

Databeskyttelsesforordningens betydning for udviklere af kunstig intelligens



Speciale af: Emil Faurby Maarup

Studienummer: 20184090

Vejleder: Majken Harbo Hansen

AALBORG UNIVERSITET

Abstract

The development of artificial intelligence has accelerated over the last years and is now having a considerable influence on the daily lives of people. This acceleration is due to the technological advancements within the necessary technology needed to develop artificial intelligence.

Companies are therefore taking advantage of this innovative technology to improve and enhance in various aspects of their business operations. Consequently, this leads to legal challenges regarding the protection of individuals' personal information, particularly in the context of its use in the development of artificial intelligence.

This master thesis aims to investigate and clarify the relevant legislation applicable to developers of artificial intelligence when utilising personal information. The primary legislation of this thesis is the General Data Protection Regulation 2016/679, with a focus on article 5. The analysis seeks to determine the implications of this article on developers of artificial intelligence. This will be achieved by analysing case law from the European Court of Justice, opinions from the article 29-workgroup and other relevant legal sources.

The thesis exclusively concentrates on the European understanding of the above-mentioned legislation. Henceforth, aim is not to give guidance resolving a specific situation but concerns the overall application and the understanding of relevant legislation. In conclusion, the thesis outlines how the developers of artificial intelligence should interpret the applicable legislation and apply it to the development of artificial intelligence trained on or utilising personal information.

Indhold

Abstract.....	1
Kapitel 1	4
Indledning.....	4
Problemfelt og problemformulering	5
Afgrænsning.....	5
Metodik og retskilder	7
Specialets opbygning	9
Kapitel 2 – Kunstig intelligens og fundamentale begreber	11
Introduktion til kunstig intelligens.....	11
Machine Learning	12
Deep Learning og neurale netværk	13
Typer af kunstig intelligens	15
Reaktiv AI	15
Begrænset hukommelsesbaseret AI	16
Theory of Mind, teori om sindet	17
Selvbevidst.....	18
Big data	18
Black Box.....	19
Brug af kunstig intelligens som udelukkende teknisk begreb.....	19
Anonymisering, pseudonymisering og aggregerede data	20
Kapitel 3 – Grundlæggende principper i artikel 5.....	23
Indledning til kapitlet.....	23
God databehandlingsskik.....	24
Princippet om formålsbegrænsning	26
Formålsbestemthedsprincippet.....	26
Udtrykkeligt angivne formål	27
Legitime formål.....	29
Viderebehandling og forenelighed	30
Undtagelser til formålsbegrænsning	37
Princippet om dataminimering.....	41
Dataminimering i forhold til kunstig intelligens.....	43
Princippet om rigtighed	44
Princippet om opbevaringsbegrænsning.....	45

Princippet om integritet og hemmeligholdelse	48
Princippet om ansvarlighed	48
Kapitel 4 – Gennemsigtighed og forklarlighed	50
Kapitel 5 – Konklusion	54
Litteraturliste	58
Figuroversigt	60

Kapitel 1

Indledning

Kunstig intelligens er et begreb, der efterhånden ikke kræver nogen forklaring, før folk ved, hvad det handler om. Tilbage i 2021 anvendte hver fjerde danske virksomhed med minimum 10 ansatte kunstig intelligens¹. Denne udvikling er bestemt ikke på retur, da mulighederne for at udvikle kunstig intelligens kun bliver nemmere. Har man ingen idé om kodning, er det ikke et problem, da alle nemt kan udvikle deres egen kunstige intelligens ved hjælp af OpenAI's nye værktøj². Kunstig intelligens er i hastig udvikling, og det vil ændre vores tilværelse på mange punkter. Imens bliver den digitale teknologi i stadig stigende grad en central del af menneskers liv på alle fronter. Derfor bør man også kunne stole på den. Kunstig intelligens er en af dataøkonomiens vigtigste værktøjer. Teknologien indeholder dog en række potentielle risici, som fx uigennemskuelige beslutningsprocesser og krænkelse af privatlivets fred.³

Europa Kommissionen udgav i 2020 en hvidbog om kunstig intelligens - en europæisk tilgang til ekspertise og tillid. Det fremgår af hvidbogen, hvordan Europa kan blive førende på verdensplan inden for innovation i dataøkonomien og dens anvendelsesmuligheder, men hvordan det også vil have en stor indvirkning på samfundet⁴. I lyset af den hastige udvikling og brugen af kunstig intelligens i samfundet er det, dog som Europa Kommissionen også selv nævner, nødvendigt at grundlæggende rettigheder respekteres. Det er derfor nødvendigt at fokusere på, hvilke juridiske udfordringer denne "nye" teknologi bringer med sig, især når blikket vendes mod privatlivets fred og beskyttelse af personoplysninger.

I dag er den essentielle beskyttelse de registrerede har mod kunstig intelligens i forhold til deres personoplysninger, forordning 2016/679 om databeskyttelse (Herefter forkortet som GDPR). Spørgsmålet ligger så i, hvorvidt denne teknologineutrale lovgivning rummer kapaciteten til at give den fornødne beskyttelse af personoplysninger, og omvendt om den rummer mulighederne for

¹ Danmarks Statistik, *Hver fjerde virksomhed bruger kunstig intelligens*, <https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=31880>, besøgt d. 28 november 2023

² OpenAI, Blog: Introducing GPTs, <https://openai.com/blog/introducing-gpts#OpenAI>, besøgt d. 28 november 2023

³ Europa Kommissionen, COM(2020) 65 final, *Hvidbog om kunstig intelligens – en europæisk tilgang til ekspertise og tillid*, side 1-2

⁴ Europa Kommissionen, COM(2020) 65 final, *Hvidbog om kunstig intelligens – en europæisk tilgang til ekspertise og tillid*, side 3

udviklere af kunstig intelligens til at medvirke til det europæiske mål om at blive førende på verdensplan.

Problemfelt og problemformulering

Dette speciale har til formål at undersøge gældende ret for brugen af personoplysninger i udviklingen af kunstig intelligens (AI) i overensstemmelse med EU-forordning 2016/679. Specialet behandler bestemmelserne i artikel 5 i GDPR og udforsker især kompleksiteten i at opfylde kravene om formålsbegrænsning, dataminimering samt sikring af gennemsigtighed og forklarlighed i beslutningsprocesserne for AI.

Specialets problemformuleringen lyder derfor således:

"Hvilken betydning har bestemmelserne i EU-forordning 2016/679 om databeskyttelse for udviklere af kunstig intelligens, især med hensyn til at opfylde kravene om formålsbegrænsning, dataminimering, samt at sikre gennemsigtighed og forklarlighed i beslutningsprocesserne?"

Afgrænsning

Kunstig intelligens er en svær disciplin at give en konkret beskrivelse af. Der vil i dette speciale blive givet en overordnet forklaring af, hvad kunstig intelligens indebærer, men det vil ikke være en dybdegående teknologisk gennemgang af alle delelementerne, da specialet er juridisk. Der vil kun blive præsenteret de fundamentale begreber og funktioner bag kunstig intelligens, der giver læseren den nødvendige teknologiske viden påkrævet for forståelsen af kunstig intelligens. Det vil også kun være de essentielle ekstra fagtermer og teknologi, der vurderes relevante for specialets problemformulering, som bliver præsenteret.

Persondataretten er et innovativt retsområde, hvor grænserne er flydende, og det kan være svært at negligere den retspolitiske tilgang, *"den ret, der bør gælde"*⁵. Specialet berører dog ikke den retspolitiske tilgang til persondataretten, da det falder uden for formålet. Specialet fokuserer på den stigende brug af kunstig intelligens i samfundet, og de problematikker, udviklere af kunstig

⁵ Blume, Peter – *Persondatarettens kilder og metoder*, side 26

intelligens står over for i efterlevelse af de retlige standarder og bestemmelser i artikel 5 i GDPR. I forlængelse heraf vil etiske problemstillinger ikke blive inddraget i specialet.

Specialet tager udgangspunkt i, at læseren har kendskab til persondataretten og GDPR.

Grundlæggende principper, som ikke er relevante for problemformulerings besvarelse, vil ikke blive bearbejdet. GDPRs retshistorie, opbygning, samtlige bestemmelser og systematik vil herved kun blive berørt og forklaret, hvis relevant og nødvendigt for besvarelsen af problemformuleringen.

Specialet fokuserer på udviklere, og ikke anvendere, af kunstig intelligens. Der vil ikke blive undersøgt problematikker såsom automatiske beslutningsprocesser og profilering, samtykke, tværgående overførsel af data eller datasikkerhed grundet specialets omfang og scope.

Anonymisering, pseudonymisering og aggregerede data vil blive beskrevet kort, da det er nødvendigt at fastlægge forståelsen og forskellen på begreberne, da de har fundamental indflydelse på, hvordan udviklere af kunstig intelligens skal forholde sig til GDPR. Det ligger dog uden for specialets scope og fokus at foretage en dybere analyse af begreberne og af, hvorvidt oplysninger er om en 'identificerbar fysisk person' som omhandlet i artikel 4, nr. 1⁶.

Lovgrundlaget vil i henhold til specialets omfang være begrænset til den danske indførelse af forordning 2017/679 om databeskyttelse. Det vil være GDPR, der er i centrum, og særlovgivning og nationale datatilsynsfortolkninger vil ikke blive inkluderet i specialet. Specialet inkluderer heller ikke analyse eller fortolkninger fra den fremtidige AI forordning⁷, og derfor heller ikke den juridiske definition, som præsenteres i den.

⁶ EU-forordningen 2016/679 – artikel 4, nr. 1

⁷ Europa-Parlamentets og Rådets Forordning – Om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens) og om ændring af visse af unionens lovgivningsmæssige retsakter – COM(2021) 206 final

Metodik og retskilder

Dette speciale har til formål at undersøge nogle af de juridiske udfordringer, som udviklere af kunstig intelligens primært står over for i forhold til GDPR. Kunstig intelligens er ikke et nyt fænomen indenfor informationsteknologien, men retstilstanden er ikke klarlagt, da GDPR, der blev indført i 2018, er teknologineutral og persondatarettens karakter af et innovativt retsområde. Den metodiske tilgang i dette speciale vil derfor være den retsdogmatiske metode. Metoden anvendes til at analysere og beskrive retsregler, samt systematisere gældende ret, og vil blive brugt til at udlede gældende ret (de lege lata)⁸. I dette speciale rettes fokus på udvalgte bestemmelser i GDPR i relation til udviklere af kunstig intelligens. GDPR er den centrale persondataretlige retskilde, der danner udgangspunktet for den nationale ret, der ikke må stride mod GDPR, medmindre hjemmel findes deri⁹. Artikel 1 i GDPR angiver formålet, der er fri dataudveksling og højt databeskyttelses niveau¹⁰. Hvad disse formål indebærer kan udledes ved at analysere de relevante præambler, og der udføres derigennem en formålsfortolkning af GDPR.

For at fastlægge kravene, som skal opfyldes for at opnå højt databeskyttelsesniveau og fri dataudveksling i udviklingen af kunstig intelligens, anvendes en kombination af ordlyds- og formålsfortolkning af de relevante retsregler i databeskyttelsesforordningen 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger¹¹.

Der vil blive inddraget relevant videnskabelig og teknologisk litteratur med det formål at give læseren en overordnet forståelse af, hvad kunstig intelligens-begrebet indebærer. Den valgte litteratur vil primært omfatte artikler, der er relevante i forhold til den overordnede besvarelse af problemformuleringen, og den vil blive anvendt som en metodisk tilgang.

EU-Domstolen er en vigtig aktør med hensyn til udvikling af persondataretlige retskilder, hvor EU-Domstolen har mulighed for at normere gældende ret, og dens afgørelser har væsentlig betydning for retsudviklingen. EU-Domstolen bestemmer, hvorledes retsakter skal forstås og fortolkes, hvilket betyder, at det er domstolen, der fastlægger GDPRs mening. Hensynet til retsenhed og ensartet

⁸ Munk-Hansen, Carsten, *Den juridiske løsning*, side 13f.

⁹ Blume, Peter – *Persondatarettens kilder og metoder*, side 56

¹⁰ Forordningen 2016/679, artikel 1

¹¹ EU-Domstolens sag C-60/22, præmis 49 og heri nævnte retspraksis

anvendelse af GDPR begrundet EU-Domstolens definitionsmagt af EU-retlige regler og regelforståelsen. På denne baggrund er EU-Domstolens domme især i præjudicielle sager en central retskilde til forståelsen af GDPRs regler, da den har regelforståelsen fremfor det konkrete faktum i centrum, og dermed bliver dommen relevant i alle medlemsstater. En dom står ved magt, til den er blevet ændret ved en nyere dom, eller at de faktiske eller retlige forhold er forandret i sådant omfang, at dommen har mistet sin værdi. EU-Domstolen stræber efter konsistens i forhold til retspraksis og regelforståelsen ved i regelfortolkningen at inddrage yderligere retskilder i form af tidligere retspraksis og præambler. Dette indebærer mere præcist, at EU-Domstolens forståelse af grundbegreber og anvendelse af bestemte regler repræsenterer en central retskilde ved fastsættelsen af gældende ret¹². Specialet behandler derfor domme fra EU-Domstolen og inddrager dommenes retskildeværdi i søgen efter gældende ret. I forlængelse heraf inddrager specialet også Generaladvokatens forslag til afgørelse af de afsagte domme fra EU-Domstolen. Forslagene har ingen retskildemæssig værdi i sig selv, men bruges som fortolkningsbidrag til forståelsen af EU-Domstolens fortolkninger i de situationer hvor der foreligger konsensus mellem fortolkningerne. Fortolkningsbidragenes retskildeværdi støttes af EU-Domstolene bruge af forslagene i deres afgørelser og direkte inddragelse af generaladvokatens anførte punkter¹³.

Dette indebærer blandt andet EU-dommene C-60/22, C-77/21 og C-439/19 og korresponderende forslag til afgørelse af Generaladvokaten, der bruges til at fortolke og udfylde de relevante begreber og retsregler, som har betydning for emnet og derved hjælper til forståelsen af, hvad de omfatter.

