede data. Herudover fremgår af det af artikel 89, stk. 1, at der skal være truffet tekniske og organisatoriske foranstaltninger for overholdelse af princippet om dataminimering. Det er dermed afgørende, at anvendere og udviklere af kunstig intelligens kun indsamler den mængde data, som de skal

[68] EU-forordning 2016/679, præambel 157.
[69] EU-forordning 2016/679, præambel 159.
[70] EU-forordning 2016/679, præambel 33.
[71] Article 29 Data Protection Working Party (2013): "*Opinion 03/2013 on purpose limitation*", side 28
[72] EU-forordning 2016/679, præambel 162.

bruge for at opnå deres formål. I forbindelse med anvendelse af kunstig intelligens, hvor modeller fodres med data med henblik på at lære eller træffe beslutninger på baggrund af mønstre, er det afgørende at dataen ikke kan henføres til individuelle personer. Pseudonymisering var eksplicit nævnt som en foranstaltning i artikel 89, stk. 1, hvilket som tidligere beskrevet ikke nødvendigvis begrænser kunstig intelligens udviklingen, og samtidig garanterer den registreredes retssikkerhed[73].

Kunstig intelligens modeller eller teknologier der betegnes som værende statistisk behandling, kan således, såfremt fornødne garantier og foranstaltninger er truffet og personoplysningerne er aggregeret, for eksempel ved hjælp af pseudonymisering, viderebehandles på baggrund af et formål, som ikke behøver at være foreneligt med indsamlingsformålet. Ligeledes gælder det for kunstig intelligens, der kan karakteriseres som videnskabelig forskning, at der er mulighed for at viderebehandle data på baggrund af et formål, som ikke nødvendigvis er foreneligt med indsamlingsformålet, da der ved videnskabelige ikke er samme krav til formålsspecifikation, som beskrevet ovenfor.
Kunstig intelligens anvendelse er således ikke nødvendigvis begrænset af disse bestemmelser, og derudover kan de, ud fra en konkret vurdering, blive undtaget fra kravet om forenelighed efter reglerne i sidste halvdel af artikel 5, stk. 1, litra b.

[73] EU-forordning 2016/679, artikel 89, stk. 1.

6.3. Princippet om dataminimering

Persondataforordningens artikel 5, stk. 1, litra c præsenterer en række væsentlige principper, der overordnet betegnes som princippet om 'dataminimering'. Bestemmelsen kræver, at der kun indsamles den mængde data, der er nødvendigt for at opnå formålet med databehandlingen. Det fremgår ikke af bestemmelsen, i hvilke situationer dette krav gøres gældende. Dataindsamlingen betragtes som værende den tidligste behandling af personoplysninger, og derfor fortolkes bestemmende således, at kravet gøres gældende allerede ved indsamlingen af personoplysninger. Kravet kan således betragtes som absolut, og dataansvarlige må dermed ikke indsamle eller være i besiddelse af personoplysninger, hvis ikke kravet om dataminimering efterleves. Det pålægges den dataansvarlige at udvise og udøve disciplin, og ikke indsamle ikke data, som 'måske kan være til nytte', men som ikke er nødvendige, for at opnå formålet med databehandlingen[74].

Som beskrevet indledningsvist, er de 3 væsentlige principper indeholdt i bestemmelsen; tilstrækkelighed, relevans og begrænsning. I relation til artikel 5, stk. 1, litra c, fremgår disse 3 begreber ikke af forordningens definitionsliste i artikel 4, og derfor vil de blive gennemgået med udgangspunkt i retslitteraturen. '*Tilstrækkelighed*' er et udtryk for, at der ikke må indsamles flere oplysninger, end dem der er nødvendige for at opnå formålet med databehandlingen. Der refereres til den datamængde, der indsamles for at opfylde formålet i forbindelse med behandlingen. Er den indsamlede data ikke tilstrækkelig, efterleves kravet ikke, og dataen må dermed ikke behandles. Selv i konkrete tilfælde hvor overskydende oplysninger findes relevante, gælder det tilstrækkelighedskravet, og den overskydende data skal slettes, således der ikke sker en dataophobning. '*Relevans*' dækker over, at dataen skal være væsentlig og nødvendig for at opnå formålet med databehandlingen. Kravet om, at personoplysningerne skal have relevans for formålet, kan ligeledes tolkes omvendt, således at det sikres, at al data, som er irrelevant for formålet, ikke indsamles. Denne fortolkning bidrager til en anskueliggørelse af processen, da det må antages at være åbenbart lettere at identificere, når data er irrelevant for den behandlingsproces en dataansvarlig står overfor. Ligeledes har denne fortolkning positiv praktisk betydning, da det må antages at der kun foretages dataindsamling som har værdi for en behandling, og der således ikke søges at indsamle data, som er irrelevant og ingen værdi har for behandlingen. I relation til kunstig intelligens gør dette sig ligeledes gældende. Ved udarbejdes af modeller af forskellig art, er formålet af træffe korrekte beslutninger og opnå korrekte resultater, hvorfor

[74] Blume, Peter (2018) "*Den nye Persondataret*", side 91.

datagrundlaget nødvendigvis skal have relevans og være korrekt. '*Begrænsning*' er på samme måde som '*tiltrækkelighed*' et udtryk for, at den mængde data der indsamles til begrænses til et minimum, således der kun indsamles den data, der er nødvendig for at opnå formålet. Denne betegnelse relaterer sig ligeledes til begrebet om dataophobning, hvor dataansvarlige ikke har ret til at indsamle og opbevare data, blot fordi dataen måske kan være til nytte[75].

Bestemmelsen skal herudover ses i relation til kravet om rimelighed i artikel 5, stk. 1, litra a, hvorfor det således, ud fra en minimeringsbetragtning, er pålagt den dataansvarlige at vurdere, hvorvidt anvendelse af direkte personhenførbare data er nødvendigt for opnåelse af formålet. Det fremgår implicit af bestemmelsen, at der skal tages stilling til, om der kan anvendes pseudonymisering, hvilket vil skjule de personhenførbare oplysninger, men samtidig ikke nødvendigvis begrænser kunstig intelligens modeller i deres lærings, - og beslutningsproces[76].

6.3.1 Dataminimering og kunstig intelligens

Princippet om dataminimering, som beskrevet ovenfor, stiller store krav til, at de oplysninger der indsamles, skal være tilstrækkelige, relevante og begrænset til, at opnå det formål de behandles for. Brugen og udviklingen af kunstig intelligens kræver imidlertid en betragtelig mængde oplysninger, og ofte personoplysninger, hvis modellerne skal være i stand til at træffe mest korrekte beslutninger, og opnå de bedste resultater. Bestemmelsen om dataminimering sikrer dog den registrerede ved, at dataansvarlige ikke kan indsamle og behandle personoplysninger, som ikke er nødvendige og relevante for opnåelse af formålet.

Indeholdt i dataminimeringsprincippet, gælder der også et 'proportionalitetsprincip'. Dataminimering er således ikke blot et begreb, der udtrykker databegrænsning, men også, at der skal være en sammenhæng mellem den data man indsamler, og indsamlingsformålet. For anvendere og udviklere af kunstig intelligens kan det være fristende, at indsamle store mængder data, eksempelvis i forbindelse med teknologien 'Big Data' der, som beskrevet i kapitel 5.5, er en stor og kompleks dataindsamling, med henblik på at kunstig intelligens modellerne, skal lære af sig selv. Af denne årsag har proportionalitetsprincippet stor betydning, da det tilsigtes at foretage et minimum af indgreb overfor den registrerede. Det pålægges således den dataansvarlige at begrænse graden af identifikation i

[75] Blume, Peter (2018) "*Den nye Persondataret*", side 91 – 92.
[76] Blume, Peter (2018) "*Den nye Persondataret*", side 92.

oplysningerne. Dette kan gøres både ved at begrænse mængden af oplysninger der bruges, og begrænse hvilke oplysninger der bruges[77].

En af de yderligere udfordringer kunstig intelligens står overfor i relation til bestemmelsen i artikel 5, stk. 1, litra c, er formuleringen: "*…hvad der er nødvendigt i forhold til de formål, hvortil de behandles*[78]". Denne formulering præsenterer kravet om, at det inden dataindsamlingen skal være identificeret, hvad dataen skal bruges til. Udviklere og anvendere af kunstig intelligens ved på tidligere stadier ikke altid hvad deres output af modellerne bliver, og derfor kan det således ikke forudses, hvilket datainput der er nødvendigt i de tidligere stadier. Som tidligere beskrevet, er kunstig intelligens i mange tilfælde bygget op omkring enorme mængder data, hvorudfra en model eller algoritme vil være i stand til at se mønstre i, eksempelvis, adfærd. Det interessante i forhold til dataminimering og kunstig intelligens, består i, at hvis en algoritme, baseret på offline kunstig intelligens, skal foretage en konkret beslutning om, hvor registrerede vælger at bosætte sig, baseret på indkomstdata. Her er der tale om simple statistiske data, som nødvendigvis uden udfordringer kan være definerede på forhånd og således iagttage alle krav. Er der imidlertid tale om en mere avanceret model, som er baseret på online kunstig intelligens, og som dermed er i stand til løbende at tilegne sig lærdom, så vil denne algoritme kunne udvikle nye parametre at måle og finde sammenhænge på[79].

