Det retlige sammenspil mellem databeskyttelsesretten og AI

Aalborg Universitet 2020

Maria N. Sevelsted & Nanna Buus Nielsen

Vejleder: Kasper Bjerre Hendrup Andersen

Kandidatafhandling | Erhvervsjura | Juridisk Institut

Antal anslag: 160.824

English summery

AI is perhaps the most influential technology at the moment and the capability of AI creates widespread and substantial benefits for the society. The use of Deep Learning and Big Data have created benefits and value for data controllers, but it is not without difficulties. Big Data uses voluminous data sets, which will often contain personal data, while other challenges can originate from the complexities of the algorithms used in Deep Learning. This can create problems when AI is used for processing personal data.

This dissertation explores the possibility of using AI as a basis for processing personal data. The legal base for data protection is Regulation 2016/679 (GDPR). Data Controllers face inherent challenges when complying with GDPR. The GDPR presents some principles and general obligations for the data controller, and this dissertation will analyze those most relevant for the use of AI. The purpose of this dissertation is to provide insight into the aforementioned technologies behind AI and the use of AI in relation to the processing of personal data.

One of the main concerns is the emerging of the Black Box that can lead to a lack of transparency. This dissertation will explore the scope of the transparency principle, and whether it is possible to uphold transparency when using AI.
Furthermore, the use of AI technology when processing personal data will result in the application of article 22 in the GDPR, defined as automated individual decision-making, including profiling. This article provides a right for the data subject not to be subject to a decision based solely on automated processing. The dissertation will explore the scope, content and exceptions of this article, including whether the article puts a stop to the use of AI in relation to the processing of personal data.

Finally, the dissertation will explore whether it is ethically sound to use AI for processing personal data. The ethical point of view can provide guidelines for when and of AI should be used, in relation to personal data. The ethics is not legally binding, but it can create an additional protection for the data subject.

A major concern regarding the processing of personal data with specific AI tools, relates to the lack of transparency of the process as well as the decision. This can create problems for the data controller when complying with the GDPR.
GDPR does not make it impossible for the data controller to comply with the responsibilities in GDPR. Though, AI models do face challenges that can make it difficult to uphold the GDPR due to the lack of general practice.

Indholdsfortegnelse

1. Indledning

"Rettens tempo er maraton, mens virkeligheden med den innovative informationsteknologi bevæger sig i sprint"[1]. Retstilstanden bliver udfordret af det moderne informationssamfund, hvilket kan forekomme problematisk, såfremt lovgivningen ikke kan følge med.[2] Det er blevet mere og mere almindeligt, at informationer spredes, og grundet mulighederne ved arbejde med enorme datamængder, er der opstået en værdi for udnyttelse af den data, som er tilgængelig. Databeskyttelsesbehovet opstår derfor især på baggrund af den grundlæggende iagttagelse om, at oplysninger om individet kommer uvedkommende til kundskab med den risiko, at oplysningerne kan misbruges med integritetskrænkelser til følge. [3] Derfor er der et behov for, at der opstilles klare retningslinjer for, hvordan behandlingen af personoplysninger skal ske.

Retningslinjerne blev til en aktualitet i 2016, hvor *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)* (Herefter benævnt Databeskyttelsesforordningen) blev vedtaget. Databeskyttelsesforordningen trådte i kraft d. 25. maj 2018[4], og er derfor i dag en integreret del af det europæiske og nationale retsgrundlag.[5] Processen for, hvordan denne nye EU-retlige lovregulering skulle se ud, var langsommelig.[6] Den nye persondatareform blev for første gang fremlagt i 2012 af Europa-kommissionen.[7] I årene forud havde der været en omfattende diskussion omkring behovet for denne nye regulering.[8] Det har således taget op mod 10 år, før en ny regulering på persondataområdet blev vedtaget. I samme periode er der sket en enorm teknologisk udvikling, blandt andet indenfor Artificial Intelligence (herefter benævnt AI).

AI er i dag et verdenskendt fænomen[9], og det er specielt indenfor det seneste årti, at AI er blevet mere og mere udbredt.[10] Grundet den teknologiske udvikling, og de betydelige praktiske og ressourcemæssige fordele, som er forbundet med AI[11], medfører dette, at AI er blevet en del af hverdagen i en stor del af

[1] *Peter Blume:* Den nye persondataret (2018) side 268
[2] *Kristian Korfits Nielsen og Anders Lotterup*: Databeskyttelsesforordningen og Databeskyttelsesloven (2020) side 158
[3] *Peter Blume:* Den nye persondataret (2018) side 267
[4] Forordning 2016/679, artikel 99, stk. 2.
[5] TEUF artikel 288
[6] *Peter Blume*: Den nye persondataret (2018) side 13-14
[7] Ibid., side 13
[8] Ibid., side 13
[9] *Centre for Information Policy Leadership:* Artificial Intelligence and Data Protection in Tension (2018), side 3
[10] Ibid., side 3
[11] *Peter Blume:* Den nye persondataret (2018) side 263

erhvervslivet, da det er offentligt kendt, hvilke muligheder samt værdi AI kan skabe.[12] Der er ingen tvivl om, at AI både kan og vil skabe værdi for samfundet, hvilket ikke blot gælder for den private sektor, men også i den offentlige sektor.[13] Til trods for de potentielle fordele inden for det tekniske område, kan der opstå betydelige potentielle negative konsekvenser ved anvendelse af AI.[14]

AI er ofte baseret på store mængder data, hvilket kan frembringe nye angrebsflader.[15] Ofte, men ikke altid, vil denne data omfatte persondata. Hvor dette er tilfældet, skal der tages højde for de databeskyttelsesretlige regler. Databeskyttelsesforordningens opgave er at beskytte det enkelte individ og dennes rettigheder og frihedsrettigheder.[16] Eftersom det tager lang tid at lave og vedtage en ny regulering, vil lovgivningsmagten formentlig aldrig opnå at kunne følge med den teknologiske udvikling. Derfor er Databeskyttelsesforordningen forsøgt udformet teknologineutralt. Dette er gjort for at undgå at skabe risiko for omgåelse af lovreglerne.[17]
Databeskyttelsesforordningen orienterer sig ikke direkte mod AI, men det kan overvejes, hvorvidt Databeskyttelsesforordningen sikrer en menneskelig kontrol af personoplysninger ved behandling baseret på AI.[18] Under alle omstændigheder repræsenterer AI en udfordring til databeskyttelsesretten.[19] Hvor stor denne udfordringer viser sig at være, forekommer dog uvist.

[12] *Centre for Information Policy Leadership:* Artificial Intelligence and Data Protection in Tension (2018), side 3
[13] Ibid., side 3
[14] *Thomas Bolander:* Kunstig intelligens: Bliver mennesker overflødige? (2017), se afsnit: *Bagsiden af kunstig intelligens*
[15] https://erhvervsstyrelsen.dk/ny-vejledning-saetter-fokus-paa-sikkerheden-ved-brug-af-kunstig-intelligens-i-praksis?fbclid=IwAR3WRqVQeIfeVqkuU_NGQ0cTyTwkrm6hDqH7vy2vAjGMAv1LDaZBmHWN4jM
[16] *Peter Blume*: Personen i Persondataretten (2019) side 11-12
[17] Forordning 2016/679, præambelbetragtning nr. 15
[18] *Peter Blume:* Den nye persondataret (2018) side 263
[19] Ibid., side 263

2. Problemformulering

På baggrund af udviklingen indenfor den moderne informationsteknologi, samt den øgede anvendelse af AI, vil nærværende afhandling undersøge hvilke problematikker, der opstår som følge af det retlige sammenspil mellem databeskyttelsesretten og den dataansvarliges anvendelse af AI.

Den overordnede problemstilling lyder som følgende:
I hvilket omfang kan en dataansvarlig behandle personoplysninger ved anvendelse af AI under hensyntagen til overholdelsen af udvalgte retlige forpligtelser indeholdt i forordning 2016/679 om databeskyttelse? Såfremt den dataansvarlig har mulighed herfor, vil en sådan anvendelse belyses ud fra etiske overvejelser om databeskyttelse.

Først i afhandlingen bliver læseren introduceret for et redegørende afsnit om de væsentligste begreber inden for AI samt relevante tekniske termer for afhandlingens hovedfokus. Den tekniske introduktion efterfølges af en redegørelse for Databeskyttelsesforordningens grundlag og dennes anvendelsesområde, samt udvalgte kernebegreber heri.
Dette følges op af en beskrivelse og analyse af udvalgt grundlæggende principper og forpligtelser indeholdt i Databeskyttelsesforordningen. Fokus vil især være på en udførlig analyse af gennemsigtighedsprincippet, samt Databeskyttelsesforordningens artikel 22, som omhandler automatiske individuelle afgørelser, herunder profilering.

Læseren vil løbende blive præsenteret for delkonklusioner, som indeholder en opsummering af centrale punkter i det tilknyttede afsnit. Til sidst i afhandlingen udledes en samlet konklusion, hvori afhandlingens problemstilling besvares.

Afslutningsvist vil afhandlingen perspektivere til, hvorvidt det med dataetiske overvejelser kan vurderes hensigtsmæssigt at anvende et AI system ved databeskyttelsesretlig behandling, herunder om en behandling ikke bør udføres af hensyn til dataetiske overvejelser.

3. Metode

For at besvare afhandlingens problemstilling er det nødvendigt at redegøre for relevante bestemmelser i Databeskyttelsesforordningen, herunder i lyset af behandling ved anvendelse af AI. Til dette anvendes den retsdogmatiske metode, de lege lata. Ved brug af denne metode beskrives og analyseres den i samtiden gældende retstilstand.[20] Opgavens formål er at finde og fastlægge de forskellige regler og principper, der især er relevante ved databeskyttelsesretlig behandling ved brugen af AI.[21] Disse regler og principper vil blive analyseret, og en eventuel retlig tvivl vil blive præciseret.[22] Den retsdogmatiske metode er ikke rettet mod at finde en løsning af konkrete problemer, men derimod at undersøge retstilstanden på et givent område.[23]

Afslutningsvist vil der i opgaven blive benyttet den retspolitiske metode, de lege ferenda.[24] Denne bruges ved at perspektivere til, hvorvidt gældende ret er etisk forsvarligt, når der er tale om databeskyttelsesretlig behandling ved anvendelse af AI. Der er ingen tvivl om, at AI bliver mere almindeligt, og derfor undersøges det i opgaven, hvilke problemstillinger, der kan opstå, når persondatabehandling ved anvendelse af AI kobles sammen med etiske værdiopfattelser. Retspolitikken anvendes derfor som en moralfilosofi, som tager udgangspunkt i de etiske standpunkter for en ønskelig regulering.[25]

3.1 Retskilder

Den primære retskilde, der benyttes i nærværende afhandling, er en forordning, som er vedtaget på europæisk plan. Databeskyttelsesforordningen har virkning som supranational ret, hvilket betyder, at den er almengyldig som en lov, og gælder direkte.[26] Databeskyttelsesforordningen er den centrale retskilde i dansk persondataret.[27]

I Databeskyttelsesforordningen er der tillagt et råderum, som kan udfyldes af national lovgivning.[28] Derfor er der i Danmark blevet vedtaget *Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger*

[20] *Carsten Munk Hansen*: Retsvidenskabsteori, (2018) side 204
[21] Ibid., side 205
[22] Ibid., side 205
[23] Ibid., side 204
[24] Ibid., side 73
[25] Ibid., side 73-74
[26] TEUF artikel 288, stk. 1.
[27] *Peter Blume*: Databeskyttelsesret (2018) side 60
[28] Ibid., side 53

(databeskyttelsesloven)[29] (herefter benævnt Databeskyttelsesloven), som supplerer Databeskyttelsesforordningen.[30]

Databeskyttelsesforordningen og Databeskyttelsesloven erstatter det tidligere gældende Persondatadirektiv[31] (herefter benævnt Persondatadirektivet), som blev implementeret i dansk ret med Persondataloven[32] (herefter benævnt Persondataloven). Hvor det anses relevant, vil Persondatadirektivet blive inddraget i afhandlingen, af hensyn til fortolkningsspørgsmål.

I afhandlingen vil der blive inddraget vejledninger fra Det Europæiske Databeskyttelsesråd (herefter benævnt Databeskyttelsesrådet), som er et uafhængigt EU-organ, hvis opgave er at sikre en ensartet anvendelse af Databeskyttelsesforordningen i EU. Databeskyttelsesrådet afløste d. 25. maj 2018 den tidligere Artikel 29-Gruppe.[33] Udover at give generel vejledning, kan Databeskyttelsesrådet også træffe bindende afgørelser omkring fortolkning af databeskyttelsesreglerne, hvor der er uenigheder tilsynene imellem.[34] Disse bliver offentliggjort i de såkaldte arbejdspapirer. Databeskyttelsesrådet består af en repræsentant fra hvert af medlemsstaternes tilsynsmyndighed, og eftersom arbejdspapirerne er udformet af dem, er det naturligt, at arbejdspapirerne lægges til grund i tilsynsmyndighedernes praksis.[35] [36] Arbejdspapirerne er ikke juridisk forpligtende for medlemsstaterne og deres datatilsyn, men har status som soft law.[37] De arbejdspapirer der anvendes i afhandlingen, er udgivet af Artikel 29-gruppen. Arbejdspapirerne er dog senere blevet endosseret af Databeskyttelsesrådet, hvorfor disse må tillægges stor betydning, på trods af, at Artikel 29-gruppen ikke længere er eksisterende.[38]

I afhandlingen inddrages der ligeledes vejledninger og lister fra Datatilsynet.
Datatilsynet fungerer som en tilsynsmyndighed, og deres primære opgave er, at vurdere alle databeskyttelsesretlige spørgsmål og træffe afgørelser med hensyn til, om en bestemt adfærd er i overensstemmelse med Databeskyttelsesforordningen og Databeskyttelsesloven.[39] Udover at træffe

[29] Lov nr. 502 af 23/05/2018
[30] *Peter Blume*: Databeskyttelsesret (2018) side 53-54
[31] Direktiv 95/46 EF
[32] Lov nr. 429 af 31/05/2000
[33] https://www.datatilsynet.dk/internationalt/databeskyttelsesraadet-edpb/
[34] Ibid.
[35] Ibid.
[36] *Peter Blume*: Databeskyttelsesret (2018) side 61-62
[37] Ibid., side 61
[38] *Peter Blume:* Den nye persondataret (2018) side 52-53
[39] *Peter Blume*: Databeskyttelsesret (2018) side 57

afgørelser, udsteder Datatilsynet også vejledninger for, hvordan der kan ske overholdelse af de databeskyttelsesretlige regler. Vejledningerne skal forstås som en beskrivelse af gældende ret, og kan derfor hjælpe til at forstå Databeskyttelsesforordningens og Databeskyttelseslovens regler. Inden for nogle områder i Databeskyttelsesforordningen er det overladt til Datatilsynet at udfylde eller uddybe reglerne. Dette er blandt andet tilfældet indenfor konsekvensanalyser, hvor der er givet Datatilsynet bemyndigelse til at lave lister over behandlinger, hvor der altid bør udarbejdes en konsekvensanalyse, jf. Databeskyttelsesforordningens artikel 35, stk. 4 og 5. Eftersom der på nuværende tidspunkt ikke foreligger relevante afgørelser i henhold til AI, vil der ikke inddrages retspraksis fra Datatilsynet i afhandlingen.

I afhandlingen vil der ligeledes blive inddraget en rapport fra det Norske Datatilsyn. Det Norske Datatilsyn har samme betydning i Norge, som Datatilsynet har i Danmark. Norge er et EØS-land, hvorfor Databeskyttelsesforordningen gælder direkte i Norge. Det er i Databeskyttelsesforordningens artikel 63 fastlagt at, hvor det er relevant, skal tilsynsmyndighederne samarbejde, for *"at bidrage til en ensartet anvendelse af denne forordning i hele Unionen"*[40]. Med baggrund i den sammenhængsmekanisme, som fremgår af Databeskyttelsesforordningen, anvendes rapporten fra det Norske Datatilsyn i afhandlingen.

I opgaven vil der ligeledes blive inddraget forskellige artikler og andet litteratur. Disse har ikke en retskildemæssig betydning, men deres effekt er at være med til at beskrive gældende ret.[41]

[40] Forordning 2016/679, artikel 63
[41] *Peter Blume*: Databeskyttelsesret (2018) side 58

4. Afgrænsning

Idet nærværende afhandling tager udgangspunkt i AI, vil der blive defineret relevante tekniske termer, men da der er tale om en juridisk afhandling, vil dette område være begrænset til, hvad der er relevant for afhandlingen. Særlig relevant anses brugen af Machine Learning, Deep Learning, herunder neuralt netværk og Big Data. AI vil blive inddelt i tre hypotetiske faser, som anvendes konsistent gennem hele afhandlingen.

Det forventes, at læseren har en generel viden om databeskyttelsesreglerne, hvorfor kun relevante begreber i Databeskyttelsesforordningen vil blive defineret i afhandlingen. Den dataansvarlige skal som pligtsubjekt iagttage adskillige pligter indeholdt i Databeskyttelsesforordningen, hvor nærværende afhandling alene vil belyse et udvalg heraf. Afhandlingen vil primært fokusere på Databeskyttelsesforordningens artikel 5, 12-14, 22, 25 og 35. Dertil vil en række yderligere bestemmelser blive behandlet overfladisk, hvor dette anses relevant.
Grundet Databeskyttelsesforordningens historiske baggrund iagttages tidligere regler af hensyn til fortolkningsspørgsmål. Disse tidligere regler vil være begrænset til Persondatadirektivet, hvorfor Persondataloven ikke vil blive omtalt.

Databeskyttelsesreglerne har virkning for både den offentlige og private sektor. I flere af Databeskyttelsesforordningens artikler forekommer der undtagelser, som ikke nødvendigvis har samme betydning for begge sektorer. I afhandlingen vil der dog ikke blive skelnet mellem de førnævnte regler samt undtagelser, men der vil blot være fokus på det overordnede billede, da dette anses værende mere relevant for afhandlingen.

Der vil i afhandlingen ikke blive fortaget en uddybelse af reglerne og problematikkerne for overførsel af personoplysninger til tredjelande samt anvendelsen af AI i forbindelse hermed.

Afslutningsvist vil afhandlingen perspektivere til etiske overvejelser. Dette vil alene ske i lyset af det allerede belyste retlige sammenspil mellem databeskyttelsesreglerne og AI.

5. Artificial Intelligence og det tekniske bagved

For 60 år siden forsøgte AI eksperten John McCarthy at definere AI begrebet på følgende måde: *"the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable."*[42] Denne definition er til en vis grad stadig gældende. I dag er der blot mere fokus på, at AI i bund og grund handler om, at få teknologien til at gøre ting, som hidtil kun har kunnet opnås af mennesker. Såfremt computeren løser en opgave som ellers kræver et intelligent menneske, kaldes det for AI.[43]

AI er i dag udbredt i både den offentlige og private sektor[44] og er særligt kendt inden for billed- og talegenkendelse, udvikling af ny medicin, selvkørende biler, robotter, søgemaskiner på nettet og aktiehandel.[45]

Særligt grundet mulighederne for at behandle store datamængder samt at udføre analyser herpå, har denne form for teknologi fået en stor værdi.[46] Før i tiden var det specielt større virksomheder, der havde mulighed for at arbejde med AI, grundet den store udgift til udvikling af et fungerende AI system, men den dag i dag bruges det i langt flere virksomheder i større eller mindre omfang.[47]

AI anses for at være meget komplekst.[48] AI forstås generelt som algoritmer, der blandt andet kan udføre kognitive funktioner. Det vil sige en maskine, som efterligner menneskelig tankegang.[49] Med dette forstås, at maskinen kan udvikle sig selv, lære at løse problemer eller planlægge ud fra en given viden.[50] AI maskinen kan opbygges, således den kan tilpasse sig løbende, hvilket kan sammenlignes med den menneskelige udvikling.

AI fungerer ikke blot ved hjælp af algoritmer. Et andet vigtigt element for en AI er data.[51] Jo mere data, en AI bliver fyldt med, jo flere mønstre bliver der dannet. Data er derfor essentiel for AI, og opbygningen og brugen

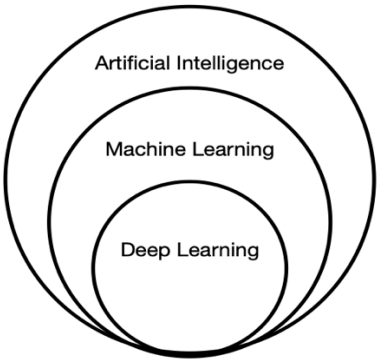
[42] *Júlio Regeto og Thiago Luis Sombra:* Artificial intelligence, data protection and the future of inventions (2018), 2. afsnit
[43] https://ida.dk/viden-og-netvaerk/temaer/kunstig-intelligens, tid: 3:00
[44] *Centre for Information Policy Leadership*: Artificial Intelligence and Data Protection in Tension (2018), side 3
[45] *Thomas Bolander*: Hvad er Kunstig Intelligens egentlig? (2018), se 1. del
[46] https://www.teknologisk.dk/ydelser/big-data-og-anvendelse-af-data/37949
[47] https://ida.dk/viden-og-netvaerk/temaer/kunstig-intelligens, tid: 7:30
[48] *Thomas Bolander*: Hvad er Kunstig Intelligens egentlig? (2018)
[49] https://ida.dk/viden-og-netvaerk/temaer/kunstig-intelligens, tid: 11:20
[50] Ibid., tid: 13:50
[51] Ibid., tid: 20:00

af maskinen vil ikke være muligt uden data. Selve kvaliteten af data spiller også en central rolle, og derfor bruges der ofte en del tid på gennemgang af dataene inden de indføres i maskinen.[52]

Teknologien er endnu ikke nået til at AI fuldt ud kan erstatte mennesker.[53] [54] Derimod benyttes AI til at udføre eller løse specifikke opgaver hurtigt og med stor korrekthed, hvorfor det i et stort omfang ses, at AI kan assistere mennesket med at træffe en endelig beslutning.[55] Endvidere er flere AI maskiner i stand til at behandle data og finde sammenhænge, som den menneskelige hjerne ikke er i stand til at overskue.[56] Nedenstående belyses udvalgte områder og definitioner indenfor AI, da disse anses for særlig relevant for nærværende afhandling.

5.1 Machine Learning og Deep Learning[57]

Det er tidligere lagt til grund, at AI ikke blot er et simpelt fænomen, hvorfor nedenstående illustration kan forklare, hvordan AI kan være bygget op. Set fra et større perspektiv er AI den yderste cirkel, hvortil Machine Learning er en undergruppe hertil.[58] Herefter kommer den inderste cirkel kendt som Deep Learning, der er en mere kompleks udgave af Machine Learning. [59]



Figur 1 "Illustration af AI's opbygning"
Kilde: *Egen tilvirkning*

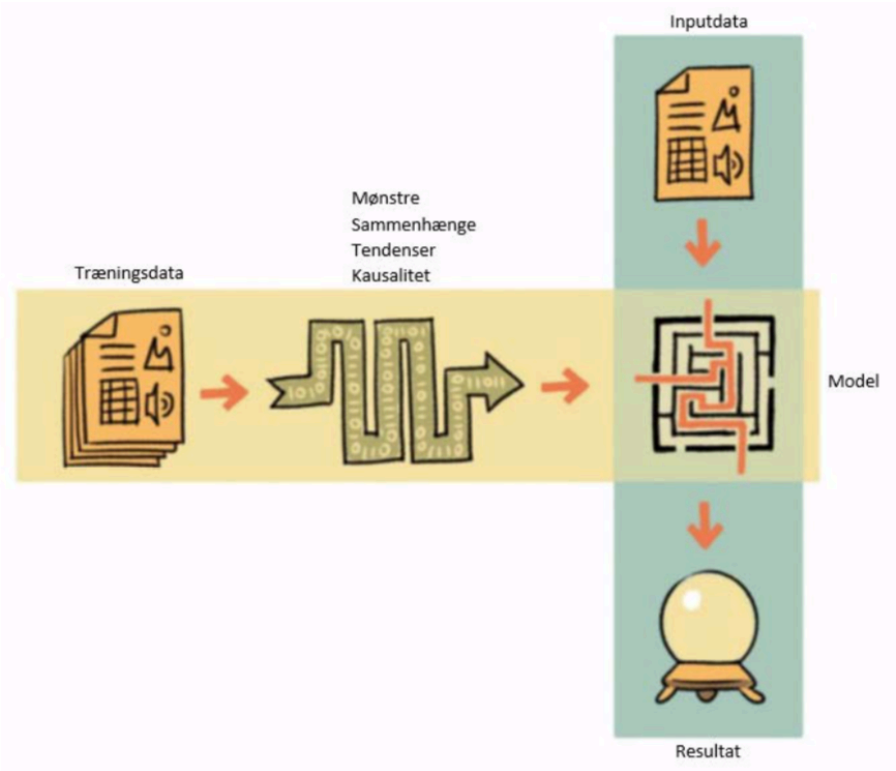
[52] https://ida.dk/viden-og-netvaerk/temaer/kunstig-intelligens tid: 20:50
[53] *Thomas Bolander:* Kunstig Intelligens: Bliver mennesker overflødige? (2017)
[54] *Louis Cruz-Filipe:* AI: Sådan laver forskere computere, der kan tænke (2020)
[55] *Centre for Information Policy Leadership*: Artificial Intelligence and Data Protection in Tension (2018), side 6
[56] *Thomas Bolander:* Kunstig Intelligens: Bliver mennesker overflødige? (2017), se afsnit: *intelligens er ikke bare intelligens*
[57] *Victor Thornton*: Hvad er forskellen på AI, Machine – og Deep Learning? (2018)
[58] *Centre for Information Policy Leadership*: Artificial Intelligence and Data Protection in Tension (2018), side 5
[59] Ibid., side 5

Kompleksiteten af et AI system vil afhænge af, hvilken model der benyttes. Det er ikke nødvendigvis alle AI systemer, som er baseret på Deep Learning. Alt afhængig af hvilken cirkel systemet opbygges ud fra, har det betydning for kompleksiteten og hvilke muligheder der er aktuelt i AI systemet.