Præamblerne til forordningen er en fuldt ud integreret del af retsakten og er medtaget for at opfylde en funktion, og de har derfor ikke bare informativ karakter. De er sædvanligvis et væsentligt fortolkningsbidrag, der tages i betragtning, når den enkelte artikel i forordningen skal forstås. De bruges ofte af EU-Domstolen til udfyldning og fortolkning af relevante artikler, da de er mere forklarende i forhold til formålet af de enkelte artikler fra lovgivers side¹⁴. Specialet behandler derfor relevante præambler som fortolkningsbidrag til forståelsen af de relevante bestemmelser.

¹² Blume, Peter – *Persondatarettens kilder og metoder*, side 68-71 og 111

¹³ EU-Domstolens sag: C-77/21, præmis 36

¹⁴ Blume, Peter – *Persondatarettens kilder og metoder*, side 61f

Det er begrænset, hvad der foreligger af domme, som vedrører netop dette speciales problemstilling. Dette kan udgøre en udfordring, da den egentlige retsstilling kan være kompliceret at klarlægge. I mangel af retspraksis kan inspiration hentes fra vejledninger og anbefalinger fra Det Europæiske Databeskyttelsesråd og deres forgænger artikel 29-arbejdsgruppen¹⁵. I forhold til almindelige persondataretlige spørgsmål har artikel 29-arbejdsgruppens dokumenter retskildeværdi, forudsat at der ikke er sket samfundsmæssige forandringer eller tydelige regelændringer¹⁶. De bestemmelser, specialet behandler, er videreført fra direktivet og i General Advokatens forslag til afgørelse til C-77/21 inddrager General Advokaten udtalelse nr. 3/2013, hvilket understøtter retskildeværdien af disse dokumenter¹⁷. Specialet behandler derfor disse dokumenter som fortolkningsbidrag til forståelsen af de relevante bestemmelser.

Retslitteratur i form af videnskabelige artikler og bøger bidrager til fortolkningen af gældende ret, men tillægges ikke en større retskildemæssig værdi, da det i almindelighed må konkluderes, at litteraturen har begrænset retskildelignende funktioner, og en forfatter ikke er en del af retssystemet, og derfor kan siges at savne legitimitet¹⁸.

Specialets opbygning

Specialet er opdelt i 5 kapitler, hvoraf kapitel 1 introducerer og præsenterer specialet og dets formål i form af indledning, problemfelt og problemformulering, afgrænsning og metodik og retskilder.

Herefter vil kapitel 2 beskrive kunstig intelligens, anonymisering, pseudonymisering og aggregerede data. Den præsenterer de fundamentale begreber og funktioner bag kunstig intelligens, der giver læseren den nødvendige teknologiske viden påkrævet for forståelsen af kunstig intelligens i denne sammenhæng. Anonymisering, pseudonymisering og aggregerede data beskrives kort for at give den nødvendige forståelse og forskel på begreberne, da de har fundamental indflydelse på, hvordan udviklere af kunstig intelligens skal forholde sig til GDPR.

I kapitel 3 undersøges det, hvilke krav udviklere af kunstig intelligens skal leve op til i henhold til GDPR. Det vil være med fokus på de retlige standarder og bestemmelser indeholdt i artikel 5 i

¹⁵ Trzaskowski, Jan: *Your Privacy Is Important to US! – Restoring Human Dignity in Data-Driven Marketing*, side 41

¹⁶ Blume, Peter – *Persondatarettens kilder og metoder*, side 66

¹⁷ Forslag til afgørelse fra generaladvokat P. Pikamäe sag: C-77/21, præmis 42

¹⁸ Blume, Peter – *Persondatarettens kilder og metoder*, side 55

GDPR, hvor andre relevante bestemmelser, præambelbetragtninger, retspraksis og vejledninger fra artikel 29-arbejdsgruppen inddrages for at fastlægge regelforståelsen af artiklen.

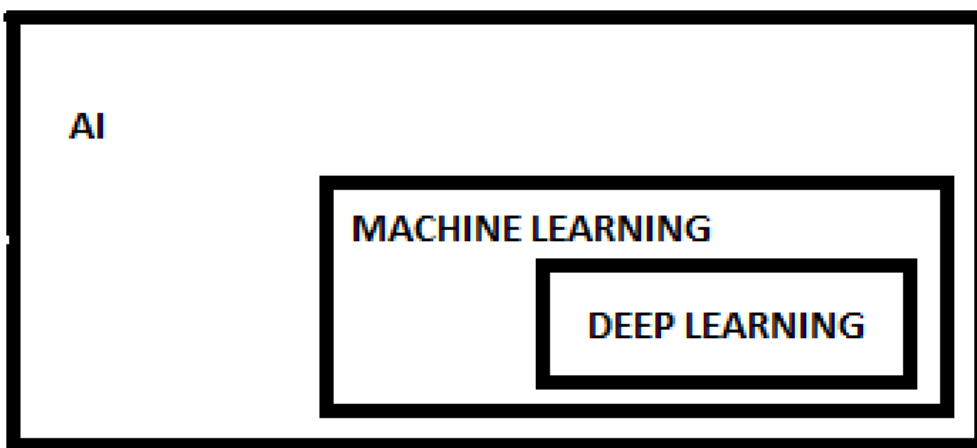
Specialets kapitel 4 analyserer Black Box-problematikken bag kunstig intelligens' behandlingsproces med fokus på, hvilke konsekvenser det har i forhold til gennemsigtighedsprincip og forklarlighed.

Specialet afsluttes derefter i kapitel 5 med en konklusion.

Kapitel 2 – Kunstig intelligens og fundamentale begreber

Introduktion til kunstig intelligens

Der har været mange definitioner af kunstig intelligens, eller AI, igennem årene, og det er stadig ikke helt konkret defineret, hvad begrebet egentligt dækker over. AI kan dog i sin simpleste form beskrives som et felt, der kombinerer computerteknologi og robuste datasæt for at muliggøre problemløsning. Eksperten John McCarthy definerede kunstig intelligens således i 2004: *"Kunstig intelligens er videnskaben og ingeniørkunsten at lave intelligente maskiner, særligt intelligente computerprogrammer"*.¹⁹ Det er dog ikke helt muligt at definere, hvad intelligens er, og derfor heller ikke muligt at definere, hvad kunstig intelligens er. Men det kan siges, at det grundlæggende betyder, at vi prøver at få computere og robotter til at udføre opgaver, som det førhen kun var mennesker, der kunne.²⁰ Denne nye form for intelligens og optimering opnår meget opmærksomhed, og der findes ikke mange mennesker i dag, der ikke kender begrebet AI. Især OpenAI's ChatGPT har slået benene væk under mange mennesker og åbent deres øjne for de massive muligheder, denne teknologi kan give til det almindelige menneske, både i personlige problemstillinger, men også i erhvervslivet.



Figur 1 Egen Tilvirkning. Viser Forholdet mellem AI, Machine Learning og Deep Learning

¹⁹ IBM - What is artificial intelligence (AI)? <https://www.ibm.com/topics/artificial-intelligence> besøgt d. 22. september 2023

²⁰ Bolander, Thomas – Hvad er kunstig intelligens (AI) egentlig? <https://videnskab.dk/teknologi/hvad-er-kunstig-intelligens-ai-egentlig/> besøgt d. 23 september 2023

Selvom der findes flere beskrivelser af, hvad begrebet AI dækker over, så bruges der ofte også andre termer som fx Machine Learning og Deep Learning, når man prøver at definere, hvordan AI fungerer. Det er værd at nævne, at disse termer ikke skal forstås som synonymer, snarere tværtimod. Den nemmeste måde at forestille sig, hvordan disse termer skal forstås i sammenhæng med hinanden, er at se dem som en serie af AI systemer fra størst til mindst, hvor hver enkelt omfatter den næste.²¹ AI er det overordnede system. Machine Learning er en delmængde af AI og er altså indeholdt under det overordnede begreb AI, da begrebet indbefatter teknologiske løsninger til opbygningen af AI. Deep Learning er en underkategori til Machine Learning og indbefatter en måde, hvorpå Machine Learning kan opbygges. Dybere gennemgang af Machine Learning og Deep Learning er beskrevet i "Machine Learning"-afsnittet og "Deep Learning"-afsnittet. For illustrativ visualisering, se ovenstående figur 1.

Machine Learning

Dette afsnit bygger videre på den korte introduktion til begrebet Machine Learning, der blev givet i "Introduktion til kunstig intelligens"-afsnittet. Machine learning er en gren af AI computerteknologi, som fokuserer på brugen af data og algoritmer til at imitere den måde, mennesker lærer og tænker på, og derved gradvist forbedre dens præcision. Dette skal ikke forveksles med tanken, at den kan tænke selv eller tænke som en menneskehjerne. Udtrykkende Deep Learning og neuralt netværk, som vil blive gennemgået senere i kapitlet, er det, man mere vil kunne sammenligne med selvtænkende eller kunstig intelligens. Det er vigtigt først at forstå, hvordan Machine Learning fungerer og den basale funktion bag træningsprocesserne, og hvordan en AI kommer frem til sine resultater. Data er byggestenene bag ved en velfungerende algoritme, så jo bedre og jo mere data algoritmen kan trænes på baggrund af, desto bedre algoritme vil du også få. Dataene samles og forberedes til at blive brugt som træningsdata. Næste skridt er, at programmørerne vælger den Machine Learning model, de vil bruge, leverer træningsdataene og lader computermodellen træne sig selv til at finde mønstre eller lave forudsigelser.²² De forskellige Machine Learning modeller vil ikke blive gennemgået i dette speciale. Træningsprocessorerne er

²¹ IBM Data and AI Team, *Machine Learning vs. Deep Learning vs. Neural Networks: What's the difference?*. <https://www.ibm.com/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks/> besøgt d. 23 september 2023

²² Brown, Sara, *Machine Learning, Explained*. <https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained> besøgt d. 23 september 2023

forskellige alt efter hvilken model eller hvilken funktion, der ønskes, at AI'en kan udføre, men der findes dog tre metoder, som programmøren bruger til at træne algoritmen. Den første er Supervised Machine Learning, hvor modellen er trænet med beskrevet datasæt og meget menneskelig indblanding, både til beskrivelse af datasættene og i løbet af træningsprocessen. Eksempelvis kan programmørerne have beskrevet en masse datasæt indeholdende billeder af hunde, hvorefter algoritmen trænes til at identificere billeder af hunde af sig selv.²³ Den anden er Unsupervised Machine Learning, hvor er datasættene ikke allerede er beskrevet af programmørerne. Algoritmen lærer at analysere og sammenkoble ubeskrevne datasæt. Den finder gemte sammenlignelige elementer eller datagrupperinger uden menneskelig indblanding. Der er også muligheden for at bruge lidt af begge disse metoder, som kaldes Semi-Supervised Machine Learning.²⁴ Den sidste metode kaldes Reinforcement Machine Learning, da den trænes på baggrund af trial-and-error tilgang til at tage den bedste beslutning ved at opbygge et belønningssystem.²⁵ På baggrund af belønningssystemet lærer algoritmen, hvilken beslutninger, der er rigtige, og hvilke, der er forkerte.

Deep Learning og neurale netværk

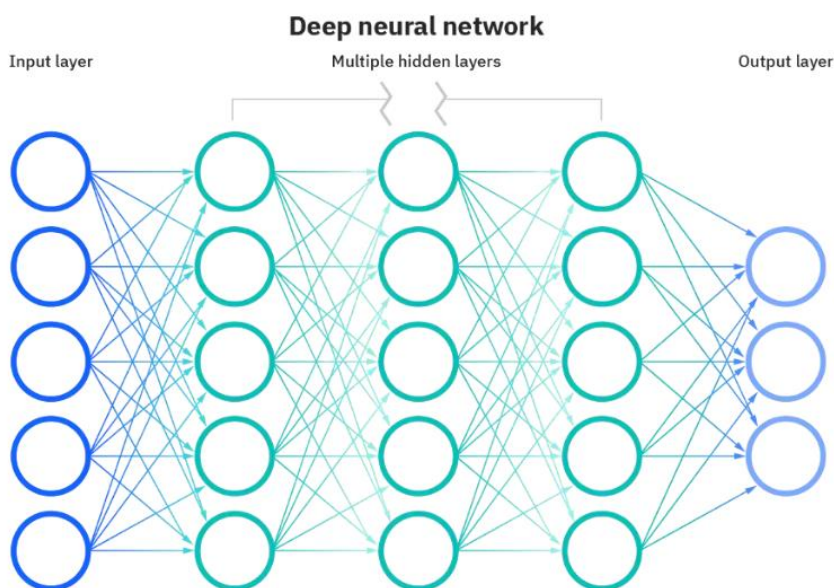
Deep Learning er, som nævnt i indledningen, en underkategori til Machine Learning, og derfor også en del af AI-begrebet. Den essentielle forskel på Deep Learning og Machine Learning er antallet af noder i det neurale netværk, som med et metaforisk udtryk udgør AI's 'hjerne'. Neurale netværk bliver derfor forklaret først. Neurale netværk er en Machine Learning algoritme. Et neuralt netværk kendes fra den menneskelige hjerne og skal ikke forveksles med fænomenet 'kunstig neuralt netværk', som beskrives i dette afsnit. Sammenligningen giver den bedste forståelse, da det lige præcis er en kunstig udgave af det neurale netværk i menneskehjernen, man prøver at genskabe igennem denne form for Machine Learning. Et neuralt netværk er bygget op af nodelag, et inputlag, en eller flere gemte lag og et outputlag. Hver enkelt node er et kunstigt neuron, der er tilkoblet den næste, og hver enkelt har en vægt og grænseværdi. Når neurons output er over grænseværdien, aktiveres noden og den sender dataene videre i netværkets næste node lag.

²³ Brown, Sara, *Machine Learning, Explained*. <https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained> besøgt d. 23 september 2023

²⁴ IBM, *What is machine learning?* <https://www.ibm.com/topics/machine-learning> besøgt d. 23 september 2023

²⁵ IBM, *What is machine learning?* <https://www.ibm.com/topics/machine-learning> besøgt d. 23 september 2023

Modsat, hvis den er under grænseværdien, sender neuronet ikke dataene videre.²⁶ Se figur 2 vist nedenunder for en visualisering af, hvordan et neuralt netværk er opbygget.