Disse situationer besværliggør efterlevelse af kravet om, at den data man agter at indsamle, skal være tilstrækkelig, relevant og begrænset, hvis man ikke indledningsvist ved, ud fra hvilke parametre algoritmen vil danne sammenhænge. Ud fra ovenstående betragtninger betyder dette, at dataansvarlige kan risikere at stå i en situation, hvor der ikke var sikret hjemmel til at indsamle oplysningerne. Er dataansvarlige ikke i stand til at determinere, om den data der indsamles, har relevans for formålet, har de indsamlet og behandlet dataen ulovligt. Ved anvendelse af deep learning modeller, er det en forudsætning, at modellen skal udvikle sig, lære og analysere sig frem til sammenhænge og mønstre, ud fra en stor mængde datainput. Den dataansvarlige ved ikke nødvendigvis hvad resultatet bliver, men formålet er, at modellen skal udvikle sig, i takt med at den får disse datainput. I dette tilfælde er det vanskeligt at determinere, hvorvidt kravet om dataminimering efterleves, da det på forhånd ikke vides, om dataen er tilstrækkelig, relevant og begrænset. Det eneste der vides med sikkerhed er, at

[77] Blume, Peter (2018) "*Den nye Persondataret*", side 91.
[78] EU-forordning 2016/679, artikel 5, stk. 1, litra c.
[79] Det Norske Datatilsyn (2018): *"Kunstig Intelligens og personvern"*, side 17.

modellen vil udvikle sig på baggrund af data, hvilket betyder at nogle personoplysninger vil være nødvendige for udviklingen, men andre vil vise sig at være unødvendige, alt afhængig af hvordan mønstrene dannes og modellen udvikler sig[80].

I deres rapport fra 2018 præsenterer det norske datatilsyn en interessant betragt, i forbindelse med overholdelse af proportionalitetsprincippet. De fremlægger, at dette kan gøres ved: "*Bruk av pseudonymiserings- eller krypteringsteknikker skjuler de registrertes identitet og bidrar til å begrense inngrepbet*[81]". Det norske datatilsyn åbner for muligheden for, at mitigerende sikkerhedsforanstaltninger kan foretages, således dataindsamling der ikke var proportionelt med formålet for databehandling, alligevel overholder kravet. I relation til kunstig intelligens må dette betragtes som være et fleksibelt værktøj ved anvendelse af deep learning modeller, hvor dataens relevans og tilstrækkelighed, som beskrevet tidligere, ikke nødvendigvis er kendt på forhånd. Det må således bero på en konkret vurdering af den enkelte situation og en lang række parametre, hvorvidt kravene til dataminimering er efterlevet. Artikel 5, stk. 1, litra c indeholder en lang række underliggende principper, som, ud fra en dynamisk fortolkning, må konkludere hvorvidt databehandling foretages på et lovligt grundlag.

[80] Det Norske Datatilsyn (2018): *"Kunstig Intelligens og personvern"*, side 17.
[81] Det Norske Datatilsyn (2018): *"Kunstig Intelligens og personvern"*, side 17.

6.4. Datakvalitet

artikel 5, stk. 1, litra d angiver princippet og "rigtighed" og fastsætter at oplysninger som behandles, skal være korrekte, og at de skal være ajourførte. Dataansvarlige har i forbindelse med udvikling og anvendelse af kunstig intelligens stor interesse i, at den data der bruges er korrekt og dette krav opfyldes, da de ønsker at opnå repræsentative og brugbare resultater. Ligesom de tidligere bestemmelser, består artikel 5, stk. 1, litra d også at flere led; (1) korrekthed og ajourføring, (2) behandling af urigtige oplysninger, (3) sletning og berigtigelse. Disse 3 led vil i det følgende vil blive analyseret og gennemgået[82].

Det fremgår af artikel 5, stk. 1, litra d at oplysninger skal være korrekte og om nødvendigt ajourførte, og at "*der skal tages ethvert rimeligt skridt for at sikre…*[83]", hvilket ud fra en formålsfortolkning af præambelbetragtning 39, må betragtes som skulle defineres ud fra en rimelighedsvurdering, da det ikke fremgår eksplicit, hvad rimelige skridt er. Det fremgår ligeledes ikke, hvordan korrekt eller ajourført skal defineres i forordningen. Den dataansvarlige er således forpligtet til, at foretage en konkret vurdering af formålet og hvilke konsekvenser brug af urigtige oplysninger har for den registrerede, og herefter foretage de foranstaltninger der vurderes nødvendige, for at sikre korrektheden af oplysningerne[84] [85].

Kravet om ajourføring skal ses i lyset af, hvad der er nødvendigt i forhold til formålet, jf. artikel 5, stk. 1, litra d. Dette betyder, at det er pålagt den dataansvarlige at vurdere, hvorvidt rigtigheden og kvaliteten af dataen er nødvendigt for at opfylde det specificerede formål. I direkte relation til kunstig intelligens er det ikke nødvendigvis forudsat, at den data der anvendes, skal være korrekt. Ved anvendelse af modeller som kræver store mængder datainput, som eksempelvis deep learning og Big Data teknologier, er det ikke væsentlig for de beslutningsprocesser maskinen gennemfører, og de resultater man vil nå frem til, at dataen er korrekt. Disse modeller udregner mønstre og tendenser, hvorfor det ikke er af afgørende betydning, at dataen er fuldstændig korrekt[86].

[82] EU-forordning 2016/679, artikel 5, stk. 1, litra d.
[83] EU-forordning 2016/679, artikel 5, stk. 1, litra d.
[84] EU-forordning 2016/679, præambel 39.
[85] Blume, Peter (2018) "*Den nye Persondataret*", side 92.
[86] EU-forordning 2016/679, artikel 5, stk. 1, litra d.

Det fremgår ligeledes af artikel 5, stk. 1, litra d, at urigtige oplysninger skal behandles med henblik på berigtigelse, hvilket betyder, at den dataansvarlige er forpligtet til at sikre, at urigtige oplysninger enten bliver korrekt opdateret eller helt slettet. Artikel 5, stk. 1, litra d skal ses i sammenhæng med artikel 16, som vedrører den registreredes rettighed til "*at få urigtige oplysninger om berigtiget…*[87]". I bestemmelsen pålægges der implicit den dataansvarlige et krav om, at kunne sikre, at den registreredes oplysninger er korrekte, og således også være i stand til at bevise det. I begge bestemmelser angives betegnelsen "urigtige" oplysninger, hvor der tidligere i persondataloven og databeskyttelsesdirektivet blev anvendt betegnelserne "ufuldstændige" og "vildledende". Da det ud fra en ordlydsfortolkning af de forskellige bestemmelser, ikke synes redegjort at forordningens bestemmelse har været tiltænkt et andet anvendelsesområde, kan det med rette antages, at "urigtige oplysninger", dermed også dækker over betegnelserne "ufuldstændige oplysninger" og/eller "vildledende oplysninger". Det er dermed ikke nok, at oplysningerne er forkerte. Hvis oplysningerne er mangelfulde eller på anden vis ikke korrekte, ifaldes kravet om berigtigelse eller sletning, jf. artikel 5, stk. 1, litra d[88].

Sidste led af artikel 5, stk. 1, litra d angiver reglerne om sletning og berigtigelse. Sletning eller berigtigelse skal ifølge bestemmelsen ske straks, hvis det konstateres, at de oplysninger man er i besiddelse af, ikke er korrekte i forhold til det specificerede formål. Der er således pålagt den dataansvarlige en pligt til at få disse data slettet eller berigtiget, når dette konstateres. Kravet i artikel 5, stk. 1, litra d er direkte pålagt den dataansvarlige, og det er således ikke den registreredes pligt. Hertil kommer bestemmelsen i artikel 17, stk. 1, som omhandler den registreredes ret til at "blive glemt" og få sine personoplysninger slettet. Udfordringerne ved sletning i relation til kunstig intelligens, er skildret i en rapport fra 2017, hvor de angiver, at: "*data deletion requirements can be considered to actually border on the edge of impossibility*[89]". Det angives i rapporten, at "sletning" er for vagt et begreb, og den udfordrer lovgivningen i den forstand, at forfatterne af rapporten ikke mener, at lovgivningen tager højde for, det den kunstig intelligens rent faktisk er i stand til. Med den komplicerede teknologi vi har indenfor den kunstige intelligens i dag, svarer det at skulle slette information fra en kunstig intelligens model, principielt til at bede et andet menneske om at slette information fra sin hukommelse. Udfordringen med sletning består i, at ved brug af komplicerede Big Data modeller, er dataen

[87] EU-forordning 2016/679, artikel 16.
[88] Justitsministeriets betænkning nr. 1565: "*Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning*", side 96.
[89] Villaronga, E.F., Kieseberg, P., & Li, T. (2017): "*Humans forget, machines remember: Artificial intelligence and the right to be forgotten*", side. 2.

ikke blot brugt og lagret ét specifikt sted i modellen, den kan findes i mange forskellige lag, og dermed er kravet om sletning vanskeligt at iagttage, i den absolutte forstand som persondataforordningen synes at præsentere. Rapporten fra 2017 angiver yderligere, at når data slettes fra en database, så slettes det ikke fuldstændigt; det markeres blot som slettet, og fjernes fra søge-indekset. Begrebet "sletning" er ikke yderligere defineret i forordningens artikel 4, men antages det, at "sletning" skal ses i relation til at få gjort "oplysningerne private", så der ikke er nogen der kan se eller tilkomme dem, så kan kravet imødekommes ved hjælpe af tekniske foranstaltninger, som for eksempel pseudonymisering eller kryptering[90] [91].