5.1.1 Machine Learning

Machine Learning er en blanding af statistik og algoritmer, der sammen arbejder på at skabe systemer og mønstre i store mængder data.[60]

Nedenstående illustration forklarer oplæringsfasen og den efterfølgende behandling. Maskinen bliver således fyldt med træningsdata, hvorefter maskinen via Machine Learning udleder mønstre og sammenhænge i træningsdata. Dette udleder en model som benyttes til en viderebehandling af inputdata, hvilket er den data, som ønskes behandlet.



Figur 2 "Illustration af oplæringsfasen".
Kilde: *Det Norske Datatilsyn*: Artificial intelligence and privacy (2018) side 6

Derfor, ved hjælp af data og en analyse heraf, kan systemet lære at bestemte inputs fører til et bestemt output. Dermed bliver systemet i stand til at lave forudsigelser eller at komme med anbefalinger.[61] På den måde skabes intelligente systemer, der kan løse komplekse opgaver, uden hver enkelt mulige handling skal

[60] *Centre for Information Policy Leadership*: Artificial Intelligence and Data Protection in Tension (2018), side 5
[61] Ibid., side 5

programmeres manuelt.[62] Der findes mange forskellige Machine Learnings modeller, men karakteristisk for alle er, at de automatiserer og effektiviserer metoder, der benyttes til håndtering af store mængder data.[63] En del af vurderingen om hvilken model, der er bedst, afhænger af den data, der skal behandles. Det er centralt at have for øje, at Machine Learning arbejder ud fra mønstre i data, hvorfor det skal være muligt for maskinen at finde et givent mønster i den indsatte data. Hvis ikke dette er aktuelt er der risiko for, at den ikke kan udlede et resultat.[64]

5.1.2 Deep Learning og Neuralt Netværk

Deep Learning er som tidligere illustreret den inderste cirkel inden for AI, da Deep Learning bygger videre på Machine Learning. Forskellen mellem de to er, at Deep Learning består af algoritmer, som er inspireret af strukturen og funktionen i hjernen, hvilket kaldes kunstige neurale netværk.[65] Herved bliver neuralt netværk mere dybdegående sammenlignet med Machine Learning.

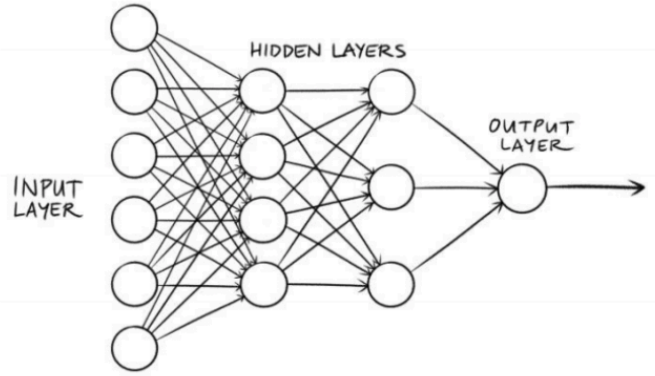
En af formålene med opbygningen af en AI maskine baseret på Deep Learning er, at den kan udvikle sig selv og lærer konstant af sine egne forudsigelser eller træk.[66] På den måde kan maskinen selv bestemme om dens forudsigelse er korrekt eller ej.[67] Ofte benytter Deep Learning større datasæt, hvorfor det er muligt at skabe store kompliceret algoritmer.[68] Disse algoritmer resulterer i modeller, der kan være i stand til at foretage en behandling, som er på samme niveau som menneskets, og i nogle tilfælde er Deep Learnings modellen trænet til at udføre langt større skarphed end mennesket.[69] Dette er begrundelsen for at sådanne modeller kan skabe værdi og blive uundværlige i blandt andet sundhedssektoren, da en AI er i stand til at opdage sygdomme langt hurtigere end den fysiske læge.[70]

For Deep Learning siges det, at en maskine har en hukommelse, hvorfor denne er i stand til at forbedre sig selv løbende.[71] Dette er ligeledes begrundelsen for, at AI maskinen til tider kan fremstå mere menneskelig, som om den responderer på den aktuelle situation.[72]

---

[62] https://iihnordic.dk/teknologi/machine-learning/?gclid=CjwKCAiAhc7yBRAdEiwAplGxX9-5EfvjQkD96qwNmCjNfUjqhmhjex7dBi5X3sJvYtfcOpSr0cXjiRoC1QEQAvD_BwE, se afsnit: *Hvad er machine learning?*
[63] *Centre for Information Policy Leadership*: Artificial Intelligence and Data Protection in Tension (2018), side 5
[64] Ibid., side 5
[65] Ibid., side 5
[66] *Victor Thornton*: Hvad er forskellen på AI, Machine – og Deep Learning? (2018), 6. afsnit
[67] Ibid., (2018) 6. afsnit
[68] *Centre for Information Policy Leadership*: Artificial Intelligence and Data Protection in Tension (2018), side 5
[69] Ibid., side 5
[70] Ibid., side 5-6
[71] *Victor Thornton*: Hvad er forskellen på AI, Machine – og Deep Learning? (2018) se afsnit: *Deep Learning – Machine Learning med hukommelse*
[72] Ibid., (2018) se afsnit: *Deep Learning – Machine Learning med hukommelse*

Oftest beskrives neuralt netværk som tre lag; Inputs, skjulte lag og output[73], hvilket er illustreret i nedenstående figur. De inputs, der indføres i AI maskinen, vil ofte være udvalgt og kontrolleret af mennesket, eftersom meningen hermed er, at mennesket ønsker en bestemt datamængde behandlet. Problematikken ligger især ved de skjulte lag, da behandlingen ikke nødvendigvis er transparent.[74] Ligeledes er det ikke altid muligt for fagfolk eller udviklere af den givende AI at forklare, hvordan inputs er blevet til et output, samt hvordan de forskellige inputs vægter i forhold til hinanden.[75] Antallet af de skjulte lag afhænger af, hvordan AI systemet er bygget, samt hvor stor en mængde data, der behandles.[76] Herudfra må det antages, at jo flere skjulte lag der er i modellen, jo større mangel på gennemsigtighed vil formentlig være tilfældet.



Figur 3 "Illustration af Neuralt Netværk"
Kilde: *Det Norske Datatilsyn*: Artificial intelligence and privacy (2018) side 14

5.2 Big Data

Som nævnt ovenfor vil en AI maskine og især Deep Learning, ofte kræve store datamængder. Jo mere data, der bliver plottet ind, jo bedre fungerer AI systemet. Derfor er det relevant at nævne Big Data. Begrebet bruges til at beskrive store datasæt, der kan samkøres med flere forskellige kilder.[77] Dataene er ofte udvundet fra flere forskellige kilder, og kan udnyttes til fordel for en virksomhed eller lignende ved hjælp af analyser af forskellige mønstre og forbindelser.[78] Flere virksomheder vil også benytte Big Data som en særlig forretningsmodel.[79] Dette kan indebære indsamling af disse store datasæt, med henblik på at forudse

[73] *Det Norske Datatilsyn*: Artificial intelligence and privacy (2018) side 14
[74] Ibid., side 14
[75] Ibid., side 14
[76] Ibid., side 14
[77] Ibid., side 5
[78] Ibid., side 5
[79] https://www.industriensfond.dk/BigData-BigBusiness

kunders forbrugsmønstre eller lave målrettet markedsføring, hvilket kan skabe værdi for virksomheden.[80] Big Data kan omfatte mange forskellige former for data. Ofte vil datasættene indeholde personoplysninger men ikke altid. Det relevante er her at se på, hvorvidt den pågældende data i sig selv kan henføres til en bestemt person. Selv hvis den enkelte oplysning ikke er henførbar, kan den blive det, når den sammenkobles med yderligere data. Eftersom Big Data er meget store datasæt, er det vigtigt at sammenholde alle oplysningerne med hinanden, når det skal vurderes, hvorvidt der er tale om personoplysninger. Hvis det er muligt at identificere enkeltpersoner på baggrund af de samlede datasæt, vil der være tale om personoplysninger.[81]

De store mængder data, der er omfattet af Big Data, er ofte komplekse, ligesom de værktøjer og processer, der skal bruges for at håndtere og udnytte den store datamængde. Ved Big Data er det derfor vigtigt, at der fokuseres på de strategiske muligheder, der er, for at benytte og anvende datasættene, så det gavner virksomhedens forretning.[82] Jo bedre virksomheden er til at udnytte og forstå den data, der er tilgængeligt, jo mere værdi, kan der opnås. Dette er særlig relevant i forbindelse med AI, herunder Deep Learning, da det er her en AI kan gøre en forskel. Mens traditionelle analytiske metoder skal programmeres til at finder ligheder og sammenhænge, vil en AI lære af al den data, den behandler.[83] Systemet kan derfor reagere kontinuerligt på nye data, og dermed justere analysen af disse data uden, at det er nødvendigt med en menneskelig indgriben. Hermed vil en AI hjælpe med at fjerne de tekniske barrierer, der tidligere har været problematiske ved analysen af Big Data.[84]

5.3 Hypotetiske faser indenfor AI

For at opnå en passende forståelse af sammenspillet mellem AI og reglerne inden for databeskyttelse i nærværende afhandling, er behandlingsprocessen inddelt i tre faser. Dette er blot for at tydeliggøre, hvilke problemstillinger samt tvister den dataansvarlige skal have fokus på, når der sker behandling via et AI system. Ligeledes er det et forsøg på at skabe et bedre overblik over en ellers til dels kompliceret proces. Fase 1 er opbygningsfasen. Det er i denne, at AI systemet designes, nærmere bestemt bliver sammensat af algoritmer, hvorefter maskinen gennemgår en træningsproces med nøje udvalgte data, også kaldet træningsdata.
I fase 2 er maskinen trænet, hvorefter den er klar til at blive brugt til den aktuelle behandlingsaktivitet. Der vil således ikke blive benyttet træningsdata længere, men i stedet den data som er gældende og relevant for en given behandling med henblik på at opnå et resultat.

[80] https://www.datatilsynet.dk/emner/big-data-profilering-og-markedsfoering/
[81] Ibid.
[82] https://www.teknologisk.dk/ydelser/big-data-og-anvendelse-af-data/37949
[83] *Centre for Information Policy Leadership*: Artificial Intelligence and Data Protection in Tension (2018), side 13
[84] *Det Norske Datatilsyn*: Artificial intelligence and privacy (2018) side 5

Fase 3 er bestående af selve resultatet. Tidligere betegnet som outputtet. Det er dette output som er relevant for den registrerede, da det er outputtet, der kan have betydning for individet. Denne betydning vil dog afhænge af den konkrete situation, samt formålet med behandlingsaktiviteten.
I hver af de tekniske faser vil eventuelle juridiske problemstillinger inden for databeskyttelsesreglerne blive belyst.

5.4 Manglende tillid til den Sorte Boks

I henhold til den Sorte Boks i relation til AI, menes der den proces som sker fra at input indføres i AI maskinen, til at der på den anden side kommer et output. I tilfælde af, at et AI system anvendes til at behandle personoplysninger, kan der forekomme betydelige problemstillinger med den Sorte Boks. Den Sorte Boks kan derved blive relevant for alle de førnævnte tre faser.
Illustreret på nedenstående figur, er det muligt at se både input og output, men hvordan selve mellemregningen udføres, er ikke muligt at se.

Figur 4 "Den sorte boks"
Kilde: *Egen tilvirkning*

Analytisk rådgiver indenfor AI ved SAS institute, Josefin Rosén forklarer det på følgende vis: *"Mellem datainput og dataoutput er der ganske mange lag og variabler, som afvejes og kombineres på forskellige måder. Dette skaber et dybt, komplekst net, et virvar, som er vanskelige at finde hoved og hale i."*[85] Det kan dermed være en udfordring at skulle vurdere, hvordan maskinen er nået frem til et givent resultat, og hvilke faktorer den ligger vægt på. Særligt ved brug af dybe neurale netværk kan der opstå lange avancerede algoritmer, der er så vanskelige, at det ikke er muligt at finde tilbage og afgøre, hvordan behandlingen blev udført.[86] Denne proces er tidligere omtalt som de skjulte lag. Der foreligger en manglende indsigt og gennemsigtighed af denne behandling, hvorfor processen omtales som den Sorte Boks.[87]

[85] *Mathias Klingenberg*: Den sorte boks er den største hindring for at bruge AI (2017), se afsnit: *Offentligheden har ret til at få en forklaring*
[86] Ibid., se afnit: *Tillid til den sorte boks*
[87] *Centre for Information Policy Leadership*: Artificial Intelligence and Data Protection in Tension (2018), side 15

5.5 Delkonklusion

Det er klargjort, at AI er et komplekst fænomen, samt at det består af flere undergrupper. Særlig relevant for afhandlingen er brugen af Big Data samt neuralt netværk. Big Data er især relevant fordi begrebet dækker over store mængder data, der kan behandles, hvorefter udfaldet kan være værdiskabende for en virksomhed. Modsat kan der dog opstå problemstillinger, idet disse datasæt ofte indeholder persondata.
Neuralt netværk, som hører under kategorien Deep Learning, kan bidrage med helt nye dimensioner i samfundet[88], som ikke før er set, men det medfører også problemstillinger grundet den manglende gennemsigtighed og dermed overblik over behandlingsprocessen. Det er ofte ved brug af neuralt netværk, at fænomener som den Sorte Boks, kan opstå. Ligeledes er problematikken ved den Sorte Boks en mangel på gennemsigtighed.
Brugen af AI kan inddeles i 3 faser, hvor fase 1 er opbygningsfasen. Fase 2 er behandlingsfasen, mens fase 3 er her, hvor der udledes et resultat af behandlingen.

Mulighederne ved AI er mange og brugen heraf er ofte værdiskabende. Dog kan brugen af teknologien også volde problemer, især hvor den anvendes på behandling af persondata eftersom lovgivningen opstiller store krav for persondatabehandlingen.

[88] *Centre for Information Policy Leadership*: Artificial Intelligence and Data Protection in Tension (2018), side 3

6. Databeskyttelsesforordningen

En af AI's grundsten er data, og i mange tilfælde vil dette indebære persondata. Databeskyttelsesretten bringer et helt nyt lag af kompleksitet på AI.[89] Derfor er det relevant at undersøge, hvordan databeskyttelsesretten har betydning for opbyggelsen og anvendelsen af et AI system. Databeskyttelsesretten har mange formål, hvor det overordnet kan siges, at den søger at bidrage til et civiliseret informationssamfund, hvor den registreredes integritet og privatliv er beskyttet overfor uønsket brug af personoplysninger.[90] Det er den enkelte persons behov for et retligt værn, der er den drivende kraft for den databeskyttelsesretlige regulering.[91] Databeskyttelsesretten er tæt forbundet med informationsteknologien, og det er denne teknologi, der i dag gør, at personoplysninger kan komme i en farezone. Teknologien udvikles konstant, og det kan derfor være svært at sikre en state of the art-databeskyttelsesret, som husker, at det er personen, der er i centrum.[92]

Nedenfor fremhæves udvalgte bestemmelser fra Databeskyttelsesforordningen, som vurderes særlig relevant for databeskyttelsesretlig behandling ved anvendelse af AI, og herunder hvilke problemstillinger der kan opstå.

6.1 Databeskyttelsesforordningens anvendelsesområde

Først og fremmest er det afgørende at klargøre, hvornår Databeskyttelsesforordningen finder anvendelse. Den materielle afgrænsning fremgår af Databeskyttelsesforordningen artikel 2 som fastlægger at reglerne "*finder anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register."* Beskyttelsesinteressen bliver derfor aktuel, når personoplysningerne bruges på en måde, der kan gøre dem hurtigt søgbare, og der dermed opstår en risiko for, at oplysningerne bliver anvendt på en integritetskrænkende måde.[93] Persondatabehandling ved anvendelse af AI, vil være omfattet af automatisk databehandling.

For at behandlingen hører under det territoriale anvendelsesområde, skal den dataansvarlig eller databehandleren være etableret i Unionen, jf. Databeskyttelsesforordningens artikel 3, stk. 1. Hermed skal

[89] *Peter Blume*: Den nye persondataret (2018) side 263
[90] *Peter Blume*: Personen i Persondateret (2019) side 11
[91] Ibid., side 11
[92] Ibid., side 11-12
[93] *Peter Blume*: Den nye persondataret (2018) side 59

forstås "*en effektiv og faktisk udøvelse af aktivitet gennem en mere permanent struktur*".[94] Det er således etableringen, der er af afgørende betydning, da det er mindre væsentligt, hvorvidt behandlingen sker indenfor eller udenfor EU.[95]

Anvendelsesområdet udvides yderligere i Databeskyttelsesforordningens artikel 3, stk. 2., som bestemmer, at også dataansvarlige eller databehandlere, der ikke er etableret i unionen, ligeledes kan blive omfattet af Databeskyttelsesforordningens regler, såfremt de udøver en persondatabehandling, som vedrører registrerede, der er i unionen. Dog kun i tilfælde, hvor behandlingsaktiviteten vedrører:

> *"a) udbud af varer eller tjenester til sådanne registrerede i Unionen, uanset om betaling fra den registrerede er påkrævet, eller*
>
> *b) overvågning af sådanne registreredes adfærd, for så vidt deres adfærd finder sted i Unionen."*[96]

Denne bestemmelse er således rettet mod dataansvarlige og databehandlere, som selv er etableret i et tredjeland. Det afgørende er derfor virkningen af den behandling der foretages, og ikke etableringsstedet. Eftersom nærværende afhandling tager udgangspunkt i persondatabehandling indenfor unionen, vil persondatabehandlingen være omfattet af det territorielle anvendelsesområde.

6.2 Den dataansvarlige

Hvad der skal forstås ved begrebet dataansvarlig klargøres i Databeskyttelsesforordningens artikel 4, som indeholder legaldefinitioner. Formålet med artikel 4 er dels at fjerne eller reducere fortolkningstvivl, hvorfor retsforskriften anvendes konsistent.[97] I artiklens nr. 7 fremgår, at den dataansvarlige er en fysisk eller juridisk person. Dertil kan det ligeledes være en offentlig myndighed, en institution eller et andet organ, hvorfor udgangspunktet er, at enhver kan være dataansvarlig.[98] Af afgørende betydning er dog, at den dataansvarlige udøver bestemmelsesretten over behandlingens formål, og på hvilken måde behandlingen foregår.[99] Dertil har den dataansvarlige rådighedsretten og det er i dennes interesse, at personoplysningerne behandles.[100]

[94] Forordning 2016/679, præambelbetragtninger nr. 22
[95] *Peter Blume*: Den nye persondataret (2018) side 66
[96] Forordning 2016/679, artikel 3, stk. 2.
[97] *Peter Blume*: Den nye persondataret (2018) side 68
[98] Ibid., side 73
[99] Ibid., side 73
[100] Ibid., side 73

Oftest er det centralt at skelne mellem en dataansvarlig og en databehandler, grundet deres forskellige ansvarsområder[101], men eftersom nærværende afhandlings fokus er på den dataansvarliges ansvarsområde, vil databehandleren ikke belyses yderligere.

6.3 Personoplysninger

Personoplysninger er som ovenstående, ligeledes en del af Databeskyttelsesforordningens definitionsliste. I artikel 4, nr. 1, er personoplysninger defineret som værende *"enhver form for information om en identificeret eller identificerbar fysisk person."* Idet der benyttes *fysisk person*, må der hermed forstås, at det ikke dækker over grupper, men blot det enkelte individ, hvoraf dennes personoplysninger kan beskyttes efter reglerne i Databeskyttelsesforordningen.[102]

Idet Databeskyttelsesforordningen finder anvendelse i forhold til identificerbare oplysninger, omfatter dette oplysninger, der indeholder en eller anden form for identifikation, hvilket indirekte gør det muligt at henføre oplysningen til en bestemt fysisk person.[103]

6.3.1 Almindelig eller følsomme oplysninger

Det er ovenstående lagt til grund, at der skal forekomme behandling af personoplysninger, før behandlingen er omfattet af Databeskyttelsesforordningen. Herefter er det relevant, at personoplysninger kan deles op i øvrige tre kategorier. De tre kategorier er; 1) Almindelige personoplysninger, 2) Særlige kategorier at oplysninger, såsom følsomme oplysninger og 3) Oplysninger om straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger.[104]

Grunden til opdelingen skyldes forskellige gældende betingelser og procedurer for behandling af personoplysninger, hvilket blandt andet fremgår af Databeskyttelsesforordningens artikel 6, 9 og 10.

Listen af følsomme personoplysninger i Databeskyttelsesforordningens artikel 9 er udtømmende, hvorfor det kun er de disse oplysninger, som kan kategoriseres som følsømme oplysninger.[105] Eksempler på følsomme personoplysninger er race og etnisk oprindelse, politiks overbevisning, genetiske data og helbredsoplysninger. De almindelige personoplysninger vil omfatte alle andre personoplysninger, end dem der falder under kategorien af følsomme personoplysninger, herunder navn, adresse, familieforhold, bolig, informationer om arbejdsstilling eller arbejdsområde med videre.

[101] *Peter Blume*: Den nye persondataret (2018) side 73-75
[102] Ibid., side 69
[103] Ibid., side 69-70
[104] https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-personoplysninger/
[105] Ibid.

Oplysninger om strafbare forhold anses efter Databeskyttelsesforordningens artikel 10, for at være almindelige oplysninger, men er særskilt reguleret i Databeskyttelsesloven, hvilket fremgår af dennes § 8, hvor de betegnes som fortrolige oplysninger. Ligeledes bliver personnummer anset som en fortrolig oplysning, som også er reguleret særskilt i Databeskyttelseslovens § 11.[106] Der er således ikke tale om følsomme oplysninger, men derimod fortrolige oplysninger, idet der er et særligt beskyttelsesbehov, som har betydning for anvendelsen af databeskyttelsesreglerne.[107]

6.3.2 Datasæt

Når der anvendes store datasæt til en behandling, er der mulighed for, at disse datasæt indeholder både personoplysninger samt ikke-personoplysninger. Såfremt en behandling af personoplysninger omfatter et blandet datasæt, som består af både personoplysninger samt ikke-personoplysninger, er det afgørende om datasættet er knyttet uløseligt sammen.[108] Hvis det kan lægges til grund, at datasættet er knyttet uløseligt sammen, finder reglerne om databeskyttelse anvendelse på hele datasættet, og ikke blot de data der kan kategoriseres som personoplysninger.[109] Dette er også gældende, hvor personoplysningerne kun udgør en mindre del af datasættet.[110] Det er særdeles relevant for den dataansvarlige i henhold til brugen af AI og Big Data, da det må antages at ved behandling af store mængder data, kan der opstå en potentiel chance for, at ikke-personoplysninger ligeledes vil være omfattet af Databeskyttelsesforordningens regler.

6.3.3 Typen af data

Ved opbygningen af et AI system skal der højst sandsynligt ikke blot bruges ét datasæt men flere. I fase 1 arbejdes der med ét slags datasæt, hvorefter der i fase 2 benyttes data fra praksis. Det er derfor relevant at skelne mellem de to datasæt. Træningsdata, som bruges i fase 1, vil i flere tilfælde blot kunne anonymiseres, da formålet i træningsfasen er at udvikle AI maskinen. Det er ikke afgørende, at den data som bruges som en del af træningen, kan henføres til en bestemt person. Såfremt der anvendes anonymiseret oplysninger, bør det undersøges, hvorvidt behandlingen er indenfor databeskyttelsesreglernes anvendelsesområde. Det fremgår af Databeskyttelsesforordningen at anonymiserede personoplysninger ikke er beskyttet af reglerne,

[106] https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-personoplysninger/
[107] Ibid.
[108] *Europa-Kommissionen:* COM(2019) 250 final, side 9
[109] Ibid., side 10
[110] Ibid., side 10

da disse oplysninger ikke kan henføres til en fysisk person.[111] Alligevel kan der i forbindelse med brugen af teknologi, herunder brugen af AI, opstå mulighed for en såkaldt reidentifikation.[112]
AI bruger ofte store mængder af data, hvilket kan skabe sammenhænge mellem forskellige oplysninger. Dette kan medvirke, at oplysninger kan blive til personoplysninger, til trods for at dette ikke oprindeligt var tilfældet.[113]
Såfremt der sker reidentifikation bliver anonymiseret oplysninger til henførbare personoplysninger til en fysisk person, hvorfor behandlingen er omfattet af Databeskyttelsesforordningen.