Figur 2 Viser et Deep neuralt netværk. Kilde: <https://www.ibm.com/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks/>

Forskellen mellem, hvornår der kun er snak om Machine Learning, og hvornår det er beskrevet som Deep Learning, ligger i, hvor mange gemte lag af noder, der er i det neurale netværk. Hvis der er over 3 lag, medregnet input og output, så beskrives det neurale netværk som en Deep Learning algoritme og ikke kun som en Machine Learning algoritme. Det er her, termen stammer fra, da jo flere gemte lag der er, desto "deeper" er systemet. Deep neuralt netværk består, som forklaret ovenfor og som vist på figur 2, af, hvordan alle disse lag er indbyrdes sammenkoblet, og på denne måde arbejder alle disse elementer sammen for mere præcist at genkende, klassificere og beskrive objekter i dataene. Det er inputlaget, hvor dataene indsættes i algoritmen, og outputlaget, der er de eneste synlige lag for dem, der udvikler algoritmen.²⁷

Det er modsat også det, der skaber problematikken bag Deep Learning, da alle de gemte lag, og hvordan de virker, ikke er synlige for dem, der udvikler algoritmen. Denne problemstilling vil blive

²⁶ IBM Data and AI Team, *Machine Learning vs. Deep Learning vs. Neural Networks: What's the difference?*. <https://www.ibm.com/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks/> besøgt d. 24 september 2023

²⁷ IBM, *What is deep learning?* <https://www.ibm.com/topics/deep-learning> besøgt d. 24 september 2023

beskrevet mere i "Black Box"-afsnittet i forhold til, hvordan det tekniske virker, og hvorfor dette er et stort problem. Det vil også blive analyseret i kapitel 4 i forhold til problemformuleringen vedrørende, hvordan udviklere sikrer overholdelse af kravene om gennemsigtighed af forklarlighed i relation til beslutningsprocesserne.

Typer af kunstig intelligens

Kunstig intelligens findes i mange forskellige typer og former. Oven for i afsnittene om Machine Learning og Deep Learning er det tekniske bag træning- og læringsprocesserne allerede blevet beskrevet, og hvilken type data, man bruger til disse processor, vil blive præsenteret i "Big Data"-afsnittet. Dette afsnit vil give en overordnet forståelse af, hvilke overordnede typer, man inddeler AI i.

Der er 4 overordnede typer af AI baseret på deres funktionalitet, som derefter inddeles i det, man kalder for svag og stærk AI. Smal AI er dog en mere retvisende term i stedet for svag AI, da de langt fra er svage i deres funktionalitet, men derimod er trænet til at udfører en specifik eller begrænset række opgaver. Brugen af termene svag og smal kan stadig godt give et misvisende billede af disse typer AI's funktionalitet. Alle de AI's, der til dags dato er udviklet, falder alle inden under definitionen smal AI. Dette er alt fra Chatbots, Apple's Siri til selvkørende biler.²⁸ De typer af AI, der falder inden for beskrivelsen smal AI vil blive beskrevet først, da de er de mest interessante for denne fremstilling, men stærk AI bliver også inddraget for at give et perspektiv og en bedre forståelse for, hvorfor termene svag og stærk bruges, og så de ikke misforstås.

Reaktiv AI

Den mest banale og mindst intelligente type af AI kaldes reaktiv AI (Reactive AI). Reaktiv AI algoritmer operer kun på nutidige data og har begrænsede kapaciteter. De har ikke nogen specifik funktionel hukommelse, hvilket betyder, at de ikke kan udnytte tidligere lært erfaring til at hjælpe med deres nutidige eller fremtidige beslutninger. Disse AI's og Machine Learning modeller med deres statistiske matematiske egenskaber er dog stadig i stand til at overveje og bearbejde store mængder data og producerer et tilsyneladende intelligent output. Dette gør dem gode til simpel klassifikation og mønstergenkendelsesopgaver. Et meget kendt eksempel på reaktive AI's, hvilket

²⁸ IBM - What is artificial intelligence (AI)? <https://www.ibm.com/topics/artificial-intelligence> besøgt d. 24. september 2023

illustrerer dens overlegenhed over den menneskelige hjerne, er skak AI's. Alle elementer i spillet skak er kendte og hver gang, der foretages et træk, vil der være næsten et uendeligt antal mulige modtræk, hvor den reaktive AI algoritme er i stand til matematisk at udregne det træk med størst sandsynlighed for sejr. Det er dog nødvendigt, at alle parametre er kendte, men så vil den også være i stand til at udregne meget hurtigere end et menneske. Problemet for Reaktive AI's er også deres mangel på egenskaben til at behandle ikke-fyldestgørende information eller historisk forståelse. I det virkelige liv vil mange af vores beslutninger dog være baseret på ikke-fyldestgørende informationer og evnen til at tilpasse os ikke-forudsigelse situationer. Et godt eksempel på dette er selvkørende biler. Her er det nødvendigt at kunne forudse og reagere på mange utænkelige og uforudsigelige situationer, hvilket den Reaktive AI-algoritme ikke er i stand til, da den ikke kan huske og lære, og kun fungerer, når alle parametre er kendte, som i det tidligere eksempel med skak.²⁹

Begrænset hukommelsesbaseret AI

De begrænsninger, som reaktive AI algoritmer har, prøver udviklere at løse ved den næste type af AI kaldet begrænset hukommelsesbaseret AI (Limited memory-based AI), hvilket har evnen til at huske og lære fra tidligere erfaring. Hvor den reaktive AI-algoritme udelukkende gør brug af Machine Learning, gør den begrænset hukommelsesbaseret AI brug af Deep Learning og teorien bag neurale netværk, som er beskrevet i "Deep Learning og neuralt netværk"-afsnittet. Egenskaben til at imitere, hvordan det neurale netværk i den menneskelige hjerne for beslutningstagen og tankeprocessor fungerer, sammenkoblet med AI's egenskab til at lære af tidligere erfaring og fejl, var en stor forbedring i forhold til den reaktive AI-algoritme. AI-modellerne er meget bedre til at absorbere karakteristikkene af deres træningsdata, men mere banebrydende er de også i stand til at forbedre sig over tid. Modellerne er også udviklet til at fungere med ikke-fyldestgørende information og derefter selv lære, hvilken beslutning, der ville være den mest optimale, og hvilke konsekvenser, det ville have i fremtidige situationer.³⁰ Denne fremstilling vil ikke dykke dybere ned i, hvordan det tekniske bag den begrænsede hukommelsesbaseret AI fungerer, da det ikke er

²⁹ Gillis S., Alexander, 4 main types of artificial intelligence: Explained
<https://www.techtarget.com/searchenterpriseai/tip/4-main-types-of-AI-explained> besøgt d. 24 september 2023

³⁰ Gillis S., Alexander, 4 main types of artificial intelligence: Explained
<https://www.techtarget.com/searchenterpriseai/tip/4-main-types-of-AI-explained> besøgt d. 24 september 2023

nødvendigt for analysen af problemformuleringen, og det ville blive en meget dybdegående teknisk forklaring.

På trods af alle disse fremskridt inden for AI er de stadig langt fra at besidde de samme kognitive egenskaber, som den menneskelige hjerne. Problemet for selv den begrænset hukommelsesbaseret AI er, at selvom de kan trænes til at mestre det enkelte miljø, er de ikke i stand til at tage den viden med til et lignende miljø. Et godt eksempel på dette er sprog. For mennesker vil det, når du har lært et sprog, være proportionelt nemmere at lære det næste og det tredje sprog. Dette er ikke muligt for AI, da den kun kan bearbejde informationer ud fra det miljø, den var trænet på baggrund af, og ikke tage disse erfaringer med over i det andet miljø, som fx et nyt sprog. Den ville være nødt til at starte helt forfra. Dette illustrerer også, hvorfor disse AI's beskrives med termen "smal", da de kan mestre en specifik opgave, men fejler gevaldigt ved bare små ændringer til den opstillede opgave.³¹

Theory of Mind, teori om sindet

Dette afsnit giver en kort gennemgang af en af de AI-typer, der benævnes som stærk AI i introduktionen. Det vil kun være en overordnet gennemgang, da den her type og den selvbevidste AI type kun bruges som illustration til, hvad AI kan udvikle sig til fremtiden, og giver et billede af, hvordan de AI's, der bruges nu, ikke besidder de egenskaber, som mange mennesker går og er bange for.

Teori om sindet referer til AI -maskinens egenskab til at henfører dens mentale tilstand til andre entiteter. Termen stammer fra psykologi og kræver, at AI kan fortolke motiver og hensigter fra andre entiteter i dens beslutninger. Dette kunne eksempelvis være overbevisninger, følelser og kropssprog eller lignende. Målet er at udvikle AI'en, så den er i stand til at genkende, simulere, overvåge og reagere til menneskelige følelser ved for eksempel at analysere stemmeleje, billede og andre former for data. Den store problemstilling for denne fremtidige form for stærk AI ligger i, at de nuværende AI-modeller egentlig ikke forstår grundlaget og baggrunden for de beslutninger eller output, den giver. Eksempelvis vil en AI, der kan generere et mesterværk af et maleri, stadig ingen

³¹ Gillis S., Alexander, 4 main types of artificial intelligence: Explained
<https://www.techtarget.com/searchenterpriseai/tip/4-main-types-of-AI-explained> besøgt d. 24 september 2023

idé have om, hvad den har malet. Det vil først være, når den har opnået teori om sindet, at den vil have overkommet denne barrierer.³²

Selvbevidst

Denne type af AI vil være den ultimative maskine, som ikke bare er i stand til at forstå, hvad den f.eks. har malet, som forklaret ovenfor, men også ligefrem være både selvbevidst om dens egen interne stadie og i stand til at forstå andre entiteters. Den vil også være i stand til at efterligne menneskelige træk som følelser, lyst og behov og være på niveau med menneskelig intelligens³³. Dette er slet ikke en realitet endnu, men bruges i denne fremstilling til at illustrere, hvor langt udviklerne er i forhold til kunstig intelligens.

Big data

Overordnet set referer Big data til store og uoverskuelige datapunkter fra ofte flere forskellige kilder. Disse kilder er alt fra f.eks. Internet of Things, sociale medier, online markedspladser, videnskabelige undersøgelser osv. Det kræver specielle metoder for effektivt at opbevare, håndtere, bearbejde og analysere disse enorme mængder af data.³⁴ Definitionen af Big data beskrives som data, der indeholder stor forskellighed i både strukturerede og ustrukturerede data, store mængder data, og hastigheden hvorpå data opsamles, analyseres og bearbejdes.³⁵ Denne form for data og muligheden for effektivt at udnytte den til forretningsmæssige årsager nødvendiggør i mange situationer brugen af AI.

Nævnt oven for i kapitlet kræver AI-algoritmer store mængder af data i træningsprocessen, især Deep Learning og de neurale netværk. Det er derfor relevant at nævne Big Data, da den skaber fundamentet, hvorpå udviklere træner AI. Det vil ofte være adgangen til disse enorme mængder data, der beslutter, hvorvidt en udvikler kan skabe en effektiv og præcis AI-algoritme. Big Data indeholder, som beskrevet ovenfor, data fra diverse kilder, men det centrale er ofte hvilken form for data, der snakkes om. Det vil ikke altid være tilfældet, men der vil være situationer, hvor denne data indeholder personoplysninger. Det er ikke kun formen for data, men også mængden og

³² Gillis S., Alexander, 4 main types of artificial intelligence: Explained
<https://www.techtarget.com/searchenterpriseai/tip/4-main-types-of-AI-explained> besøgt d. 24 september 2023

³³ Gillis S., Alexander, 4 main types of artificial intelligence: Explained
<https://www.techtarget.com/searchenterpriseai/tip/4-main-types-of-AI-explained> besøgt d. 24 september 2023

³⁴ Bahrynovska, Tanya, *Exploring the intersection of Big Data and AI: Unlocking Insights and Driving Innovation*
<https://forbytes.com/blog/big-data-and-ai/> besøgt d. 25 september 2023

³⁵ Oracle, *What is Big Data?* <https://www.oracle.com/big-data/what-is-big-data/> besøgt d. 25 september 2023

formålet med brugen af store mængde persondata, der ofte vil være svært for udviklere at begrunde. Denne problemstilling analyseres nærmere i kapitel 3.

Black Box

En af de store problemstillinger ved AI er, når udviklere og brugere ikke kan forklare, hvordan AI'en er kommet frem til sit resultat. De er ikke i stand til at forklare beslutningsprocesserne bag outputtet. Som beskrevet i "Deep Learning"-afsnittet og vist på figur 2, kan et neuralt netværk bestå af mange gemte lag imellem inputtet og outputtet. Det er disse gemte lags beslutninger og ikke-beslutninger, man teknisk beskriver som 'Black Box' problemet. Det kommer sig af, at udviklere ikke ved, hvad der foregår, men kun er i stand til at se outputtet. Dette skaber mange problemstillinger for udviklere, da de for eksempel, hvis AI'en giver det rigtige output, ikke ved hvorfor, eller vice versa. Et eksempel er, hvis en selvkørende bil kører en fodgænger ned i stedet for at trykke på bremsen. Her vil vi ikke være i stand til at analysere AI'ens beslutning, da vi ikke ved, hvilke tankeprocesser, der fik den til at tage den beslutning.³⁶ Der vil ikke i denne fremstilling blive gået i dybden med de etiske overvejelser, men dette er i teorien en stor problemstilling for udviklere, når de arbejder med Black Box problemstillingen. I kapitel 4 - Gennemsigtighed og forklarlighed vil det tekniske begreb Black Box blive inddraget og analyseret i forhold til det forklaringsproblem og den manglende gennemsigtighed, som disse AI modeller har i deres behandlingsprocesser.