I relation til artikel 5, stk. 1, litra d skal som tidligere beskrevet ses artikel 16, som omhandler den dataansvarliges pligt til at berigtige de urigtige oplysninger, der måtte opbevares og behandles om den registreredes. Udfordringen ved "sletning", som beskrevet ovenfor, gør sig ligeledes gældende ved "berigtigelse". Dette absolutte krav kan være vanskeligt for udviklere og anvendere af kunstig intelligens, da modeller baseret på Big Data eller deep learning, vil lagre dataen i forskellige niveauer, hvilket besværliggør berigtigelsesprocessen, og om muligt umuliggør den, som rapporten fra 2017 angiver. Den tekniske løsning præsenteret ovenfor er ligeledes aktuel i relation til berigtigelse. Pseudonymisering og kryptering er anvendelige foranstaltninger, som sikrer af dataen ikke kan henføres til enkelte individer og således sikrer oplysningernes privathed[92].

Overordnet set varier relevansen af datakvaliteten og mulighederne for udbedring, i forbindelse med kunstig intelligens, af hvilken model man bruger. Som beskrevet ovenfor, afhænger eksempelvis ajourføringskravet af, hvorvidt formålet påvirkes af, at dataen er urigtig. Kunstig intelligens rummer, som beskrevet tidligere, flere modelformer af varierende kompleksitet, hvilket betyder, at ved anvendelse af en simpel offline model baseret på machine learning, vil berigtigelse og sletning ikke nødvendigvis være en udfordring, hvorimod det kan vise sig problematisk ved anvendelse af mere komplekse online modeller.

[90] Villaronga, E.F., Kieseberg, P., & Li, T. (2017): "*Humans forget, machines remember: Artificial intelligence and the right to be forgotten*", side 10.
[91] Justitsministeriets betænkning nr. 1565: "*Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning*", side 96.
[92] Villaronga, E.F., Kieseberg, P., & Li, T. (2017): "*Humans forget, machines remember: Artificial intelligence and the right to be forgotten*", side 12 – 13.

6.5. Tidsbegrænsning

Artikel 5, stk. 1, litra e fastlægger et tidsbegrænsningsprincip. For dataansvarlige kan det være fordelagtigt at lagre oplysninger, i tilfælde af, at de kan blive anvendelig på et senere tidspunkt, selvom dette ikke er defineret på indsamlingstidspunktet. Tidsbegrænsningsprincippet er, på samme måde som princippet om dataminimering i artikel 5, stk. 1, litra c, for at undgå uretmæssig dataophobning. Kravet om tidsbegrænsnings skal således ses i forlængelse af kravet om dataminimering, hvor der pålægges den dataansvarlige en forpligtelse til løbende at holde sig bevidst om oplysningernes fortsatte relevans for formålet [93].

Bestemmelsen i artikel 5, stk. 1, litra e er formuleret således, at der ikke er pålagt et krav om sletning af data, blot at "*det ikke er muligt at identificere den registrerede…*[94]", hvilket ud fra en ordlydsfortolkning betyder, at dataen kan gemmes, såfremt den ikke kan henføres til den registrerede. I relation til kunstig intelligens er denne bestemmelse mere fleksibel, og det må antages at behovet for store mængder data, gør at dataansvarlige ønsker at beholde sig meget data som muligt. Som tidligere beskrevet er det en vanskelig opgave for dataansvarlige, at implementere foranstaltninger til løbende sletning af data for at efterleve tidsbegrænsningsprincippet, specielt ved anvendelse af deep learning og online modeller. Med denne formulering er dataansvarlige således i stand til at maskere dataen ved hjælp af anonymisering, pseudonymisering eller kryptering, hvilket er en særdeles mindre omkostningstung opgave at udføre. Artikel 5, stk. 1, litra e indeholder derudover en undtagelsesmulighed identisk med bestemmelsen i artikel 5, stk. 1, litra b om formålsbegrænsning, hvor det er muligt at opbevare dataen i et længere tidsrum, hvis det er i forbindelse med behandling til arkivformål i samfundets interesse, hvis det er i forbindelse med behandling til videnskabelige eller historiske forskningsformål, eller hvis det behandles til statistiske formål[95].

[93] Blume, Peter (2018) "*Den nye Persondataret*", side 93.
[94] EU-forordning 2016/679, artikel 5, stk. 1, litra e.
[95] Blume, Peter (2018) "*Den nye Persondataret*", side 94.

6.6. Sikkerhed

Som noget nyt ved indførsel af persondataforordningen er '*sikkerhed*' blevet et af de overordnede principper for databehandling, og bestemmelsen i artikel 5, stk. 1, litra f fastslår dette sikkerhedsprincip, det såkaldte princip om integritet og fortrolighed. Når der tales om "*passende tekniske og organisatoriske foranstaltninger*[96]", så fungerer dette som et fleksibelt værktøj for den dataansvarlige, da det ikke konkretiseres yderligere i bestemmelsen, hvorledes dette skal udføres i praksis. Overordnet set indeholder artikel 5, stk. 1, litra f en række formuleringer, som giver anledning til yderligere analyse, da de i sig selv ikke bidrager til hvordan den dataansvarlige i praksis skal sikre sig. Bestemmelsen indeholder formuleringer som: "*[Personoplysninger skal] behandles på en måde, der sikrer tilstrækkelig sikkerhed…*[97]". Formuleringer som denne, må betegnes som værende af generel karakter, og begrænser dermed ikke mulighederne for fortolkning. Tekniske og organisatoriske foranstaltninger kan således, ud fra bestemmelsens ordlyd, variere alt efter hvilken databehandling der foretages og hvilket sikkerhedsniveau der vurderes tilstrækkeligt. Der lægges dermed op til konkrete vurderinger. For at kunne forstå bestemmelsen i relation til kunstig intelligens, undersøges og belyses den nærmere i det følgende.

Formuleringen; "*[Personoplysninger skal] behandles på en måde, der sikrer tilstrækkelig sikkerhed…*", udgør et minimumskrav. Formuleringer som; "*på en måde*" og "*tilstrækkelig*", angiver, at den dataansvarlige skal foretage sikkerhedsforanstaltninger, der så sikre, at der ingen risici eksisterer for dataen. I persondataforordningens artikel 32, præsenteres de generelle regler for behandlingssikkerhed. Ifølge artikel 32, stk. 1, er den dataansvarlige forpligtet til at have et passende sikkerhedsniveau, som tager hensyn til de risici, der er forbundet med databehandlingen. Herudover er artikel 32, stk. 1 mere vidtgående end artikel 5, stk. 1, litra f, da artikel 32, stk. 1, da den præsenterer mulige tekniske og organisatoriske foranstaltninger, som kan sikre et højt sikkerhedsniveau. Der er således ikke overensstemmelse mellem de 2 artikler, da artikel 5, stk. 1, litra f ikke angiver hvorledes disse tekniske og organisatoriske foranstaltninger kan træffes, hvorimod artikel 32, stk. 1, præsenterer den dataansvarlige for nogle konkrete værktøjer[98].

[96] EU-forordning 2016/679, artikel 5, stk. 1, litra f.
[97] EU-forordning 2016/679, artikel 5, stk. 1, litra f.
[98] Blume, Peter (2018) "*Den nye Persondataret*", side 155.

Artikel 32, stk. 1 angiver sikkerhed på et teknisk niveau, hvilket er et krav der rettes imod de risici der er forbundet med den digitale databehandling. Det fremgår af præambelbetragtning 83, at den dataansvarlige bør vurdere hvilke risici der er forbundet med databehandlingen, og således indføre foranstaltninger, der kan begrænse disse risici[99]. Sikkerhedsniveauet skal dermed tilpasses de risici, som er aktuelle i forbindelse med den pågældende databehandling. Det fremgår eksplicit af artikel 32, stk. 1, at risiciene kan have "*varierende sandsynlighed*", hvilket kan vise sig som en udfordring, da det er pålagt den dataansvarlige at vurdere og afgøre hvilke konkrete risici der er forbundet med den behandling der foretages. Determinering af risici af denne karakter kan være yderst vanskelig og kræve en teknisk snilde, som kun kan tilegnes ved lange tekniske videregående uddannelser[100].

6.6.1. Foranstaltninger

Som tidligere beskrevet i denne afhandling, eksisterer der en lang række trusler mod IT-sikkerheden. Artikel 32, stk. 1, lister i litra a – d en række af de foranstaltninger, som der kan gennemføres for at sikre i mod de risici der er forbundet med en given databehandling. I den forbindelse præsenterer ENISA's rapport fra 2016 mulige løsninger til, hvordan nogle af disse foranstaltningsforslag i artikel 32, stk. 1, litra a – d kan gennemføres.

Litra a angiver muligheden for pseudonymisering og kryptering af personoplysningerne, hvilket tidligere er blevet beskrevet i denne afhandling, og som med rette kan anbefales i relation til kunstig intelligens, da det er en simpel løsning i forhold til at maskere data, og gøre dem ikke-personhenførbare. Kunstig intelligens der er baseret på Big Data modeller, som deep learning, vil ikke blive begrænset af pseudonymisering, da den er designet til at se mønstre og tendenser ud fra en enorm mængde data, og den træffer således ikke beslutninger eller opnår resultater, baseret på om adresser eller cpr-numre er korrekte. Det afgørende er data-flowet, og derfor er pseudonymisering anbefalelsesværdigt i relation til kunstig intelligens. Kryptering er ligeledes brugbart værktøj for anvendere og udviklere af kunstig intelligens, dog er kryptering ikke blot maskering af data, det er en foranstaltning, som sikrer imod ulovlig indtrængen til dataen og at dataen skulle sive ud af systemet. Udfordringen med kryptering opstår dog ved den praktiske anvendelse, da kryptering af data betyder anvendelse af krypteringsnøgler, hvilket betegnes som en udfordring i relation til Big Data. Ved anvendelse af disse krypteringsnøgler opstår der et helt nyt sikkerhedsproblem. Udfordringen består i den øgede

[99] EU-forordning 2016/679, præambel 83.
[100] Blume, Peter (2018) "*Den nye Persondataret*", side 156.

kompleksitet der opstår ved forbruger-leverandørforholdet, og den komplekse infrastruktur der kræves, for at sikkerheden omkring disse krypteringsnøgler er tilstrækkelig høj. Ideelt set skal disse nøgler beskyttes og udleveres til mindst mulige, men den kunstige intelligens kræver datainput og adgang til informationer, hvorfor kryptering kan vise sig vanskeligt i praksis i relation til kunstig intelligens[101].