6.3.4 Bias i data[114]

Begrebet bias kommer oprindeligt fra det engelske begreb[115]. Den danske ordbog definerer bias som, "*forvrængning af undersøgelsesresultatet, målelige størrelser eller lignende som især skyldes forudindtagethed eller metodiske fejl"*[116]*.* Altså kan der forekomme bias, hvis en person ikke er tilstrækkeligt opmærksom på, at den ellers neutrale beslutning måske bliver præget af egen holdning og forudindtagethed.[117]

I fase 1 kan der være en risiko for, at systemet præges af bestemte holdninger, som kan have betydning for udfaldet. Derfor er det særlig vigtigt, at oplæringen af en AI maskine udføres nøje, således der opnås et brugbart slutprodukt. AI maskinen vil ikke i sig selv være bias, men det er derimod måden hvorpå, den bliver sammensat og især den specifikke data, som bliver benyttet til at træne maskinen, den dataansvarlige skal være opmærksom omkring.
Et udbredt eksempel er diskrimination, herunder både mellem kvinder og mænd i ansættelsessituationer, forskelsbehandling på personlig baggrund og/eller hudfarve. Amazon oplevede det med deres nye rekrutteringssystem, hvor det viste sig, at AI systemet nedgraderede alle CV, som indeholdt ordet kvinde, kvinder eller lignende.[118] Grunden herfor var, at maskinen var oplært på den praksis, som havde været gældende i Amazon i de sidste 10 år. AI systemet afslørede derfor, at organisationens arbejde var bias, men ikke at de nødvendigvis var opmærksom herom.[119] Såfremt AI systemet benytter flere faktorer som led i

[111] Forordning 2016/679, præambelbetragtninger nr. 26
[112] *Peter Blume*: Den nye persondataret (2018) side 70-71
[113] Ibid., side 70
[114] *Craig S. Smith:* Dealing With Bias in Artificial Intelligence (2020)
[115] https://ordnet.dk/ddo/ordbog?query=bias
[116] Ibid.
[117] Ibid.
[118] *Marethe Eckhardt*: Domstolsstyrelsen: Kunstig intelligens afslører fordomme mod køn og hudfarve (2019) se afsnit: *Twitter lærte chatrobat at tale grimt*
[119] Ibid., se afsnit: *Twitter lærte chatrobat at tale grimt*

vurderingen inden den endelige konklusion, skal AI systemet oplæres til at inddrage kategorier som miljø, opvækst og andre elementer, fremfor kategorier som køn, alder, race med videre. På den måde kan opbygningen af maskinen justeres og der kan arbejdes hen mod en mindre grad af bias eller slet ingen.[120]

Det er derfor særlig relevant, at det sæt træningsdata, som skal benyttes til at oplære AI maskinen, er gennemgået inden den kommer ind i AI systemet. Selve kodningen af AI maskinen vil også have en væsentlig betydning, eftersom opbygningen af algoritmerne skal være sammensat, så AI maskinen er bygget til at bedømme objektivt og ikke blot vægte bestemte begreber eller ord højere end andre. Dette vil ofte være problemet med menneskelig vurdering, hvorfor AI kan være behjælpelig til at sørge for, at en vurdering er fordomsfri.[121]

6.4 De grundlæggende principper og deres betydning for AI

I Databeskyttelsesforordningens artikel 5 opstilles de grundlæggende principper for behandling af personoplysninger. Baggrunden for at principperne er tydeliggjort i Databeskyttelsesforordningen, er for at beskytte den registreredes privatliv på den bedst givne måde. Principperne skal overholdes ved enhver form for persondatabehandling, som er omfattet af Databeskyttelsesforordningens anvendelsesområde. Dette gælder også når der sker behandling af personoplysninger ved anvendelse af en AI maskine.
Ved brugen af personoplysninger i forbindelse med opbygningen og anvendelsen af AI, kan der opstå udfordringer med de grundlæggende principper. Dette skyldes især, at en AI er baseret på meget komplekse algoritmer, hvorfor systemet ofte vil komme i karambolage med de grundlæggende principper.[122] Principperne skal overholdes igennem hele behandlingsprocessen, hvor der sker behandling af personoplysninger, hvorfor de skal tilgodeses i alle de førnævnte tre faser.

I det følgende vil udvalgte principper blive uddybet. De udvalgt principper fremgår af Databeskyttelsesforordningens artikel 5, stk. 1, litra a og d. Disse er udvalgt, på baggrund af deres relevans for AI og nærværende afhandlings undersøgelsesområde.

6.4.1 Lovlighed, rimelighed og gennemsigtighed

Det fremgår af artikel 5, stk. 1, litra a, at personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede. De første to krav, lovligt og rimeligt, stemmer overens med

[120] *Centre for Information Policy Leadership*: Artificial Intelligence and Data Protection in Tension (2018), side 13
[121] *Jake Silberg og James Manyika:* Tackling bias in artificial intelligence (and in humans) (2019), 1.-10. Afsnit
[122] *Centre for Information Policy Leadership*: Artificial Intelligence and Data Protection in Tension (2018), side 16

tidligere gældende ret, hvorfor disse må antages at fastsætte en standard om god databehandlingsskik.[123] Kravet om gennemsigtighed er ny i forhold til Persondatadirektivet. Af Databeskyttelsesforordningens præambelbetragtning nr. 39 fremgår det blandt andet, at princippet om gennemsigtighed betyder, *"at enhver information og kommunikation vedrørende behandling af disse personoplysninger er lettilgængelig og letforståelig, og at der benyttes et klar og enkelt sprog."*[124] Der er særlige oplysninger, som løbende skal være tilgængelig for den registrerede, herunder hvem den dataansvarlige er, formålet med behandlingen samt hvordan den registrerede gør brug af sine rettigheder.[125] Ligeledes bør den registrerede gøres bekendt med risici forbundet med behandlingen.[126] [127] På trods af at indførelsen af gennemsigtighedsprincippet i Databeskyttelsesforordningens artikel 5, stk. 1, litra a er en nyskabelse i forhold til tidligere gældende ret, kan kravet ikke antages at medføre en ændring i retstilstanden.[128] Den tidligere tilsynspraksis på området, må derfor anses for fortsat at være relevant i henhold til Databeskyttelsesforordningens artikel 5, stk. 1, litra a.[129]

Det forekommer, at princippet om gennemsigtighed ligeledes omtales som transparens. I den engelske version af Databeskyttelsesforordningen er begrebet gennemsigtighed omtalt som "*Transparency*" hvilket antages at være begrundelsen for, at det er udbredt at benytte begge begreber. Transparens og gennemsigtighed er synonymer til hinanden,[130] [131] hvorfor det antages, at de har samme betydning. Det er forskelligt, hvilken betegnelse fagfolk benytter, når de omtaler dette begreb i databeskyttelsessammenhænge. I nærværende afhandling benyttes det begreb, som ligeledes fremgår af Databeskyttelsesforordningen, nemlig *Gennemsigtighed*. Gennemsigtighedsprincippet, herunder hvilke problemstillinger der kan opstå som følge af brugen af AI, vil blive uddybet yderligere i afsnit 8.

Princippet om lovlighed fastlægger, at der skal foreligge et hjemmelsgrundlag, før en behandling er lovlig, også når der er tale om persondatabehandling ved anvendelse af AI. Dette hjemmelsgrundlag kan for eksempel findes i Databeskyttelsesforordningens artikel 6 eller artikel 9. Dog kan der forekomme yderligere restriktioner til lovligheden, såfremt en behandling er omfattet af artikel 22. Artikel 22 vil blive uddybet yderligere i afsnit 9.

---

[123] *Kristian Korfits Nielsen og Anders Lotterup*: Databeskyttelsesforordningen og Databeskyttelsesloven (2020) side 314
[124] Forordning 2016/679, præambelbetragtning nr. 39
[125] Forordning 2016/679, artikel 13 og 14
[126] *Kristian Korfits Nielsen og Anders Lotterup*: Databeskyttelsesforordningen og Databeskyttelsesloven (2020) side 314
[127] Betænknings nr. 1565, side 92-93
[128] *Kristian Korfits Nielsen og Anders Lotterup*: Databeskyttelsesforordningen og Databeskyttelsesloven (2020) side 314
[129] Ibid., side 314
[130] https://ordnet.dk/ddo/ordbog?query=gennemsigtigheden
[131] https://ordnet.dk/ddo/ordbog?query=transparens

Rimelighedsprincippet kræver at enhver behandling af persondata skal udføres med respekt for den registreredes interesser, og at personoplysningerne kun bruges i overensstemmelse med, hvad den registrerede rimeligt kan forvente.[132] Anvendes der et AI system til behandlingen af personoplysninger, er det en naturlig tanke, at denne behandling vil være mere objektiv end, hvis behandlingen foretages af et menneske, eftersom AI systemet ikke vil blive påvirket af følelser eller andet.[133] Som tidligere anført, kan der dog opstå et problem, såfremt et AI system udviser bias. Når alt kommer til alt, vil systemet trods alt ikke udvise større objektivitet end det menneske, der har opbygget det.[134] For at overholde rimelighedsprincippet, er det derfor vigtigt, at den dataansvarlige gennemfører foranstaltninger for at forhindre vilkårlig diskriminerede behandling af personoplysninger.[135] Herudover skal AI systemet trænes med relevant og korrekt data, og herunder lære hvilke data, der skal fremhæves.[136] Udviser et AI system bias, vil det således være i strid med rimelighedsprincippet og god databehandlingsskik.[137] Ud fra det tidligere nævnte eksempel, hvor Amazon anvendte et AI system til at sortere i ansøgninger, vil dette system skulle kodes på en måde, hvor det ser bort fra køn, alder, etnisk oprindelse, politisk eller religiøs overbevisning, helbredsstatus og seksuel orientering med videre, for at systemet ikke udviser bias, og derved overholder rimelighedsprincippet.[138]

6.4.2 Rigtighed

Databeskyttelsesforordningens artikel 5, stk. 1, litra d, rummer princippet om rigtighed. Med dette forstås, at den dataansvarlige skal sikre, at enhver personoplysning som behandles, er korrekt. Det fremgår af præambelbetragtning nr. 39, at der bør træffes enhver rimelig foranstaltning for at sikre, at urigtige oplysninger berigtiges eller slettes.[139] Indholdsmæssigt anses artikel 5, stk. 1, litra d, for stort set at være identisk med sin forgænger, hvorfor der med Databeskyttelsesforordningens ikrafttræden ikke er sket en ændring i retstilstanden.[140] Rigtighedsprincippet kræver, at personoplysninger om nødvendigt skal være ajourførte. Derfor påhviler det, den dataansvarlige at foretage en kontrol.[141] For at udføre denne kontrol, bør den dataansvarlige implementere rimelige foranstaltninger, som kan være behjælpelig med at beskytte den

[132] *Det Norske Datatilsyn*: Artificial intelligence and privacy (2018) side 16
[133] Ibid., side 16
[134] Ibid., side 16
[135] Ibid., side 16
[136] Ibid., side 16
[137] Ibid., side 16
[138] Ibid., side 16
[139] Betænknings nr. 1565, side 98
[140] *Kristian Korfits Nielsen og Anders Lotterup*: Databeskyttelsesforordningen og Databeskyttelsesloven (2020) side 332
[141] Ibid., side 331

registreredes personoplysninger.[142] Omfanget af kontrollen, og hvad der anses for værende rimelige foranstaltninger, vil afhænge af den konkrete persondatabehandling alt efter, hvad der er nødvendigt for at opretholde sikkerheden.[143]

Urigtige personoplysninger kan have konsekvenser for den registreredes rettigheder og frihedsrettigheder, såfremt de leder til en ukorrekt afgørelse. Som tidligere anført er en personoplysning en *"information om en identificeret eller identificerbar fysisk person"*[144]. Der er tale om en bred definition, hvorfor begrebet omfatter alle oplysninger, der kan henføres til en fysisk person.[145] Såfremt en person kan identificeres ud fra en urigtig oplysning, vil denne oplysning således stadig være en personoplysning, selvom den ikke er korrekt, og dermed være omfattet af Databeskyttelsesforordningen.

Rigtighedsprincippet er især vigtigt, når et AI system opbygges og anvendes.[146] I fase 1 anvendes der træningsdata. Såfremt denne data ikke er korrekt, vil dette kunne få betydelige konsekvenser for fremtidig persondatabehandling i fase 2. Derfor bliver en central del af opbygningen af en AI maskine at sørge for, at de træningsdata, som anvendes, er rigtige, for at opnå præcise og korrekte afgørelser. [147] Selvom træningsdataene ikke indeholder personoplysninger, for eksempel fordi disse er anonymiseret, vil urigtige oplysninger kunne få betydning for fremtidig persondatabehandling. Det er derfor ikke nødvendigvis et krav, at rigtighedsprincippet overholdes på træningsdata, såfremt træningsdata ikke vil være omfattet af de databeskyttelsesretlige regler. Men såfremt der sker en persondatabehandling i fase 2, som bygger på grundlaget af træningsdataene fra fase 1, er det et krav at rigtighedsprincippet overholdes, da det ellers kan lede til urigtige resultater.[148]

Microsofts chatbot Tay er et godt eksempel på, hvad der sker, når træningsdata ikke bliver kvalitetssikret. Det var hensigten, at Tay skulle bruge Twitter-samtaler som ufiltrerede træningsdata, og dermed lære at tweete som en teenager.[149] Dette resulterede dog i at Chatbotten blev fyldt med racistiske udsagn, hvorefter Tay var racistisk. Tay var derfor selvlærende, hvilket var formålet, men eftersom de træningsdata, den blev

[142] Forordning 2016/679, præambelbetragtning nr. 39
[143] Forordning 2016/679, præambelbetragtninger nr. 53-54
[144] Forordning 2016/679, artikel 4, stk. 1, nr. 1
[145] *Kristian Korfits Nielsen og Anders Lotterup*: Databeskyttelsesforordningen og Databeskyttelsesloven (2020) side 237
[146] *Databeskyttelsesrådet*: Guidelines 4/2019 on Article 25 (2019) side 21-22
[147] Ibid., side 21
[148] Ibid., side 21-22
[149] *Mathias Klingenberg:* ´Den sorte boks´ er den sorte hindring for at bruge AI (2017), se afsnit: *Kvalitetssikring af data*

fyldt med, ikke var kvalitetssikret, fik det konsekvenser. Microsoft endte med at tilbagetrække Tay dagen efter lanceringen. [150]

Der kan fremkomme andre situationer, hvor urigtige oplysninger kan lede til urigtige afgørelser, hvor dette har enorme konsekvenser for den registrerede.[151] I tilfælde, hvor der bruges et AI system til at diagnosticere patienter, kan ukorrekte oplysninger lede til en ukorrekt diagnose eller uretmæssig behandling. Hvis en bank benytter et AI system til at lave profiler over kunder, der ansøger om lån, er det vigtigt, at systemet har brugt træningsdata, der ikke blot er rigtig, men som også repræsenterer befolkningen, således der ikke opstår partiskhed. Rigtighedsprincippet er derfor ikke blot vigtig, hvad angår det enkelte individs personoplysninger, men også hvad angår træningsdata, således en afgørelse ved anvendelse af AI er repræsentativ for, hvordan befolkningen ser ud.[152]

6.5 Delkonklusion

Når det lægges til grund, at der sker en persondatabehandling, som er omfattet af Databeskyttelsesforordningens territorielle og materielle anvendelsesområde, vil dennes regler finde anvendelse. Dette er tilfældet, hvor der sker en persondatabehandling ved anvendelse af AI indenfor unionen. I forbindelse hermed er det især relevant at undersøge, hvilke data der lægger til grund for behandlingen. Er der tale om blandede datasæt, som indeholder både personoplysninger og ikke-personoplysninger, vil hele datasættet være omfattet af Databeskyttelsesforordningens regler, såfremt oplysningerne er knyttet uløseligt sammen.

Databeskyttelsesforordningen opstiller nogle grundlæggende principper, som finder anvendelse ved enhver form for persondatabehandling. Særlig relevant ved AI er princippet om lovlighed, rimelighed og gennemsigtighed, samt princippet om rigtighed. I fase 1 anvendes der træningsdata, hvor det er muligt, at der kan forekomme bias. Såfremt dette er tilfældet, vil det være i strid med rimelighedsprincippet. For at den dataansvarlige overholder rimelighedsprincippet, er det derfor vigtig med kvalitetssikring af data, samt at AI systemet lærer, hvilke kategorier af data der skal vægtes i en given behandlingsproces. Rigtighedsprincippet foreskriver, at enhver oplysning skal være korrekt. Ukorrekte oplysninger kan føre til ukorrekte resultater, hvilket kan have betydelige konsekvenser for den registrerede.

[150] *Mathias Klingenberg:* ´Den sorte boks´ er den sorte hindring for at bruge AI (2017), se afsnit: *Kvalitetssikring af data*
[151] *Databeskyttelsesrådet*: Guidelines 4/2019 on Article 25 (2019) side 21
[152] Ibid., side 21

7. Den dataansvarliges generelle forpligtelser

Det fremgår af Databeskyttelsesforordningens artikel 5, stk. 2, at den dataansvarlige har et ansvar for at sikre overholdelse af de grundlæggende principper. Ligeledes fremgår det af Databeskyttelsesforordningens artikel 24, stk. 1, at den dataansvarlige skal kunne sikre og påvise, at behandlingen er i overensstemmelse med Databeskyttelsesforordningen. Såfremt reglerne ikke bliver overholdt, kan det have enorme konsekvenser for den dataansvarlige.[153]

Databeskyttelsesforordningen fastlægger generelle forpligtelser for den dataansvarlige, og udspecificere områder, hvor det er påkrævet at foretage nødvendige foranstaltninger for at beskytte individets rettigheder og frihedsrettigheder. Selv i de tilfælde, hvor det ikke er obligatorisk for den dataansvarlige at udføre analyser eller tage passende foranstaltninger, kan den dataansvarliges handlinger have en positiv betydning, da databehandlingsprocessen bliver dokumenteret.[154]
I det følgende vil der blive fokuseret på den dataansvarliges forpligtelser indenfor databeskyttelse gennem design og konsekvensanalyse, da reglerne herom kan have betydning for arbejdet med AI.

7.1 Databeskyttelse gennem design

Med Databeskyttelsesforordningen er der kommet betydeligt flere krav til den dataansvarlige, der arbejder med personoplysninger. Dette omfatter blandt andet kravet i Databeskyttelsesforordningens artikel 25, stk. 1 – Databeskyttelse gennem design.
Databeskyttelse gennem design stiller et krav til, at den dataansvarlige skal tage stilling til databeskyttelsen, allerede når et nyt system opbygges.[155] Kravet gælder både, når der udvikles ny software, når der bestilles nye systemer og services, samt når der videreudvikles på disse. Reglen medvirker således til, at der skal tænkes databeskyttelse ind i alle stadier af systemudvikling, rutiner og dagligt brug.[156] Artikel 25, stk. 1 er derfor særdeles relevant, når der udvikles et nyt AI system (fase 1), samt når dette system tages i brug (fase 2).

Artikel 25, stk. 1 oplister nogle krav til den dataansvarlige. Først og fremmest er der en række forholdsregler, der skal tages højde for. Når der designes et nyt system, skal der implementeres passende og effektive foranstaltninger, hvis formål er at opfylde kravene til implementering af de øvrige principper i

[153] Forordning 2016/679, artikel 83
[154] *Artikel 29-gruppen*: 17/DA WP 248 (2017) side 21
[155] *Databeskyttelsesrådet*: Guidelines 4/2019 on Article 25 (2019) side 5
[156] *Det Norske Datatilsyn*: Artificial intelligence and privacy (2018) side 25

Databeskyttelsesforordningen effektivt, hvilket skal føre til en reduceret risiko for den registrerede. En af disse foranstaltninger kan være pseudonymisering. Samtidig skal der tages højde for proportionalitetsprincippet.[157] Overholdelse af artikel 25, stk. 1 er derfor et vigtigt værktøj for systemudvikleren og den dataansvarlige, for at kunne påvise overholdelse af Databeskyttelsesforordningen generelt.[158]

7.1.1 Passende foranstaltninger og fornødne garantier

Det fremgår af Databeskyttelsesforordningens artikel 25, stk. 1, at den dataansvarlige skal implementere *"passende tekniske og organisatoriske foranstaltninger (…) med henblik på integrering af de fornødne garantier i behandlingen for at opfylde kravene i denne forordning og beskytte de registreredes rettigheder."*

Begrebet foranstaltninger har en bred betydning, og skal forstås som enhver metode eller middel, den dataansvarlige kan tage i brug for at overholde databeskyttelsesreglerne. Foranstaltningerne skal være passende, hvilket betyder, at de skal være egnet til at opnå det bestemte formål, for eksempel at implementere Databeskyttelsesforordningens principper i et AI system på en effektiv måde, ved at reducere eventuelle risici forbundet med persondatabehandlingen.[159] At bestemmelsen nævner både tekniske og organisatoriske foranstaltninger betyder, at der kan være tale om alt fra avanceret tekniske løsninger til træning af personale, i forhold til hvordan de skal håndtere persondata.[160] Der er ikke et krav om, hvor avanceret den enkelte foranstaltning skal være, så længe den er egnet til det givne formål.[161] Hvad en passende foranstaltning er, vil derfor afhænge af den givne situation, både i forhold til hvilket system der er tale om, samt hvilke former for persondatabehandling der sker, herunder hvor indgribende behandlingen er for det enkelte individ.

Fornødne garantier skal anses som et ekstra niveau af beskyttelse af den registreredes rettigheder og frihedsrettigheder i forbindelse med persondatabehandlingen.[162] Hvis databeskyttelsesprincipperne er implementeret korrekt og effektivt, har den dataansvarlige integreret de fornødne garantier, der er nødvendige for at sikre deres effektivitet igennem hele databehandlingsperioden.[163] Eksempler på fornødne

[157] Forordning 2016/679, præambelbetragtning nr. 4
[158] Forordning 2016/679, præambelbetragtning nr. 78
[159] *Databeskyttelsesrådet*: Guidelines 4/2019 on Article 25 (2019) side 6
[160] Ibid., side 6
[161] Ibid., side 6
[162] Ibid., side 6
[163] Ibid., side 6

garantier kan være at give den registrerede automatisk og gentagne informationer omkring, hvilken persondata der lagres, samt andre metoder til at opfylde den registreredes rettigheder på.

Der er således ikke et korrekt eller konkret svar på, hvad passende foranstaltninger eller fornødne garantier er, da dette vil afhænge af den givne situation. Når den dataansvarlige skal fastsætte disse, er det derfor vigtigt at huske på de grundlæggende principper i Databeskyttelsesforordningens artikel 5, den registreredes rettigheder i artikel 12-22, samt andre grundlæggende frihedsrettigheder. Den dataansvarlige skal have en forståelse for, hvad disse principper og rettigheder betyder, for at kunne implementere passende foranstaltninger eller fornødne garantier.[164]
Artikel 25, stk. 1 er alene rettet mod den dataansvarlige. I praksis vil denne dog givetvis ofte købe færdigudviklede produkter, herunder AI systemer. Disse vil således være udviklet af andre end den dataansvarlige, hvorfor den dataansvarlige er afhængig af, at der i AI systemerne er indtænkt databeskyttelse gennem design, for at kunne overholde bestemmelsen.[165] De systemudviklere, som udvikler systemer, der behandler personoplysninger, bør tilskyndes at tage højde for de databeskyttelsesretlige regler i forbindelse med udviklingen og designet af disse systemer.[166] Der forekommer derfor ikke direkte et krav i Databeskyttelsesforordningen til at systemudviklere tænker databeskyttelses gennem design ind fra starten, men det bør de gøre, såfremt de ønsker at videresælge deres produkter til en dataansvarlig, således den dataansvarlige er i stand til at opfylde dennes databeskyttelsesforpligtelser.[167] Den dataansvarlige har til opgave at kunne påvise, at der er implementeret passende foranstaltninger, og herunder at enhver implementeret foranstaltning har en reel effekt, og ikke blot er generisk.[168]

For at finde frem til de rette foranstaltninger og fornødne garantier opsætter artikel 25, stk. 1 en række elementer, der skal tages højde for. For det første skal de leve op til det aktuelle tekniske niveau. Dette er et dynamisk koncept, som ikke kan defineres specifikt, og som hele tiden ændrer sig.[169] Derfor skal det passende tekniske niveau vurderes løbende. Det betyder samtidig, at den dataansvarlige kan risikere ikke at overholde kravene i artikel 25, stk. 1, såfremt den dataansvarlige ikke holder sig opdateret på den teknologiske udvikling.

[164] *Databeskyttelsesrådet*: Guidelines 4/2019 on Article 25 (2019) side 6
[165] *Kristian Korfits Nielsen og Anders Lotterup*: Databeskyttelsesforordningen og Databeskyttelsesloven (2020) side 593
[166] Forordning 2016/679, præambelbetragtning nr. 78
[167] *Kristian Korfits Nielsen og Anders Lotterup*: Databeskyttelsesforordningen og Databeskyttelsesloven (2020) side 593
[168] *Databeskyttelsesrådet*: Guidelines 4/2019 on Article 25 (2019) side 7
[169] Ibid., side 7-8

For det andet, skal der tages højde for implementeringsomkostningerne. Dette referer til de generelle ressourcer, der skal bruges til at implementere foranstaltningerne, herunder tid og løn til ansatte.[170] Samtidig skal der tages højde for omkostningerne både ved implementeringen af foranstaltningerne, samt vedligeholdelsen heraf.

For det tredje skal der tages højde for den pågældende behandlings karakter, omfang, sammenhæng og formål. Ved udviklingen af et nyt system, skal udvikleren og den dataansvarlige derfor hele tiden have for øje, hvad systemet skal bruges til.[171] Såfremt der er tale om en persondatabehandling, der er meget indgribende overfor den registreredes rettigheder, for eksempel fordi der behandles følsomme personoplysninger, vil der blive stillet større krav til systemet og de foranstaltninger, der implementeres heri, fremfor hvis der blot er tale om en simpel persondatabehandling, uden den store betydning for den registrerede.[172] Hertil stiller bestemmelsen ligeledes et krav om, at risiciene ved persondatabehandlingen skal defineres og sandsynligheden heraf skal fastslås.[173] Dette kan blandt andet gøres ved at lave en konsekvensanalyse.

7.1.2 Databeskyttelse gennem design i forbindelse med AI

I en fremadgående digital verden er det vigtigt, at den dataansvarlige lever op til kravene om databeskyttelse gennem design, da kravene heri spiller en afgørende rolle indenfor beskyttelse af personoplysninger.[174] Ud over at den dataansvarlige kan risikere store bøder, såfremt den ikke overholder kravene i Databeskyttelsesforordningen, vil artikel 25, stk. 1 samtidig medvirke til at identificere potentielle risici ved anvendelse af et AI system. Det vigtigste designmål er effektiv implementering af de generelle principper for databeskyttelse, samt den registreredes rettigheder.[175]

Artikel 25, stk. 1 bliver i almindelighed betragtet som en af de vigtigste nyskabelser i Databeskyttelsesforordningen, set i forhold til tidligere lovgivning på området.[176] Der kan argumenteres for, at dette skyldes den stigende udvikling, der finder sted indenfor teknologien, hvorfor det i dag er nemmere at designe systemer, på en måde hvor databeskyttelsen er indbygget. Det generelle formål med bestemmelsen er, at den dataansvarlige skal etablere et miljø omkring forberedelse og iværksættelse af

[170] *Databeskyttelsesrådet*: Guidelines 4/2019 on Article 25 (2019) side 8-9
[171] Ibid., side 9
[172] Ibid., side 9
[173] Ibid., side 9
[174] Ibid., side 25
[175] Ibid., side 25
[176] *Peter Blume*: Den nye persondataret (2018) side 143

persondatabehandlingen, som er egnet til, at Databeskyttelsesforordningen bliver overholdt.[177] Der skal foreligge et almindeligt, grundlæggende beskyttelsesniveau, uden det kræver yderligere handlinger. Artikel 25, stk. 1 vil ikke som udgangspunkt i sig selv være en regel om datasikkerhed, men såfremt der laves et godt design, vil sikkerheden være et af elementerne heri.[178]

Idet databeskyttelse gennem design skal tænkes ind fra starten, når der opbygges et nyt system, er reglen særdeles relevant for fase 1 ved opbygning af et AI system. Den dataansvarlige skal indføre passende foranstaltninger i opbygningsfasen, således det er muligt at opretholde et højt beskyttelsesniveau af den persondata, som følgende behandles i systemet. Dette kan eksempelvis være ved at implementere slettefrister. Såfremt der allerede er opbygget et system, kræves der af den dataansvarlige, at denne inkorporer passende foranstaltninger og fornødne garantier i fase 2, hvor artikel 25, stk. 1 i Databeskyttelsesforordningen stadig skal overholdes.