Brug af kunstig intelligens som udelukkende teknisk begreb

Dette kapitel har introduceret de essentielle tekniske begreber og underelementer, samt forklaret den tekniske definition af AI og dens bagvedliggende teknologi. Der er givet en grundlæggende forklaring, da det ikke er nødvendigt for analysen af problemformuleringen at give mere dybdegående teknologisk beskrivelse af AI og dens underelementer. Der foreligger ikke i retsvidenskaben endnu en juridisk definition af AI og den tekniske definition danner derfor grundlaget for fortolkningen og analysen.

³⁶ Blouin, Lou, *AI's mysterious 'black box' problem, explained*, <https://www.datacamp.com/blog/what-is-symbolic-ai> besøgt d. 25 september 2023

Anonymisering, pseudonymisering og aggregerede data

Dette afsnit beskriver kort anonymisering af data og konsekvenserne ved behandling af anonymiseret data, samt pseudonymisering og aggregerede data. Det er, som ved kunstig intelligens, nødvendigt at have en dybere teknisk forståelse af disse begreber, især pseudonymisering og aggregerede data, da de vil indgå i analysen i kapitel 3 og er fundamentale for de sikkerhedsforanstaltninger og fornødne garantier, hvorpå kunstig intelligens ofte behandler personoplysninger. Det ligger uden for specialets scope at foretage en dybere analyse af begreberne, og hvorvidt oplysninger er om en 'identificerbar fysisk person', som omhandlet i artikel 4, nr. 1 af GDPR³⁷. Det er dog nødvendigt at fastlægge forståelsen af og forskellen på begreberne, da det har fundamental indflydelse på, hvordan udviklere af kunstig intelligens skal forholde sig til GDPR.

Definitionen på anonyme oplysninger fremgår af præambelbetragtning 26, der lyder: "*... anonyme oplysninger, dvs. oplysninger, der ikke vedrører en identificeret eller identificerbar fysisk person, eller for personoplysninger, som er gjort anonyme på en sådan måde, at den registrerede ikke eller ikke længere kan identificeres. Denne forordning vedrører derfor ikke behandling af sådanne anonyme oplysninger, herunder til statistiske eller forskningsmæssige formål*"³⁸. Anonyme oplysninger er derfor oplysninger, som førhen var identificerbare til en fysisk person, men hvor identifikationen ikke længere er mulig. Det vil være situationsbestemt og afhænge af en konkret vurdering, hvorvidt den er gjort anonym på en sådan måde, at den registrerede ikke kan identificeres. Dette afsnit, som beskrevet ovenfor, analyserer ikke dybdegående, hvorvidt der er tale om anonyme oplysninger, men inddrager definitionen udelukkende for at give den tekniske forståelse af, hvad anonymiseringsbegrebet betyder. Det er dog værd at nævne aggregerede data i sammenhæng med anonymiseret data. Aggregerede data er en summarisk behandling af oplysninger om flere personer, som er kombineret og samlet uden fokus på den enkelte person³⁹. Aggregerede data kan være anonyme, hvis det ikke længere er muligt at identificere den registrerede person ud fra de aggregerede data. Som det fremgår af præambelbetragtningen, vedrører denne forordning derfor ikke behandling af sådanne anonyme oplysninger, og hvis

³⁷EU-forordningen 2016/679 – artikel 4, nr. 1

³⁸EU-forordningen 2016/679 – præambel 26

³⁹ Datatilsynet, *Hvad er personoplysninger?* <https://www.datatilsynet.dk/hvad-siger-reglerne/grundlaeggende-begreber/hvad-er-personoplysninger>, besøgt d. 20/11/2023

anonyme oplysninger behandles, vil udviklere af kunstig intelligens ikke være nødsaget til at tage forbehold for forordningen og dens bestemmelser om databeskyttelse. Aggregerede data kan, som beskrevet ovenfor, være anonymiseret, men det afhænger af metoden brugt til at aggregere dataene, da det på modsat vis også kan være muligt at identificere de enkelte personer. Der vil ikke blive givet en dybere teknisk gennemgang af metoderne til at aggregere data, men det er vigtigt at fastslå, at valget af metode har betydning i forhold til fortolkningen af, hvilke sikkerhedsforanstaltninger de bidrager med, især hvis de bruges i kombination med pseudonymiseret data. Aggregerede data vil blive inddraget i afsnittene "Viderebehandling og forenelighed" og "Undtagelser til formålsbegrænsning" i kapitel 3.

Pseudonymisering omhandler processen ved at skjule identiteter. Formålet med sådan en proces er muligheden for at indsamle yderligere data vedrørende den samme person uden at kende identiteten. Pseudonymisering muliggør ved hjælp af en sammenlignelighedsliste, at det på et senere tidspunkt er muligt at genidentificere den registrerede. Det er denne form for senere genidentifikation, der medfører, at pseudonymiseret data vil kunne blive kategoriseret som indirekte identifikation af en person. Det er, som forklaret, kun muligt at genidentificere personen under specifikke omstændigheder eller, som i eksemplet, med en sammenlignelighedsliste. Selvom databeskyttelsesreglerne vil være gældende, vil risikoen for den registrerede være væsentlig lavere og håndhævelsen af bestemmelserne være mere fleksible, end hvis det var på en direkte identificerbar fysisk person⁴⁰. Især denne tilgang og sammenhængen med tilstedeværelsen af fornødne garantier i artikel 6, stk. 4 vil blive beskrevet i "Viderebehandling og forenelighed"-afsnittet og undtagelserne til forenelighed i artikel 5, stk. 1, litra b beskrevet i "Undtagelser til formålsbegrænsning"-afsnittet.

Det vil, som beskrevet ovenfor, være anonymisering, hvis det ikke er muligt at genidentificere den registrerede. Især denne forskel på, hvornår det er anonymisering og pseudonymisering, er, som beskrevet ovenfor, central, da GDPRs anvendelse afhænger af, hvilken form for krypteringsmetode, der er brugt på personoplysningerne, som udviklere af kunstig intelligens behandler. Det findes derfor relevant for specialet først at fastslå konsekvenserne ved anonymiseret data og udelukkelsen af GDPRs anvendelse for derefter at fokusere på, hvordan udviklere af kunstig

⁴⁰ Artikel 29-arbejdsgruppens udtalelse nr. 4/2007 *on the concept of personal data*, side 18

intelligens overholder de retlige krav i GDPR. Begreberne pseudonymisering og aggregerede data er som beskrevet ovenfor centrale i fortolkningen af fornødne garantier og sikkerhedsforanstaltninger, der vil blive gennemgået i kapitel 3.

Kapitel 3 – Grundlæggende principper i artikel 5

Indledning til kapitlet

Før analysen og gennemgangen af artikel 5 i GDPR påbegyndes, præsenteres kort GDPRs hovedelementer, og hvad de indeholder, for overblikkets skyld. Efter afgrænsningen af GDPRs formål og område opstilles legaldefinitioner i artikel 4, hvilke vil blive brugt igennem kapitlet uden yderligere forklaringer. Efterfølgende begynder den egentlige regulering i artikel 5, der angiver en række almene principper, der skal følges for alle persondatabehandlinger. Der findes dog undtagelser i artikel 23 til brugen af nogen af principperne, når de er relateret til artikel 12-22 i national ret. Hjemmel behandles i artikel 6-10, og de registreredes rettigheder fastlægges i artikel 12-22. Disse udgør GDPRs kerne, og de øvrige regler, der også har stor praktisk betydning, tager sigte på, at disse bestemmelser bliver realiseret og fungerer effektivt⁴¹. Dette kapitel kommer til at fokusere på de generelle principper i artikel 5 og til kort at berøre andre artikler, der har relevans for forståelsen af de generelle principper og problemformuleringen.

GDPR indeholder, som nævnt ovenfor, nogle almene principper i artikel 5. Disse retlige standarder angiver ikke fuldt ud en specifik regel, men derimod mere en retningspil for tilrettelæggelsen af persondatabehandlingen. Anvendelsen af retlige standarder er næsten uundgåelig i persondataretten, og de viser tydeligt reguleringens dynamiske karakter⁴². Denne mangel på præcision kan skabe en vis usikkerhed om, hvordan de enkelte principper skal fortolkes i den konkrete situation. Især for udviklere af kunstig intelligens er det essentielt, at de ved, hvilket spillerum de har, og hvornår de må behandle personoplysninger i skabelse og træning af deres algoritme.

Dette kapitel gennemgår først de overordnede retlige standarder lovlighed, rimelighed og gennemsigtighed, og derefter vil de andre delelementer af artikel 5 blive gennemgået.

Gennemgangen kommer til at sammenkoble de retlige standarders overordnede retlige forståelse med de tekniske begreber, der er blevet præsenteret i kapitel 2, for at prøve at kortlægge retslandskabet for udviklere af kunstig intelligens. Kapitlet opdeler principperne og analyserne i underafsnit for sig selv, men deres generelle natur nødvendiggør, at nogle af principperne vil blive

⁴¹ Blume, Peter – *Persondatarettens kilder og metoder*, side 59

⁴² Blume, Peter – *Persondatarettens kilder og metoder*, side 60f

brugt i flere underafsnit. Denne opbygning er valgt for at gøre det nemmere for læseren at holde overblikket og den røde tråd igennem kapitlet.

God databehandlingsskik

Personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede, jf. artikel 5, stk. 1, litra a. Denne bestemmelse svarer til princippet om god databehandlingsskik, som førhen fandtes i persondataloven⁴³.

Behandling af personoplysninger skal være lovlig. Dette betyder, at det både skal være lovligt i henhold til andet lovgivning og til forordningen. Lovligheden af behandling af persondata i henhold til GDPR selv findes i artikel 6. Den oplister en række forhold, der skal gøre sig gældende, før behandling er lovlig. Dette betyder, at der skal foreligge mindst en af de forhold nævnt i artiklen, før behandling af personoplysninger er lovlig, men at listen ikke er kumulativ. Der findes altså flere forskellige belæg i artiklen for lovlig behandling, men listen er udtømmende og fuldstændig. Dette kapitel kommer til at berøre artikel 6, stk. 4 i GDPR, der vil blive inddraget i forhold til fortolkningen af ikke-uforenelige formål i "Viderebehandling og forenelighed"-afsnittet.

Den anden del af den retlige standard vedrørende andet lovgivning illustrerer, hvordan persondataretten ikke står alene, men ofte opstår i sammenhæng med anden retlig regulering. Dette illustreres i præambelbetragtning 4, der beskriver, hvordan persondataforordningen respekterer hele EU-chartret om grundlæggende rettigheder⁴⁴. GDPR går også videre og beskriver direkte i præambelbetragtning 4, at retten til beskyttelse af personoplysninger ikke er en absolut ret, men skal ses i sammenhæng med sin funktion i samfundet og afvejes i forhold til andre grundlæggende rettigheder⁴⁵. Det er altså ikke nok, at behandlingen af personoplysninger er lovlig i henhold til GDPR, men den skal også overholde alle de andre rettigheder, som for eksempelvis EU-chartret. Det belyser, hvordan GDPRs reguleringsmetode er åben for anden ret, da den f.eks. ved lovlighed kan inddrage andre retskilder til at udfylde denne retlige standard.

Rimelighedsbegrebet i artikel 5, stk.1, litra a er en generalklausul, der beskytter GDPRs formål vedrørende højt databeskyttelsesniveau for pligtsubjektet. Den foreskriver, at selv, hvis en

⁴³ Højlund, Dorte – *Persondataret*, side 34

⁴⁴ Blume, Peter – *Persondatarettens kilder og metoder*, side 24f

⁴⁵ EU-forordningen 2016/679 - præambel 4

databehandling vil være lovlig i henhold til andre bestemmelser i GDPR, vil behandlingen stadig være ulovlig, hvis den ikke er rimelig. Det er nødvendigt at lave en skønsafvejning. Det fremgår af præambelbetragtning 39, at det er nødvendigt at iagttage de registreredes rettigheder og interesser, for at en behandling kan være lovlig og rimelig. Ydermere bør personoplysninger kun behandles, hvis formålet med behandlingen ikke kan opfyldes på anden måde⁴⁶. Det er ikke kun i formålsspecifikationen rimelighedsvurderingen er nødvendig, men også når oplysningspligten iagttages i sammenkobling med gennemsigtighedsprincippet. I overensstemmelse med præambelbetragtning 60 og 61 til GDPR kræver princippet om rimelighed og gennemsigtighed, at den registrerede informeres om behandlingseksistens og -formål⁴⁷. Dette vil blive uddybet yderligere efter gennemgangen af gennemsigtighedsprincippet lige nedenfor.

Gennemsigtighedsprincippet er et centralt element i artikel 5, stk. 1, litra a i GDPR. Den foreskriver den fundamentale ret i, at det bør være gennemsigtigt for den registrerede, at personoplysninger, der vedrører dem, indsamles, anvendes, tilgås eller på anden måde behandles, og i hvilket omfang både nutidig og fremtidig behandling vil foregå⁴⁸. Både præambelbetragtning 39 og artikel 12 foreskriver, at enhver meddelelse til den registrerede skal være i *”letforståelig og lettilgængelig form og i et klart og enkelt sprog”*⁴⁹. Princippet sikrer, at den registrerede er oplyst og informeret om, hvorvidt dens personoplysninger behandles, og hvordan de behandles. Oplysningspligten indeholder flere delelementer, som ikke vil blive gennemgået i dette kapitel, da det ligger uden for specialets scope. Gennemsigtighedsprincippet er dog essentielt og vigtigt for udviklere af kunstig intelligens i mange former for lovligt at kunne behandle den registreredes personoplysninger. Den anden del af problemformuleringen vedrørende gennemsigtighed og forklarlighed vil blive gennemgået i kapitel 4, hvor der vil blive fokuseret på, hvordan udviklere af kunstig intelligens kan leve op til disse krav i udviklingsfasen. For den videre analyse i dette kapitel vil gennemsigtighedsprincippet ikke blive uddybet mere i dette afsnit, men blive nævnt i de kommende relevante delafsnit, hvor dens rolle og samspil med de andre principper og bestemmelser vil blive forklaret.