Af artikel 32, stk. 1, litra b, fremgår bestemmelsen: "*evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester*[102]". Formuleringen "vedvarende" henviser til, at de foranstaltninger der træffes, på baggrund af eksisterende risici, skal være permanente. Det er ikke tilstrækkeligt, at indbygge midlertidige sikkerhedsforanstaltninger, eller først indbygge foranstaltningerne, efter man har været ude for et angreb. Foranstaltningerne skal være indbygget på forhånd og de skal være permanente. Som bestemmelsen her beskriver, og som ligeledes tidligere beskrevet i denne afhandling, så er sikkerhed ikke kun et spørgsmål om fortrolighed, men også om integritet. Det er således et krav i bestemmelsen, at sikkerhedsforanstaltningerne er i stand til at forebygge mod konsekvenser, som ikke har været forudset, uanset hvordan og af hvem disse konsekvenser måtte være forårsaget. Formuleringen "robusthed" er værd at bemærke, da den relaterer til behandlingssystemet og således til det tekniske miljø hvor i personoplysningerne bliver opbevaret og behandlet. Det pålægges den dataansvarlige, at vurdere hvilke risici der er forbundet med behandlingen, og ud fra den betragtning, vurdere hvor høj kvaliteten af tekniske IT-system skal være[103].

Det fremgår af litra c, at den dataansvarlige er forpligtet til at sikre, at genopretning af tilgængelighed og adgang til oplysninger er mulig, i tilfælde af en brist af en given karakter. Heri ligger der implicit et krav om at vurdere, hvorvidt denne foranstaltning er relevant, da genskabning af data karakteriseres som en databehandling, og dermed opstår en lang række krav, blandt andet oplysningskravet. Langt de fleste IT-eksperter vil argumentere for, at alt skal sikkerhedskopieres, men ikke desto mindre skal den dataansvarlige være opmærksom på, det regelsæt der gælder, når der vælges at genskabe personoplysninger. I relation til kunstig intelligens adskiller de tekniske krav til sikkerhedskopiering sig ikke væsentligt fra kravene til mere normal software. Som tidligere beskrevet er kunstig intelligens, og de algoritmer der er indeholdt, ikke altid under udvikleren eller anvenderes kontrol, hvorfor fejl

[101] ENISA (2016): "*Big Data Threat Landscape and Good Practice guide*", side 33.
[102] EU-forordning 2016/679, artikel 32, stk. 1, litra b.
[103] Blume, Peter (2018) "*Den nye Persondataret*", side 155-156.

eller uregelmæssigheder i softwaren, en såkaldt "bug", kan opstå. Disse "bugs" er vanskelige at undgå, og i forbindelse med kunstig intelligens kan de vise sig ganske kritiske for modellen eller algoritmens udvikling, og de beslutninger og resultater som de når frem til. Eksempelvis kan "bugs" resultere i, at en algoritme vil vægte et givent datasæt for lidt eller for meget, hvilket kan betyde beslutninger eller resultater, som er behæftet med fejl eller unøjagtigheder. I sådanne tilfælde er det ikke nok, at have sikkerhedsforanstaltninger som kan sikre genopretning, men det er også nødvendigt for at sikre kvaliteten og integriteten af algoritmen. Det fremgår af litra d, at der skal implementeres en procedure for at sikre, at alle tekniske og organisatoriske foranstaltninger er afprøvet så der kan vurderes og evalueres på effekten. Som bestemmelsen indirekte foreskriver, er det ikke muligt at kategorisere en sikkerhedsforanstaltning som tilstrækkelig, før det igennem prøver og tests er det blevet påvist, at den lever op til de relevante krav[104].

Både artikel 5, stk. 1, litra f og artikel 32 indeholder principper og regler som relaterer sig til, og har betydning for, udviklere og anvendere af kunstig intelligens. Iagttagelse af kravet om integritet og fortrolighed betyder, at den dataansvarlige skal identificere hvad der skal beskyttes, hvad det skal beskyttes i mod, og hvorledes det skal beskyttes. Den dataansvarlige skal vurdere hvilke sikkerheds-foranstaltninger der er tilstrækkelige og proportionelle med trussels-niveauet, eksempelvis pseudo-nymisering, som tidligere beskrevet.

6.6.2. Privacy by default & privacy by design

Det fremgår af persondataforordningens artikel 25, stk. 1 og 2, at der igennem design og standard-indstillinger kan sikres databeskyttelse. Databeskyttelse igennem design handler i sin enkelthed om, at man tænker databeskyttelse ind i systemet ved udvikling eller implementering. Databeskyttelse igennem standardindstillinger handler om, at databehandling skal foregå på den registreredes aktive tilvalg. Det bør ikke være automatisk indstillet, at den registrerede accepterer en hjemmesides brug af personlige oplysninger, med mindre de fravælger det. Det skal den registrerede selv have mulighed for at tilvælge. I relation til kunstig intelligens er det i særlig grad databeskyttelse igennem design, der lægger op til udfordringer og betragtninger, da dette krav forpligter anvendere og udviklere at tænke databeskyttelse direkte ind i systemet i udviklingsfasen.

[104] Blume, Peter (2018) "*Den nye Persondataret*", side 155-156.

Kravet om privacy by design forekommer som beskrevet i artikel 25, stk. 1, og omhandler implementeringen af tekniske og organisatoriske foranstaltninger, hvilket ligeledes er et krav, som fremgår af artikel 32, stk. 1 om behandlingssikkerhed. Det fremgår eksplicit af artikel 25, stk. 1, at databeskyttelse igennem design ikke blot omhandler implementering af tekniske og organisatoriske foranstaltninger, men også omhandler iagttagelse af de øvrige krav og principper i forordningen. Dataminimering står eksempelvis konkret nævnt som et princip der skal efterleves. Bestemmelsen i artikel 25, stk. 1 omhandler desuden også et implicit krav om, at dataansvarlige ved udvikling af et system skal have sikret sig imod databehandlinger, som strider med formålet og som ikke har hjemmel til databehandling. Det giver anledning til, at vende tilbage til det grundlæggende princip om integritet og fortrolighed i artikel 5, stk. 1, litra f. Heri nævnes eksplicit et krav om "*beskyttelse mod uautoriseret eller ulovlig behandling*[105]", hvilket skal baseres på en risikovurdering af, hvilke sikkerhedsforanstaltninger der er nødvendige for at undgå ulovlig behandling af personoplysninger. Med bestemmelsen i artikel 25, stk. 1, er den dataansvarlige i stand til at realisere dette krav, da der ved udvikling af systemet, som skal behandle persondata, er pålagt et krav om at indarbejde foranstaltninger imod behandlinger som strider med det oprindelige formål, og behandlinger som er ulovlige[106].

I relation til kunstig intelligens er der fordele og ulemper forbundet med kravet om privacy by design. Som tidligere beskrevet kan det være en udfordring for anvendere og udviklere af kunstig intelligens, på forhånd at designe et system, der tager højde for alle formål og beslutningsprocesser, da det i en lang række tilfælde ikke er forudbestemt, hvilke typer behandling en algoritme skal igennem, eksempelvis ved anvendelse af Big Data og deep learning teknikker. ENISA (European Union Agency For Network And Information Security) argumenterer således for det modsatte, at kunstig intelligens vil have udfordringer ved at løfte kravet om privacy by design, hvis det systemerne og modellerne skal ændres efterfølgende, da dette kan påvirke modellens funktionalitet. ENISA argumenterer for, at det er nødvendigt at dataansvarlige "*take the necessary steps to integrate privacy and data protection safeguards in the heart of big data*[107]". Dataansvarlige bør således sikre, at privacy og sikkerhed indføres i hjertet af Big Data værdikæden.

[105] EU forordning 2016/679, artikel 5, stk. 1, litra f.
[106] EU forordning 2016/679, artikel 25, stk. 1.
[107] ENISA (2015): "*Privacy by design in big data: An overview of privacy enhancing technologies in the area of big data analytics*", side 5.

ENISA præsenterer altså en korrelation imellem kunstig intelligens og privacy: "*It is not a matter of clash, but a matter of prosperity*[108]". Dataansvarlige bør omfavne de teknologiske muligheder, og bruge dem som værktøjer i forbindelse med efterlevelse af privay-reglerne. Hvis ikke, så vil dataansvarlige, og udviklere og anvendere af kunstig intelligens ikke være i stand til at imødekomme de registreredes behov og krav. ENISA præsenterer således et nødvendigt skifte i fokus. I lang tid har dataansvarlige arbejdet ud fra overbevisningen "*big data versus privacy*" og nu argumenterer ENISA for værdien i, at arbejde med "*privacy with big data*[109]", og på den måde adoptere reglerne og principperne, og inkorporere dem i Big Data-værdikæden. I relation til kunstig intelligens kan den praktiske udfoldelse af kravet om privacy by design være udfordrende, men ikke desto mindre har ENISA en valid pointe i, at lovgivningen skal respekteres og der bør søges ind i, hvorledes man kan omfavne reglerne og indbygge dem i systemet, således de skaber værdi for hele kæden[110].