Det kan være svært for udvikleren af et AI system at forstå hvilke forpligtelser, der følger af artikel 25, stk. 1. Forpligtelserne kan i et vist omfang fremtræde forholdsvist overfladiske og upræcise, hvilket kan begrundes i, at det er svært at konkretisere eksempler på disse forpligtelser på forordningsniveau, uden at aktualisere en risiko for at disse forpligtelser hurtigt forældes, som følge af den teknologiske udvikling.[179] Som tidligere anført er Databeskyttelsesforordningen forsøgt udformet teknologineutralt, hvilket også kan begrunde en manglende konkretisering.[180] Samtidig kan det diskuteres, hvorvidt artikel 25, stk. 1 medfører yderligere forpligtelser, som ikke allerede følger af Databeskyttelsesforordningens andre bestemmelser.[181] Det er tvivlsomt, om dette er tilfældet, men konkret kan det siges, at formålet med artikel 25, stk. 1 må være at fastslå, at der skal anlægges et helhedssyn, hvor databeskyttelsen er i centrum. Dette gælder også ved udviklingen af et AI system.[182]

7.2 Art. 35 – Konsekvensanalyse

Databeskyttelsesforordningen tillægger ansvarlighed stor betydning, hvorfor dette er en af grundstenene i Databeskyttelsesforordningen.[183] Databeskyttelsesforordningen opridser flere måder og redskaber, som kan hjælpe den dataansvarlige, hvor en af disse er konsekvensanalyse. Reglerne for konsekvensanalyse fremgår

[177] *Peter Blume*: Den nye persondataret (2018) side 143
[178] Ibid., 143-144
[179] Ibid., side 145
[180] Forordning 2016/679, præambelbetragtning nr. 15
[181] *Peter Blume*: Den nye persondataret (2018) side 145
[182] Ibid., side 145
[183] Ibid., side 85

af Databeskyttelsesforordningens artikel 35, hvoraf formålet med en sådan analyse er at beskrive persondatabehandlingen, vurdere behandlingens nødvendighed og proportionalitet, samt bidrag til at belyse og håndtere de risici, der måtte være ved en behandling af personoplysninger.[184] [185] En konsekvensanalyse hjælper ikke blot den dataansvarlige med at sikre overholdelse af kravene i Databeskyttelsesforordningen, men den kan også påvise, at behandlingsaktiviteten er nøje vurderet, og at der herefter er truffet de nødvendige foranstaltninger.[186] Derfor skal det ses som en proces, der kan bidrage til at skabe og samtidig påvise overensstemmelse.[187]

7.2.1 Selve udarbejdelsen af analysen

Udførelsen af en konsekvensanalyse er ifølge Databeskyttelsesforordningen ikke altid obligatorisk. Det bliver det dog i de tilfælde, hvor behandlingen af personoplysninger "*sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder"*[188]*.*[189] Det er derfor den dataansvarliges ansvar at vurdere om de givende behandlingsaktiviteter hører under kategorien *høj risiko*. Det fremgår ikke klart af Databeskyttelsesforordningen, hvad der skal forstås ved *høj risiko*.[190] Derfor kan det være en kompleks opgave, idet vurderingen er forskellig fra behandling til behandling. Med baggrund i en ordlydsfortolkning af artikel 35, stk. 1 og præambelbetragtning nr. 90, skal den dataansvarlige udarbejde konsekvensanalysen forud for behandlingen, hvorfor det ikke er tilladt at påbegynde en behandling, hvis denne sandsynligvis vil indebære en høj risiko.[191]

Databeskyttelsesforordningen oplister i artikel 35, stk. 3 specifikke tilfælde, hvor en udførelse af en konsekvensanalyse navnlig er påkrævet. Listen skal dog ikke betragtes som udtømmende.[192] Ligeledes er det i artikel 35, stk. 4 klargjort, at tilsynsmyndighederne udarbejder samt offentliggør en liste over de yderligere behandlingsaktiviteter, som er underlagt en konsekvensanalyse.

[184] Forordning 2016/679, præambelbetragtning nr. 84
[185] *Artikel 29-gruppen*: 17/DA WP 248 (2017) side 4
[186] Ibid., side 4
[187] Ibid., side 4
[188] Forordning 2016/679, artikel 35, stk. 1
[189] *Artikel 29-gruppen*: 17/DA WP 248 (2017) side 9
[190] *Kristian Korfits Nielsen og Anders Lotterup*: Databeskyttelsesforordningen og Databeskyttelsesloven (2020) side 679
[191] Ibid., side 690
[192] *Artikel 29-gruppen*: 17/DA WP 248 (2017) side 10

Datatilsynet har på denne baggrund udarbejdet en liste, der understøtter samme formål som de kriterier[193] Artikel 29-gruppen fastslår i deres vejledning[194]. Generelt mener Artikel 29-Gruppen, at jo flere kriterier, som er opfyldt ved en behandling, desto mere sandsynligt vil det være at selve behandlingen udgør en høj risiko for de registreredes rettigheder og frihedsrettigheder, hvorfor en konsekvensanalyse er påkrævet. Listen fra Datatilsynet er udformet med afsæt i Artikel 29-gruppens retningslinjer.[195] Relevant kan nævnes:

- *Behandling ved brug af nye teknologier i sammenhæng med mindst et yderligere kriterie fra artikel 29 gruppens retningslinjer.*
- *Behandling der fører til afgørelse om en fysisk persons rettigheder til et produkt, en service en potentiel mulighed for begunstigelse, der er baseret på hvilken som helst form for automatiseret afgørelser (herunder profilering).*
- *Behandling der omfattet profilering af fysiske personer i stor skala, sådan som dette er defineret i artikel 29-gruppens retningslinjer.*
- *Behandling ad personoplysninger om sårbare personer eller hvor der er tale om behandling af følsomme oplysninger (særlige kategorier) og hvor, der benyttes profilering eller andre former for automatiserede afgørelser.*[196]

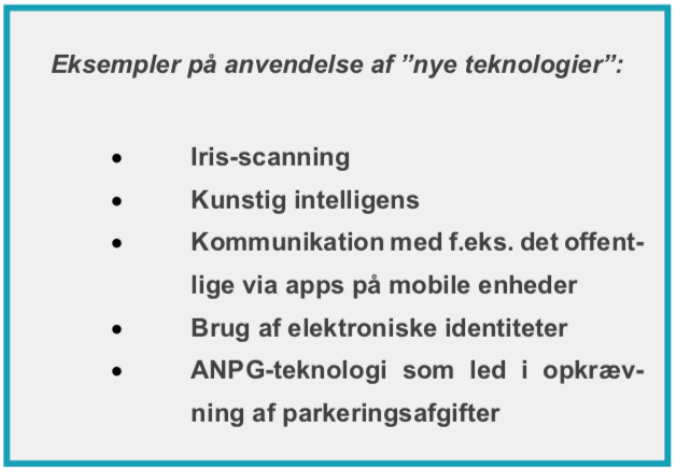
Det tydeliggøres dertil, at listen ikke er udtømmende, hvorfor den dataansvarlige stadig er forpligtet til at vurdere behandlingsprocessen.[197] Eftersom både profilering og automatiseret beslutningstagen er nævnt, hvilket er særskilt reguleret i Databeskyttelsesforordningens artikel 22, vil en definition heraf blive specificeret i afhandlingens afsnit 9. Dertil nævnes behandling ved brug af ny teknologi, hvorfor det anses relevant at undersøge, hvad der hører under kategorien *nye teknologier*.

7.2.2 Hvad er ny teknologi?

Udgangspunktet er, at der objektivt set skal være tale om ny teknologi, så blot fordi den dataansvarlige udskifter en IT-platform, betyder det ikke nødvendigvis at denne platform går under kategorien af *nye teknologier*.[198] Databeskyttelsesforordningen bruger ordet *navnlig*, når den omtaler ny teknologi.[199] Hermed skal det fortolkes således, at der ikke behøver at blive implementeret en helt ny teknologi, men det centrale

[193] *Artikel 29-gruppen*: 17/DA WP 248 (2017) side 10
[194] Ibid.
[195] https://www.datatilsynet.dk/media/6935/datatilsynets-liste-over-behandlinger-der-altid-er-underlagt-kravet-om-en-konsekvensanalyse.pdf side 1-2
[196] Ibid., side 1-2
[197] Ibid., side 1-2
[198] *Datatilsynet*: Konsekvensanalyse (2018) side 5
[199] Forordning 2016/679, præambelbetragtning nr. 89

er hvorvidt den dataansvarlige er nok bekendt med hvorledes teknologien virker og om der er kan foreligge høj risiko i behandlingen.[200] Datatilsynet har i deres vejledning om konsekvensanalyse[201] oplistet eksempler på, hvad der hører under kategorien af *nye teknologier*.



Figur 5 "Eksempler på anvendelse af nye teknologier"
Kilde: *Datatilsynet*: Konsekvensanalyse (2018) side 7

I ovenstående boks er det klargjort at kunstig intelligens, AI, hører under betegnelsen *nye teknologier*, hvorfor det antages, at der bør udføres en konsekvensanalyse ved brug af disse teknologier. Såfremt en behandling anvendes igennem en af ovenstående nævnte eksempler samtidig med at behandlingen foretages på følsomme personoplysninger, bliver sandsynligheden for at der skal udarbejdes en konsekvensanalyse større.[202] Et eksempel herpå er, hvis AI anvendes til at diagnosticere patienter og efterfølgende anbefaler en behandling. [203]

Begrundelsen for hvorfor udarbejdelsen af en konsekvensanalyse er særlig relevant ved anvendelse af ny teknologi, fremgår af Databeskyttelsesforordningens artikel 35, stk. 1 og præambelbetragtning nr. 89 og 91. Ud fra en ordlydsfortolkning må det lægges til grund, at brug af ny teknologi kan indebære nye former for dataindsamling og dataanvendelse, hvorved der kan opstå høj risiko for fysiske personers rettigheder og frihedsrettigheder. Hertil kan de personlige og sociale konsekvenser ved ibrugtagning af ny teknologi være ukendte, hvorfor det antages at der er en større sandsynlighed for, at persondatabehandlingen kan indebære

[200] *Peter Blume*: Den nye persondataret (2018) side 163
[201] *Datatilsynet*: Konsekvensanalyse (2018) side 7
[202] Ibid., side 6
[203] Ibid., side 6-7

en høj risiko for den registreredes rettigheder. En konsekvensanalyse skal hjælpe den dataansvarlige med at forstå og behandle disse risici.[204] [205]

7.2.3 Konsekvensanalyser i forbindelse med AI

Som fastlagt ovenstående går AI under betegnelsen *nye teknologier*, hvorfor det kan være en udfordring for den dataansvarlige at tage stilling til, hvilke passende foranstaltninger der skal implementeres for at beskytte de indsamlede personoplysninger. Meningen med konsekvensanalysen er at identificere de væsentligste risici, som er forbundet med behandlingen. Samtidig beskrives det, hvordan eventuelle risici kan nedbringes eller helt fjernes fra et AI system.[206]

Det er en afgørende faktor for, om der skal udføres en konsekvensanalyse, at statuere, hvorvidt der anvendes personoplysninger eller ej. Anvendes der anonymiseret data i fase 1, vil behandlingen som udgangspunkt ikke være indenfor Databeskyttelsesforordningens anvendelsesområde, hvorfor der ikke skal udføres en konsekvensanalyse. Det er dog tidligere lagt til grund at anonymiseret data kan blive henførbar til en fysisk person i tilfælde af reidentifikation, hvorfor en behandlingsaktivitet ved anvendelse af AI alligevel kan blive underlagt databeskyttelsesreglerne. Det må derfor lægges til grund, at den dataansvarlige skal vurdere den konkrete behandling samt foretage en vurdering løbende.[207] Såfremt det antages, at Databeskyttelsesforordningen først finder anvendelse i fase 2, bør udarbejdelsen af konsekvensanalysen foretages inden behandlingen igangsættes.[208]
Det fremgår af Databeskyttelsesforordningens præambelbetragtning nr. 90, at når der udføres en konsekvensanalyse *"bør den dataansvarlige inden behandlingen foretage en konsekvensanalyse"*. Ligeledes gør Artikel 29-gruppen det klart, at konsekvensanalysen *bør* ses som et redskab til beslutningsprocessen for en behandlingsaktivitet.[209] Idet både Artikel 29-gruppen samt Databeskyttelsesforordningens præambelbetragtning nr. 90 benytter ordet *bør,* må det antages, at der ikke altid foreligger et retligt krav, men det skal i stedet vurderes fra behandling til behandling om, hvorvidt en konsekvensanalyse er nødvendig.

[204] *Datatilsynet*: Konsekvensanalyse (2018) side 5
[205] *Artikel 29-gruppen*: 17/DA WP 248 (2017) side 12
[206] Ibid., side 12
[207] Ibid., side 7
[208] Forordning 2016/679, præambelbetragtning nr. 90
[209] *Artikel 29-gruppen*: 17/DA WP 248 (2017) side 16

Ved anvendelse af AI, hvor der er tale om ny teknologi, er behandlingsaktiviteten omfattet af én af de ni kriterier[210], hvor myndighederne har vurderet, at behandlingen sandsynligvis vil føre til en høj risiko, hvorfor den dataansvarlige enten skal udføre en konsekvensanalyse eller foretage en nøjere vurdering af, hvorvidt en konsekvensanalyse skal udarbejdes.[211] Såfremt det vurderes, at det ikke er nødvendigt at udarbejde en konsekvensanalyse, skal den dataansvarlige kunne bevise, hvorfor dette er tilfældet, idet den dataansvarlige er underlagt et dokumentationskrav. Med ordet *bør* skal der således ikke forstås, at det er et valg for den dataansvarlige, hvorvidt denne vil foretage en konsekvensanalyse eller ej. Den Dataansvarlige er underlagt et ansvarlighedsprincip, hvorfor den under alle omstændigheder skal kunne sikre og påvise overholdelse af Databeskyttelsesreglerne, og herunder artikel 35. [212]

I Databeskyttelsesforordningen lægges det til grund, at en konsekvensanalyse skal ajourføres.[213] Ved eventuelle ændringer af en behandlingsaktivitet eller hvor risikobilledet ændrer sig, skal den dataansvarlige, hvis dette anses nødvendigt, foretage en ny vurdering af behovet for, om der skal udføres en ny konsekvensanalyse.[214] Hvis AI systemet består af neuralt netværk, er AI maskinen i stand til at udvikle sig selv og samtidig kan nogle AI maskiner forbedre sig selv løbende. Fordi AI maskinerne er kodet til at tænke som mennesker vil sandsynligheden for, at behandlingsprocessen kan ændre sig, være høj.[215] Præcist derfor er der endnu større grund til, at den dataansvarlige løbende foretager vurderinger, således den registreredes rettigheder og frihedsrettigheder er tilgodeset samt beskyttet.

Til trods for at en bearbejdningsproces kan være ukendt, skal der tages højde for, om udførelse af en konsekvensanalyse kan være nødvendigt.[216] Artikel 29-gruppen fremhæver at "*gennemførelsen af en konsekvensanalyse for databeskyttelse er en løbende proces, ikke en engangsforeteelse."*[217] Dette medvirker til, at der løbende sørges for, at behandlingen er sikker og at behandlingsaktiviteten således er i overensstemmelse med Databeskyttelsesforordningen.[218]

[210] *Artikel 29-gruppen*: 17/DA WP 248 (2017) side 10
[211] Forordning 2016/679, præambelbetragtning nr. 83 og 84
[212] Forordning 2016/679, artikel 5, stk. 2 og artikel 24, stk. 1
[213] Forordning 2016/679, artikel 24, stk. 1
[214] Forordning 2016/679, artikel 35, stk. 11
[215] *Victor Thornton*: Hvad er forskellen på AI, Machine – og Deep Learning? (2018) se afsnit: *Deep Learning – Machine Learning med hukommelse*
[216] *Artikel 29-gruppen*: 17/DA WP 248 (2017) side 16
[217] *Ibid.,* side 17
[218] *Ibid.,* side 16-17

Idet AI løsninger ofte indebærer behandlingsaktiviteter af store datasæt, vil sandsynligheden for, at data ikke blot indeholder personoplysninger men også følsomme personoplysninger være stor, hvorfor det er endnu vigtigere, at der udføres en konsekvensanalyse ved AI.[219]

I forlængelse heraf kan den dataansvarlige af strategiske hensyn overveje en offentliggørelse af konsekvensanalysen, da eventuelle risici herved bliver offentliggjort.[220] Dog er en offentliggørelse ikke et krav, men det kan have en positiv effekt for overholdelse af gennemsigtighedsprincippet.[221]

7.3 Delkonklusion

Når en dataansvarlig foretager persondatabehandling ved anvendelse af AI, skal Databeskyttelsesforordningens forpligtelser overholdes. Særligt relevant er forpligtelserne om databeskyttelse gennem design i artikel 25, stk. 1 og konsekvensanalyse i artikel 35.
Det er utvivlsomt, hvorvidt databeskyttelse gennem design fremsætter yderligere forpligtelser, end hvad der allerede fremgår af Databeskyttelsesforordningens øvrige bestemmelser. Hovedsigtet med artikel 25, stk. 1 er derfor at klargøre overfor den dataansvarlige, at denne skal tænke databeskyttelse ind allerede fra start, ved for eksempel at designe et AI system, hvori der er implementeret passende foranstaltninger og fornødne garantier.

At databeskyttelse skal tænkes ind allerede fra start, stemmer ligeledes overens med Databeskyttelsesforordningens krav til at foretage en konsekvensanalyse. Er der sandsynlighed for, at en behandlingsaktivitet indebærer høj risiko for den registreredes rettigheder og frihedsrettigheder, opstiller artikel 35 et krav til den dataansvarlige om, at denne skal udarbejde en konsekvensanalyse. Ved persondatabehandling ved anvendelse af AI, er der tale om ny teknologi, hvorfor behandlingsaktiviteten sandsynligvis indebærer en høj risiko for den registrerede. I langt de fleste tilfælde, vil der derfor være et krav til den dataansvarlige om at foretage en konsekvensanalyse forud for, at persondatabehandlingen udføres. Den dataansvarlige er underlagt et ansvarlighedsprincip, hvorfor den skal kunne påvise og sikre overholdelse af Databeskyttelsesreglerne. Formålet med at udføre en konsekvensanalyse er, at undersøge hvor der forekommer store risici samt hvilke risici. På baggrund heraf, kan der således implementeres passende foranstaltninger.

[219] *Datatilsynet*: Konsekvensanalyse (2018) side 6
[220] *Artikel 29-Gruppen*: 17/DA WP 260 (2018) side 24
[221] *Ibid.,* side 21

8. Gennemsigtighed

I afhandlingens afsnit 6.4 er det klargjort at gennemsigtighed er et af de grundlæggende principper, jf. Databeskyttelsesforordningen artikel 5, stk. 1, litra a, hvorfor det er den dataansvarliges ansvar at overholde gennemsigtighedsprincippet, jf. artikel 5, stk. 2.
Der foreligger derfor en klar forpligtelse til overholdelse af gennemsigtigheden, der med Databeskyttelsesforordningen er blevet tydeliggjort i forhold til tidligere gældende retstilstand. Til trods for at gennemsigtigheden er blevet tydeliggjort, herunder i artikel 5, kan det dog ikke antages at medføre en ændring i forhold til den tidligere gældende retstilstand.[222]
Gennemsigtigheden har betydning for at fysiske personer kan forstå, hvordan deres personoplysninger bliver behandlet og til hvilket formål.[223] Gennemsigtighed har ligeledes betydning for erhvervsdrivende og deres arbejde i at sikre et ensartet beskyttelsesniveau for borgere i hele EU.[224] Det er forståeligt at gennemsigtigheden er central både for Databeskyttelsesforordningen generelt, men også for individet, således det er muligt for den fysiske person, at kunne gøre sine rettigheder gældende om nødvendigt.

Ved anvendelse af AI opstår der nye problematikker i henhold til overholdelse af de databeskyttelsesretlige regler, herunder særligt ved gennemsigtighedsprincippet. Mulighederne for at bruge Big Data til persondatabehandling skaber værdi, hvorfor det bliver mere og mere interessant for samfundet at udnytte denne værdi. Som tidligere nævnt er et af fænomenerne inden for brug af AI, den Sorte Boks. Denne opstår, når den dataansvarlige behandler personoplysninger igennem et neuralt netværk, og grundet den store datamængde, bliver behandlingsprocessen utrolig avanceret, hvilket kan medføre en snæver - eller slet ingen gennemsigtighed. Hermed opstår derfor en problemstilling i forhold til overholdelse af Databeskyttelsesforordningen.

Spørgsmålet er ikke, hvordan den dataansvarlige arbejder uden om gennemsigtigheden ved brug AI, men i stedet hvordan gennemsigtigheden præcist skal forstås, således der kan findes en vej, hvor et AI system både fungerer højteknologisk og samtidig overholder de databeskyttelsesretlige regler.

[222] *Kristian Korfits Nielsen og Anders Lotterup*: Databeskyttelsesforordningen og Databeskyttelsesloven (2020) side 314
[223] *Artikel 29-Gruppen*: 17/DA WP 260 (2018) side 4
[224] Forordning 2016/679, præambelbetragtning nr. 13

8.1 Gennemsigtighed i Databeskyttelsesforordningen

I Databeskyttelsesforordningen opstilles der rettigheder til den registrerede, hvilket modsvares af pligter for den dataansvarlige. Overholdelse af disse rettigheder og forpligtelser kan undertiden forekomme ressourcemæssigt hårdt for den dataansvarlige.[225] Det er derfor ønskeligt at finde et balancepunkt, hvor det både er attraktivt for den dataansvarlige at behandle persondata, samtidig med at den registreredes personoplysninger er underlagt et tilstrækkeligt beskyttelsesniveau. Især hvor behandlingen sker i en digital kontekst. Det må være en samfundsmæssig interesse, at der kan drages nytte af digitaliseringens fordele, herunder AI, hvorfor det ikke er Databeskyttelsesrettens formål at blokere for anvendelsen heraf i en databeskyttelsesretligt sammenhæng.[226] På baggrund heraf, må gennemsigtigheden, og herunder oplysningspligten, spille en betydelig rolle i at AI og Databeskyttelsesforordningen skal kunne fungere i sammenspil.