⁴⁶ EU-forordningen 2016/679 - præambel 39

⁴⁷ Forslag til afgørelse fra generaladvokat P. Pikamäe sag: C-77/21, præmis 45

⁴⁸ EU-forordningen 2016/679 - præambel 39

⁴⁹ EU-forordningen 2016/679 - præambel 39 og artikel 12

Principperne om lovlighed, rimelighed og gennemsigtighed beskrevet i dette afsnit kan betragtes som overordnede principper eller retlige standarder, hvilke de efterfølgende principper understøtter eller konkretiserer. Det er nødvendigt for at fastholde overblikket og forstå sammenspillet mellem disse retlige standarder og de enkelte principper og bestemmelser i artikel 5, stk. 1, hele tiden at huske, at når der for eksempelvis forklares om legitime formål, er dette princip med til at konkretisere den retlige standard om lovlighed. Det legitime formål skal dog stadig være rimeligt samt gennemsigtigt for den registrerede, og principperne vil, som tidligere forklaret, derfor blive inddraget i delanalyserne løbende igennem kapitlet for bedre at forklare sammenspillet.

Princippet om formålsbegrænsning

Formålsbestemthedsprincippet

Artikel 5, stk. 1, litra b indeholder flere delelementer og principper, som vil blive gennemgået i dette kapitel, men først vil formålsbestemthedsprincippet kort blive gennemgået.

Princippet indeholder flere delelementer, hvis betydning endnu ikke er fastlagt, som gør det svært at give en kort og præcis forklaring af, hvad det overordnede princip egentlig indeholder. Princippet om formålsbestemthed fastsat i artikel 5, stk. 1, litra b indeholder dog to overordnede delelementer, idet personoplysninger på den ene side skal indsamles til 'udtrykkeligt angivne og legitime formål' og på den anden side ikke må 'viderebehandles på en måde, der er uforenelig' med disse formål⁵⁰. Det er altså nødvendigt for udviklere af kunstig intelligens, der behandler personoplysninger, at formålet er udtrykkeligt angivet, følger et legitimt formål og, hvis der ønskes viderebehandling, ikke må være uforenelig med det oprindelige formål. Det skal bemærkes, at artiklen ikke angiver, at hvis der ønskes viderebehandling, at formålet skal være 'foreneligt', men at det ikke må være 'uforeneligt', for alt andet lige gør dette også bestemmelsen mindre restriktiv. Den angiver dog i sidste led, at "*viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål*"⁵¹. De

⁵⁰ Forslag til afgørelse fra generaladvokat P. Pikamäe sag: C-77/21, præmis 27 og EU-Domstolens sag: C-77/21, præmis 25-26

⁵¹ EU-forordningen 2016/679 – artikel 5, stk. 1, litra b

kommende afsnit dykker dybere ned i de enkelte delelementer for at give en tydeligere beskrivelse af det overordnede formålsbestemthedsprincip.

For klarhedens skyld og for at holde den røde tråd vil formålbestemshedsprincippet blive opdelt i afsnit omhandlende "Udtrykkeligt angivne formål", "Legitime formål", "Viderebehandling og forenelighed" og "Undtagelser til formålsbegrænsning".

Udtrykkeligt angivne formål

GDPRs artikel 5, stk. 1, litra b lyder som følger: "*[Personoplysninger skal] indsamles til **udtrykkeligt angivne** og legitime **formål** og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål.*"⁵². Kravet om, at formål skal være udtrykkeligt angivne, er forbundet med den grundlæggende garanti for forudsigelighed og retssikkerhed, da det medvirker til, at den registrerede kan forstå, hvordan hans eller hendes oplysninger eventuelt vil blive brugt, og giver den registrerede mulighed for at træffe informerede beslutninger⁵³. Det er nødvendigt, at formålet er tydeligt og specifikt identificeret, så det er muligt at identificere, hvilke behandlinger, der er inkluderet, og hvilke, der ikke er⁵⁴. Formål, der beskrives vagt eller generelt vil ofte ikke møde kriteriet omkring udtrykkeligt angivne formål. Artikel 29-arbejdsgruppen angiver selv nogle eksempler på, hvornår det er for vagt, eller generelt i form af 'forbedre brugeroplevelsen', 'marketing', 'IT-sikkerhed' eller 'fremtidig forskning'. Det er dog altid en konkret vurdering i henhold til den kontekst, data og personoplysninger bliver indsamlet i, der er determinerende for, hvor præcis formål skal beskrives⁵⁵. Det vil for udviklere af kunstig intelligens afhænge af, hvilken form for kunstig intelligens, de udvikler, og hvad dens funktioner er. Det vil dog ikke være præcist nok bare at angive, at formålet er at 'forbedre brugeroplevelsen', eller 'kunstig intelligens-relaterede formål', især ikke hvis der gøres brug af Big Data, men kræve en højere form for præcision. Vurderingen af konteksten og præcisionen af formål for udviklere af kunstig intelligens, hænger også sammen med rimelighed- og gennemsigtighedsprincippet, som beskrevet oven for i "God databehandlingsskik"-afsnittet, da den store mængde behandling af persondata for

⁵² EU-forordningen 2016/679, artikel 5, stk. 1, litra b

⁵³ Forslag til afgørelse fra generaladvokat P. Pikamäe sag: C-77/21, præmis 41

⁵⁴ Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, side 15

⁵⁵ Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, side 52

at være rimelig og gennemsigtig for den registrerede også vil påvirke konteksten, hvori kravet til præcision af formål vurderes. Det er ikke muligt at give en overordnet definition på, hvor præcis formål skal beskrives, da det, som beskrevet ovenfor, afhænger af konteksten, men det vil for udviklere af kunstig intelligens ofte kræve større præcision af det angivne formål, da de i mange tilfælde bearbejder 'Big Data'.

Der i ovenstående gennemgang brugt ordet 'præcision' mange gange, og Artikel 29-arbejdsgruppen angiver også nogle retningslinjer til, hvordan 'præcis' skal forstås i sammenhæng med formål. 'Præcis' betyder ikke, at længere og mere detaljerede specifikationer altid vil være hjælpsomme eller nødvendige for den registrerede, men vil i nogle situationer have den modsatte effekt⁵⁶. Præcisionen af formål skal være formuleret på sådan en måde, at det vil blive forstået på samme måde af den dataansvarlige og den registrerede⁵⁷. Det kan udledes, at eksemplet med 'kunstig intelligens-relaterede formål' nævnt ovenfor ikke vil give den samme forståelse hos udvikleren og den registrerede og derfor ikke overholde den nødvendige præcision. Det er ikke kun Big Data i sig selv, som nævnt ovenfor, der besværliggør formålsbeskrivelsen for udviklere af kunstig intelligens, men også at præcisere selve behandlingsprocessen, der sker i Deep Learnings neurale netværk, jf. beskrivelsen i "Deep Learning og neurale netværk"-afsnittet. Denne tekniske problemstilling vedrørende at forklare behandlingsprocesserne er kort forklaret i "Black Box"-afsnittet, og den juridiske problemstilling i forhold til gennemsigtighed og forklarlighed vil blive gennemgået i kapitel 4.

Der er bevidst i ovenstående gennemgang blevet brugt formål i flertal, da GDPR tager højde for og tillader dette, hvilket også fremgår af ordlyden af artikel 5, stk. 1, litra b, samt præambelbetragtning 32 og 50⁵⁸. Denne tilgang tilfredsstiller kravet om den nødvendige pragmatisme og fleksibilitet i forhold til den komplekse og foranderlige behandling af personoplysninger i den digitale tidsalder⁵⁹. I nogle tilfælde vil formålene være sammenlignelige, men i andre situationer slet ikke. Det er muligt i scenariet med sammenlignelige formål at have en overordnet formålsbeskrivelse, men det vil afhænge af en konkret vurdering, hvorvidt det

⁵⁶ Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, side 16

⁵⁷ Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, side 17

⁵⁸ EU-forordningen 2016/679, artikel 5, stk. 1, litra b, samt præambel 32 og 50

⁵⁹ Forslag til afgørelse fra generaladvokat P. Pikamäe sag: C-77/21, præmis 40

vurderes, at formålene er sammenlignelige⁶⁰. Det vil stadig være nødvendigt for at overholde kravet om udtrykkeligt angivne formål, at de sammenlignelige formål, der defineres i sammenhæng med hovedformålet, stadig er præcise nok defineret, så den registrerede er i stand til på et oplyst grundlag at forstå databehandlingen og tage et informeret valg.

Det er, som ovenfor forklaret, nødvendigt udtrykkeligt at angive formål med behandlingen, men det følger også EU-retspraksis, at *"formålene med behandlingen skal identificeres senest ved indsamlingen af personoplysninger"*⁶¹. Dette krav kan være yderst besværlig for udviklere af kunstig intelligens, da formålet i starten af udviklingsfasen sagtens kan ændre sig i løbet af den kunstige intelligens' udviklingsfase i sammenhæng med, at den lærer af sine egne beslutninger. Dette vil blive gennemgået yderligere i "Viderebehandling og forenelighed"-afsnittet.

Legitime formål

GDPRs artikel 5, stk. 1, litra b lyder som følgende: *"[Personoplysninger skal] indsamles til udtrykkeligt angivne og **legitime formål** og må ikke viderebehandles på en måde, der er uforenelig med disse formål;..."*⁶². Ordlyden her skal ikke forveksles med den retlige standard 'lovlighed' beskrevet i "God databehandlingsskik"-afsnittet, men lægger sig meget tæt op af. Tidligere stod beskrevet, hvordan selve behandlingen og indsamlingen skulle være lovlig, og her ses, som tidligere forklaret, hvordan GDPR konkretiserer de retlige standarder i form af, at GDPR skriver, at formålet skal være legitimt. Kravet her går, ligesom den retlige standard, længere end en simpel sammenligning med belægget for lovlig behandling i artikel 6. Det er dog stadig et krav, for at formålet er legitimt, at behandlingen er baseret på en af de legale behandlingsgrundlag i artikel 6, men at kravet om formålets legitimitet er bredere end artikel 6. Det kræves, at formålet skal være i overensstemmelse med alle andre bestemmelser af gældende databeskyttelsesret og anden gældende lovgivning såsom ansættelse, kontrakt, forbrugerbeskyttelse osv. Derudover dækker det brede omfang også alt skreven og almindelig ret, primær og sekundær lovgivning, grundlæggende rettigheder, andre juridiske principper og retspraksis⁶³.

⁶⁰ Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, side 16

⁶¹ EU-Domstolens sag: C-77/21, præmis 27

⁶² EU-forordningen 2016/679, artikel 5, stk. 1, litra b

⁶³ Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, side 19f

Dette afsnit er separat fra det ovenstående "Udtrykkeligt angivne formål"-afsnit, men som angivet i "Formålsbestemthedsprincippet"-afsnittet angiver retspraksis dem i sammenhæng, når de benævnes. Denne opbygning er valgt af analytiske årsager og for overblikkets skyld, men delkonklusionen her vil i stedet sammenkoble de to, da de i sagens natur hører tæt sammen og fortolkes mest præcis i sammenhæng. Det kan udelades af dette afsnit, at formålet for at overholde legitimitetskravet skal være i overensstemmelse med alt relevant regulering og lovgivning både i form af GDPR og andet. Sammenkobles det med, at det også skal være 'udtrykkeligt angivne formål', er det nødvendigt, at formålet er saglig og velbegrundet i henhold til de konkrete omstændigheder, samt præcist nok defineret, så den registrerede er i stand til på et oplyst grundlag at forstå databehandlingen og tage et informeret valg.

Kravene til den oprindelige indsamling og behandling af den registreredes data i forhold til formålsbegrænsning er nu gennemgået, og de kommende afsnit vil analysere muligheden for viderebehandling. Dette er yderst interessant for udviklere af kunstig intelligens, da det, som benævnt tidligere i "Udtrykkeligt angivne formål"-afsnittet, ofte vil være tilfældet, at formålet vil ændre sig i løbet af udviklingsfasen af kunstig intelligens.

Viderebehandling og forenelighed

GDPRs artikel 5, stk. 1, litra b lyder som følgende: "*[Personoplysninger skal] indsamles til udtrykkeligt angivne og legitime formål og må **ikke viderebehandles** på en måde, der er **uforenelig med disse formål**;...*"⁶⁴. Det er nødvendigt først at fastslå, hvornår der foreligger en 'viderebehandling'. Artikel 29-arbejdsgruppen angiver, at alle processor efter indsamlingen uden at tage forbehold for, om det var det oprindelige formål eller understøttende formål, skal opfattes som 'viderebehandling'⁶⁵. Denne fortolkning følger EU-domstolen også i praksis, da de angiver, at 'viderebehandling' i sædvanlig sprogbrug udgør enhver behandling af personoplysninger, der sker efter den oprindelige behandling, uafhængigt af formålet med viderebehandlingen⁶⁶. Det kan derfor udledes, at enhver behandling efter den oprindelige indsamling vil udgøre en 'viderebehandling', og det er derfor relevant at fokusere på, hvornår de efterfølgende behandlinger vil være 'uforenelige' med det oprindelige formål.

⁶⁴ EU-forordningen 2016/679, artikel 5, stk. 1, litra b

⁶⁵ Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, side 21

⁶⁶ EU-Domstolens sag: C-77/21, præmis 31

I stedet for at pålægge krav om 'forenelighed', har lovgiverne af GDPR valgt at forbyde 'uforenelighed'. Den fastslår, at viderebehandling er lovligt, så længe den ikke er uforenelig og overholder kravene til lovlighed, hvilket viser, at hensigten bag GDPR er at give en vis form for fleksibilitet⁶⁷. Denne tankegang stemmer overens med den tilgang vedrørende flere formål beskrevet i "Udtrykkeligt angivne formål"-afsnittet. Det betyder, at selvom viderebehandlingen i nogle situationer vil tjene et andet formål, betyder det ikke vice versa, at den er uforenelig. Denne fleksibilitet afspejler hensynet til de dataansvarlige og samfundet, da der kan være situationer, hvor den dataansvarlige ikke ved specificeringen af det oprindelige formål kunne forudse, at yderligere formål ville være nødvendige, hvis det viste sig, at dataene kunne være nyttige til andre formål⁶⁸. Det er dog stadig nødvendigt, at det modsatte hensyn til den registrerede i form af grundlæggende garanti for forudsigelighed og retssikkerhed, som beskrevet i "Udtrykkeligt angivne formål"-afsnittet, er taget i betragtning, når disse situationer vurderes.