[108] ENISA (2015): "*Privacy by design in big data: An overview of privacy enhancing technologies in the area of big data analytics*", side 17.
[109] ENISA (2015): "*Privacy by design in big data: An overview of privacy enhancing technologies in the area of big data analytics*", side 5.
[110] ENISA (2015): "*Privacy by design in big data: An overview of privacy enhancing technologies in the area of big data analytics*", side 17 – 18.

7. Yderligere principper og regler

Udover de grundlæggende principper i artikel 5, findes der en række yderligere bestemmelser, som har særlig relevans for dataansvarliges iagttagelse af persondataforordningens principper i relation til kunstig intelligens.

7.1 Automatiske afgørelser

Som beskrevet i afsnit 5 er kunstig intelligens i stand til at træffe beslutninger og fremskaffe resultater baseret på mængden af datainput. Kunstig intelligens kan således fungere som et værktøj, der er i stand til at opstille en række rammer og kasser, som den registrerede kan placeres i. Automatiske afgørelser fungerer som en evaluering af et individ, der er baseret på automatisk databehandling og beslutningstagen uden menneskelig involvering. Det bruges i stigende grad i den offentlige forvaltning i forbindelse med sagsbehandling, og ligeledes i den finansielle sektor i forbindelse med udarbejdelse af kreditværdighed. Denne type evalueringer betragtes som særegne i databeskyttelsesretlig forstand, på trods af, at registrerede ikke behandles som individer, men nærmere som ting der skal vurderes på baggrund af den voksende informationsteknologi. På samme måde er databehandlingen heller ikke et udtryk for personlig eller menneskelig behandling, men reglerne i persondataforordningen tilkendegiver, at der skal foretages en menneskelig vurdering af en afgørelse eller beslutning. Dette vil blive uddybet nedenfor[111].

Det fremgår af persondataforordningens artikel 22, at "*den registrerede har ret til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling*[112]". Artikel 22, stk. 1 er således en barriere for dataansvarlige og begrænser deres brug af fuldautomatisk databehandling, da registrerede har ret til ikke at være genstand for en automatisk afgørelse, der har retsvirkning eller på tilsvarende vis påvirker den registrerede. Det fremgår dog af artikel 22, stk. 2, at der er undtagelser til denne regel. Reglerne i stk. 1 finder ikke anvendelse, hvis afgørelse er nødvendig for opfyldelse af en kontrakt, er hjemlet i EU-retten eller medlemsstaternes nationale ret, eller hvis den er baseret på den registreredes samtykke. Herudover fremgår det af præambelbetragtning nr. 71 og artikel 22, stk. 4, at undtagelserne kun gælder almindelige personoplysninger og, at "*særlige kategorier af personligoplysninger bør kun tillades under særlige omstændigheder*[113]". Det fremgår imidlertid af artikel

[111] Blume, Peter (2018) "*Den nye Persondataret*", side 138 – 139.
[112] EU-forordning 2016/679, artikel 22.
[113] EU-forordning 2016/679, præambel 71.

22, stk. 4, at behandling af følsomme personoplysninger er tilladt efter artikel 9, stk. 1, hvis behandlingen er hjemlet i artikel 9, stk. 2, litra a (baseret på samtykke) eller litra g (baseret på nødvendighed for varetagelse af væsentlige samfundsinteresser).

Som beskrevet længere oppe kunne et eksempel på automatiske afgørelser være kreditværdighedsvurderinger, hvor der således er krav om menneskelig involvering, jf. forordningens regler. Dette eksempel fungerer som udgangspunkt for diskussionen om, hvorvidt en afgørelse er truffet automatisk eller fysisk ved menneskelig indvirkning. En kreditværdighedsvurdering, hvor en algoritme angiver individers kreditværdighed, vil som udgangspunkt være en automatisk afgørelse, der ikke kræver menneskelig involvering. Benyttes der imidlertid kun kunstig intelligens som et hjælpeværktøj i forbindelse med kreditværdighedsvurderingen, så falder processen udenfor artikel 22's anvendelsesområde, da der er en grad af menneskelig involvering, i form af eksempelvis en sagsbehandler. Dette betyder således, at før en registreret kan gøre kravet i artikel 22 gældende, så er det forudsat, at behandlingen er fuld automatisk uden menneskelig involvering af nogen karakter. Herved opstår det interessante spørgsmål; hvornår forelægger der tiltrækkelig menneskelige involvering, således kravet i artikel 22 ikke kan gøre gældende? Article 29 Data Protection Working party angiver, at en kunstig intelligens model godt kan fungere som værktøj og udstikke anbefalinger og vurderinger, men det skal ultimativt være den enkelte sagsbehandler der træffer den endegyldige beslutning. Ligeledes skal den enkelte sagsbehandler ikke følge modellens anbefalinger blindt, på samme måde som en dataansvarlig ikke må konstruere eller fabrikere menneskelig involvering i en afgørelsesproces. Der skal være tale om en kompetent og fagligt dygtig sagsbehandler, som selv er i stand til at træffe disse afgørelser. Menneskeligt tilsyn og involvering er en forpligtelse i artikel 22, men også en forudsætning for, at bestemmelsen kan finde anvendelse[114].

7.1.2 Profilering

Profilering er også indeholdt i artikel 22, stk. 1, og herudover fremgår det af artikel 4, nr. 4, at profilering er: "*enhver form for automatisk behandling af personoplysninger, der består i at anvende personoplysninger til at evaluere bestemte personlige forhold vedrørende en fysisk person, navnlig for at analysere eller forudsige forhold, vedrørende den fysiske persons arbejdsindsats, økonomiske situation, helbred, personlige præferencer, interesser, pålidelighed, adfærd, geografisk position eller*

[114] Article 29 Data Protection Working Party (2018): "*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*", side 21.

bevægelser[115]". Profilering er således den bedømmelse, evaluering eller vurdering som der foretages af den registrerede. Den er indeholdt i artikel 22, stk. 1, og er dermed at betragte som en underkategori af den automatiske afgørelse. Profilering kan være et særdeles brugbart værktøj i forbindelse med markedsføring og anvendelse af Big Data teknikker, hvor det er muligt at indsamle enorme mængder data og kunder eller potentielle kunders indkøbsadfærd og/eller mønstre. I sådan en situation er der ikke tale om en automatisk afgørelse, som har retsvirkning for den registrerede, hvorfor kravene i artikel 22 ikke kan gøres gældende, dog skal princippet om formålsbestemthed tages i betragtning, da Article 29 Data Protection Working Party argumenterer for, at det er afgørende at man anerkender den registreredes oprindelige formål med at udlevere dataen, og den dataansvarlige ikke viderebehandler dataen for virksomhedens egen vindings skyld, eksempelvis til marketingsformål. Profilering bruges til en lang række formål af en lang række forskellige virksomheder. Ud fra en stor mængde data er de dataansvarlige i stand til at opstille en profil, og enkelte individer kan dermed placeres i disse profiler, ud fra dataen fra individerne. På denne måde er dataansvarlige i stand til at målrette eksempelvis marketingskampagner mod de registrerede[116].

I relation til kunstig intelligens har udviklingen af avancerede teknologier og komplekse modeller, muliggjort udnyttelsen af automatisk databehandling og afgørelser. Automatisk afgørelse eller profilering må betragtes som en indgribende proces i forbindelse med behandling af den registreredes personlige oplysninger. Article 29 Data Protection Working Party angiver i deres vejledning, at konsekvensanalysen, eller DPIA, er et kritisk værktøj, som skal tages i brug i forbindelse med automatisk databehandling og profilering med henblik identificering af risici og håndtering af disse, hvilket reguleres i artikel 35, stk. 3, litra a. Herudover skal der, i de tilfælde hvor der udføres automatisk databehandling efter artikel 22, stk. 2, litra a og c, foretages passende foranstaltninger for at beskytte den registreredes rettigheder, frihedsrettigheder og legitime interesser, jf. artikel 22, stk. 3. Denne artikel skal ses i forlængelse af præambelbetragtning nr. 71, hvori der står, at der skal foretages tiltag for at sikre den registrerede, og disse tiltag skal være passende matematiske eller statistiske procedurer til profileringen. I forbindelse med den registreredes indsigtsret præsenterer artikel 15, stk. 1, litra h en række potentielle udfordringer for udviklere og anvendere af kunstig intelligens. Det fremgår af denne bestemmelse, at registrerede har ret til at få information om forekomsten af automatiske

[115] EU-forordning 2016/679, artikel 4, nr. 4.
[116] Article 29 Data Protection Working Party (2018): "*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*", side 11.

databehandlinger, oplysninger om logikken heri, og de forventede konsekvenser af behandlingen. Herudover fremgår det ligeledes af præambelbetragtning 71, at den registrerede har krav på en forklaring på afgørelsen. Som nævnt kan dette præsentere udfordringer for dataansvarlige, samt anvendere og udviklere af kunstig intelligens, da logikken og de mange beslutningslag der ligger bag en afgørelse i, eksempelvis, en deep learning model, ikke altid er mulige at få adgang til. Som beskrevet i afsnit 5.4 om den sorte boks, så vil de mange komplekse og avancerede beslutningslag og processer betyde, at det der ligger til grund for en models beregninger ikke altid vil være til rådighed, når der bliver anvendt deep learning. Article 29 Data Protection Working Party påpeger ligeledes, at den stigende kompleksitet ved machine learning-teknikker gør det problematisk at forstå, hvorledes en automatisk afgørelsesproces eller profiling fungerer. De angiver, at det er op til den enkelte dataansvarlige at finde metoder til at simplificere informationerne og rationalerne bag de automatiske beslutningsprocesser. Herudover siger de, at det ikke er påkrævet, at kompleksiteten bag modellerne skal forstås, men det skal være tydeligt hvad der er blevet lagt vægt på i afgørelserne. Denne betragtning gør, at anvendere og udviklere af kunstig intelligens har markant nemmere ved at iagttage kravene forbundet med automatisk databehandling og profiling[117] [118] [119].