Gennemsigtighed er en overordnet forpligtelse i henhold til Databeskyttelsesforordningen og finder anvendelse på følgende områder: "*1) meddelelse af oplysninger til registrerede om en rimelig behandling, 2) hvordan den dataansvarlige kommunikerer med registrerede i forbindelse med deres rettigheder i henhold til persondataforordningen, og 3) hvordan dataansvarlige gør det lettere for registrerede at udøve deres rettigheder."*[227]

Af Databeskyttelsesforordningens kapitel III, *Den registreredes rettigheder,* fremgår endvidere de vigtigste artikler vedrørende gennemsigtighed.[228]

8.1.1 Databeskyttelsesforordningens artikel 12

I Databeskyttelsesforordningens artikel 12, 13 og 14, bliver gennemsigtigheden nærmere udspecificeret.[229] I artikel 12, stk. 1 og 2 tydeliggøres en række generelle betingelser for den dataansvarlige for, hvordan denne skal kommunikere for at opnå opfyldelse af oplysningspligterne i henhold til artikel 13 og 14.[230] Efterfølgende i artikel 12, stk. 3-8, fastsættes en række processuelle regler for udøvelsen af den registreredes rettigheder.[231]

[225] *Peter Blume*: Den nye persondataret (2018) side 114
[226] Ibid., side 114
[227] *Artikel 29-Gruppen*: 17/DA WP 260 (2018) side 4
[228] Ibid., side 7
[229] Ibid., side 7
[230] *Kristian Korfits Nielsen og Anders Lotterup*: Databeskyttelsesforordningen og Databeskyttelsesloven (2020) side 452
[231] Ibid., side 452

Det er den dataansvarliges opgave at oplysninger eller meddelelser vedrørende behandling blandt andet skal være kortfattet, gennemsigtig, letforståelig og lettilgængeligt, jf. artikel 12, stk. 1. Heraf er det overordnede formål, at den registrerede skal kunne forstå de informationer, som den dataansvarlige giver.[232] Derfor skal den dataansvarlige fremlægge oplysningerne effektivt og præcist for at undgå informationstræthed.[233] Den dataansvarlige skal skelne mellem målgruppen, særligt hvis denne er børn[234] og de registrerede skal ikke være nødsaget til at opsøge oplysningerne på eget initiativ.[235]

En central overvejelse vedrørende gennemsigtighedsprincippet er, *"at den registrerede på forhånd bør kunne afgøre, hvad omfanget og konsekvenserne af behandlingen indebærer, og at de ikke på et senere tidspunkt bør blive overrasket over, hvordan deres personoplysninger er blevet brugt"*[236].[237] I forlængelse heraf bør den dataansvarlige præcisere de vigtigste konsekvenser ved en databehandling, som er kompleks, teknisk eller uventet. Med andre ord skal der i databeskyttelsesmeddelelsen til den registrerede beskrives, hvilken betydning behandlingen faktisk kan have for den registrerede.[238]

8.1.2 Databeskyttelsesforordningens artikel 13 og 14

Databeskyttelsesforordningens artikel 13 og 14 afspejler ligeledes gennemsigtigheden, da disse artikler indeholder individets ret til indsigt, hvilket også kan forstås, som den dataansvarliges oplysningspligt.[239] I de to bestemmelser skildres mellem om oplysningerne er indsamlet hos den registrerede eller ej, ved direkte eller indirekte indsamling.[240] Både i artikel 13 og 14 er oplistet kriterierne for de konkrete oplysninger, der skal oplyses til den registrerede. Oplysninger skal gives for at sikre en rimelig og gennemsigtig behandling.[241] Fordi der i artikel 13 og 14 skelnes mellem hvordan indsamlingen har fundet sted, opstiller Databeskyttelsesforordningen forskellige krav i artiklerne. Når indsamlingen sker direkte, kan der stilles større informationskrav. Ved indirekte indsamling kan der være saglige årsager til at mindske kravet til den dataansvarlige, idet kravene kan være særligt krævende, begrundet i selve indsamlingen og den manglende direkte kontakt.[242]

[232] *Peter Blume*: Den nye persondataret (2018) side 115
[233] *Artikel 29-Gruppen*: 17/DA WP 260 (2018) side 7
[234] Ibid., side 7
[235] Ibid., side 8
[236] *Artikel 29-Gruppen*: 17/DA WP 260 (2018) side 8
[237] Ibid., side 8
[238] Ibid., side 8
[239] *Kristian Korfits Nielsen og Anders Lotterup*: Databeskyttelsesforordningen og Databeskyttelsesloven (2020) side 462
[240] *Peter Blume*: Den nye persondataret (2018) side 117
[241] *Kristian Korfits Nielsen og Anders Lotterup*: Databeskyttelsesforordningen og Databeskyttelsesloven (2020) side 462
[242] *Peter Blume*: Den nye persondataret (2018) side 117

Idet Databeskyttelsesforordningens artikel 13 og 14 indeholder en oplysningspligt menes, at den dataansvarlige har en pligt til på eget initiativ at opfylde de udspecificerede regler i artikel 13 og 14. Der er således ikke tale om regler, der blot skal opfyldes, hvis den registrerede fremsætter begæring herom.[243] For at opfylde oplysningspligten skal den dataansvarlige tage aktive skridt for at give oplysningerne til den registrerede. Her er nøgleordet *give*, hvormed menes, at den dataansvarlige aktivt skal arbejde mod, at den registrerede nemt kan finde oplysningerne eller lede den registrerede hen til oplysningernes placering.[244] Det er ikke tilstrækkeligt, at oplysningerne blot ligger på en hjemmeside, som den registrerede selv skal finde på eget initiativ.[245]

Artikel 13 og 14 fastlægger, hvilke oplysninger der skal gives til den registrerede ved påbegyndelsen af behandlingscyklussen.[246] Det fremgår dog ikke af oplysningspligten, at den dataansvarlige har pligt til at give den registrerede databeskyttelsesmeddelelsen flere gange.[247] I stedet er det aktuelt at den information, som bliver givet, kan ændre sig, hvorfor spørgsmålet er, om der derfor aktualiseres en fornyet oplysningspligt.[248] Ifølge Artikel 29-gruppen gælder gennemsigtighedsprincippet igennem hele behandlingscyklussen, hvorfor der skal ske en løbende opdatering. [249]

I Databeskyttelsesforordningens artikel 13, stk. 4 og 14, stk. 5, fremgår undtagelser til oplysningspligten, hvilket kan antages at indsnævre den dataansvarliges forpligtelser i henhold til overholdelse af gennemsigtighedsprincippet. Undtagelserne bør fortolkes snævert og forsigtigt.[250]
Oplysningspligten ved direkte indsamling i artikel 13, kan kun fraviges, såfremt den registrerede kender informationen på forhånd, men grundet en stor sandsynlighed for, at den registrerede giver oplysninger til mange forskellige dataansvarlige, samt at det er den dataansvarlige som har bevisbyrden, vil undtagelsen formentlig være svær at bevise, hvorfor det vil være bedst at informere den registrerede.[251]
I artikel 14, stk. 5 fremgår fire undtagelser. Begrundelsen for at der her foreligger flere undtagelser må være, at personoplysningerne ikke er indsamlet hos den registrerede men i stedet fra andre personer, hvorfor andre og flere undtagelser anses nødvendigt sammenlignet med artikel 13. I Databeskyttelseslovens § 22 og

[243] *Kristian Korfits Nielsen og Anders Lotterup*: Databeskyttelsesforordningen og Databeskyttelsesloven (2020) side 462
[244] Ibid., side 463
[245] Ibid., side 463
[246] *Artikel 29-Gruppen*: 17/DA WP 260 (2018) side 16
[247] *Peter Blume*: Den nye persondataret (2018) side 123
[248] Ibid., side 123
[249] *Artikel 29-Gruppen*: 17/DA WP 260 (2018) side 18
[250] *Peter Blume*: Den nye persondataret (2018) side 121
[251] Ibid., side 121

23 fremgår yderligere undtagelser til artikel 13 og 14. Da disse ikke anses for yderligere relevante for afhandlingen vil de dog ikke blive uddybet nærmere.

8.2 Gennemsigtighedens betydning for AI

Ovenstående er reglerne om gennemsigtighed i Databeskyttelsesforordningen belyst. I det følgende afsnit skal reglerne stilles op imod AI for at undersøge om persondatabehandling ved anvendelse af AI, herunder den Sorte Boks, kan overholde gennemsigtighedsprincippet eller om dette ikke er muligt ved en sådan behandling.

8.2.1 Hvad betyder gennemsigtig behandling?

Der fremgår ikke en klar definition af gennemsigtighed i Databeskyttelsesforordningen, men princippet er dog forsøgt tydeliggjort i præambelbetragtning nr. 39, som anført i afsnit 6.4.1.
Når gennemsigtighed bliver slået op i en ordbog, fremgår følgende betydninger; "*det at noget er transparent og at man kan se igennem det*", "*det at noget er let at forstå eller gennemskue*"[252] og "*a situation in which business and financial activities are done in an open way without secrets, so that people can trust that they are fair and honest*".[253]

Ved flere af definitionerne fremgår det, at gennemsigtighed skal forstås som noget, der er transparent. Ved andre definitioner skal gennemsigtigheden eksistere ved, at situationen er tilgængelig uden hemmelighed, således almindelige mennesker kan stole på handlingen, og at denne er udført med retfærdighed.

I Databeskyttelsesforordningens artikel 12 fremgår, at behandlingsprocessen skal forklares og beskrives for den registrerede i et sprog, så dette er forståeligt for målgruppen. Dette kan anses som problematisk, idet almenheden vil have svært ved at forstå algoritmerne i et AI system, da dette kan indeholde utrolig komplekse beregninger.[254] Spørgsmålet er derfor om almindelige mennesker vil være i stand til at forstå forklaringen af, hvordan deres personoplysninger behandles.
En antagelse er, at mennesker opsøger tryghed, hvorfor de i bund og grund blot har behov for at vide, at alt er godt, og at de ikke skal være bekymret, når rettighederne og frihedsrettighederne er i behold. Ifølge den

[252] https://ordnet.dk/ddo/ordbog?query=gennemsigtigheden
[253] https://dictionary.cambridge.org/dictionary/english/transparency
[254] http://denstoredanske.dk/It,_teknik_og_naturvidenskab/Informatik/Software,_programmering,_internet_og_webkommunikation/algoritme

kendte psykolog Maslow er sikkerhed menneskets andet største behov for at kunne fungere[255]. Ved blot at berolige individet med en forstående forklaring af en given behandling, vil det formentlig mindske tvivlen og frygten, hvorfor individet vil være i bedre stand til at stole på behandlingen og processen i øvrigt.[256]
Eksperten i AI, Evert Haasdijk siger, at en af grundene til at mennesker frygter AI er, at teknologien bag AI kan være svært at forklare.[257] Nogle former for AI er mere ligetil, hvor andre, såsom Deep Learning og den Sorte Boks, ofte er mere kompliceret. Dog udtaler Evert Haasdijk, at det ikke behøver at være så skræmmende.[258] En central del i at gøre en AI mere gennemsigtig er, at lade mennesker se, hvordan AI modellen er blevet testet samt meningen bag maskinen, hvorefter de kan forstå udfaldet af en beslutning.[259] Med dette menes, at den Sorte Boks kan *åbnes*, og det herudfra kan være muligt at forklare, hvordan en AI er kommet frem til resultatet. Hvorvidt det er muligt at beskrive behandlingsprocessen i et enkelt og let forståeligt sprog, er mere tvivlsomt.

Såfremt der kan skabes en forklaring af, hvordan et AI system er bygget op samt en god formulering, der forklarer, hvordan de registreredes rettigheder er tilgodeset, og herunder at de bliver behandlet retfærdigt, vil dette formentligt være en imødegåelse af gennemsigtighedsprincippet. Hvorvidt dette er nok til at gennemsigtigheden faktisk er overholdt, er dog endnu et ubesvaret spørgsmål.

8.2.2 Konsekvenserne for den registrerede

I Databeskyttelsesforordningens artikel 12, stk. 1 tydeliggøres, at den dataansvarlige skal være i stand til at præcisere, hvilke konsekvenser en databehandling kan medføre for den registrerede. Dette er særligt interessant, når der sker persondatabehandling ved anvendelse af AI, herunder Deep Learning, fordi der er mulighed for, at der opstår problematikker blandt andet med den Sorte Boks. Herved medfører dette, at behandlingsprocessen ikke nødvendigvis er gennemsigtig, idet den dataansvarlige ikke kan forklare, hvordan en behandling har fundet sted, samt hvordan udfaldet er blevet, som det er.[260] Sandsynligheden for at den dataansvarlige ikke er bekendt med alle mulige konsekvenser anses derfor at være en aktualitet. Databeskyttelsesforordningen stiller krav til at der udføres en konsekvensanalyse, som tidligere beskrevet i afsnit 7.2, da formålet hermed er, at den dataansvarlige bliver bekendt med mulige risici ved databehandlingen. Såfremt det antages, at der opstår den Sorte Boks ved en behandlingsproces af

[255] Maslows behovspyramide
[256] *Deloitte NL*: Transparency and responsibility in artificial intelligence (2019) side 6
[257] Ibid., side 6
[258] Ibid., side 6
[259] Ibid., side 4
[260] *Centre for Information Policy Leadership*: Artificial Intelligence and Data Protection in Tension (2018) side 15

personoplysninger, er det lagt til grund, at den dataansvarlige bruger konsekvensanalysen til at tydeliggøre konsekvenserne, hvorfor det herefter anses for muligt at beskrive disse for den registrerede. Det er dog et faktum at alle behandlingsprocesser ikke er ens, hvorfor det må formodes, at der skal ske en konkret vurdering af den givne situation. Det er tidligere lagt til grund, at en vurdering samt en udførelse af en konsekvensanalyse kan belyse eventuelle risici. Hvor der forekommer den Sorte Boks, og i tilfælde af at behandlingsaktiviteten er uigennemsigtig, kan det være en udfordring for den dataansvarlige at foretage en fyldestgørende vurdering af risici. Igen er det den Sorte Boks som formentlig skaber de største problematikker i henhold til Databeskyttelsesforordningen.

Samtidig fremgår det af Databeskyttelsesforordningens artikel 12-14, at den registrerede ikke på et senere tidspunkt skal blive overrasket over, hvordan personoplysningerne egentligt er blevet brugt.[261] Dermed skal den dataansvarlige være i stand til at have det fulde overblik over behandlingen. Det kan dog blive et problem, såfremt AI systemet er bygget op på neuralt netværk, hvorfor AI maskinen kan videreudvikle sig selv. Antages dette at være aktuelt, vil den dataansvarlige formentlig blive udfordret, da processen kan være svær at gennemskue. Et helt konkret svar, vil dog afhænge af den givne situation, da der er flere parametre, som kan have betydning for svaret. Herunder formålet med behandlingen, hvilken type oplysninger der behandles samt hvor indgribende behandlingen er for den registreredes rettigheder.

8.2.3 Oplysningspligten igennem behandlingscyklussen

Særligt ved persondatabehandling ved anvendelse af AI kan reglen om oplysningspligten igennem hele behandlingscyklussen være relevant, såfremt behandlingsprocessen ikke fuldt ud er fastlagt, hvilket kan være gældende i både fase 1 og 2. Hvis databehandlingen med tiden udvikler sig, eller AI systemet er bygget op via neuralt netværk, hvor AI systemet kan videreudvikle sig selv, vil det ikke være utænkeligt at behandlingsprocessen på den baggrund ændres. Hensynet til gennemsigtighed taler for, at der løbende skal ske en opdatering, hvorimod hensynet til den dataansvarliges byrder herved taler i mod. På den baggrund kan det antages, at en opdatering af databeskyttelsesmeddelelsen til den registrerede kun skal ske, såfremt den pågældende information anses væsentlig for den registreredes mulighed for at kunne varetage sin databeskyttelse.[262] Dermed må det være den dataansvarliges opgave at være særlig opmærksom på om der opstår ændringer, således der forekommer en oplysningspligt til den registrerede. Hvorvidt reglen skal håndhæves samt hvornår afhænger af den givne situation.

[261] *Artikel 29-Gruppen*: 17/DA WP 260 (2018) side 8
[262] *Peter Blume*: Den nye persondataret (2018) side 123

8.2.4 Yderligere tiltag

Såfremt den dataansvarlige kan efterkomme de ovenstående omtalte problematikker, må det antages, at den dataansvarlige er langt i processen med overholdelse af artikel 12-14. Endnu et tiltag, som kan hjælpe til gennemsigtighedsprincippet, er at offentliggøre den udarbejdede konsekvensanalyse. Dette vil muligvis kunne fremme tilliden til databehandlingsprocessen og påvise både gennemsigtighed samt ansvarlighed fra den dataansvarliges side. Offentliggørelsen er dog ikke obligatorisk, men ved at gøre den offentlig, vises der udadtil, at den dataansvarlige intet har at hemmeligholde, men i stedet er åben om processen og arbejdet bag behandlingen.[263]

Det er ikke et krav i Databeskyttelsesforordningen, at gennemsigtighedsprincippet skal gennemføres alene ved sproglig kommunikation.[264] Der er således mulighed for at benytte visualiseringsværktøjer, herunder ikoner, certificeringsmekanismer og databeskyttelsesmærkninger.[265] Fordelen ved at bruge standardiserede ikoner er, at den dataansvarlige kan reducere behovet for at præsentere store mængder skriftlige oplysninger, der skaber informationstræthed, og derved kan ikonerne i stedet øge gennemsigtigheden. Det er dog nødvendigt, at symbolerne og billederne kan anvendes og genkendes på samme måde i hele EU som synonymer for disse oplysninger.[266]
Formålet med certificeringsmekanismer og databeskyttelsesmærkninger er, at det er muligt for den registrerede hurtig at kunne vurdere databeskyttelsesniveauet i den enkelte situation[267], og derved øges gennemsigtigheden for den registrerede. Dertil vil godkendte certificeringsmekanismer og databeskyttelsesmærkninger medvirke til den dataansvarliges dokumentation for overholdelse af de databeskyttelsesretlige regler.[268]

Netop fordi AI er avanceret og formentlig kan være svært at forklare, vil ikoner, herunder billeder og symboler være en mulig løsning på bedre at kunne forklare og illustrere, hvad en behandlingsproces ved anvendelse af AI indeholder og indebærer. Ligeledes vil certificeringsmekanismer og databeskyttelsesmærkninger formentlig være en mulighed, hvis disse kan standardiseres og godkendes, således de kan benyttes på samme vilkår i hele EU. De nærmere regler samt krav herfor vil dog ikke belyses yderligere, men det lægges blot til grund at de med sandsynlighed kan fremme gennemsigtighedsprincippet.

[263] *Artikel 29-Gruppen*: 17/DA WP 260 (2018) side 24
[264] Ibid., side 27
[265] Ibid., side 27
[266] Ibid., side 28
[267] Forordning 2016/679, præambelbetragtning nr. 100
[268] *Artikel 29-Gruppen*: 17/DA WP 260 (2018) side 28

8.3 Gennemsigtighedens paradoks

Det er ovenstående tydeliggjort, at gennemsigtigheden spiller en vigtig rolle i overholdelse af Databeskyttelsesforordningen og ligeledes er gennemsigtigheden ved AI ofte kompleks og kan ikke blot anses at indeholde fordele. Blandt andet AI eksperten Andrew Burt[269] omtaler gennemsigtigheden ved AI som et paradoks, hvor processerne og forklaringerne skal tænkes nøje efter.[270]

En af fordelene ved gennemsigtigheden er, at det blandt andet kan være behjælpeligt til at løse problemer vedrørende rimelighed, diskrimination samt øge tilliden til et AI system,[271] men efter AI er blevet mere og mere udbredt, medfører det også en højere opmærksomhed. Derved har gennemsigtighed blandt andet ført til cyber-kriminalitet inden for AI.[272] Idet, der er stor fokus på, at en AI maskine skal være gennemsigtig i behandlingsprocessen samt ved opbygningen af maskinen, kan dette blive en åben bog for eventuelle risici. Derfor kan en AI maskine være mere sårbar overfor angreb.[273] Andrew Burt udtaler, "*To navigate this paradox, organizations will need to think carefully about how they're managing the risk of AI, the information they're generating about these risks, and how that information is shared and protected.*"[274] Efterfølgende udtaler han, at det i flere undersøgelser samt demonstrationer fremgår, at i nogle situationer er der så stor opmærksomhed på gennemsigtigheden, at risici bliver overset.[275]

Konklusionen bliver derfor, "*the more a model's creators reveal about the algorithm, the more harm a malicious actor can cause. This means that releasing information about a model's inner working may actually decrease its security or expose a company to more liability. All data, in short, carries risks*."[276] Det er således tydeliggjort at til trods for, at der arbejdes hårdt på, at gennemsigtigheden overholdes, må sikkerheden ikke glemmes i processen, da denne kan være mindst lige så essentiel for at beskytte de personoplysninger, der indgår i behandlingsaktiviteten.

Som et led i overholdelsen af gennemsigtighedsprincippet, må sikkerhedsforanstaltningerne og deres betydning ikke undervurderes.[277] Det er den dataansvarliges opgave, at alle forpligtelser overholdes og samtidig at dette foretages på en harmonisk måde, hvorpå den registreredes rettigheder beskyttes på den bedst givne måde. Da AI er et højteknologisk fænomen, kræver det også, at der skal tænkes fremadrettet

[269] https://www.andrewdburt.com
[270] *Andrew Burt*: The AI transparency paradox (2019), 3. afsnit
[271] Ibid., 1. Afsnit
[272] Ibid., 2. Afsnit
[273] Ibid., 3. Afsnit
[274] Ibid., 3. Afsnit
[275] Ibid., 4-8. Afsnit
[276] Ibid., 9. Afsnit
[277] https://erhvervsstyrelsen.dk/ny-vejledning-saetter-fokus-paa-sikkerheden-ved-brug-af-kunstig-intelligens-i-praksis?fbclid=IwAR3WRqVQeIfeVqkuU_NGQ0cTyTwkrm6hDqH7vy2vAjGMAv1LDaZBmHWN4jM

med sikkerheden. Det er ikke nok, at der bliver taget de samme foranstaltninger som tidligere. Chef for Center for Cybersikkerhed udtaler i forbindelse med en ny vejledning fra Erhvervsstyrelsen vedrørende sikkerheden ved anvendelse af AI i praksis, at der skal opretholdes et godt risikobaseret sikringsniveau, hvor det ikke blot er nok at tage højde for de traditionelle it-risici, men det er nødvendigt at indtænke nye risici, som brugen ved AI kan introducere.[278]

Således bør eventuelle fremtidsscenarier gennemtænkes og vurderes for, at den dataansvarlige er i stand til at tage sine forholdsregler. I takt med at udviklingen bliver mere og mere avanceret inden for AI, sker samme udvikling inden for IT-kriminalitet, herunder hacking af IT-systemer.[279] Kravene til den dataansvarlige bliver derfor også automatisk højere og højere, da den dataansvarlige skal efterleve de udfordringer, som samfundet skaber, således den dataansvarlige stadig kan beskytte den registreredes personoplysninger. Dermed skal sikkerhedsforanstaltningerne tages på forhånd. Ikke nok med at sikkerhedsforanstaltningerne er vigtige, men tilliden til de digitale løsninger har ligeledes en afgørende betydning for, hvordan AI kan bruges i fremtiden.[280]

8.4 Delkonklusion

Gennemsigtighedsprincippet fremgår af Databeskyttelsesforordningens artikel 5, stk. 1, litra a, og er forsøgt uddybet i artikel 12-14, idet bestemmelserne indeholder den dataansvarliges oplysningspligt over for den registrerede. Såfremt der foretages persondatabehandling ved anvendelse af AI, antages det dog, at den dataansvarlige kan blive udfordret i henhold til opfyldelse af oplysningspligten. Herunder i tilfælde af at den dataansvarlige benytter et AI system, hvor der foreligger den Sorte Boks. Hvorvidt den dataansvarlige er i stand til at forklare konsekvenserne af persondatabehandlingen i AI systemet i et klart og enkelt sprog, må være en konkret vurdering. Dertil skal den dataansvarlige kunne oplyse om eventuelle konsekvenser for den registrerede ved persondatabehandlingen, og såfremt der sker ændringer i behandlingscyklussen, som kan have væsentlig betydning for den registrerede, kræver oplysningspligten at den dataansvarlige meddeler herom.

Yderligere kan den dataansvarlige implementere andre tiltag, som kan fremme gennemsigtigheden. Heriblandt kan nævnes konsekvensanalyse og visualiseringsværktøjer, herunder ikoner,

[278] https://erhvervsstyrelsen.dk/ny-vejledning-saetter-fokus-paa-sikkerheden-ved-brug-af-kunstig-intelligens-i-praksis?fbclid=IwAR3WRqVQeIfeVqkuU_NGQ0cTyTwkrm6hDqH7vy2vAjGMAv1LDaZBmHWN4jM
[279] Ibid.
[280] Ibid.

certificeringsmekanismer og databeskyttelsesmærkninger. Tiltagene kan ikke blot bidrage til en høj gennemsigtighed, men har ligeledes en positiv effekt for den dataansvarliges dokumentationskrav, herunder den dataansvarliges ansvarlighedsprincip, jf. Databeskyttelsesforordningens artikel 5, stk. 2 og 24.

Blandt andet AI ekspert Andrew Burts påpeger, at sikkerhed ikke bør undervurderes i henhold til gennemsigtigheden, således den dataansvarlige ikke vægter gennemsigtighedsprincippet højere end sikkerhedsforanstaltninger. Kravene til IT-sikkerheden har altid være høje, og det er særdeles vigtigt at tage de passende sikkerhedsforanstaltninger, hvilket fortsat vil være gældende i forbindelse med AI og ved anvendelse af nye digitale løsninger.

Diskussionen om, hvad der egentlig kan forstås med gennemsigtighed samt, hvad der kræves for at gennemsigtighedsprincippet er opfyldt, vil forblive et åbent spørgsmål, idet der ikke foreligger et egentlig svar herpå. Dog kan det statueres, at ved behandling ved anvendelse af AI bør den dataansvarlige tilgodese både overholdelse af gennemsigtighedsreglerne samt at opretholde et tilstrækkeligt sikkerhedsniveau.

9. Automatiske afgørelser

Når der sker databeskyttelsesretlig behandling af personoplysninger ved anvendelse af AI, er det relevant at se på Databeskyttelsesforordningens artikel 22, som omhandler automatiske individuelle afgørelser, herunder profilering. De teknologiske fremskridt indenfor Big Data og AI har gjort det nemmere at oprette profiler og træffe automatiske afgørelser, der i væsentlig grad kan påvirke den registreredes rettigheder og frihedsrettigheder.[281] Automatiske afgørelser har en del fordele, som blandt andet omfatter øget effektivitet og ressourcebesparelser.[282] Dog kan det samtidig udgøre en betydelig risiko for det enkelte individ, idet processerne kan være uigennemsigtige.[283] Der er risiko for at profilering kan udvise bias, ved at fastholde eksisterende stereotyper og social adskillelse, eller fastholde personer i en bestemt kategori, og dermed begrænse udfaldet. Dette kan i visse tilfælde føre til unøjagtige forudsigelser, eller at der udøves urimelig forskelsbehandling. [284]

Derfor indeholder Databeskyttelsesforordningen bestemmelser vedrørende håndtering af risiciene forbundet med automatiske afgørelser og profilering.[285] Det er alene artikel 22, som specifikt omhandler brugen af automatiske afgørelser. Såfremt en databehandling er omfattet af artikel 22, har den dataansvarlige pligt til at informere den registrerede herom, jf. Databeskyttelsesforordningens artikel 12.

9.1 Automatiske individuelle afgørelser, herunder profilering

Overskriften på artikel 22 refererer til både automatiske individuelle afgørelser og profilering. Profilering defineres i Databeskyttelsesforordningens artikel 4, stk. 4, som: "*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 bevægelser".*

Profilering består således af tre elementer, der skal opfyldes. For det første skal der være en automatisk form for behandling. For det andet, skal denne udføres på grundlag af personoplysninger. For det tredje skal formålet med profilering være at vurdere personlige forhold vedrørende en fysisk person.