Artikel 29-arbejdsgruppen betegner vægtningen af disse hensyn som en forenelighedstest, hvor det er nødvendigt at kigge på den konkrete situation og hver enkelt behandling hver for sig⁶⁹. Artikel 5, stk. 1, litra b i GDPR indeholder ikke nogen angivelser om, hvilke betingelser en viderebehandling skal overholde for at være forenelig med det oprindelige formål, men det er i stedet nødvendigt at kigge på den sammenhæng, hvori bestemmelsen indgår, da det giver nogle nyttige præciseringer⁷⁰. Sammenholdes artikel 5, stk. 1, litra b med artikel 6, stk. 1, litra a og artikel 6, stk. 4 i GDPR, kan det udledes, at problemstillingen i forhold til forenelighed kun opstår, hvor formålene med viderebehandlingen ikke er identiske med formålene for den oprindelige indsamling⁷¹.

"Det fremgår desuden af denne artikel 6, stk. 4, sammenholdt med 50. betragtning til nævnte forordning, at når behandlingen til et andet formål end det, hvortil oplysningerne blev indsamlet, ikke er baseret på den registreredes samtykke eller EU-retten eller en medlemsstats lovgivning, skal der ved afgørelsen af, om behandlingen til et andet formål er forenelig med det formål, hvortil personoplysningerne oprindeligt blev indsamlet, bl.a. tages hensyn til, for det første

⁶⁷ Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, side 21

⁶⁸ Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, side 21

⁶⁹ Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, side 21

⁷⁰ EU-Domstolens sag: C-77/21, præmis 32 og 33

⁷¹ EU-Domstolens sag: C-77/21, præmis 34

om der foreligger en eventuel forbindelse mellem formålet med indsamlingen af personoplysningerne og formålet med den påtænkte viderebehandling, for det andet den sammenhæng, hvori personoplysningerne er blevet indsamlet, navnlig hvad angår forholdet mellem de registrerede og den dataansvarlige, for det tredje personoplysningernes art, for det fjerde den påtænkte viderebehandlings mulige konsekvenser for de registrerede, og endelig for det femte tilstedeværelsen af fornødne garantier både inden for rammerne af den oprindelige behandling og den påtænkte viderebehandling”⁷².

Dette lange citat fra EU-Domstolen lægger sig meget tæt op ad ordlyden af artikel 6, stk. 4 i GDPR. Der blev lige ovenfor nævnt artikel 29-arbejdsgruppens forenelighedstest. Som forklaret i ”Metodik og retskilder”-afsnittet, er denne gruppes vejledninger baseret på det gamle direktiv og ikke GDPR. Det er dog tydeligt, at både artikel 6, stk. 4 i GDPR og EU-Domstolens fortolkning af den, er udtryk for den samme juridiske fortolkning af ’forenelighed’. Den nedenstående analyse af forenelighed vil inddrage artikel 29-arbejdsgruppens vejledning i forhold til forenelighed de steder, hvor EU-Domstolen overlader fortolkningen til den nationale domstol, da dette speciale ikke inkluderer national rets fortolkning af EU-ret. Selvom dette kapitel fokuserer på artikel 5 i GDPR, inddrages artikel 6, stk. 4, da som beskrevet lige ovenfor, da den angiver de præciseringer, der er nødvendig for at kunne forstå den sammenhæng artikel 5, stk. 1, litra b indgår i. Der vil dog ikke blive fokuseret på første del af citatet, det angivet inden hensynene, da det ikke er relevant for dette speciales problemformulering, men udelukkende er hensynene til at forstå forenelighed der inddrages.

Det første hensyn ”... om der foreligger en eventuel forbindelse mellem formålet med indsamlingen af personoplysningerne og formålet med den påtænkte viderebehandling...”⁷³, hvilket også fremgår af artikel 6, stk. 4, litra a i GDPR, henviser ikke kun til den konkrete tekstuelle sammenligning mellem det oprindelige formål og viderebehandlingsformålet. Det fokuserer mere på substansen af forholdet mellem det oprindelige formål og viderebehandlingsformålet⁷⁴. For udviklere af kunstig intelligens vil det oprindelige formål måske ikke ligge tekstuel tæt op ad viderebehandlingsformålet, men det vil i nogle situationer være muligt at vise, at substansen er

⁷² EU-Domstolens sag: C-77/21, præmis 35

⁷³ EU-Domstolens sag: C-77/21, præmis 35

⁷⁴ Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on purpose limitation, side 24

sammenlignelig. Kravet til sammenlignelig substans stiger dog også i sammenhæng med, hvor forskelligt de to formål er. Et tænkt scenarie vil være, hvor det oprindelige formål er udvikling af kunstig intelligens (her tages ikke forbehold for præcisionskravet benævnt i ”Udtrykkeligt angivne formål”-afsnittet). Herefter ønsker udviklere af kunstig intelligens senere i processen at gentræne den allerede færdigudviklede algoritme på de oprindelige personoplysninger, der var indsamlet. Her vil det for viderebehandlingsformålet, altså at gentræne algoritmen, være nødvendigt at substansen af de to formål er forenelige. At påvise den nødvendige forenelighed i forhold til substans vil teknisk kunne lade sig gøre, som også vist i det ovenstående, simplificerede scenarie, men vil også ændre sig løbende i takt med den teknologiske udvikling og menneskers forståelse for kunstig intelligens. Dette kommer til udtryk i hensynet i artikel 6, stk. 4, litra b og hænger sammen med ”...den sammenhæng, hvori personoplysningerne er blevet indsamlet, navnlig hvad angår forholdet mellem de registrerede og den dataansvarlige...”⁷⁵ Her vil det være en konkret afvejning, der også tager udgangspunkt i den registreredes legitime forventning til den senere anvendelse af deres personoplysninger⁷⁶. Det er dog også nødvendigt at udviklere af kunstig intelligens forholder sig til, i hvilken kontekst de oprindelige personoplysninger var indsamlet, og tager forbehold for magtforholdet mellem den registrerede og dataansvarlige⁷⁷. Det vil, hvis udviklere af kunstig intelligens gør brug af Big Data, ofte være situationen, at de registrerede er meget svagt stillet i magtforholdet. Hensynet opstiller dog en skønsafvejning, hvori der også skal tages forbehold for vanlig og almindelig praksis i det givne forhold mellem registrerede og dataansvarlig⁷⁸. Det må dog udledes, at magtforholdet mellem de registrerede og dataansvarlige i kontekst af Big Data ikke kan forsvares på vanlig og almindelig praksis. Det må også udledes, at i den nuværende tidsalder vil udviklere af kunstig intelligens efter en skønsafvejning og den konkrete situation have svært ved at påvise forenelighed i henhold til disse to hensyn. Det skal dog fremhæves, at der her fortolkes hensyn, og det er en helhedsvurdering, hvor hver enkelt hensyn inddrages og vægtes i forhold til formålet. Denne diskussion vil blive gennemgået nedenfor efter at de resterende hensyn er fortolket.

⁷⁵ EU-Domstolens sag: C-77/21, præmis 35

⁷⁶ EU-Domstolens sag: C-77/21, præmis 44

⁷⁷ Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, side 24

⁷⁸ Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, side 24

Det tredje hensyn "*...personoplysningernes art...*"⁷⁹ og det fjerde hensyn "*...den påtænkte viderebehandlings mulige konsekvenser for de registrerede...*"⁸⁰ omhandler, hvorvidt der for eksempelvis er snak om personfølsomme oplysninger og mulige skadelige konsekvenser for de registrerede. Personoplysningernes art spiller en central rolle i GDPR, og hvis der behandles personfølsomme oplysninger, vil dette også medføre en indsnævring af omfanget af forenelighed. Den yderligere beskyttelse gælder ikke kun personfølsomme oplysninger, men også for personoplysninger vedrørende registrerede så som børn, psykisk sygdom eller lignende, som efter GDPR har et højere beskyttelsesniveau⁸¹. En sammenkobling af de to er derfor valgt i analysen, da de mulige skadelige konsekvenser ofte hænger sammen med personoplysningers art. Det følger af GDPRs andre bestemmelser, at der er andre strenge krav og sikkerhedsmekanismer, der skal tages forbehold for ved forskellige personoplysninger, som eksempelvis personfølsomme oplysninger som nævnt lige ovenfor, men det er altså ikke nok for udviklere af kunstig intelligens kun at iagttage disse bestemmelser. Det vil også være nødvendigt at overveje disse to hensyn i henhold til fastsættelsen af ikke-uforenelig viderebehandling. Disse nødvendige overvejelser viser det komplicerede sammenspil, der ligger i at overholde ikke kun GDPRs fastlagte bestemmelser, men også de bagvedliggende hensyn i de mere uklare bestemmelser. I forhold til at vurdere skadevirkningen af viderebehandlingen skal der både tages forbehold for positive og negative konsekvenser⁸². Et eksempel på dette kunne være i den situation, hvor en algoritme bruges til profilering eller til automatiske afgørelser, hvorefter GDPRs artikel 22 vil finde anvendelse. Antages det, at udviklere af kunstig intelligens i det oprindelige formål og i deres udvikling har lavet en lovlig behandling af personfølsomme oplysninger, betyder det ikke, når viderebehandlings forenelighed vurderes, at selve viderebehandlingen tager hensyn til konsekvenserne. Algoritmen, som tidligere forklaret i kapitel 2, baserer sit output på, hvilke data den er blevet trænet på, og hvilket input den modtager. Der vil være situationer, hvor dens output kan have en diskriminerende karakter på baggrund af dens behandlingsproces. Profilering og automatiske afgørelser og hele problemstillingen vedrørende dette inddrages ikke, men er her taget med i kort form for at belyse, hvordan for eksempel en algoritme ville kunne have positive konsekvenser for

⁷⁹ EU-Domstolens sag: C-77/21, præmis 35

⁸⁰ EU-Domstolens sag: C-77/21, præmis 35

⁸¹ Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, side 25

⁸² Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, side 25

bestemte registrerede, men modsatvist også ville kun få negative konsekvenser for andre. Det kan derfor udledes, at udviklere af kunstig intelligens, for at efterleve disse to hensyn og for ikke at lave en uforenelig viderebehandling, vil være tvunget til at kunne forklare, hvordan algoritmens beslutninger både har negative og positive konsekvenser for de registrerede.

Det sidste hensyn "*...tilstedeværelsen af fornødne garantier både inden for rammerne af den oprindelige behandling og den påtænkte viderebehandling*"⁸³ hænger også tæt sammen med det fjerde hensyn beskrevet lige ovenfor, da det er omfanget af disse garantier, der kan have en stor betydning i forhold til, hvilke konsekvenser det vil have for den registrerede. Artikel 6, stk. 4, litra e nævner selv kryptering og pseudonymisering som potentielle sikkerhedsgarantier⁸⁴. Især inden for kunstig intelligens er pseudonymisering et oplagt valg, da outputtet ofte ikke tager højde for, hvorvidt dataene er pseudonymiseret eller ej. Der foreligger også muligheden for brugen af aggregerede data i sammenkobling med pseudonymisering. Begreberne pseudonymisering og aggregerede data og især tilgangen, at risikoen for den registrerede vil være væsentlig lavere og håndhævelsen af bestemmelserne være mere fleksible, hvis pseudonymisering foretages, er beskrevet i "Anonymisering, pseudonymisering og aggregerede data"-afsnittet. Modsatvis vil det også betyde, at hvis udviklere af kunstig intelligens ikke gør brug af nogle af de ovennævnte metoder, vil der kunne være tale om tilsidesættelse af hensynet, og der vil ikke være tilstedeværelse af fornødne garantier. Det understreger også vigtigheden af, at udviklere af kunstig intelligens især fokuserer på dette hensyn, da de andre hensyn, som tidligere beskrevet, kan være svære at leve fuldstændig op til. Artikel 29-arbejdsgruppen pointerer, at en fundamental karakteristik ved sådan en helhedsvurdering, der skal foretages i forhold til forenelighed, er, at mangler ved nogle hensyn kan kompenseres ved bedre præstation i andre hensyn. Det er ikke kun i forhold til de andre hensyn, men også generelt i de situationer, hvor det oprindelige formål måske har været lidt upræcist beskrevet, eller der har været ændring af formålet⁸⁵.

⁸³ EU-Domstolens sag: C-77/21, præmis 35

⁸⁴ EU-forordningen 2016/679, artikel 6, stk. 4, litra e

⁸⁵ Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, side 26

Opsamling på viderebehandling og forenelighed

Der er i dette afsnit blevet præsenteret 5 hensyn, der alle indgår i den konkrete vurdering af viderebehandlingens forenelighed. Det er vigtigt at understrege, at de hensyn i artikel 6, stk. 4 litra a-e i sammenhæng med præambelbetragtning 50 ikke er de eneste hensyn, en udvikler af kunstig intelligens skal tage, da den bestemmelse bruger beskrivelsen "bl.a.". Der er dog igennem denne analyse blevet inddraget relevante vejledninger fra artikel 29-arbejdsgruppen og retspraksis fra EU-Domstolen, og der foreligger endnu ikke et eksempel på et andet konkret hensyn. Det er dog vigtigt at pointere, at imens teknologi, især her kunstig intelligens, samfundet og forretningspraksis udvikler sig, vil nogle af hensynene blive mere vigtige, mens andre vil blive mindre vigtige⁸⁶. Dette kan allerede formodes at være tilfældet i forhold til fornødne garantier, da kravet til disses beskyttelsesbarriere stiger i takt med, at muligheden for at bryde dem bliver lettere. For det andet er det vigtigt at nævne, at disse hensyn er kumulative, og det er en overordnet konkret vurdering, hvor hver enkelt hensyn inddrages, eller udelades, samt vægtes i forhold til relevans, der danner baggrund for viderebehandlingens forenelighed. Det kan derfor udledes, at selvom, som beskrevet ovenfor, at udviklere af kunstig intelligens vil have svært ved at tage nogle af de nødvendige hensyn, kan eksempelvis tilstedeværelsen af fornødne garantier godt pege i den anden retning i helhedsvurderingen. GDPRs valg af ordlyden "hensyn" bevirker også, at det ikke er et enten-eller-spørgsmål, om de dataansvarlige har taget hensyn, men en fortolkning af, om de har taget de nødvendige "hensyn", og om de hver især kan have forskellig relevans i den konkrete situation. Det er hensynet til de dataansvarlige og samfundet vægtet op imod de registreredes grundlæggende garanti for forudsigelighed og retssikkerhed, der overordnet set tages i betragtning i de konkrete situationer. Til sidst skal det nævnes, at GDPRs valg om at definere, at viderebehandling ikke må være uforenelig med formålet, i stedet for at den skal være forenelig, kombineret med ovenstående i forhold til hensyn, tydeliggør at bestemmelsen måske ikke er så restriktiv, som det ville kunne antages. Med den manglende retspraksis på området og EU-Domstolens hjemsendelse til national ret i forhold til vurderingen om forenelighed i sagen C-77/21⁸⁷ er det dog ikke muligt at give et helt klart billede af, hvordan disse hensyn skal fortolkes i en konkret situation. EU-Domstolen og artikel 29-arbejdsgruppens vejledning giver dog en regelforståelse af principperne i GDPR, og på hvilken måde de skal anvendes. Det er dog, som nævnt ovenfor, desværre ikke muligt

⁸⁶ Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, side 27

⁸⁷ EU-Domstolens sag: C-77/21, præmis 44 og 45

at give et eksempel på en konkret vurdering med den ovenstående gennemgangs regelforståelse, da specialet udelukkende beskæftiger sig med regelforståelsen og ikke den direkte anvendelse i de nationale domstole.