[117] EU-forordning 2016/679, præambel 71.
[118] EU-forordning 2016/679, artikel 15, stk. 1, litra h.
[119] Article 29 Data Protection Working Party (2018): "*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*", side 12.

7.2. Ansvarlighedsprincippet

Princippet om ansvarlighed er et nyt, men meget væsentligt og centralt, princip i persondataforordningen. Det fremgår således af persondataforordningens artikel 5, stk. 2, at: "*Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes*[120]", hvilket betyder, at den dataansvarlige ikke blot skal efterleve reglerne og principperne i forordningens artikel 5, stk. 1, litra a – f, men også er forpligtet til at kunne dokumentere, at reglerne efterleves. Kravene i artikel 5, stk. 2, bliver forstærket af reglerne i artikel 24 omkring den dataansvarliges ansvar. Det fremgår af artikel 24, stk. 1, at: "*Under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med denne forordning. Disse foranstaltninger skal om nødvendigt revideres og ajourføres*[121]". Udover dokumentationskravet, som ligeledes blev præsenteret i artikel 5, stk. 2, indeholder artikel 24, stk. 1 en forpligtelse for den dataansvarlige til løbende at overvåge, opdatere og ajourføre de tekniske og organisatoriske foranstaltninger som skal gennemføres. Med formuleringen "*under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder*", lægges der op til en konkret vurdering af disse aspekter, hvorefter der skal tages stilling til den risiko som databehandlingen står overfor, og således skal der implementeres de nødvendige foranstaltninger[122].

I en række yderligere bestemmelser i forordningen, pålægges der den dataansvarlige en række tiltag som skal implementeres, i det omfang det vurderes nødvendigt og relevant i forbindelse med den konkrete databehandling. Artikel 24, stk. 2 fremstiller forpligtelsen for den dataansvarlige om indførsel af databeskyttelsespolitikker, hvis det står i rimeligt forhold til de behandlingsaktiviteter der foretages. Igen er det pålagt den dataansvarlige at vurdere behandlingen og de forskellige aspekter indeholdt i behandlingen, og således vurdere hvorvidt det er nødvendigt at inkorporere databeskyttelsesprincipper i virksomheden. På samme måde som reglerne om 'fortegnelser' i artikel 30, hvor det er pålagt den dataansvarlige at føre fortegnelser over behandlingsaktiviteterne, hvis det vurderes nødvendigt og relevant, bør der implementeres databeskyttelsespolitikker, som skal appellere til den gode

[120] EU-forordning 2016/679, artikel 5, stk. 2.
[121] EU-forordning 2016/679, artikel 24, stk. 1.
[122] Det Norske Datatilsyn (2018): *"Kunstig Intelligens og personvern*", side 24.

databehandlingsskik og appellere til ansvarligheden hos databehandlere. Det fremgår herudover af forordningens artikel 37, at dataansvarlige skal udpege en databeskyttelsesrådgiver, hvis den databehandling der udføres, er omfattet af reglerne i artikel 37, stk. 1, litra a – c.

I relation til kunstig intelligens er der, som tidligere beskrevet, en række udfordringer forbundet med efterlevelsen af reglerne i artikel 5, stk. 1, litra a – f, og denne udfordring bliver ikke mindre med kravet i artikel 5, stk. 2, hvor efterlevelsen skal kunne dokumenteres. Udfordringen med anvendelse af deep learning teknikker og problematikken omkring den sorte boks gør, at det at implementere procedurer og databeskyttelsespolitikker som led i udøvelsen af ansvarlighed, ikke er tilstrækkelige. De informationer og oplysninger der kræves adgang til, er ikke altid tilgængelige eller forståelige, når de er behandlet i en online model der er baseret på deep learning, da det er her den sorte boks opstår. Efterlevelse af reglerne om ansvarlighed i artikel 5, stk. 2 og de grundlæggende principper i artikel 5, stk. 1, litra a – f, nødvendiggør behovet for tekniske foranstaltninger. Brugen af Big Data er ofte forbundet med store indsamlinger af data, med henblik på at gennemskue mønstre og tendenser, og i denne forbindelse kan princippet om formålsspecifikation, som tidligere beskrevet, være vanskeligt at efterleve. Dette besværliggør yderligere kravet i artikel 5, stk. 2 og artikel 24, stk. 1, da dokumentation og løbende revidering og ajourføring af, eksempelvis, online kunstig intelligens modeller, kan vise sig vanskeligt i praksis. Implementering af tekniske løsninger direkte i den kunstige intelligens kan være afgørende for iagttagelse af disse krav, da online kunstig intelligens modeller ikke kan bære den manuelle proces, og dermed er afhængig af en indbygget automatik, der kan løfte disse krav om, eksempelvis formålsspecifikation og dokumentation.

7.3 Troværdig kunstig intelligens

I det følgende afsnit vil der, med udgangspunkt i Den Uafhængige Ekspertgruppe På Højt Niveau om Kunstig Intelligens' (herefter Ekspertgruppen) artikel: "*Etiske retningslinjer for pålidelig kunstig intelligens*", blive redegjort for hvordan troværdig kunstig intelligens opnås, på baggrund af nogle få komponenter, som skal være indeholdt og overholdt igennem hele den kunstige intelligens' levetid. Ekspertgruppen er nedsat af EU-kommissionen med det formål, at fremme forståelsen og ultimativt brugen af kunstig intelligens, igennem retningslinjer og guidelines til hvordan kunstig intelligens-systemer skal anvendes. Gruppen ønsker således at maksimere fordelene ved kunstig intelligens-systemer og samtidig forebygge og minimere risiciene ved anvendelsen af kunstig intelligens[123].

Ekspertgruppen fremstiller 3 komponenter, som skal opfyldes gennem hele systemets levetid, hvis troværdig og pålidelig kunstig intelligens skal opnås; (1) lovlighed, (2) etik og (3) robusthed. Disse 3 komponenter er nødvendige hver for sig, men løser ikke nødvendigvis problemet, med mindre de implementeres og anvendes i harmoni med hinanden. Ekspertgruppen anbefaler herudover, at det er vores individuelle og kollektive ansvar som samfund at sikre, at disse 3 komponenter er implementeret og hjælper med at sikre pålideligheden at kunstig intelligens. Kravet om lovlighed er som tidligere beskrevet indeholdt i persondataforordningens artikel 5, stk. 1, litra a, men i denne sammenhæng skal lovlighed ses i overordnet sammen i et horisontalt perspektiv. Det er således ikke kun persondataforordningens regler og principper der skal betragtes, det er al lovgivning der skal iagttages og efterleves. I relation til kunstig intelligens fremsætter lovgivningen både positive og negative forpligtelser, det vil sige forpligtelser om ting som *ikke* må gøres, og ting som *skal* gøres[124].

På trods af regler og love på området, skal samfundet og folkene i det have tillid til, at de systemer og teknologier der anvendes til kunstig intelligens, ikke kunne gøre skade i nogen form. Ekspertgruppen angiver, at robusthed skal sikres ved at indføre sikkerhedsforanstaltninger, der således kan forebygge mod uforudsete negative indvirkninger. Ekspertgruppen bakker således op omkring de tekniske og organisatoriske foranstaltninger, som i forordningen bliver præsenteret som tiltag der skal implementeres[125].

---

[123] Den Uafhængige Ekspertgruppe På Højt Niveau om Kunstig Intelligens (2019): "*Etiske retningslinjer for pålidelig kunstig intelligens*", side 4.
[124] Den Uafhængige Ekspertgruppe På Højt Niveau om Kunstig Intelligens (2019): "*Etiske retningslinjer for pålidelig kunstig intelligens*", side 5 – 7.
[125] Den Uafhængige Ekspertgruppe På Højt Niveau om Kunstig Intelligens (2019): "*Etiske retningslinjer for pålidelig kunstig intelligens*", side 7.

7.3.1 Etiske retningslinjer

Den tredje komponent er etik, og den åbner op for nogle interessante betragtninger, der bevæger sig længere end lovgivning og tekniske løsninger. Lovgivningen og teknologierne bag kunstig intelligens er tidligere blevet beskrevet i denne afhandling, men de etiske betragtninger og retningslinjer, som Ekspertgruppen argumenterer for er række essentielle komponenter for opnåelse af pålidelig kunstig intelligens, som ikke er blevet berørt indtil nu. Efterlevelse af lovgivningens regler og implementering af passende og organisatoriske sikkerhedsforanstaltninger er, efter Ekspertgruppens vurdering, ikke nok til at opnå pålidelig kunstig intelligens, da anvendelsen og udførslen skal være tilpasset de etiske normer[126].

Kunstig intelligens-etik er en gren indenfor den anvendte etik, som Ekspertgruppen beskriver det. De etiske overvejelser forbundet med kunstig intelligens, kan være forbundet med en lang række formål, men det bør tilskyndes at hovedformålet er for beskytte registrerede og deres personlige oplysninger. En lang række lovgivning beskytter menneskets grundlæggende rettigheder, som for eksempel menneskerettighedskonventionen, og disse er meget væsentlige for anvendelsen af kunstig intelligens og opnåelse af pålideligheden. Baseret på disse grundlæggende rettigheder og allerede eksisterende lovgivning, har Ekspertgruppen udarbejdet 4 etiske principper, som bør overholdes i forbindelse med udvikling og anvendelse af kunstig intelligens[127].