[281] *Artikel 29-gruppen*: 17/DA WP251 (2018) side 5
[282] Ibid., side 5
[283] Ibid., side 5
[284] Ibid., side 5-6
[285] Ibid., side 6

Udgangspunktet for profilering er Big Data, som betegner meget store datamængder. Denne datamængde kan mikroanalyseres ved brug af datamining.[286] Herved kan oplysninger om det enkelte individ lokaliseres, og der sker en profilering af personen, som giver en viden om nye sammenhænge.[287] Profilering vil i Databeskyttelsesforordningens sammenhæng være automatiseret brug af persondata med henblik på, at der evalueres personlige træk hos det enkelte individ.[288] Dette kan for eksempel være at forudsige fremtidig adfærd i forskellige situationer eller at afdække personlige præferencer og interesser. Ved profilering vil der derfor ofte blive anvendt et AI system, idet dette, som tidligere anført, giver øget muligheder for udnyttelsen af Big Data.[289] AI systemer kan derved medvirke til at skabe mere dybdegående og komplekse profiler, end traditionelle analytiske metoder kan. Det afgørende ved, om der er tale om profilering, er formålet med klassificeringen af data.[290] En simpel klassificering baseret på alder eller køn, er ikke nødvendigvis en profilering, såfremt klassificeringen sker ud fra statistiske formål. Såfremt klassificeringen derimod bruges til at foretage forudsigelser eller drage konklusioner om den enkelte, er der derimod tale om en profilering.[291]

Af artikel 4, stk. 4 fremgår det, at profilering er *"enhver form for automatisk behandling",* hvorimod Databeskyttelsesforordningens artikel 22, stk. 1 kun finder anvendelse ved *"afgørelser, der alene er baseret på automatisk behandling".* Det er således uklart, om en profilering *alene* skal være baseret på automatisk behandling, før artikel 22 vil finde anvendelse. Artikel 29-gruppen udtrykker i deres retningslinjer, at alle former for automatisk behandling kan udgøre profilering, og at en menneskelig indgriben ikke udelukker, at der er tale om en profilering.[292] Ud fra denne opfattelse, kan en profilering således godt være omfattet af artikel 22, selvom afgørelsen ikke *alene* er baseret på automatisk behandling.[293] Dog fremgår det af Databeskyttelsesforordningens præambelbetragtning nr. 71, at profilering kun er omfattet af artikel 22, når den har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende.[294]

Automatiske afgørelser har et andet anvendelsesområde end profilering, men kan delvist overlappe eller være resultatet af profilering.[295] Det fremgår af artikel 22, stk. 1 at automatiske afgørelser er afgørelser

[286] *Peter Blume*: Den nye persondataret (2018) side 72
[287] Ibid., side 72
[288] Ibid., side 72
[289] *Det Norske Datatilsyn*: Artificial intelligence and privacy (2018) side 5
[290] *Artikel 29-gruppen*: 17/DA WP251 (2018) side 7
[291] Ibid., side 7
[292] Ibid., side 7
[293] Ibid., side 7
[294] Betænknings nr. 1565, side 375
[295] *Artikel 29-gruppen*: 17/DA WP251 (2018) side 8

baseret på automatisk behandling. Databeskyttelsesforordningens artikel 4, stk. 1, nr. 2 definerer en behandling som *"enhver aktivitet eller række af aktiviteter — med eller uden brug af automatisk behandling — som personoplysninger eller en samling af personoplysninger gøres til genstand for"*. At behandlingen er automatisk betyder, at den er truffet ved brug af teknologiske midler uden menneskelig indgriben.[296] Eftersom en automatisk afgørelse skal være baseret på automatisk behandling, vil behandlingen blive foretaget ved anvendelse af AI.

Automatiske afgørelser kan derfor være truffet med eller uden profilering, samtidig med at profileringer også kan finde sted uden automatiske afgørelser. Ligeledes kan en i første omgang simpel automatisk afgørelse blive til en afgørelse baseret på profilering alt efter, hvordan dataene anvendes.[297] Et eksempel herpå, kan være pålægning af hastighedsbøder, som udelukkende er baseret på dokumentation fra hastighedskameraer. Her vil der være tale om en automatisk behandling, som ikke nødvendigvis indebærer profilering.[298] Såfremt den enkeltes kørselsvaner overvåges over tid, og størrelsen på bøden er en vurdering, der afhænger af andre faktorer, vil det imidlertid blive en afgørelse baseret på profilering.[299]

9.2 Forbud eller rettighed

Generelt vil den dataansvarlige kunne foretage profilering og træffe automatiske afgørelser, hvis den kan opfylde Databeskyttelsesforordningens grundlæggende principper, samt har et hjemmelsgrundlag for behandlingen. I tilfælde af at der er tale om afgørelser, der alene er baseret på automatisk behandling, herunder profilering, vil artikel 22 finde anvendelse, og den dataansvarlige vil blive pålagt yderligere garantier og restriktioner.

Artikel 22, stk. 1 lyder: *"Den registrerede har ret til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende".* Ud fra en naturlig forståelse af ordlyden, indeholder denne bestemmelse derfor en ret for den registrerede til ikke at være genstand for en sådan afgørelse. Artiklens ordlyd er umiddelbart enslydende med dens forgænger i Persondatadirektivets artikel 15, som omhandlede edb-behandlede individuelle afgørelser. Denne bestemmelse havde retsvirkning som en rettighed, og skulle derfor påberåbes af den registrerede, før den fandt anvendelse.[300]

[296] *Artikel 29-gruppen*: 17/DA WP251 (2018) side 8
[297] Ibid., side 8-9
[298] Ibid., side 8
[299] Ibid., side 8
[300] Betænknings nr. 1565/2016, side 371

Eftersom artikel 22 er formuleret på ovenstående måde, vil en naturlig fortolkning derfor være, at der også her er tale om en rettighed, som den registrerede kan gøre gældende, såfremt vedkommende bliver udsat for en afgørelse, der alene er baseret på automatisk behandling uden menneskelig indgriben. Dette understøttes ligeledes af justitsministeriets betænkning nr. 1565/2016.[301] Denne ligger vægt på, at ordlyden af Databeskyttelsesforordningens artikel 22 næsten er identisk med Persondatadirektivets artikel 15, hvorfor forståelsen må være den samme. Derfor må der alene være tale om en indsigelsesret, som skal aktiveres af den registrerede, og ikke et direkte forbud.[302]

Denne opfattelse deles dog ikke af Artikel 29-gruppen. De udtrykker at *ret* ikke er ensbetydende med, at der er tale om en rettighed for den registrerede.[303] I stedet mener de, at artikel 22 indeholder et generelt forbud mod afgørelser, der alene er baseret på automatisk behandling.[304] Ved at fortolke artikel 22 som et forbud, og ikke som en ret, der skal påberåbes, medvirker det til, at den registrerede er beskyttet mod de potentielle virkninger, som denne type behandling kan have, og det styrker idéen om, at den registrerede har kontrol over sine personoplysninger.[305] At dette er hensigten, understøttes ligeledes af Databeskyttelsesforordningens præambelbetragtning nr. 71, hvori det lyder: "*Afgørelser baseret på en sådan behandling, herunder profilering, bør dog være tilladt, når EU-ret eller medlemsstaternes nationale ret (…) eller hvis det er nødvendigt for indgåelse eller opfyldelse af en kontrakt (…) eller når den registrerede har givet sit udtrykkelige samtykke".* Idet præambelbetragtningen anvender udtrykket "*bør dog være tilladt"*, må det forstås som, at kun såfremt undtagelserne i artikel 22, stk. 2 finder anvendelse, er en automatisk afgørelse, herunder profilering, som er omfattet af anvendelsesområdet i stk. 1, lovlig.[306] Samtidig kan der argumenteres for, at undtagelsen i Databeskyttelsesforordningens artikel 22, stk. 2, litra c, hvor en behandling efter artikel 22 kan udføres, såfremt den registrerede giver samtykke hertil, ikke vil give mening, såfremt der er tale om en rettighed og ikke et forbud.[307] Den registrerede kan ikke give samtykke og fremsætte indsigelser mod den samme behandling.[308]

[301] Betænknings nr. 1565/2016, side 375
[302] Ibid., side 375
[303] *Artikel 29-gruppen*: 17/DA WP251 (2018) side 20
[304] Ibid., side 20
[305] Ibid., side 21
[306] Ibid., side 21
[307] *Christopher Kuner, et al:* The EU General Data Protecion Regulation (GDPR) A Commentary, (2020) side 530
[308] *Artikel 29-gruppen*: 17/DA WP251 (2018) side 37

Bestemmelsen er således underlagt betydelig uenighed. Selvom den tidligere bestemmelse i Persondatadirektivet var formuleret som en rettighed, var der dog også nogle medlemsstater som anvendte denne som et forbud.[309] Justitsministeriets betænkning nr. 1565/2016 er fra år 2016, og på dette tispunkt var Artikel 29-gruppens vejledning om anvendelsen af Databeskyttelsesforordningens artikel 22, som er fra 2018, endnu ikke eksisterende. Samtidig er Artikel 29-gruppen et EU-organ, hvorfor der sikres en harmonisering igennem hele EU ved at bruge deres fortolkning frem for Justitsministeriets betænkning, som blot er rettet mod Danmark. Ligeledes kan der argumenteres for, at Det Europæiske Databeskyttelsesråd ikke har været ude og ændre eller modsige Artikel 29-gruppens synspunkt, men derimod endosseret deres arbejde.[310] Det at gøre artikel 22 til et kvalificeret forbud vil ligeledes styrke dens betydning, og give den registrerede yderligere beskyttelse.[311] Disse er stærke argumenter for, at der med artikel 22 foreligger et forbud, men dette strider direkte imod ordlyden af artikel 22, stk. 1. Såfremt bestemmelsens formål er, at pålægge den dataansvarlige et forbud mod denne type behandling, ville ordlyden af bestemmelsen være anderledes.[312] Der kan blandt andet henvises til artikel 22, stk. 4, hvor det fremgår, at en behandling af følsomme oplysninger ikke må finde sted. Denne er formuleret direkte som et forbud.

På baggrund af det ovenstående, og på baggrund af at artikel 22 er placeret i Databeskyttelsesforordningens kapitel III, som omhandler den registreredes rettigheder, må det konkluderes, at artikel 22 skal fortolkes som en rettighed og ikke et forbud. Såfremt bestemmelsen skal være underlagt en anden fortolkning, må dette afklares i praksis.[313]

9.3 Afgørelser der alene er baseret på automatisk behandling

I artikel 22 anvendes ordlyden *"der alene er baseret"* på automatisk behandling. Dette må forstås som, at der ikke er nogen menneskelig indgriben i beslutningsprocessen.[314] Det betyder således samtidig, at såfremt der er en menneskelig indgriben, er behandlingen udenfor artikel 22's anvendelsesområde. For at der kan være tale om en menneskelig indgriben, skal den dataansvarlige sikre, at dette indgreb er meningsfuldt og ikke blot en tom gestus.[315] Spørgsmålet er herefter, hvor meget der skal til, før der er tale om en menneskelig indgriben.

[309] *Christopher Kuner, et al:* The EU General Data Protecion Regulation (GDPR) A Commentary, (2020) side 530
[310] *Peter Blume:* Den nye persondataret (2018) side 52-53
[311] *Christopher Kuner, et al:* The EU General Data Protecion Regulation (GDPR) A Commentary, (2020) side 531
[312] Ibid., side 531
[313] *Kristian Korfits Nielsen og Anders Lotterup*: Databeskyttelsesforordningen og Databeskyttelsesloven (2020) side 575
[314] *Artikel 29-gruppen*: 17/DA WP251 (2018) side 21
[315] Ibid., side 22

9.3.1 Menneskelig indgriben

Det kan være svært at forestille sig et system, som fungerer fuldstændig uden menneskelig indgriben. Der findes dog på nuværende tidspunkt mange automatiserede systemer. Både indenfor den offentlige forvaltning, og indenfor private virksomheder, bliver der i dag benyttet mange automatiserede systemer, og nogle af afgørelserne heraf vil have betydelige konsekvenser for de registrerede.[316] Dog vil meget få af afgørelserne fungere uden at have et menneske involveret i beslutningsprocessen.[317] Her vil den automatiske afgørelse i stedet fungere som et støttesystem til beslutningsprocessen.[318]

Hvis en hvilken som helst grad af menneskelig indgriben betyder, at kravet i Databeskyttelsesforordningens artikel 22, om at en afgørelse skal være foretaget alene ved brug af automatisk behandling, ikke er opfyldt, vil bestemmelsen ud fra en naturlig ordlydsfortolkning betyde, at den kun finder anvendelse i meget få situationer. Det vil være relativt nemt for en offentlig forvaltning eller virksomhed, at strukturere sig ud af problemstillingen.[319] Dette kan gøres ved at inddrage en minimal menneskelig indgriben eller tilsyn i processen, for eksempel ved at blåstemple alle afgørelse lavet af et AI system, og dermed ekskludere en afgørelse fra artikel 22's anvendelsesområde.[320]

Dette vil stride direkte imod intentionen med bestemmelsen. Det fremgår af Databeskyttelsesforordningens præambelbetragtning nr. 68, at den registrerede skal have en øget kontrol over behandlingen af dennes personoplysninger, når behandlingen foretages automatisk. Denne øget kontrol vil således ikke blive pålagt den automatiske afgørelse, såfremt denne ikke er omfattet af artikel 22. Derfor understreger Artikel 29-gruppen ligeledes, at den dataansvarlige ikke kan nøjes med blot at efterse eller blåstemple en afgørelse.[321] Såfremt den menneskelige indflydelse er uden betydning for selve afgørelsen, vil systemet blive anset for at være alene automatisk.[322] Ved vurderingen af om tilsynet er meningsfyldt, kan der blandt andet undersøges, hvor ofte mennesket er uenig med den automatiske afgørelse, og dermed ændrer eller argumenterer imod afgørelsen.[323]

---

[316] *Michael Veale og Lilian Edwards*: Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling (2018) side 400
[317] Ibid., side 400
[318] Ibid., side 400
[319] Ibid., side 400
[320] Ibid., side 400
[321] *Artikel 29-gruppen*: 17/DA WP251 (2018) side 21
[322] Ibid., side 21-22
[323] *Michael Veale og Lilian Edwards*: Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling (2018) side 400

Artikel 29-gruppens synspunkter for vurderingen af, hvorvidt der foreligger menneskelig indgriben, kan opsummeres i tre punkter.

- Tilsynsføreren skal vurdere AI systemets anbefalinger, og bør ikke rutinemæssigt efterkomme disse afgørelser.
- Anbefalingerne skal vurderes og gennemgås på baggrund af alle relevante oplysninger og faktorer, som har resulteret i den konkrete afgørelse.
- Tilsynet skal være aktivt og meningsfuldt, og det skal foretages før afgørelsen får retsvirkninger for den registrerede.[324]

I bedømmelsen af, om tilsynet er aktivt og meningsfuldt, skal der lægges vægt på to forhold. For det første skal tilsynet foretages af en person, der har den fornødne kompetence, og for det andet skal denne person have mulighed for at ændre afgørelsen.[325] Hvorvidt en person har mulighed for at ændre en afgørelse, giver ikke anledning til tvivl. Dog kan det første forhold skabe fortolkningsproblemer. Artikel 29-gruppen bidrager ikke med, hvordan dette skal fortolkes. Fornødne kompetence kan forstås, som at tilsynsføreren skal være bemyndiget til at foretage eventuelle ændringer til afgørelserne. Det er dog uvist, hvorvidt denne bemyndigelse kræver, at tilsynsføreren er kompetent til at kunne forstå den tekniske og juridiske vurdering, der ligger til grund for afgørelsen. Der kan dog argumenteres for, at tilsynsføreren skal have en vis forståelse for, at et tilsyn er meningsfuldt.
Det ligger klart, at den menneskelige indgriben ikke må fingeres. Derfor skal tilsynsføreren vurdere AI systemets afgørelse, og ikke uden videre acceptere enhver afgørelse. For at efterkomme dette, må tilsynsføreren have en vis forståelse for grundlaget for en given afgørelse. På baggrund af denne fortolkning, kan der således udledes en form for indirekte krav til, at tilsynsføreren har en vis forståelse for systemets indhold og virkemåde. Konklusionen må derfor blive, at et meningsfuldt menneskeligt indgreb kun kan finde sted, såfremt tilsynet udøves af en person, som har en tilstrækkelig teknisk og juridisk viden omkring, hvordan systemet fungerer, og herunder hvordan systemet kommer frem til et bestemt resultat.

Det er ikke uproblematisk at pålægge tilsynsføreren sådanne krav. Sker der eksempelvis en profilering, hvor AI systemet er opbygget som Deep Learning, ved at tage udgangspunkt i en meget stor datamængde, vil det ikke altid være muligt med menneskelig indgriben. Såfremt selve processen er uigennemsigtig, vil dette besværliggøre det meningsfulde menneskelige indgreb.[326] Processen eller algoritmerne kan være så

[324] *Artikel 29-gruppen*: 17/DA WP251 (2018) side 21-22
[325] Ibid., side 22
[326] *Privacy International:* Data is Power: Profiling and Automated Decision-Making in GDPR (2017) side 13-14

komplekse, at meget få personer rent faktisk vil forstå, hvordan disse fungerer. Denne problematik kommer særligt til udtryk, såfremt AI systemet indeholder den Sorte Boks. Rent praktisk kan dette betyde, at selvom det i sidste ende er et menneske, som foretager en afgørelse, vil denne ikke have en reel mulighed for at lave et meningsfuldt tilsyn med beslutningsprocessen. Et tilsyn kan ikke være meningsfuldt, såfremt selve processen er uigennemsigtig.[327] Tilsynsføreren skal være i stand til at vurdere, hvorvidt afgørelsen eller profileringen er nøjagtig, retfærdig og ikke-diskriminerende.[328] Dette kræver, at tilsynsføreren skal overveje og gennemse alle tilgængelige input og output, hvilket ikke altid vil være muligt ved Big Data analyser og Deep Learning.[329]

En anden årsag til, at et meningsfuldt tilsyn kan besværliggøres, kan forekomme idet, at algoritmer og AI begynder at blive bedre end mennesker til af lave afgørelser. Allerede i dag findes der AI systemer, der har vist sig bedre end mennesker til at foretage konkrete afgørelser, og dermed minimere fejl i beslutningsfasen. Et eksempel herfor kan ses indenfor medicinalindustrien, hvor et AI system, opbygget som et neuralt netværk, har vist sig bedre end hjertespecialister til at finde og identificere hjertefejl hos patienterne.[330] Hovedårsagen til den store succes er, at AI systemet anvender et stort datasæt, samtidig med at de mange lag i det neurale netværk, er med til at lave dybdegående analyser af patienternes sundhedsmæssige forhold.[331] Problematikken med et meningsfuldt menneskeligt tilsyn vil her opstå, når dette tilsyn skal bevises. Når AI systemer bliver bedre til at lave korrekte afgørelser, vil det samtidig betyde, at det menneskelige tilsyn minimeres.[332] Indgrebene vil derfor blive færre, og bevisbyrden for, at der er foretaget et meningsfuldt indgreb i beslutningsprocessen, vil blive sværere at løfte.[333] Såfremt det ikke kan bevises, at der er ydet et meningsfuldt menneskeligt tilsyn af en person med den fornødne kompetence i situationer, hvor dette rent faktisk er tilfældet, vil disse afgørelser blive anset for alene at være baseret på automatisk behandling. Dette vil give den dataansvarlige problemer med at strukturere sig ud af artikel 22's anvendelsesområde.[334]

[327] *Privacy International:* Data is Power: Profiling and Automated Decision-Making in GDPR (2017) side 14
[328] Ibid., side 14
[329] Ibid., side 14
[330] *Pranav Rajpurkar, et al.*: Cardiologist-Level Arrhythmia Detection with Convolutional Neural Networks (2017) side 5-6
[331] Ibid., side 5-6
[332] *Michael Veale og Lilian Edwards*: Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling (2018) side 400-401
[333] Ibid., side 400-401
[334] Ibid., side 400-401

Selve konceptet med at have en tilsynsfører med den fornødne kompetence, er med til at sikre, at systemet fungerer korrekt. Konceptet er dog ikke uproblematisk, da det bevirker, at mennesket og AI systemet deler kontrollen over en given behandling.[335] Der kan tænkes at opstå situationer, hvor et menneske kan blive holdt ansvarlig for en afgørelse, som vedkommende ikke forstår eller har mulighed for at forstå, grundet de mange skjulte og komplekse lag, der kan ligge bag en automatisk individuel afgørelse.[336] I dette tilfælde vil det ligeledes, som statueret ovenstående, blive besværliggjort at foretage et meningsfuldt menneskeligt indgreb, grundet uigennemsigtigheden.

9.4 "Retsvirkning" eller "på tilsvarende vis betydeligt påvirker"

Det er i Databeskyttelsesforordningen anerkendt, at en automatisk afgørelse eller profilering, kan have betydelige konsekvenser for den enkelte.[337] Kun hvor der er tale om en *"retsvirkning eller på tilsvarende vis betydeligt påvirker den registrerede"*[338], vil en afgørelse være omfattet af artikel 22. Dog fremgår der ikke nogen definition i Databeskyttelsesforordningen omkring, hvornår dette er tilfældet.

At en afgørelse har retsvirkning forudsætter, at afgørelsen berører den registreredes juridiske rettigheder. Dette kan både være generelle rettigheder, såsom retten til at stemme, eller det kan være noget, der påvirker den registreredes retlige status, hvor en automatisk afgørelse eksempelvis kan føre til, at en person får ret til eller afslag på en bestemt social ydelse.[339] Der kan også være tale om rettigheder i henhold til en kontrakt eller lignende.[340]

En automatisk afgørelse, herunder profilering, behøver ikke at have retsvirkning for den enkelte, men kan også på tilsvarende vis betydeligt påvirke den enkelte for at være indenfor anvendelsesområdet af artikel 22. Tærsklen for betydning af den automatiske afgørelse må derfor være den samme, som for en afgørelse, der påvirker den enkeltes juridiske rettigheder.[341] Hvis databehandlingen skal kunne anses for betydeligt at påvirke en person, skal afgørelsen potentielt kunne betydeligt påvirke den registreredes situation, adfærd eller valg, eller have langvarig eller permanent indvirkning på den pågældende eller medføre udelukkelse

[335] *Michael Veale og Lilian Edwards*: Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling (2018) side 401
[336] Ibid., side 401
[337] Forordning 2016/679, præambelbetragtning nr. 68
[338] Forordning 2016/679, artikel 22, stk. 1
[339] *Artikel 29-gruppen*: 17/DA WP251 (2018) side 22
[340] Ibid., side 22
[341] Ibid., side 22

eller forskelsbehandling af den registrerede i meget ekstreme tilfælde.[342] Det kan ikke præcist anføres, hvor meget der skal til for, at en afgørelse er tilstrækkelig *betydelig* til at opfylde tærsklen. Nogle afgørelser, der kan falde ind under artikel 22, kan for eksempel være afgørelser, der påvirker en persons økonomi, adgang til sundhedsydelser, adgang til uddannelse med videre. [343]

En anvendelse af automatiske individuelle afgørelser, som er meget anvendt i dag, er annonceringer på internettet, herunder målrettet annoncering baseret på profilering.[344] I langt de fleste tilfælde vil denne type automatiske afgørelser, herunder profilering, ikke betydeligt påvirke den registrerede, hvorfor denne type afgørelser ikke vil skulle overholde de ekstra krav i artikel 22, men blot de generelle principper og krav Databeskyttelsesforordningen opstiller. Der kan dog stadig forekomme tilfælde, hvor en sådan databehandling alligevel vil falde indenfor artikel 22's anvendelsesområde, alt afhængigt af sagens særlige karakter.[345] Der kan for eksempel være tale om en situation, hvor en person, der med sikkerhed er i finansielle vanskeligheder, og som regelmæssigt modtager målrettet annoncering vedrørende lån med høj rente. Hvis der er tale om en person af en vis sårbarhed, som sandsynligvis vil acceptere disse tilbud, kan der være tale om en profilering, som betydeligt påvirker den registrerede.[346] Det vil derfor komme an på den enkelte situation, og de konkrete omstændigheder, når det skal vurderes, hvorvidt der er tale om en automatisk afgørelse, herunder profilering, der betydeligt påvirker den registrerede. [347]

9.5 Undtagelser

Såfremt en persondatabehandling er omfattet af artikel 22, stk. 1, har den registrerede en ret til at modsige sig denne behandling. Det er dog ikke Databeskyttelsesforordningens formål at forbyde denne type behandling, hvorfor der fremgår tre undtagelser hertil af Databeskyttelsesforordningens artikel 22, stk. 2, litra a, b og c. Disse består af følgende:

> *"2. Stk. 1 finder ikke anvendelse, hvis afgørelsen:*
>
> *a) er nødvendig for indgåelse eller opfyldelse af en kontrakt mellem den registrerede og en dataansvarlig*

[342] *Artikel 29-gruppen*: 17/DA WP251 (2018) side 22-23
[343] Ibid., side 22-23
[344] Ibid., side 23
[345] Ibid., side 23
[346] Ibid., side 23
[347] Ibid., side 23

b) er hjemlet i EU-ret eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt, og som også fastsætter passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder samt legitime interesser eller

c) er baseret på den registreredes udtrykkelige samtykke."

I forhold til den første undtagelse, opfyldelse af kontrakt, kan denne forekomme, hvor den dataansvarlige mener, at en automatisk behandling er den mest hensigtsmæssige måde at nå målet på. Den dataansvarlige skal kunne godtgøre, at denne form for behandling er nødvendig, og at der ikke foreligger en anden metode, der er mindre indgribende for privatlivets fred.[348] Det fremkommer af undtagelsen, at behandlingen skal være nødvendig, hvilket ikke vil være tilfældet, såfremt der findes andre mere effektive og mindre indgribende måder, at nå frem til samme mål.[349]

Den anden undtagelse giver ikke anledning til tvivl. Dog er det et krav, at den relevante lovgivning fastsætter passende foranstaltninger til beskyttelse af den registreredes rettigheder, frihedsrettigheder og legitime interesser.[350]

Afslutningsvist kan der forekomme afgørelser, der alene er baseret på automatisk behandling, hvor den registrerede har givet sit udtrykkelige samtykke hertil. Formålet hermed er, at det enkelte individ bør have et højt niveau af kontrol over dennes personoplysninger, da en persondatabehandling efter artikel 22 kan indebære betydelige databeskyttelsesrisici.[351]
Databeskyttelsesforordningen opstiller dog en række krav til samtykke, herunder at det skal være specifikt, jf. Databeskyttelsesforordningens artikel 7. En problemstilling kan herefter opstå, når den registrerede, skal afgive samtykket på et specifikt og informeret grundlag, eftersom det tidligere er lagt til grund, at det kan være svært for en almindelig person, at forstå, hvordan en behandling ved anvendelse af AI sker. Denne problemstilling vil ikke blive uddybet yderligere i afhandlingen, eftersom samtykkereglerne er omfattende, men det skal blot påpeges, at der her kan opstå en problemstilling.