Undtagelser til formålsbegrænsning

Ovenstående gennemgang af, hvorvidt der foreligger ikke uforenelig viderebehandling, kan det helt undgås at tage højde for, i henhold til sidste del af GDPRs artikel 5, stk. 1, litra b, der siger ”

*[Personoplysninger skal] indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; **viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål.***⁸⁸. Der er, som beskrevet i ”Formålsbestemthedsprincippet”-afsnittet, direkte i

bestemmelsen fire undtagelser til kravet om forenelighed. De er, som også citeret lige ovenfor, for det første arkivformål i samfundets interesse, for det andet videnskabelige formål, for det tredje historiske formål og for det fjerde statistiske formål. Disse fire formål skal dog være i overensstemmelse med GDPRs artikel 89, stk. 1. Artikel 89, stk. 1 foreskriver, at de fire formål ”... skal være underlagt fornødne garantier for registreredes rettigheder og frihedsrettigheder i overensstemmelse med denne forordning. Disse garantier skal sikre, at der er truffet tekniske og organisatoriske foranstaltninger, især for at sikre overholdelse af princippet om dataminimering...⁸⁹”. Princippet om dataminimering vil blive gennemgået i ”Princippet om dataminimering”-afsnittet. Det vil, hvis formålet er en af de fire ovenstående, og databehandlingen indeholder de fornødne garantier, være muligt for udviklere af kunstig intelligens at overholde kravet om formålsbegrænsning og foretage en lovlig viderebehandling, selvom den i henhold til hensynene beskrevet i ”Viderebehandling og forenelighed”-afsnittet, ville have været uforenelig. Fornødne garantier og forståelsen af dem er beskrevet i ”Viderebehandling og forenelighed”-afsnittet vedrørende tilstedeværelsen af fornødne garantier. Den kommende gennemgang fokuserer i stedet på undtagelserne i henhold til formålsdefinitionen med fokus på videnskabelige forskningsformål og statistiske formål. Viderebehandling til arkivformål og historiske

⁸⁸ EU-forordningen 2016/679, artikel 5, stk. 1, litra b

⁸⁹ EU-forordningen 2016/679, artikel 89, stk. 1

forskningsformål har ikke et nært tilknytningsforhold til kunstig intelligens og udlades derfor fra gennemgangen. Det er her nødvendigt at kigge på de relevante præambelbetragtninger⁹⁰.

Præambelbetragtning 157 til GDPR beskriver, hvordan videnskabelig forskning kan levere solid viden af høj kvalitet, der kan danne grundlag for forbedret livskvalitet og effektivitet af sociale tjenester. Der er især fokus på registre og muligheden for at viderebehandle personoplysninger fra disse til at opnå afgørende viden⁹¹. Sidste sætning i præambelbetragtningen skriver *"For at fremme videnskabelig forskning kan personoplysninger behandles til videnskabelige forskningsformål under iagttagelse af passende betingelser og garantier i EU-retten eller medlemsstaternes nationale ret."*⁹². Det er her vigtigt at understrege, at der udelukkende fokuseres på formålsbegrænsning, og når personoplysninger behandles til videnskabelige forskningsformål, finder GDPRs andre bestemmelser stadig anvendelse på denne behandling⁹³. Det fremgår af Præambelbetragtning 159, at *"... Behandlingen af personoplysninger til videnskabelige forskningsformål bør med henblik på denne forordning fortolkes bredt og f.eks. omfatte teknologisk udvikling og demonstration, grundforskning, anvendt forskning og privat finansieret forskning..."*⁹⁴. Det vil være en konkret vurdering i hver enkelt sag, men udviklere af kunstig intelligens, der især udvikler algoritmer inden for sundhedssektoren, vil kunne argumentere for, at deres forskning og udvikling vil kunne danne grundlag for forbedret livskvalitet og effektivitet af sociale tjenester, som nævnt ovenfor. Det fremgår også af præambelbetragtning 33, at *"Det er ofte ikke muligt fuldt ud at fastlægge formålet med behandling af personoplysninger til videnskabelige forskningsformål, når oplysninger indsamles. De registrerede bør derfor kunne give deres samtykke til bestemte videnskabelige forskningsområder, når dette er i overensstemmelse med anerkendte etiske standarder for videnskabelig forskning. Registrerede bør have mulighed for kun at give deres samtykke til bestemte forskningsområder eller dele af forskningsprojekter i det omfang, det tilsigtede formål tillader det"*⁹⁵. Sammenkobles disse betragtninger, kan det udledes, at der er et vist spillerum for udviklere af kunstig intelligens til at viderebehandle personoplysninger, hvis formålet er videnskabelig forskning. Eksemplet ovenfor i forhold til sundhedssektoren er specifikt valgt, da det

⁹⁰ Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, side 28

⁹¹ EU-forordningen 2016/679, præambel 157

⁹² EU-forordningen 2016/679, præambel 157

⁹³ EU-forordningen 2016/679, præambel 159

⁹⁴ EU-forordningen 2016/679, præambel 159

⁹⁵ EU-forordningen 2016/679, præambel 33

fremgår af ordlyden af de inddragne præambelbetragtninger, at især denne form for videnskabelig forskning skal kunne tillades. Ordlyden af præambelbetragtninger sammenkoblet med det formål, de vægtes op imod, giver en klar indikation af, at det især også er samfundets interesse i denne videnskabelige forskning, der vil indgå i helhedsvurdering. De angiver direkte, at videnskabelige forskningsformål skal fortolkes bredt i ovenstående citat fra præambelbetragtning 159, men det kan udledes, at der her fokuseres mest på den tekniske form af forskning. Der er altså, som nævnt i henhold til præambelbetragtninger, et stort spillerum, men det må pointeres, at der mest fokuseres på ovenstående, nævnte typer af videnskabelig forskning. Det er ikke muligt at lave en direkte modsat konklusion og sige, at andre former for videnskabelig forskning, der ikke er inden for sundhedssektoren og i samfundets interesse, vil falde uden for ordlyden af videnskabelige forskningsformål i artikel 5, stk. 1, litra b i GDPR. Det giver dog, ud fra en ordlyds- og formålsfortolkning og ovenfor gennemgået analyse, et klart billede af, hvilke former for videnskabelig forskning, der giver den største adgang til undtagelsen om uforenelig viderebehandling.

Det andet formål, som er centralt for udviklere af kunstig intelligens og undtager dem for kravet om forenelighed, er Præambelbetragtning 162, der skriver følgende: *"... EU-retten eller medlemsstaternes nationale ret bør inden for rammerne af denne forordning fastsætte statistisk indhold, adgangskontrol, præciseringer for behandling af personoplysninger til statistiske formål og passende foranstaltninger til at beskytte den registreredes rettigheder og frihedsrettigheder og sikre statistisk fortrolighed. Ved statistiske formål forstås enhver indsamling og behandlingen af personoplysninger, der er nødvendig for statistiske undersøgelser eller frembringelse af statistiske resultater. Disse statistiske resultater kan videreanvendes til forskellige formål, herunder videnskabelige forskningsformål...⁹⁶".* Præambelbetragtningen angiver begreb definitionen på statistiske formål, men overlader i først del af det indsatte citat kompetencen til at udfylde den yderligere begrebsforståelse til EU-retten og national ret. Den beskriver derefter, at *"... Det statistiske formål indebærer, at resultatet af behandling til statistiske formål ikke er personoplysninger, men aggregerede data, og at dette resultat eller personoplysningerne ikke anvendes til støtte for foranstaltninger eller afgørelser, der vedrører bestemte fysiske personer.⁹⁷".*

⁹⁶ EU-forordningen 2016/679, præambel 162

⁹⁷ EU-forordningen 2016/679, præambel 162

Det er altså et direkte krav for at leve op til undtagelsen vedrørende statistiske formål, at resultatet er aggregerede data og ikke personoplysninger. Begrebet aggregerede data er beskrevet i "Anonymisering, pseudonymisering og aggregerede data"-afsnittet, hvor der også beskrives, hvordan der findes forskellige former og niveauer af at aggregere data. Ordlyden af præambelbetragtningen er dog ikke klar i forhold til, hvilket omfang af at aggregere data der er nødvendigt, men bare at resultatet skal være aggregerede data. Dette er lidt tvetydigt og misvisende, da aggregerede data, som forklaret i "Anonymisering, pseudonymisering og aggregerede data"-afsnittet, med forbehold for metoden stadig vil være at definere som personoplysninger i forhold til GDPR, hvis ikke de rigtige anonymiserings- og pseudonymiseringmetoder er brugt i sammenhæng med aggregeringen. Dette skal ses i sammenhæng med, at undtagelsen skal være i overensstemmelse med artikel 89 i GDPR i forhold til fornødne garantier. Det må derfor udledes fra en ordlydsfortolkning i henhold til formålet med undtagelsen, at lovgivers hensigt har været, at resultatet ikke må indeholde personoplysninger, der er direkte eller indirekte henførbare til en fysisk person i GDPRs forstand, men skal være aggregerede data med fornødne garantier. Det vil her få en direkte konsekvens, hvilken form for og effektivitet af aggregering der er foretaget af udviklere af kunstig intelligens. I forhold til kunstig intelligens vil det dog ofte ikke have betydning for algoritmen, hvorvidt der er brugt aggregerede data, og algoritmen vil stadig være i stand til at behandle dataene, hvis der foreligger et højt niveau af aggregering. Det er også vigtigt at understrege sidste del af citat vedrørende bestemte fysiske personer. Vil det statistiske formål være, at den kunstige intelligens bliver trænet til i sit output at generere foranstaltninger eller afgørelser i forhold til bestemte personer, vil den ikke leve op til denne undtagelse om formålsbegrænsning.

Ovenstående gennemgang viser, at der for udviklere af kunstig intelligens foreligger muligheder for at kunne leve op til undtagelsen i sidste led af artikel 5, stk. 1 litra b i GDPR om uforenelig viderebehandling. Det vil være en konkret helhedsvurdering, men det tekniske grundlag en kunstig intelligens bygges på vil i flere tilfælde, med de ovenfor nævnte formål, være i stand til at leverer de fornødne garantier, nævnt i artikel 89 i GDPR for de registrerede, og vil være i stand til igennem disse garantier at levere de nødvendige tekniske og organisatoriske foranstaltninger, der sikrer de registreredes rettigheder. Dette afhænger, som beskrevet ovenfor, af valget af pseudonymisering og aggregering, og vil være en konkret helhedsvurdering af de implementerede foranstaltninger. Til

sidst skal nævnes, at den ovenstående gennemgang kun vedrører undtagelsen til uforenelighed i forhold til formålsbegrænsning og som nævnt flere gange i ovenstående fritager dette ikke udviklere af kunstig intelligens for at overholde de retlige standarder og andre relevante bestemmelser i GDPR. Artikel 89 i GDPR foreskriver, at de fornødne garantier især skal sikre overholdelse af dataminimeringsprincippet, som bliver analyseret i ”Princippet om dataminimering”-afsnittet.