De 4 principper er: (1) Respekt for menneskers autonomi. (2) Forebyggelse af skade. (3) Retfærdighed. (4) Forklarlighed. Som allerede anført udspringer disse af allerede eksisterende lovgivning, hvorfor de også omfattes af kravet om lovlig kunstig intelligens. Det første princip *'respekt for menneskers autonomi'* omhandler den registreredes ret til at forblive selvbestemmende i forbindelse med at interagere med kunstig intelligens. Den registrerede, eller mennesket i det hele taget, har ret til at få sin frihed respekteret og i den forbindelse må kunstig intelligens ikke tvinge, manipulere eller på andre måder styre den registrerede. I relation til kunstig intelligens anbefaler Ekspertgruppen, at systemerne i stedet programmeres til at forstærke, supplere og fremme den menneskelige kognition og sociale færdigheder. Systemet skal være designet ud fra devisen om, at mennesket skal være i centrum og i kontrol med systemet. Det andet princip *'forebyggelse af skade'* omhandler det systemiske omkring

[126] Den Uafhængige Ekspertgruppe På Højt Niveau om Kunstig Intelligens (2019): "*Etiske retningslinjer for pålidelig kunstig intelligens*", side 7.
[127] Den Uafhængige Ekspertgruppe På Højt Niveau om Kunstig Intelligens (2019): "*Etiske retningslinjer for pålidelig kunstig intelligens*", side 9.

kunstig intelligens, og de tekniske og organisatoriske foranstaltninger der bør være implementeret for at sikre tilstrækkelig robusthed og sikkerhed for den registrerede. Systemerne og de miljøer hvori de anvendes bør være beskyttede i en sådan grad, at mennesker ikke påvirkes negativt, eller at skade hverken kan forårsages eller forværres. Det tredje princip *'retfærdighed'* omhandler registreredes ret til ikke at blive udsat for diskrimination eller stigmatisering i forbindelse med anvendelse af kunstig intelligens-systemer. Ligeledes indeholder dette princip en mulighed for den registrerede til at kunne anfægte eller søge effektive retsmidler mod de beslutninger, som træffes af disse systemer. Det fjerde princip indeholder et krav om '*forklarlighed*', hvilket betyder, at registrerede har ret til at indsigt i, hvad deres personoplysninger brugt til, og hvad der ligger til grund for de afgørelser eller beslutninger, som systemet måtte komme frem til. Dette er afgørende for tilliden til systemerne, og uden denne indbyggede mulighed i systemet, er det ikke muligt for registrerede at anfægte en beslutning, hvilket betyder at det tredje princip ligeledes ikke overholdes[128].

Efterlevelse af disse 4 principper kommer ikke uden udfordringer for anvendere og udviklere af kunstig intelligens. Alle 4 principper indeholder elementer som kan genkendes fra forordningens krav, som denne afhandling allerede har beskrevet og analyseret. Princippet om '*forklarlighed*' udgør en udfordring, da den enorme mængde data og de mange komplekse beslutningslag i en online model baseret på deep learning gør, at det ikke altid er muligt at udtrække de oplysninger eller informationer der ligger til grund for en afgørelse eller beslutning. Dette er også beskrevet i afsnit 5.4 om den sorte boks. Det samme gør sig gældende ved princippet om *'respekt for menneskers autonomi'*. Ekspertgruppen anvender et eksempel om en kunstig intelligens model der kan udføre forudsigende politiarbejde, som kan hjælpe med at nedbringe kriminaliteten. Udfordringen er naturligvis, at dette medfører overvågning af forskellige former, som kan have en krækende effekt på den enkeltes privatliv og frihed. Anvendere og udviklere af kunstig intelligens skal ikke blot efterleve de regler og principper der fremstilles i forordningen, men bør ud fra et kollektivt samfundsmæssigt perspektiv også iagttage disse etiske principper, således tilliden til kunstig intelligens er sikret. Det er ikke desto mindre utænkeligt, at der opstår konkrete situationer hvor brugen af kunstig intelligens kunne skabe værdi for den enkelte, men hvor den etiske afvejning ikke findes acceptabel. Som eksemplet med forudsigende politiarbejde. Det fremgår ligeledes af Ekspertgruppens retningslinjer, at visse rettigheder, og

[128] Den Uafhængige Ekspertgruppe På Højt Niveau om Kunstig Intelligens (2019): "*Etiske retningslinjer for pålidelig kunstig intelligens*", side 12 – 13.

principperne knyttet hertil, må betragtes som absolutte, og på den måde ikke kan være genstand for afvejning eller skønsmæssig vurdering[129].

7.3.2 Gennemsigtighed

En kritisk komponent for opnåelse af pålidelige kunstig intelligens er princippet om gennemsigtighed. Gennemsigtighed er hjemlet i persondataforordningens artikel 5, stk. 1, litra a og Ekspertgruppen præsenterer ligeledes princippet i deres engelske rapport om pålidelig kunstig intelligens. De angiver, at gennemsigtighed opnås ud fra 3 komponenter: (1) Sporbarhed. (2) Forklarlighed (3) Kommunikation. For at sikre tillid til kunstig intelligens, er det væsentligt at kravet om '*sporbarhed*' ('traceability') er efterlevet. Udviklere og anvendere af kunstig intelligens skal i udviklingen af kunstig intelligens modeller sikre, at det data og de processer, som beslutninger og afgørelser træffes på baggrund af, er tilstrækkeligt dokumenterede, således de er sporbare. Der skal implementeres løsninger og foranstaltninger, der kan imødekomme denne forpligtelse, hvis det ultimative krav om gennemsigtighed skal efterleves. Kravet om '*forklarlighed*' ('Explainability') er ligeledes tidligere gennemgået, og Ekspertgruppen tilføjer i deres engelske rapport, at dette princip skal sikre, at de tekniske processer i den kunstige intelligens, samt ræsonnementerne bag beslutningerne, skal kunne forklares. Det skal være muligt for den registrerede at få indsigt i, hvordan vedkommendes data benyttes og på hvilken baggrund beslutninger eller afgørelser træffes, da den registrerede har ret til at bestride eller sætte spørgsmålstegn ved disse. Den tredje komponent i gennemsigtighedskravet er, ud fra Ekspertgruppens vurdering, *'åben kommunikation'* ('Open communication'). Det angiver at systemets muligheder og begrænsninger ud fra den konkrete situation, skal kommunikeres ud til de registrerede. Der bør implementeres mekanismer som sikrer, at eksempelvis formål, kriterier og begrænsninger ved beslutningsprocessen i den kunstige intelligens, bliver kommunikeret ud til de registrerede[130].

Som tidligere gennemgået i denne afhandling er princippet om gennemsigtighed en del af forordningens altoverskyggende hovedprincip, hvilket findes i artikel 5, stk. 1, litra a. I relation til kunstig intelligens er disse 3 komponenter med til at nedbryde kravet om gennemsigtighed i flere dele, således det for udviklere og anvendere fremstår håndgribeligt. Ud fra en teknisk og praktisk betragtning er der ikke desto mindre udfordringer forbundet med efterlevelse af krav som '*sporbarhed*' og

[129] Den Uafhængige Ekspertgruppe På Højt Niveau om Kunstig Intelligens (2019): "*Etiske retningslinjer for pålidelig kunstig intelligens*", side 14.
[130] Independent High-Level Expert Group on Artificial Intelligence (2019): "*The Assessment List for Trustworthy Artificial Intelligence (ALTAI)*", side 14 – 15.

'*forklarlighed*', da kompleks kunstig intelligens baseret på online modeller vanskeliggør muligheden for at spore data, og dermed vanskeliggør det at give forklaringer på, hvad der ligger bag beslutninger eller afgørelser.

7.3.3 Retfærdighed

'*Retfærdighed*' bliver, i denne afhandling, som bekendt introduceret af Ekspertgruppen som ét af de 4 etiske principper der bør overholdes, hvis pålidelig kunstig intelligens skal opnås. Princippet nævnes imidlertid ligeledes i andre rapporter, eksempelvis i den skrevet af det Norske Datatilsyn, og forekommer mere grundlæggende end som så. Princippet er tæt beslægtet med det altoverskyggende princip i artikel 5, stk. 1, litra a om "*lovlighed, rimelighed og gennemsigtighed*", men fremgår ikke eksplicit i forordningen. Princippet om '*retfærdighed*' skal forstås i relation til hvordan den kunstige intelligens model vægter og kvalificerer daten under en databehandlingsproces. Registrerede har krav på ikke at blive forskelsbehandlet på baggrund af usaglige eller diskriminerende faktorer, såsom race, religion, politisk overbevisning og lignende. Ekspertgruppen angiver herudover at tilsidesættelse af kravet om 'retfærdighed' (eller 'Fairness'), også kan gøres ved uretmæssigt forsætlig udnyttelse af registreredes forbrugsdata, som led i at skabe unfair konkurrencevilkår. Dette vil betyde manglende gennemsigtighed i et marked, der ellers skal være homogent og drevet på lige vilkår. Kunstig intelligens systemer skal være designet til at have den registrerede i centrum, og skal have respekt for de registreredes interesser. Det Norske Datatilsyn foreslår, at der i udviklingen af den kunstige intelligens model, ikke alene skal bruges matematiske eller statistiske fremgangsmåder, men også intensiv træning af modellen, således den lærer, at vægte relevante og rigtige oplysninger i den konkrete databehandling. På denne måde sikres det, at der ikke lægges vægt på usaglige eller forkerte oplysninger, der vil lede til diskriminerende afgørelse eller beslutninger[131] [132].