Såfremt en automatisk afgørelse er omfattet af artikel 22, stk. 2, litra a eller c, skal den dataansvarlige gennemføre passende foranstaltninger for beskyttelse af den registreredes rettigheder, jf. Databeskyttelsesforordningens artikel 22, stk. 3. En af disse foranstaltninger kan være muligheden for

[348] *Artikel 29-gruppen*: 17/DA WP251 (2018) side 24
[349] Ibid., side 24
[350] Ibid., side 25
[351] Ibid., side 25

menneskelig indgriben. Det vil derfor i praksis ofte være en væsentlig mulighed for den registrerede at anmode om en genoptagelse af sagen, hvor der foretages en fornyet behandling, hvori der foreligger menneskelig indgriben.[352] I praksis vil dette bevirke, at undtagelserne ikke har den store betydning. Såfremt den registrerede også her vil kunne anmode om menneskelig indgriben, vil samme problematik som efter stk. 1 opstå.

Såfremt en afgørelse efter artikel 22, stk. 2, omfatter behandlingen af følsomme personoplysninger, vil der være forbud herimod, jf. artikel 22, stk. 4. Her fremkommer der således et direkte forbud, og ikke blot en rettighed, som er tilfældet ved behandling af almindelige personoplysninger. Dette er grundet, at disse personoplysninger, i kraft af deres karakter, er særligt følsomme i forhold til den registreredes grundlæggende rettigheder og frihedsrettigheder.[353] Der er dog ikke tale om et absolut forbud, hvorfor der forekommer undtagelser hertil, i tilfælde hvor der gives udtrykkeligt samtykke, eller hvis behandlingen er nødvendig af hensyn til væsentlige samfundsinteresser.[354] Ved følsomme personoplysninger vil det således ikke være nok, at behandlingen er nødvendig for indgåelse af en kontrakt eller hjemlet i EU eller national ret.[355] Ud over at undtagelserne er skærpede ved følsomme oplysninger, er det her ligeledes et krav, at der fastsættes passende foranstaltninger, jf. Databeskyttelsesforordningens artikel 22, stk. 4.

9.6 Konsekvenser af at de registrerede påberåber sig artikel 22

Der er ovenstående redegjort for, at med den nuværende fortolkning af artikel 22, er der tale om en rettighed for den registrerede. Konsekvenserne af dette må betyde, at den dataansvarlige altid kan lave persondatabehandling ved brug af automatiske individuelle afgørelser, herunder profilering, som falder under artikel 22. Dette er dog med risiko for, at den registrerede påberåber sig rettigheden, hvorefter den dataansvarlige er nødsaget til at foretage menneskelig indgriben på afgørelsen.
Det må formodes at der kan opstå problemstillinger i tilfælde af, at den dataansvarlige behandler persondata ved anvendelse af et AI system, hvori der kan opstå den Sorte Boks. Dette kan særligt være tilfældet, hvis AI systemet er baseret på neuralt netværk. Opstår den Sorte Boks vil behandlingsprocessen være uigennemsigtig, hvorfor den dataansvarlige ikke nødvendigvis kan redegøre for, hvilke parametre AI systemet har lagt til grund for den givende afgørelse.

[352] *Kristian Korfits Nielsen og Anders Lotterup*: Databeskyttelsesforordningen og Databeskyttelsesloven (2020) side 581
[353] Forordning 2016/679, præambelbetragtning nr. 51
[354] Forordning 2016/679, artikel 9, stk. 2, litra a og g, jf. artikel 22, stk. 4.
[355] *Artikel 29-gruppen*: 17/DA WP251 (2018) side 25

Hvis ikke den dataansvarlige er bekendt med behandlingsprocessen i fase 2, kan den dataansvarlige blive udfordret i fase 3. Såfremt den registrerede gør brug af sin rettighed efter denne har fået afgørelsen i fase 3, er den dataansvarlige nødsaget til at gå tilbage i fase 2 for at gennemse behandlingsprocessen. Såfremt denne behandlingsproces er uigennemsigtig, kan den dataansvarlige ikke foretage et meningsfuldt menneskeligt indgreb og dermed ikke opfylde den registreredes rettighed i henhold til artikel 22. Dette kan resultere i, at den dataansvarlige er tvunget til at foretage en behandling på ny, som ikke bunder i en automatisk afgørelse.

Hermed kan det udledes, at den registrerede besidder en magt, og et følgende spørgsmål er derfor om en behandling, der falder under artikel 22's anvendelsesområde, kan blive for byrdefuld for den dataansvarlige. Dette vil i praksis afhænge af, hvorvidt den registrerede gør brug af sin magt, og om den dataansvarlige har mulighed for at lave et meningsfuldt menneskeligt indgreb, uden at foretage afgørelsen på ny.

9.7 Delkonklusion

Med artikel 22 er der i Databeskyttelsesforordningen indsat restriktioner overfor automatiske individuelle afgørelser, herunder profilering. Det er omdiskuteret, hvorvidt der er tale om et generelt forbud mod automatiske afgørelser, eller om bestemmelsen skal anses som en rettighed, som den registrerede kan påberåbe sig. Ud fra en ordlydsfortolkning må det dog lægges til grund, at der er tale om en rettighed, hvorfor bestemmelsen kun finder anvendelse når den registrerede gør brug heraf.

Bestemmelsen finder anvendelse på både automatiske afgørelser og profilering. For at en automatisk afgørelse er omfattet af artikel 22, skal den alene være baseret på automatisk behandling. Dette er tilfældet, når der ikke foreligger nogen menneskelig indgriben i beslutningsprocessen. Det menneskelige indgreb skal være meningsfuldt og foretages af en person med den fornødne kompetence. Denne tilsynsperson skal dermed have en vis forståelse både for det tekniske og juridiske grundlag, der ligger bag afgørelsen. Dette kan i visse tilfælde vise sig vanskeligt, eftersom nogle AI systemer er meget komplekse og uigennemsigtige. Det kan resultere i, at den dataansvarlige kan have problemer med at bevise et menneskeligt tilsyn i situationer, hvor dette rent faktisk er sket. Bestemmelsen stiller ikke samme krav til profilering, hvorfor en profilering, hvori der er et menneskeligt indgreb, godt kan være omfattet af artikel 22.

Både en automatisk afgørelse og profilering, skal have retsvirkning eller på betydeligt vis påvirke den registrerede, før de er omfattet af artikel 22. Der findes ingen grænse for, hvornår en afgørelse på betydeligt vis påvirker den registrerede, men vurderingen må være den samme, som når en afgørelse har retsvirkning.

Det vil sige, at afgørelsen skal påvirke den registrerede på en sådan måde, at det får betydelige konsekvenser for denne. Dette kan for eksempel være økonomiske konsekvenser, hvor et AI system benyttes til at vurdere, hvorvidt en person kan optage lån eller ej.

Af artikel 22, stk. 2 fremgår der undtagelser til den registreredes rettighed. Disse undtagelser vil dog formodes at have meget lille betydning i praksis, eftersom der ved anvendelsen heraf stadig skal gennemføres passende foranstaltninger, som for eksempel den registreredes mulighed for menneskelig indgriben. Undtagelserne vil afhænge af, hvorvidt der er tale om almindelige eller følsomme oplysninger.

Såfremt den registrerede gør brug af sin rettighed, vil den dataansvarlige være nødsaget til at lave et menneskeligt indgreb i afgørelsen. Dette kan fremkomme problematisk, hvor der opstår den Sorte Boks. Processerne i behandlingen kan her være uigennemsigtig, hvorfor den dataansvarlige kan være nødsaget til at foretage persondatabehandlingen på ny.

10. Den Sorte Boks kan være den største hindring for at anvende AI

Som det er lagt til grund i ovenstående, opstår de største problemstillinger, når der som en del af en teknisk behandling, opstår den Sorte Boks. Undersøgelser viser, at de største bekymringer ved anvendelse af AI er manglende tillid til den Sorte Boks.[356] Flere udviklere af AI har en manglende tillid til den Sorte Boks samt det resultat, der kommer ud af boksen, grundet den manglende gennemsigtighed i behandlingsprocessen.[357] Dette gælder særligt når AI systemet er bygget op på dybe neurale netværk, såkaldt Deep Learning. Formålet hermed er, at AI maskinen er i stand til at lære. Dette er blandt andet grundet adgangen til den enorme datamængde, tidligere omtalt som Big Data. Bagsiden af medaljen er, at det resulterer i lange avancerede algoritmer, og grundet disse, kan det være en udfordring for den dataansvarlige at finde tilbage og afgøre, hvorfor og hvordan en behandling er blevet udført.[358] Derfor skal det vurderes, hvilke konsekvenser dette kan medføre i henhold til overholdelse af de databeskyttelsesretlige regler.

Det er essentielt, at den dataansvarlige er bevidst om, at udfaldet fra den Sorte Boks kan påvirke den registrerede og ligeledes kan behandlingsprocessen have en stor betydning for den registreredes rettigheder. For at undgå problematikker har Databeskyttelsesforordningen fokus på gennemsigtigheden, for netop at kunne kontrollere en behandling samt dens betydning for den registreredes rettigheder og frihedsrettigheder. Dette fremgår af Databeskyttelsesforordningens artikel 5, stk. 1, litra a, og artikel 12-14.[359]

Hvis der sker persondatabehandling ved brug af neuralt netværk, kan det resultere i, at gennemsigtigheden bliver svækket, hvilket over tid kan medføre at reglerne om netop gennemsigtighed i Databeskyttelsesforordningen ikke er opfyldt. I et sådant scenarie er det ikke blot gennemsigtighedsprincippet, som ikke bliver opfyldt, men det kan også have betydning for reglerne ved automatiske individuelle afgørelser, herunder profilering i Databeskyttelsesforordningens artikel 22.

10.1 Faserne og den Sorte Boks

Det formodes, at den Sorte Boks, og herunder gennemsigtighed, har en betydning for alle tre faser, når den dataansvarlige udfører persondatabehandling ved anvendelse af AI. Den dataansvarlige skal allerede i fase 1 være i stand til at give den registrerede oplysninger om behandlingen, således oplysningspligten overholdes. Dog er dette kun en aktualitet, såfremt der anvendes personoplysninger i træningsprocessen, og

[356] *Mathias Klingenberg*: Den sorte boks er den største hindring for at bruge AI (2017), se afsnit: *Tillid til den sorte boks*
[357] Ibid., se afsnit: *Tillid til den sorte boks*
[358] Ibid., se afsnit: *Tillid til den sorte boks*
[359] *Christopher Kuner, et al:* The EU General Data Protecion Regulation (GDPR) A Commentary, (2020) side 416

behandlingen er inden for Databeskyttelsesforordningens anvendelsesområde. I tilfælde af at personoplysningerne er anonymiseret er det tidligere lagt til grund, at behandlingen ikke er underlagt de databeskyttelsesretlige regler. Dog bør den dataansvarlige være sikker på, at der ikke kan ske reidentifikation, hvormed personoplysninger kan blive henførbare som led i en behandling.

Som tidligere omtalt, fremgår det af de grundlæggende principper, at et AI system ikke må udvise bias. Såfremt der forekommer gennemsigtighed i behandlingsprocessen, må det antages, at den dataansvarlige er i stand til at opdage samt fjerne bias. Ved den Sorte Boks vil den dataansvarlige ikke være i stand til at se, hvilke parametre der lægges til grund for en afgørelse, hvorfor den dataansvarlige ikke vil kunne vurdere, hvorvidt der foreligger bias.

Herefter er selve behandlingen i fase 2 vigtig, da der her sker behandling af den registreredes personoplysninger, hvorfra der udledes et resultat, som kan have en stor betydning for den registrerede. For at den dataansvarlige kan overholde oplysningspligten i Databeskyttelsesforordningens artikel 12-14, skal oplysningerne om behandlingen gives forud for behandlingsprocessen. Såfremt der sker ændringer, som kan have væsentlig betydning for den registreredes mulighed for at påberåbe sine rettigheder, skal den dataansvarlige oplyse om eventuelle ændringer i behandlingsprocessen. Fremgår der en snæver gennemsigtighed, vil dette formentlig have en betydning for, hvordan den dataansvarlige fyldestgør sin oplysningspligt overfor den registrerede.

Ligeledes er fase 3 vigtig, da denne fase kan have særlig betydning i henhold til reglerne ved automatiske afgørelser, herunder profilering, fordi den registrerede kan gøre krav på, at der skal ske et meningsfuldt menneskeligt indgreb af en person med den fornødne kompetence, hvori resultatet samt behandlingsprocessen vurderes. Hvis ikke den dataansvarlige kan stå inde for behandlingen, herunder forklare baggrunden for en afgørelse, kan den datasvarlige ikke nødvendigvis fyldestgøre sin opgave og overholde databeskyttelsesreglerne ved at udføre et meningsfuldt menneskeligt indgreb. Dette vil sandsynligvis medføre, at den dataansvarlige skal tilbage i fase 2 og udføre en ny behandling, såfremt det antages, at den dataansvarlige ikke har nok gennemsigtighed til at vurdere behandlingsprocessen.

10.2 Den Sorte Boks' betydning for automatiske individuelle afgørelser

Der er ingen tvivl om, at den Sorte Boks kan påvirke reglerne i Databeskyttelsesforordningen, men hvorvidt der kan ske opfyldelse af Databeskyttelsesforordningen artikel 22, hvis der forekommer en snæver gennemsigtighed, er forsøgt undersøgt nedenstående.

Det kan blive problematisk for en dataansvarlig, hvis neurale netværk kommer til at få indflydelse i en behandlingsaktivitet, således det ikke er muligt at se hvilke faktorer, som ligger til grund for en beslutning. Det er heraf nærliggende at undersøge, hvor meget gennemsigtighed der skal til for at den dataansvarlige kan fyldestgøre Databeskyttelsesforordningens artikel 22, hvor der sker en automatisk persondatabehandling ved anvendelse af AI.

Når der træffes en automatisk individuel afgørelse som beskrevet i Databeskyttelsesforordningens artikel 22, stk. 1, skal den dataansvarlige være særligt opmærksom på dennes oplysningspligt, herunder gennemsigtighedsforpligtelserne i henhold til artikel 13, stk. 2, litra f og artikel 14, stk. 2, litra g.[360] Det klargøres i reglerne, at den dataansvarlige skal informere den registrerede om, at der udøves denne form for aktivitet. Ligeledes skal den dataansvarlige give meningsfulde oplysninger om logikken bag behandling og forklare betydningen af behandlingen samt konsekvenserne af behandlingen.[361] Tilvejebringelsen af førnævnte oplysninger, vil ligeledes hjælpe den dataansvarlige med at sikre overholdelse af de fornødne garantier i henhold til Databeskyttelsesforordningens artikel 22, stk. 3 og præambelbetragtning nr. 71.[362]

Artikel 29-gruppen ligger til grund, at grundet væksten og kompleksiteten inden for Machine Learning, kan det være vanskeligt at forklare den registrerede, hvordan en automatisk afgørelse eller profilering fungerer.[363] Derfor bør den dataansvarlige forklare baggrunden for en afgørelse eller de kriterier, der lægges til grund for afgørelsen på en enkel måde. Det er ikke et krav, at der skal foreligge en forklaring af de anvendte algoritmer, men i stedet skal der gives relevante oplysninger om logikken heri.[364] Det lægges dog til grund, at oplysningerne skal være tilstrækkeligt omfattende til, at den registrerede kan forstå årsagerne til afgørelsen.[365] Det afgørende for om databeskyttelsesmeddelelserne kan anses som værende tilstrækkelig, afhænger derfor af, om den registrerede kan forstå ræsonnementet bag afgørelsen.[366] Et eksempel herpå kan være, hvis der er tale om en kreditvurdering. Her bør den dataansvarlige oplyse den registrerede om, hvilke personoplysninger der behandles, hvad formålet med behandlingen er, og hvordan logikken bag det anvendte AI system leder til en afgørelse. Ligeledes giver den dataansvarlige den registrerede kontaktoplysninger i tilfælde af, at den registrerede vil gøre brug af sin rettighed til at kræve et menneskeligt indgreb i behandlingen ifølge Databeskyttelsesforordningens artikel 22, stk. 1.

[360] *Artikel 29-gruppen*: 17/DA WP251 (2018) side 26
[361] Ibid., side 26
[362] Ibid., side 26
[363] Ibid., side 26
[364] Ibid., side 26
[365] Ibid., side 26
[366] Ibid., side 26

Herudfra må det lægges til grund, at der forekommer en rettighed for den registrerede, da denne har krav på at blive oplyst om behandlingen inden denne finder sted, men den registrerede har ikke en decideret ret til en forklaring af, hvordan resultatet er blevet, som det er. I stedet kan den registrerede blot gøre krav på at få menneskelig indgriben. Som tidligere statueret, skal dette indgreb være meningsfuldt, hvorfor det skal udføres af en person med den fornødne kompetence, og som har mulighed for at ændre afgørelsen, såfremt det bliver nødvendigt.

Derfor er det vigtigt, at gennemsigtigheden skal forekomme inden behandlingen finder sted, således den registrerede kan blive tilstrækkeligt oplyst om den givende behandling. Såfremt den registrerede gør brug af sin ret til at kræve, at den automatiske afgørelse pålægges menneskelig indgriben, bliver gennemsigtigheden afgørende for den dataansvarlige. I tilfælde af at den dataansvarlige ikke er i stand til at gennemskue behandlingsprocessen samt hvilke parametre, som ligger til grund for afgørelsen grundet den Sorte Boks, er den dataansvarlige nødsaget til at foretage en afgørelse på ny.

Derfor anses det for muligt for den dataansvarlige, at denne ved opfyldelse af oplysningspligten kan overholde gennemsigtighedsprincippet. Hvorvidt der forekommer nok gennemsigtighed senere i processen, som gør det muligt for den dataansvarlige at kunne bevare overblikket over en given behandling, er dog stadig uklart og må afhænge af den enkelte situation. Det må formodes at være en byrde for den dataansvarlige, såfremt denne er tvunget til at foretage en ny behandling. Den registrerede er i besiddelse af en magt overfor den dataansvarlige, og hvor store konsekvenserne er i tilfælde af, at denne magt bliver udnyttet, er uvisse. Det er tidligere statueret, at Databeskyttelsesforordningens formål er at beskytte den registrerede. Men samtidig er det ikke meningen, at Databeskyttelsesforordningen skal forbyde eller gøre det for kompliceret for den dataansvarlige at anvende avancerede teknologier, herunder AI.

10.3 Delkonklusion

Den Sorte Boks skaber betydelige problematikker for gennemsigtigheden, hvorfor dette kan resultere i at reglerne inden for Databeskyttelsesforordningen ikke kan opfyldes tilstrækkeligt. Det kan skabe problemer med overholdelse af oplysningspligten, såfremt den dataansvarlige ikke kan give tilstrækkelige oplysninger til den registrerede vedrørende dennes behandlingsrisici. I tilfælde af at den registrerede påberåber sig rettigheden i Databeskyttelsesforordningens artikel 22, skal den dataansvarlige foretage et meningsfuldt menneskeligt indgreb. Dette anses at blive problematisk, såfremt behandlingsprocessen ikke er gennemsigtig og i værste tilfælde vil den dataansvarlige kunne risikere at skulle foretage behandlingen på ny.

11. Eftertidens aspekter

AI er kompliceret og en vurdering af hvorvidt persondatabehandlingen overholder reglerne vil afhænge af den givne situation, herunder formålet med behandlingen. Grundet den manglende retspraksis på området samt den konstante udvikling, vil det formentlig være nødvendigt at disse problematikker løses i praksis.

Peter Blume udtrykker, *"det kan kritisk iagttages, at forordningen er for tro imod den retlige fortid og er for traditionel i forhold til den virkelighed, som digitaliseringen har skabt og skaber hver ny dag."*[367] Særligt kan det diskuteres om Databeskyttelsesforordningen vil kunne følge samfundets samt teknologiens udvikling. Hertil udtrykker Peter Blume at reguleringsparadigmet burde have være efterset med nye og friske øjne hvorfor der skulle være udarbejdet *"en kurs, der mere sandsynligt på en samfundsmæssigt fremtidsorienteret måde ville have ført frem til en realisering af de mål, som persondataretten forfølger."*[368] Det står derfor klart for ham at mange fænomener vil udfordre den databeskyttelsesretlige regulering, herunder udnyttelsen af Big Data og udviklingen samt anvendelsen af AI.[369]

For Europa-Kommissionen er der ingen tvivl om, at AI er vejen frem, og der skal findes en vej, hvor både AI og databeskyttelse kan samarbejde. Ursula von der Leyen, som er Præsident for Europa-Kommissionen, udtrykker i sine seneste tanker og planer for fremtiden, at der skal arbejdes mod "*A Europe that is fit for the digital age*"[370]. Hun udtaler, at de i Europa-Kommissionen vil arbejde på lovregler, hvor både AI og menneskers rettigheder kan forenes, da dette er fremtiden, og at teknologien skal være med til at styrke samfundet og erhvervslivet.[371] I hendes guidelines udtaler hun; "*Data and AI are the ingredients from innovation that can help us find solutions to societal challenges, from health to farming, from security to manufacturing."*[372] Dette understøtter blot, at fordi AI fremadrettet vil spille en større del af udviklingen, skal der findes en vej, hvor gældende regler kan bruges og håndhæves i samarbejde med teknologien inden for AI. Dette er ikke ensbetydende med at arbejdet frem til et resultat vil blive nemt, men netop som udviklingen skrider frem vil det være en nødvendighed for at kunne bibeholde et konkurrerende marked både i EU men også i forhold til resten af verden.[373]

[367] *Peter Blume*: Den nye Persondataret (2018) side 260
[368] Ibid., side 260
[369] Ibid., side 261
[370] *Ursula von der Leyen*: A Union that strives for more, my agenda for Europe (u.å.) side 13
[371] Ibid., side 13
[372] Ibid., side 13
[373] Ibid., side 4

12. Konklusion

Den teknologiske udvikling medfører, at der i dag er langt flere muligheder for behandling af personoplysninger, herunder ved anvendelse af AI. Såfremt en AI opbygges som Deep Learning, herunder neuralt netværk der samtidig anvender Big Data, kan der opstå mange potentielle fordele. Samtidig kan dette dog også resultere i betydelige potentielle risici. Eftersom individets rettigheder og frihedsrettigheder er i centrum, opstiller Databeskyttelsesforordningen krav til den dataansvarlige, når denne behandler personoplysninger. I Databeskyttelsesforordningen fremgår nogle grundlæggende principper, hvoraf rimelighed og gennemsigtighed samt rigtighedsprincippet er særlig relevant ved brugen af AI.

Ved overholdelse af rimelighedsprincippet skal den dataansvarlige sikre, at AI systemet ikke udviser bias, hvorfor sortering samt kvalitetssikring af data bør udføres inden behandlingsprocessen. For overholdelse af rigtighedsprincippet er det ligeledes afgørende, at der behandles korrekte data, da ukorrekte personoplysninger kan føre til ukorrekte resultater. AI systemet kan ikke skelne mellem rigtige og forkerte data. Den dataansvarlige er underlagt et ansvarlighedsprincip, hvorfor den dataansvarlige blandt andet skal kontrollere samt sikre at de grundlæggende principper overholdes.
Udover at den dataansvarlige skal overholde de grundlæggende principper, fremgår der yderligere forpligtelser af Databeskyttelsesforordningen. Ved databeskyttelses gennem design er det centralt at den dataansvarlige tænker databeskyttelse ind i hele processen – fra start til slut. Når der designes AI systemer skal der implementeres passende foranstaltninger og fornødne garantier, som er egnet til at beskyttet den registreredes personoplysninger. Ved anvendelse af AI kan det statueres, at den dataansvarlige altid bør udarbejde en konsekvensanalyse. Begrundelsen herfor er, at den dataansvarlige skal kunne beskrive eventuelle risici ved persondatabehandlingen.

Den dataansvarlige er ifølge af Databeskyttelsesforordningen underlagt en oplysningspligt, hvilket omfatter at den registrerede skal oplyses omkring formålet med en behandling, hvilke oplysninger der behandles med videre. Når en persondatabehandling sker ved anvendelse af AI, skal den registrerede ligeledes oplyses herom. Dette indebærer, at den registrerede skal gøres bekendt med risici ved behandlingsprocessen. Dog kan den registrerede ikke gøre krav på at få en kompliceret forklaring af de anvendte algoritmer. Oplysninger skal blot være tilstrækkeligt omfattende til, at den registrerede kan forstå årsagerne, som lægges til grund for afgørelsen.

Såfremt den dataansvarlige kan overholde de grundlæggende principper, samt de øvrige forpligtelser som Databeskyttelsesforordningen opstiller, vil det være muligt for den dataansvarlige at behandle

personoplysninger ved anvendelse af AI. Dog skal den dataansvarlige være opmærksom på, at en sådan behandling vil falde ind under Databeskyttelsesforordningens artikel 22. Artikel 22 skal fortolkes som en rettighed, hvorfor den registrerede skal gøre denne gældende, før bestemmelsen finder anvendelse. En afgørelse er omfattet af artikel 22, når den automatiske behandling er foretaget uden menneskeligt indgreb, eller hvor der foreligger profilering, og hvis denne har retsvirkning eller på betydeligvis påvirker den registrerede. Såfremt den registrerede gør brug af rettigheden i artikel 22, vil den dataansvarlige være nødsaget til at foretage et meningsfuldt menneskeligt indgreb på afgørelsen. For at indgrebet er meningsfuldt, skal det foretages af en tilsynsperson med den fornødne kompetence, som har mulighed for at ændre afgørelsen.