[131] Det Norske Datatilsyn (2018): *"Kunstig Intelligens og personvern*", side 15.
[132] Independent High-Level Expert Group on Artificial Intelligence (2019): "*The Assessment List for Trustworthy Artificial Intelligence (ALTAI)*", side 16.

8. Litteraturliste

- **Article 29 Data Protection Working Party** (2013): "*opinion 03/2013 on purpose limitation*".

- **Article 29 Data Protection Working Party** (2018): "*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*".

- **Blume, P**. (2018): "*Den nye persondataret*" 2. udgave. Jurist – og Økonomforbundets forlag.

- **Den Uafhængige Ekspertgruppe På Højt Niveau om Kunstig Intelligens** (2019): "*Etiske retningslinjer for pålidelig kunstig intelligens*". Etableret af Europa-Kommissionen i juni 2018.

- **Det Norske Datatilsyn** (2018): "*Kunstig Intelligens og Personvern*".

- **Digitaliseringsstyrelsen** - https://digst.dk/strategier/kunstig-intelligens/strategi-for-kunstig-intelligens/ (Artikel fra marts 2019. Downloadet den 15/2 2021)

- **ENISA, European Union Agency for Network And Information Security** (2016): "*Big Data Threat Landscape and Good Practice Guide*".

- **ENISA, European Union Agency for Network And Information Security** (2015): "*Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics*".

- **Etisk råd** - https://www.etiskraad.dk/etiske-temaer/optimering-af-mennesket/homo-arte-fakt/leksikon/kunstig-intelligens (Artikel fra september 2007. Downloadet den 16. februar 2021)

- **Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016** om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EØS-relevant tekst)

- **Evald, J**. (2020): "*Juridisk teori, metode og videnskab*" 2. udgave. Jurist – og Økonomforbundets forlag.

- **Faktalink** - https://faktalink.dk/titelliste/kunstig-intelligens (Artikel fra januar 2015. Opdateret april 2018. Downloadet 24. januar 2021)

- **High Level Expert Group on AI** (AI HLEG) (2019): "*The Assessment List For Trustworthy Artificial Intelligence*".

- **Horten** - https://www.horten.dk/viden/artikler-2018/kunstig-intelligens-gdpr-og-andre-juridiske-udfordringer (Artikel fra april 2020. Downloadet 10. februar 2021)

- **IBM** - https://www.ibm.com/cloud/learn/what-is-artificial-intelligence (Artikel fra juni 2020. Downloadet den 23. februar 2021)

- **Independent High-Level Expert Group on Artificial Intelligence** (2019): "*The Assessment List for Trustworthy Artificial Intelligence (ALTAI)*". Set by the European Union.

- **Justitsministeriets betænkning nr. 1565** (2017): "*Databeskyttelsesforordningen (2016/679) – og de retlige rammer for dansk lovgivning*". Bind 1 – del 1.

- **Maryville University** - https://online.maryville.edu/blog/big-data-is-too-big-without-ai/ (Artikel fra ukendt. Downloadet den 12. februar 2021)

- **Munk-Hansen, C**. (2018): "*Retsvidenskabsteori*" 2. udgave.

- **UMBEL – Costumer Data Platform** (2015): "*AI meets Big Data*".

- **Videnskab.dk** - https://videnskab.dk/teknologi-innovation/black-box-problemet-naar-vi-ikke-forstaar-den-kunstige-intelligens (Artikel fra november 2017. Downloadet den 27. februar 2021)

- **Villaronga, E. F., Kieseberg, P.,** & **Li, T**. (2017): "*Humans forget, machines remember: Artificial intelligence and the right to be forgotten*".

- **Von Eyben, W. E**. (1991): "*Juridisk Grundbog Bind 1 – Retskilderne*" 5. udgave. Jurist – og Økonomiforbundets forlag.

9. Figuroversigt

Figur 1:

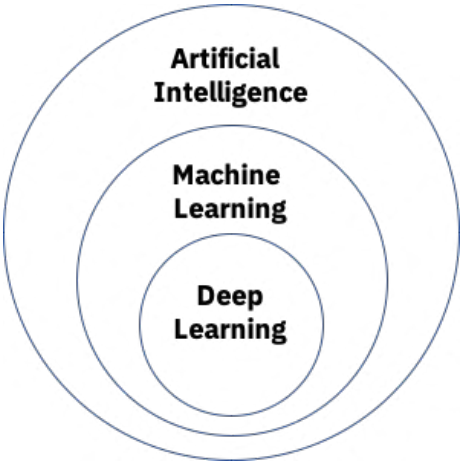


Illustration af sammenhængen mellem begreberne:

"*Artificial Intelligence*", "*Machine Learning*" og "*Deep Learning*".

Kilde: IBM Cloud Education: https://www.ibm.com/cloud/learn/what-is-artificial-intelligence …… side 12.

Figur 2:

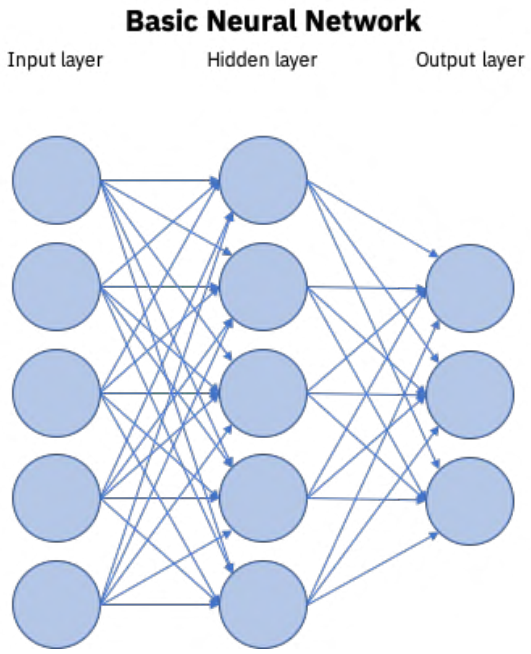


Illustration af sammenhæng mellem de 3 niveauer i det basale neurale netværk.

Kilde: IBM Cloud Education: https://www.ibm.com/cloud/learn/what-is-artificial-intelligence …….…….. side 17.

Figur 3:

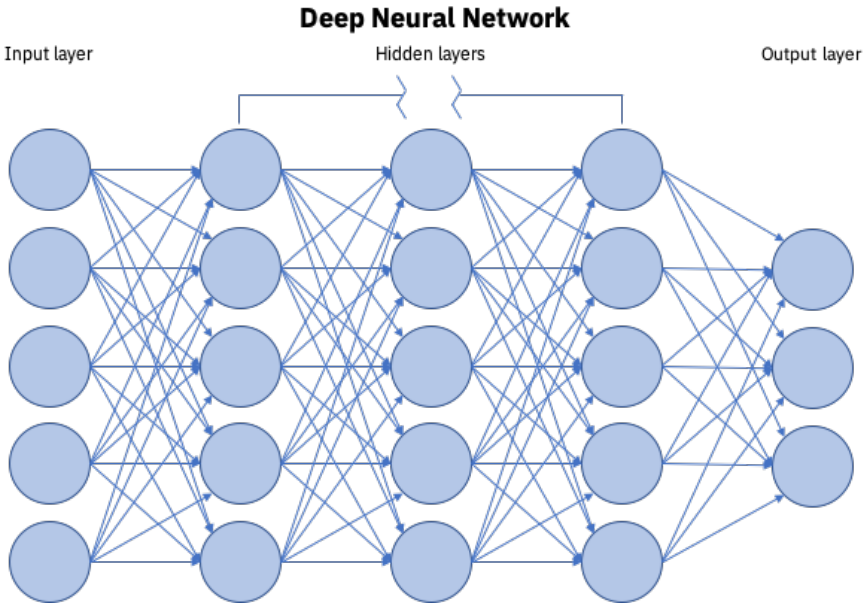


Illustration af sammenhæng mellem niveauerne i det dybe neurale netværk.

Kilde: IBM Cloud Education: https://www.ibm.com/cloud/learn/what-is-artificial-intelligence …… side 20.

Figur 4:

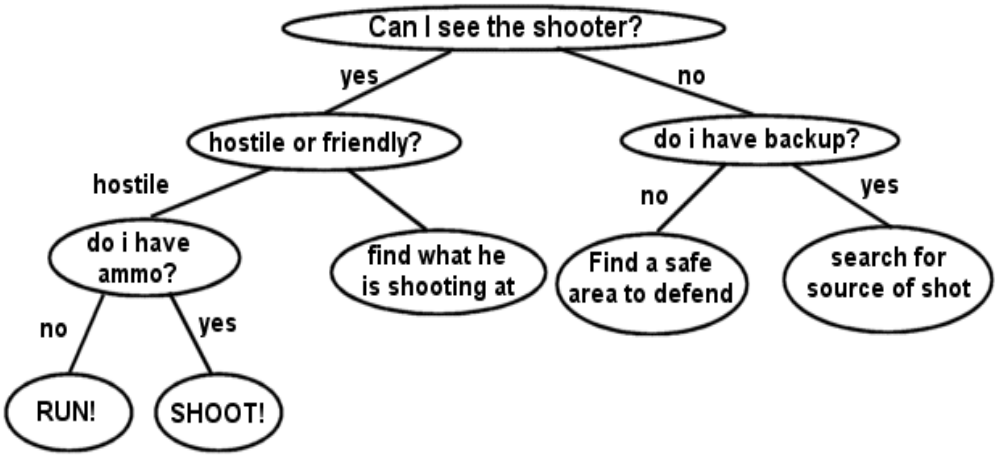


Illustration af et beslutningstræ.

Kilde: https://corydesmondai.wordpress.com/2014/10/01/the-island-genre-and-implementation-of-ai/ …….. side 24.