På baggrund af ovenstående, skal den dataansvarlige således sikre sig, at såfremt der behandles personoplysninger ved anvendelsen af AI, skal det være muligt at foretage et meningsfuldt indgreb efterfølgende. Dette kan forekomme problematisk, såfremt der i AI systemet forekommer den Sorte Boks. Her vil der foreligge en manglende gennemsigtighed i behandlingsprocessen, hvorfor den dataansvarlige ikke nødvendigvis kan redegøre for, hvordan AI systemet er kommet frem til den konkrete afgørelse, herunder hvilke parametre der er lagt til grund. I dette tilfælde, vil der ikke kunne foretages et meningsfuldt menneskeligt indgreb, hvorfor den dataansvarlige vil være nødsaget til at foretage behandlingen på ny. Artikel 22 vil derfor være en væsentlig faktor, når den dataansvarlige skal vurdere, hvorvidt den vil anvende AI til at behandle personoplysninger, og herunder om det kan betale sig. Fremtiden er uvis, og det er omdiskuteret hvorvidt Databeskyttelsesforordningen tilgodeser den teknologiske udvikling, på trods af at den er udformet teknologineutralt. Der er ingen tvivl om, at det er muligt at behandle personoplysninger ved anvendelse af AI, men spørgsmålet er, om det kan blive for byrdefuldt for den dataansvarlige.

13. Generelle dataetiske overvejelser

I debatten om databeskyttelse, herunder hvordan denne bedst opnås, er dataetik rykket op på dagsordenen.[374] Personens beskyttelsesinteressen er i centrum indenfor persondataretten, hvorfor der kan argumenteres for, at dataetiske overvejelser udvider denne beskyttelse.[375] Etikken understøtter personen og kan potentielt give personen en mere fremtrædende placering.[376] De dataetiske regler kan gå videre i beskyttelsen af personoplysninger end, hvad lovreglerne tilsiger, mens der samtidig er et ønske om at bruge ny teknologi, herunder Big Data analyser og AI.[377]

Det er i ovenstående konklusion lagt til grund, at den dataansvarlige kan foretage databeskyttelsesretlig behandling ved anvendelse af AI. Her kan der dog opstå et spørgsmål omkring, hvorvidt denne behandling er etisk korrekt, og om etiske overvejelser kan medvirke til, at den dataansvarlige alligevel ikke bør anvende AI.

At anvende etikken på lige fod med de databeskyttelsesretlige regler kan forekomme problematisk. Det kan diskuteres, hvorfra det dataetiske grundlag stammer, samt hvem der bestemmer, hvad der er etisk korrekt. Databeskyttelsesforordningen og andre databeskyttelsesretlige regler er vedtaget på et demokratisk grundlag, idet de er gennemført i en politisk proces.[378] Modsatrettede hensyn er blevet vurderet, og reglerne har en politisk legitimitet udledt af samfundsmæssigt anerkendte institutioner.[379] Det samme gør sig ikke gældende for dataetikken, idet ophavet heraf ofte er usikkert. I princippet kan de dataetiske regler stamme alle steder fra, idet der ikke er regler for, hvem der kan tilkendegive disse principper. Der forekommer heller ikke en konkret fremgangsmåde, for hvordan dataetiske principper skal udformes, og det er heller ikke klart, hvorfor de skal overholdes.[380] Ved anvendelsen af dataetikken, skal der således være opmærksomhed på dennes ophav, men det betyder ikke, at de dataetiske principper er uden betydning.

Dataetikken kan fremgøre et helt nyt lag af beskyttelse til databeskyttelsesretten, men behøver ikke nødvendigvis være i opposition til aktuel praksis, idet den kan understøtte de gode facetter, der allerede i dag fremgår af Databeskyttelsesforordningen.[381] Der kan argumenteres for, at med Databeskyttelsesforordningens udformning, fremgår der allerede nogle grundlæggende etiske overvejelser.

[374] *Peter Blume*: Personen i Persondataretten (2019) side 169
[375] Ibid., side 169
[376] Ibid., side 169
[377] *Henning Mortensen, et al.:* Kan dataetik siges at følge de persondataretlige regler? side 1
[378] *Peter Blume*: Personen i Persondataretten (2019) side 170
[379] Ibid., side 170
[380] Ibid., side 170
[381] Ibid., side 170

En del af de databeskyttelsesretlige regler har en etisk dimension, mens andre regler er tekniske, hvorfor de hverken fremkommer etiske eller uetiske.[382] Eftersom alle reglerne skal ses og forstås i sammenhæng med øvrige regler, kan der dog argumenteres for, at der alligevel forekommer en etisk dimension i Databeskyttelsesforordningen som helhed.

13.1 Etik i Databeskyttelsesforordningen

Et af de grundlæggende principper i Databeskyttelsesforordningens artikel 5, stk. 1, litra a, er rimelighed. Hvad der specifikt skal forstås med ordet rimelighed og betydningen heraf uddybes ikke i Databeskyttelsesforordningen eller dens præambelbetragtninger, men det er tidligere i afhandlingen lagt til grund, at rimelighedsprincippet kræver, at al behandling af persondata skal udføres med respekt for den registreredes interesser, og at der ved en persondatabehandling ikke må udvises bias.

Af den engelske udgave af Databeskyttelsesforordningen fremgår rimelighed som *fair.* Oxford Dictionary definerer fair som *"Treating people equally without favouritism or discrimination"*[383]. I den danske ordbog defineres rimelighed som *"passende og fornuftig under de givne omstændigheder; som er på sin plads"*[384]. Ud fra de forskellige sproglige versioner, kan der argumenteres for, at den dataansvarlige skal gøre det *rigtige* med persondata, for at sikre, at den konkrete behandling af data er rimelig i henhold til den registrerede og dennes rettigheder og frihedsrettigheder. Der kan således argumenteres for, at det er nødvendigt at foretage en etisk vurdering, for at kunne opnå rimelighed på trods af, at Databeskyttelsesforordningen ikke bruger ordet etik. [385]

I Databeskyttelsesforordningen kobles rimelighed ofte sammen med gennemsigtighed, og efter Peter Blumes vurdering, er disse *"udtryk for et bredt handleprincip, som i en vis forstand henviser til noget udenfor retten*"[386]. Dette udledes ofte på en måde, hvor den dataansvarlige skal handle i overensstemmelse med Databeskyttelsesforordningens *ånd*.[387] Dette kan være en identifikation om, at en persondatabehandling skal være etisk forsvarlig.[388] Som anført tidligere i afhandlingen er Databeskyttelsesforordningen forsøgt udformet teknologineutralt, hvilket også kan begrunde, at der ikke fremkommer en klar og tydelig definition af, hvad der skal forstås med rimelighed. Teknologien og anvendelsen heraf vil udvikle sig over tid, hvorfor det må formodes, at de dataetiske principper også vil udvikle sig. På denne baggrund vil

[382] *Peter Blume*: Personen i Persondataretten (2019) side 182
[383] https://www.lexico.com/definition/fair
[384] https://ordnet.dk/ddo/ordbog?query=rimelig
[385] *Henning Mortensen, et al.:* Kan dataetik siges at følge de persondataretlige regler? side 1
[386] *Peter Blume*: Personen i Persondataretten (2019) side 182
[387] Ibid., side 182
[388] Ibid., side 182

rimelighedsprincippet ligeledes udvikle sig, og hvad der er rimeligt i dag, er ikke nødvendigvis rimeligt i morgen.[389] Dataetikken kan derfor være med til at udfolde begrebet rimelighed over tid.[390]

Selvom den dataansvarlig har mulighed for at foretage persondatabehandling ved anvendelse af AI, bliver spørgsmålet herefter om den alligevel burde lade være på baggrund af etiske overvejelser. Databeskyttelsesretten lægger op til, at der altid skal foretages en vurdering af rimelighed, hvorfor der skal vurderes, om en behandling er etisk ansvarlig. Databeskyttelsesforordningen stiller dog ikke krav til denne vurdering, hvorfor det må være op til den dataansvarlige, hvilken vurdering der skal tages. Der er udarbejdet flere dataetiske tjeklister, herunder en guideline fra EU vedrørende etik i AI[391]. Denne er som udgangspunkt ikke obligatorisk for den dataansvarlige at anvende, men kan bidrage med nogle overvejelser. Blandt andet indeholder denne Guideline princippet *fair*, hvoraf det fremgår, at der ikke må forekomme bias, stigmatisering og diskrimination.[392] Det fremhæves, at dataansvarlige, som anvender AI, skal *"respect the principle of proportionality between means and ends, and consider carefully how to balance competing interests and objectives*"[393]. Disse synspunkter stemmer overens med, hvordan rimelighedsprincippet skal forstås, og det må derfor konkluderes at, ved at foretage en vurdering af rimelighedsprincippet, foretages der samtidig en vurdering af etikken.

En anden etisk overvejelse er, hvorvidt den registrerede burde have en ret til udvidet gennemsigtighed. Det er i afhandlingen lagt til grund, at den registrerede har ret til gennemsigtighed i behandlingen af dennes personoplysninger, jf. Databeskyttelsesforordningens artikel 5, ved at oplysningspligten i artikel 13 og 14 overholdes. Spørgsmålet er herefter, om der bør gives en udvidet ret til gennemsigtighed indenfor teknologiens virkemåde således, at et resultat af en behandling forklares og begrundes med henblik på, hvordan et AI system er kommet frem til det givende resultat.[394] Dette er for at opnå menneskelig kontrol med behandlingerne, herunder en vurdering af behandlingernes konsekvenser.[395] Det kan imidlertid forekomme problematisk, såfremt en behandlingsproces er uigennemsigtig, hvor en etisk overvejelse kan være, at når teknologien ikke kan forklares tilstrækkeligt, bør den ikke anvendes til persondatabehandling.

[389] *Henning Mortensen, et al.:* Kan dataetik siges at følge de persondataretlige regler? side 5
[390] Ibid., side 4
[391] *Europa-Kommissionen:* Etichs Guidelines for Trustworthy AI (2019)
[392] Ibid., side 12-13
[393] Ibid., side 12-13
[394] *Henning Mortensen, et al.:* Kan dataetik siges at følge de persondataretlige regler? side 6
[395] Ibid., side 6

13.2 Etik som en yderligere beskyttelse

På baggrund af, at en dataetisk overvejelse er en del af rimelighedsprincippet, har tilsynsmyndighederne selv mulighed for at benytte rimelighed til at fastsætte etiske rammer for behandling af personoplysninger, og der kan argumenteres for, at dataetikken allerede er en del af databeskyttelsesretten. [396] Datatilsynet har endnu ikke i Danmark offentliggjort retningslinjer for, hvordan behandlingen ved anvendelse af AI skal foretages, hvorfor de heller ikke har fastsat etiske rammer herfor. Som redegjort ovenfor er dataetikken ikke underlagt en demokratisk politisk beslutningsproces, og først når dataetikken optages i praksis eller lovgivning, vil den derfor være retligt bindende.[397] Så selvom der kan argumenteres for, at der med rimelighedsprincippet allerede er inkluderet etiske overvejelser, er det uvist, hvor vidt disse vil gå, og dette må afklares i praksis. Dataetiske principper kan kun blive retligt bindende, hvis de bliver en konkret del af Datatilsynets praksis i forhold til udfyldning af det grundlæggende princip om rimelighed.[398] Ligeledes er en ret til udvidet gennemsigtighed ikke retligt bindende, så længe dette ikke fremkommer af Datatilsynets praksis. Dataetiske principper kan ikke siges at udvide datebeskyttelsesretten, idet lovgivningen allerede tager højde herfor, men såfremt principperne går videre end praksis, kan de øge persondatabeskyttelsen.[399]

Hvorvidt en persondatabehandling ved anvendelse af AI burde anses for uetisk, vil komme an på den konkrete behandling, herunder hvor indgribende den er for den registrerede. Eksempler på situationer hvor de dataetiske overvejelser kan være nyttige, er i tilfælde, hvor behandlingen går videre end, hvad den registrerede retligt kan forvente. *Version2* har skrevet en historie om, at Gladsaxe kommune vil *"udvikle et dataanalytisk værktøj, der skal opspore familier med udsatte børn*".[400] Kommunen vil anvende en Machine Learning model til at sammenholde forskellige data, indsamlet til forskellige formål, og på den baggrund udpege potentielt udsatte børn, som kommunen ikke allerede er bekendt med.[401] Ud fra en etiske betragtning, kan det diskuteres, hvorvidt dette er rimeligt. Der vil blive indsamlet og sammenholdt informationer om alle kommunens børn, også selvom de ikke er udsatte. På trods af at formålet med behandlingen er at hjælpe børnene, må behandlingsprocessen formentlig være for indgribende, og dermed ikke rimelig set ud fra en etisk betragtning.

[396] *Henning Mortensen, et al.:* Kan dataetik siges at følge de persondataretlige regler? side 4
[397] Ibid., side 4
[398] Ibid., side 6
[399] Ibid., side 6
[400] *Tania Andersen*: Juridiske eksperter: Gladsaxes algoritme overtræder persondata-lov (2019)
[401] Ibid.

Internetmediet *The Intercept* har ligeledes skrevet en historie, om et nyt europæisk forskningsprojekt, Roborder.[402] Formålet med projektet er at lave teknologiske løsninger, som med hjælp fra droner, AI og andre teknologier skal beskytte EU's grænser mod illegale indvandrere.[403]

Tanken er, at grænserne skal overvåges med en række teknologier, som kan finde mennesker i grænseområder. Herefter tjekkes deres mobilsignaler for at finde menneskets eksakte geografiske placering for herefter at sende en alarm til grænsevagterne.[404] For at finde frem til illegale indvandrere, er det således en nødvendighed, at systemet undersøger alle, der befinder sig nær EU's grænser, og ikke blot dem som udgør en trussel. Vil dette være etisk korrekt? Projektet har som udgangspunkt ikke et militært formål, men på baggrund af den allerede avancerede teknologi, er der ingen tvivl om, at der hurtigt kan kobles biometrisk genkendelse og eventuelt våben på enhederne.[405] Herfra kan enheden sende oplysninger til en grænsevagt, som så skal vurdere, hvorvidt mennesket udgør en trussel eller ej. Alternativt kan projektet hurtigt ændres fra passivt moniterende til offensivt besluttende, således det er systemet, der via AI skal beslutte, hvorvidt en person udgør en trussel eller ej.[406] Dette vil formentlig ikke være etisk korrekt, eftersom en AI i dette tilfælde vil fungere som lovgivningsmagt. *"There is a thin line between using robots to monitor a border and using them to enforce one. Weaponizing a drone is relatively easy"*[407]. På denne baggrund, kan der argumenteres for, at på trods af, at forskningsprojektet blot et tænkt som en monitering af grænseovergangene, vil det stadig kunne anses som etisk ukorrekt, grundet de potentielle risici sådanne teknologier kan medføre.

Dataetikken kan således tilbyde principper og retningspile for, hvornår et AI system bør anvendes til persondatabehandling. Meget tyder på, at dataetikken vil kunne samvirke med databeskyttelsesretten i bestræbelsen på at realisere en god databeskyttelse, hvor personen er i centrum.[408] Allerede i dag fremgår der etiske overvejelser af Databeskyttelsesforordningens rimelighedsprincip, men der kan forekomme tilfælde, hvor en etisk vurdering bør gå videre, end hvad der er retligt bindende. Den dataansvarlige bør derfor vurdere den konkrete behandlingssituation for at vurdere, om der forekommer proportionalitet mellem anvendelsen af et AI system og formålet med behandlingen, for herefter at vurdere hvorvidt behandlingen er etisk korrekt.

[402] *Zach Campbell:* Swarms of drones, piloted by artificial intelligence, may soon patrol Europe's borders (2019)
[403] Ibid.
[404] Ibid.
[405] *Henning Mortensen, et al.:* Kan dataetik siges at følge de persondataretlige regler? side 5
[406] Ibid. side 5
[407] *Zach Campbell:* Swarms of drones, piloted by artificial intelligence, may soon patrol Europe's borders (2019)
[408] *Peter Blume*: Personen i Persondataretten (2019) side 190

14. Litteraturliste

14.1 Love

Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (Persondatadirektivet)

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) (Databeskyttelsesforordningen)

Lov om behandling af personoplysninger, Lov nr. 429 af 31/05/2000 (Persondataloven)

Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, Lov nr. 502 af 23/05/2018 (Databeskyttelsesloven)

Traktat om den Europæiske Unions Funktionsmåde

14.2 Vejledninger

Artikel 29-gruppen: 17/DA WP 248 rev. 01 (Retningslinjer for konsekvensanalyse vedrørende databeskyttelse og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679) (2017)
https://www.datatilsynet.dk/media/6839/konsekvensanalyser-vedroerende-databeskyttelse-dpia-wp248.pdf
Link testet den: 14/05/2020

Artikel 29-gruppen: 17/DA WP 251 rev. 01 (Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til Forordning 2016/679) (2018)
https://www.datatilsynet.dk/media/6914/wp251rev01_da-profilering.pdf
Link testet den: 14/05/2020

Artikel 29-gruppen: 17/DA WP 260 rev. 01 (Retningslinjer om Gennemsigtighed i henhold til Forordning 2016/679) (2018)
https://www.datatilsynet.dk/media/6925/wp260rev01_da.pdf
Link testet den: 14/05/2020

Databeskyttelsesrådet: Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, (2019)
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf
Link testet den: 14/05/2020

Datatilsynet: Konsekvensanalyse (2018)
https://www.datatilsynet.dk/media/6563/konsekvensanalyse.pdf
Link testet den: 14/05/2020

Det Norske Datatilsyn: Artificial intelligence and privacy, (2018)
https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf
Link testet den: 14/05/2020

Europa-Kommissionen: COM(2019) 250 final (Vejledning vedrørende forordningen om en ramme for fri udveksling af andre data end oplysninger i Den Europæiske Union) (2019)
https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX%3A52019DC0250&from=EN
Link testet den: 14/05/2020

Europa-Kommissionen: Ethics Guidelines for Trustworthy AI (2019)
https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (Engelsk udgave)
Link testet den: 14/05/2020

14.3 Betænkninger

Justitsministeriets betænkning om Databeskyttelsesforordningen (2016/679), Del 1, Bind 1. Betænknings nr. 1565

14.4 Bøger

Carsten Munk Hansen: Retsvidenskabsteori, 2. udgave, Djøf Forlag (2018)

Christopher Kuner, et al: The EU General Data Protecion Regulation (GDPR) A Commentary, Oxford University Press (2020)

Kristian Korfits Nielsen og Anders Lotterup: Databeskyttelsesforordningen og Databeskyttelsesloven, Jurist- og Økonomforbundets Forlag (2020)

Peter Blume: Databeskyttelsesret, 5. udgave, Jurist- og økonomforbundets forlag (2018)

Peter Blume: Den nye Persondataret, 2. udgave, Jurist- og Økonomforbundets Forlag (2018)

Peter Blume: Personen i Persondataretten, Djøf Forlag (2019)

14.5 Tidsskrift

Henning Mortensen et.al.: Kan dataetik siges at følge de persondataretlige regler? (2019) RR.9.2019.48 (Pdf hentet via Karnov, 14/05/2020)

14.6 Artikler og rapporter

Andrew Burt: The Ai Transparency Paradox, (2019)
https://hbr.org/2019/12/the-ai-transparency-paradox
Link testet den: 14/05/2020

Centre for Information Policy Leadership: Artificial Intelligence and Data Protection in Tension (2018)
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf
Link testet den: 14/05/2020

Craig S. Smith: Dealing with Bias in Artificial Intelligence, (2020)
https://www.nytimes.com/2019/11/19/technology/artificial-intelligence-bias.html
Link testet den: 14/05/2020

Deloitte NL: Transparancy and Responsibility In Artificial Intelligence (2019)
https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/innovatie/deloitte-nl-innovation-bringing-transparency-and-ethics-into-ai.pdf
Link testet den: 14/05/2020

Jake Silberg og James Manyika: Tackling bias in artificial intelligence (and in humans) (2019)
https://www.mckinsey.com/featured-insights/artificial-intelligence/tackling-bias-in-artificial-intelligence-and-in-humans
Link testet den: 14/05/2020

Júlio Regeto og Thiago Luis Sombra: Artificial intelligence, data protection and the future of inventions (2018)
https://iapp.org/news/a/artificial-intelligence-data-protection-and-the-future-of-inventions/
Link testet den: 14/05/2020

Luís Cruz-Filipe: AI: Sådan laver forskere computere, der kan tænke (2020)
https://videnskab.dk/teknologi-innovation/ai-saadan-laver-forskerne-computere-der-kan-taenke
Link testet den: 14/05/2020

Marethe Eckhardt: Domstolsstyrelsen: Kunstig intelligens afslører fordomme mod køn og hudfarve (2019)
https://www.altinget.dk/artikel/domstolsstyrelsen-kunstig-intelligens-afsloerer-fordomme-mod-koen-og-hudfarve
Link testet den: 14/05/2020

Mathias Klingenberg: Den sorte boks er den største hindring for at bruge AI (2017)
https://ing.dk/artikel/sorte-boks-stoerste-hindring-at-bruge-ai-209212
Link testet den: 14/05/2020

Michael Veale og Lilian Edwards: Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling (2018).
https://www.sciencedirect.com/science/article/pii/S026736491730376X/pdfft?md5=2ad151483ed9ba05fce602e3e889fe65&pid=1-s2.0-S026736491730376X-main.pdf
Link testet den: 14/05/2020

Pranav Rajpurkar, et al.: Cardiologist-Level Arrhythmia Detection with Convolutional Neural Networks (2017)
https://arxiv.org/pdf/1707.01836.pdf?fbclid=IwAR2M-9AVrUMVWhyUErFSG8GVWhocRlVEfNVKBGfh4WcEGN3JIBYG3KJpMM4
Link testet den: 14/05/2020

Privacy International: Data is Power: Profiling and Automated Decision-Making in GDPR (2017)
https://privacyinternational.org/sites/default/files/2018-04/Data%20Is%20Power-Profiling%20and%20Automated%20Decision-Making%20in%20GDPR.pdf
Link testet den: 14/05/2020

Tania Andersen: Juridiske eksperter: Gladsaxes algoritme overtræder persondata-lov (2019)
https://www.version2.dk/artikel/juridiske-eksperter-gladsaxes-algoritme-overtraeder-persondata-lov-1087407?fbclid=IwAR3iLMK9UD-soAuiWFFarVdC-SJHtmaNzXqdb0704C9NggWjedG5l4DD52k
Link testet den: 14/05/2020

Thomas Bolander: Hvad er Kunstig Intelligens egentlig? (2018)
https://videnskab.dk/teknologi-innovation/hvad-er-kunstig-intelligens-egentlig
Link testet den: 14/05/2020

Thomas Bolander: Kunstig intelligens: Bliver mennesker overflødige? (2017)
https://videnskab.dk/teknologi-innovation/kunstig-intelligens-bliver-mennesker-overfloedige
Link testet den: 14/05/2020

Ursula von der Leyen: A Union that strives for more, My agenda for Europe (u.å.)
https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf
Link testet den: 14/05/2020

Victor Thornton: Hvad er forskellen på AI, Machine – og Deep Learning? (2018)
https://markedsforing.dk/artikler/klumme/hvad-er-forskellen-p-ai-machine-og-deep-learning
Link testet den: 14/05/2020

Zach Campbell: Swarms of drones, piloted by artificial intelligence, may soon patrol Europe's borders (2019) https://theintercept.com/2019/05/11/drones-artificial-intelligence-europe-roborder/?fbclid=IwAR1At2GASn9rHinOsjU2CaoCMbXWPHDW4rZ7YZVD1ubfLSgsFHVtVzawDHA

Link testet den: 14/05/2020

14.7 Hjemmesider

http://denstoredanske.dk/It,_teknik_og_naturvidenskab/Informatik/Software,_programmering,_internet_og_webkommunikation/algoritme?fbclid=IwAR3MxdLkgi4Zi1X2RQq_BzWYz54CVIKntR6bPNaNmJYqiwibkLOm9Vcu0hM

Link testet den: 14/05/2020

https://dictionary.cambridge.org/dictionary/english/transparency

Link testet den: 14/05/2020

https://erhvervsstyrelsen.dk/ny-vejledning-saetter-fokus-paa-sikkerheden-ved-brug-af-kunstig-intelligens-i-praksis?fbclid=IwAR3WRqVQeIfeVqkuU_NGQ0cTyTwkrm6hDqH7vy2vAjGMAv1LDaZBmHWN4jM

Link testet den: 14/05/2020

https://ida.dk/viden-og-netvaerk/temaer/kunstig-intelligens

Link testet den: 14/05/2020

https://iihnordic.dk/teknologi/machine-learning/?gclid=CjwKCAiAhc7yBRAdEiwAplGxX9-5EfvjQkD96qwNmCjNfUjqhmhjex7dBi5X3sJvYtfcOpSr0cXjiRoC1QEQAvD_BwE

Link testet den: 14/05/2020

https://ordnet.dk/ddo/ordbog?query=bias

Link testet den: 14/05/2020

https://ordnet.dk/ddo/ordbog?query=gennemsigtigheden

Link testet den: 14/05/2020

https://ordnet.dk/ddo/ordbog?query=rimelig&fbclid=IwAR3OL1kaDCnEo7Uj27darB0e39zoyYx2dN2parBb2-hReyiqNTPUgsmIqcQ

Link testet den: 14/05/2020

https://ordnet.dk/ddo/ordbog?query=transparens

Link testet den: 14/05/2020

https://www.andrewdburt.com

Link testet den: 14/05/2020

https://www.datatilsynet.dk/emner/big-data-profilering-og-markedsfoering/

Link testet den: 14/05/2020

https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-personoplysninger/

Link testet den: 14/05/2020

https://www.datatilsynet.dk/internationalt/databeskyttelsesraadet-edpb/

Link testet den: 14/05/2020

https://www.datatilsynet.dk/media/6935/datatilsynets-liste-over-behandlinger-der-altid-er-underlagt-kravet-om-en-konsekvensanalyse.pdf?fbclid=IwAR1apV2mAZoNkC46xSM1QJtu1LVmHXftLQIcnjQWgMEiLG6wukgs96P4_s4

Link testet den: 14/05/2020

https://www.industriensfond.dk/BigData-BigBusiness?fbclid=IwAR1ITIWNghnzz3ZoRS0sit7PJY2yZBvzPVdEDKjXBpXlyP5T-5jGeZCXUBs

Link testet den: 14/05/2020

https://www.lexico.com/definition/fair?fbclid=IwAR1tNoAvqFdKNt9yMj8xlhbmT8Hnbshbt9vjlMo3GVGcnjAjv-b9yIPuDNk

Link testet den: 14/05/2020

https://www.teknologisk.dk/ydelser/big-data-og-anvendelse-af-data/37949

Link testet den: 14/05/2020