Princippet om dataminimering

Artikel 5, stk. 1, litra c lyder som følger: ” *[Personoplysninger skal] være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles*

*(»dataminimering«)*⁹⁸. Det fremgår af ordlyden, at der foreligger tre kumulative betingelser, der skal være nødvendige i forhold til formålet. En direkte ordlydsfortolkning af ’betingelserne’ som ’tilstrækkelig, relevante og begrænset’ til vil dog ikke være retvisende, da de, som beskrevet ovenfor, skal sættes i perspektiv til, hvad der er nødvendigt i forhold til formålet. Det centrale er her, hvad der ligger i begrebet ’nødvendigt’, og om ordlyden af begrebet er ens i alle bestemmelser i GDPR. Begrebet ’nødvendigt’ optræder flere steder i GDPR, hvor reglers anvendelse gøres betinget af nødvendighed, og dette medfører en usikker åbenhed. Denne form for regulering er især repræsenteret i artikel 6 i GDPR, der definerer behandlingsbetingelserne, undtaget artikel 6, stk. 1, litra a vedrørende samtykke. Artikel 6, stk. 1, litra b-f knytter alle deres indhold til nødvendighed i forhold til en bestemt materiel betingelse, som for eksempel at det er i samfundets interesse eller legitim interesse. Begrebet er ikke legaldefineret, og det kan ikke fortolkes, at det altid vil have den samme betydning, da nødvendighed er situationsbestemt og refererer til forskellige aspekter af persondatabehandlingen⁹⁹. Den ovenstående inddragelse af artikel 6 i GDPR vil blive brugte igennem analysen i dette afsnit, da behandlingen af personoplysninger i overensstemmelse med princippet om dataminimering i artikel 5, stk. 1, litra c ikke tilsiger at indføre et generelt og absolut forbud, men åbner op for, at det er nødvendigt, at videregive personoplysninger til for eksempel offentligheden, når denne videregivelse er nødvendig af hensyn til udførelse af en opgave i samfundets interesse, som omhandlet i artikel 6, stk. 1, litra e¹⁰⁰. Det er

⁹⁸ EU-forordningen 2016/679, artikel 5, stk. 1, litra c

⁹⁹ Blume, Peter – *Persondatarettens kilder og metoder*, side 93

¹⁰⁰ EU-Domstolens sag: C-439/19, præmis 104

altså ikke muligt i forhold til nødvendighed nævnt i artikel 5, stk. 1, litra c at iagttage denne isoleret, så man må kigge på den sammenhæng, hvori den bruges. Den ovenfor nævnte tilgang, hvor der ikke fokuseres på ordlyden af de tre betingelser nævnt i artikel 5, stk. 1, litra c bygger på EU-Domstolens retspraksis. EU-Domstolen angiver, at artikel 5, stk. 1, litra c er udtryk for proportionalitetsprincippet¹⁰¹, hvilket også vil blive belyst i denne analyse. *”Det fremgår af fast retspraksis, at proportionalitetsprincippet som et generelt EU-retligt princip kræver, at de foranstaltninger, som iværksættes ved en EU-retsakt, skal være egnede til at nå det tilsigtede mål og ikke må gå ud over, hvad der er nødvendigt for at nå det”*¹⁰². Proportionalitetsprincippet har ikke været inddraget i specialet endnu, da det har været antaget, at læseren er indforstået med princippet, og da det ikke er fokus for besvarelsen af problemformuleringen. Det bliver dog inddraget her, da det, som tydeliggjort ovenfor, udfylder og beskriver forståelsen af dataminimering. Det vil ikke være en konkret fortolkning og diskussion af selve princippet, men af den rolle, det spiller, i forhold til artikel 5, stk. 1, litra c.

Det tidligere nævnte valg fra EU-Domstolens side i at fastlægge, at artikel 5, stk. 1, litra c er udtryk for proportionalitetsprincippet bevirker, at artiklen fortolkes ud fra egnethed og nødvendighed, som forstået i proportionalitetsprincippet. Hvorvidt formålene er egnede til at opnå formålet, er en konkret vurdering, men det interessante er, at artiklen bruger begreberne ’tilstrækkelige’ og ’relevante’, men at retspraksis ikke medtager disse begreber, men udelukkende fortolker ud fra begrebet ’egnethed’ i henhold til proportionalitetsprincippet. Der bliver i stedet fokuseret på nødvendighed. Det skal i denne forbindelse, som også nævnt ovenfor, bemærkes, at beskyttelse af personoplysninger ikke er absolutte rettigheder, men skal ses i sammenhæng og vurderes i forhold til deres funktion i samfundet¹⁰³. Det er derfor navnlig nødvendigt at efterprøve, om hensyn til alvoren af det indgreb i retten til beskyttelse af personoplysninger er begrundet og navnlig forholdsmæssig, med henblik på at nå de forfulgte mål¹⁰⁴. Det vil altså være nødvendigt at foretage en rimelig afvejning af de forskellige interesser, der er til stede. EU-Domstolen inddrager også præambelbetragtning 39 til GDPR, der beskriver, at nødvendighedskravet ikke er opfyldt, hvis det

¹⁰¹ EU-Domstolens sag: C-439/19, præmis 98 og heri nævnt retspraksis

¹⁰² Forslag til afgørelse fra generaladvokat M. Szpunar sag: C-439/19, præmis 110

¹⁰³ EU-Domstolens sag: C-439/19, præmis 105

¹⁰⁴ EU-Domstolens sag: C-439/19, præmis 106

omhandlende formål med rimelighed kan opnås på anden måde¹⁰⁵. Nødvendighedsbegrebet bliver derfor i denne sammenhæng også fortolket ud fra de retlige standarder rimelighed og lovlighed, beskrevet i "God databehandlingsskik"-afsnittet. Dette viser den sammenkobling og vigtighed, der ligger i hele tiden at forholde sig til de retlige standarder.

Det kan derfor udledes, at for at overholde kravet om dataminimering i henhold til artikel 5, stk. 1, litra c er det en helhedsvurdering af, hvorvidt behandlingen er nødvendig. Den kontekst, hvori nødvendighed skal fortolkes i henhold til bestemmelsen, ligger i det overordnede proportionalitetsprincip, og de retlige standarder angivet i artiklens litra a. Der er ikke meget fortolkning og hjælp til forståelsen at hente i selve ordlyden af bestemmelsen, da det, som beskrevet ovenfor, ikke er de tre betingelser, tilstrækkelig, relevant og begrænset til der ligges vægt på fra EU-Domstolens side. Det kan diskuteres, hvorvidt disse betingelser i sin sproglige form minder meget om elementerne i proportionalitetsprincippet. Der er, som beskrevet ovenfor, en vis sammenlignelighed i 'tilstrækkelig' og 'relevant' med begrebet egnethed og 'begrænset til' ligger sig op af nødvendighedsbetingelsen i proportionalitetsprincippet. Det er dog ikke muligt at give et konkret svar på denne problemstilling, da det, som vidst i dette afsnit, ikke er noget, EU-Domstolen tager stilling til. Proportionalitetsprincippet i sammenkobling med rimelighed og lovlighed udgør derfor regelforståelsen af nødvendighed i bestemmelsen og sidste ende også, hvad princippet om dataminimering indeholder.

Dataminimering i forhold til kunstig intelligens

Den ovenstående gennemgang viser, hvordan der ikke er standarder eller retningslinjer, men en konkret helhedsvurdering, der afgør, hvorvidt databehandlingen er nødvendig og proportionel. Det opstiller også en balance mellem indgrebet på de registreredes databeskyttelse og hensynet til dataansvarlige. Udviklere af kunstig intelligens, står her over for en svær problemstilling. Det vil i de fleste tilfælde, grundet en algoritmes behov for store mængder data, være Big Data, som udviklere af kunstig intelligens vil gøre brug af. Det vil være en svær balance for udviklere af kunstig intelligens at vurdere, hvorvidt der kan bruges færre og mindre præcise personoplysninger for at opnå det samme formål. Det står dog klart, at der foreligger en begrænsning og en nødvendighed i at begrænse mængden af personoplysninger i henhold til dataminimeringskravet. Det er altså ikke

¹⁰⁵ EU-Domstolens sag: C-439/19, præmis 110

kun nødvendigt at vurdere rimelighed og muligheden for at opnå formålet med andre midler, men også nødvendigt at inddrage omfanget af det indgreb, udviklere af kunstig intelligens foretager. Bestemmelsen virker som en naturlig stopklods i forhold til mulighederne for bare at fodre algoritmen med alt den data, der er til rådighed. Landskabet i forhold til Big Data og brugen af den i forhold til princippet om dataminimering er uklart, da der ikke ligger retspraksis fra EU-Domstolen i forhold til deres fortolkning af dette koncept.

Eksempelvis vil det kunne argumenteres, at hvis en algoritme skal kunne forudse muligheden for, at en patient får kræft, er det nødvendigt og rimeligt, at den er blevet trænet på flest mulige personoplysninger, da dens formål er at give et præcist svar på, hvorvidt den nuværende patient vil få kræft. Outputet er altså ud fra tidligere patienters personoplysninger at forudse, hvad chancen er, for at den nuværende patient får kræft. Der ligger mange delelementer i forhold til præcist at kunne forudse dette som for eksempel aldersgrupper, etnisk baggrund, gener, levestandard osv. Problematikken ligger i at vurdere, hvorvidt det er nødvendigt og rimeligt for at algoritmen kan opnå sit formål og forudse chancen for kræft, at den også bliver trænet på personoplysninger vedrørende alle de delelementer nævnt ovenfor.

Det beskrevne eksempel ovenfor kaster lys over nogle af de tanker, der er nødvendige at vurdere for udviklere af kunstig intelligens, hvis de vil leve op til kravet om dataminimering. Det iscenesætter også de uklarheder, der er i nuværende retstilstand.

Princippet om rigtighed

Artikel 5, stk. 1, litra d i GDPR lyder ” *[Personoplysninger skal] være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges (»rigtighed«)* ”¹⁰⁶.

Princippet opsætter et generalkrav om, at personoplysninger skal være korrekte og nødvendigt ajourførte, og fastsætter, at der skal tages rimelige skridt for at sikre dette ved, at de personoplysninger, der er urigtige i forhold til formålet, straks slettes eller berigtiges. Ordlyden af ethvert rimeligt skridt må fortolkes ud fra en formålsfortolkning af præambelbetragtning 39 i GDPR, da bestemmelsen ikke angiver en definition af ethvert rimeligt skridt. Ligeledes angiver GDPR heller ikke, hvordan korrekt og ajourført skal fortolkes. Det må derfor være op til udviklere af

¹⁰⁶ EU-forordningen 2016/679, artikel 5, stk. 1, litra d

kunstig intelligens at foretage en konkret vurdering af formålet, og hvilke konsekvenser brugen af 'urigtige' personoplysninger har for den registrerede og derefter foretage de nødvendige foranstaltninger for at sikre, at personoplysninger bliver korrekte og nødvendigt ajourførte. Det er dog vigtigt at belyse, at kravet om ajourføring skal fortolkes i lyset af, hvad der er nødvendigt i forhold til formålet, og udviklere af kunstig intelligens skal vurdere, om rigtigheden og kvaliteten af datene overhovedet er nødvendigt for at opfylde det specificerede formål. Henvises der til brugen af Deep Learning og Big Data for udviklere af kunstig intelligens, vil det dog ikke altid være nødvendigt, at personoplysninger er helt korrekte. Disse teknologiers beslutningsprocesser afhænger ikke af, at personoplysninger er helt korrekte, da disse modeller udregner mønstre og tendenser, og rigtigheden af dataene vil ikke altid have en stor indflydelse på resultatet og derved ej heller på det formål personoplysninger behandles på baggrund af. Udviklere af kunstig intelligens skal dog være opmærksomme på, at dette princip hænger sammen med artikel 16 i GDPR omkring ret til berigtigelse og artikel 17 om ret til sletning¹⁰⁷. Dette speciale bearbejder ikke artikel 16 og 17, og den direkte sammenhæng de har med rigtighedsprincippet i artikel 5, stk. 1, litra d, men er inddraget, da rigtighedsprincippet stadig vil være noget, udviklere af kunstig intelligens skal være opmærksomme på ved behandling af personoplysninger. En dybere analyse af datakvalitet og inddragelse af det tekniske aspekt af, hvordan behandlingsprocesserne i kunstig intelligens opererer, og hele diskussionen om, om det overhovedet er muligt for udviklere af kunstig intelligens at tjekke, om personoplysningerne er korrekte, og påvise dette i henhold til artikel 5, stk. 2, jf. "Princippet om ansvarlighed"-afsnittet, vil som beskrevet ovenfor ikke blive gennemgået.

Princippet om opbevaringsbegrænsning

Artikel 5, stk. 1, litra e angiver princippet om opbevaringsbegrænsning og lyder som følger: "

[Personoplysninger skal] opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles; personoplysninger kan opbevares i længere tidsrum, hvis personoplysningerne alene behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, under forudsætning af, at der implementeres passende tekniske og organisatoriske

¹⁰⁷ EU-forordningen 2016/679, artikel 16 og 17

*foranstaltninger, som denne forordning kræver for at sikre den registreredes rettigheder og frihedsrettigheder («opbevaringsbegrænsning»)*¹⁰⁸. Artiklen indeholder nogle interessante elementer, hvis man foretager en ordlydsfortolkning i forhold til formålet med bestemmelsen. Især kan fremhæves ordlyden af *”...at det ikke er muligt at identificere de registrerede...”*, som vil blive gennemgået længere nede i afsnittet i sammenhæng med udviklere af kunstig intelligens. EU-Domstolen slår fast, at det utvetydigt af artiklens ordlyd fremgår, at princippet kræver, at den dataansvarlige er i stand til at påvise, at opbevaringen af personoplysninger kun sker så længe, det er nødvendigt af hensyn til de formål, hvortil de er indsamlet eller viderebehandlet¹⁰⁹. Det understreges her, at EU-Domstolen igen fastslår, at det er den samme form for nødvendighed¹¹⁰, som er gennemgået i *”Princippet om dataminimering”*-afsnittet. De nævner ikke direkte proportionalitetsprincippet og forståelsen af nødvendighed i denne sammenhæng, men det må udledes, at der er tale om den samme form for ’nødvendighed’. Dette underbygges af General Advokatens forslag til afgørelsen af ovenfor-refererede sag, der direkte citerer: *”... at opbevaringsbegrænsning er et udtryk for proportionalitetsprincippet...”*¹¹¹. General Advokaten beskriver dog efterfølgende, at *”I forbindelse med princippet om opbevaringsbegrænsning hænger spørgsmålet om behandlingens nødvendighed set i et tidsperspektiv sammen med spørgsmålet om opretholdelsen af dens formål.”*¹¹² Dette er for at understrege, at ’nødvendighed’, som gennemgået i *”Princippet om dataminimering”*-afsnittet, forholder sig til dataminimering, men at det her er opbevaringsbegrænsning, nødvendighed skal forstås i sammenhæng med. Det ændrer ikke på begrebsforståelsen af nødvendighed, men ændrer, hvilket formål, altså opbevaringsbegrænsning, det hænger sammen med. Fortolkningen af nødvendighedsbegrebet gennemgås derfor ikke igen, da fortolkningen af princippet følger analysen i *”Princippet om dataminimering”*-afsnittet. Det skal dog understreges, at EU-Domstolen pointerer, at denne fortolkning er i overensstemmelse med formålet i artikel 5, stk. 1, litra e, der består i at sikre et højt beskyttelsesniveau for fysiske personer¹¹³. Det kan udledes, at dette indsnævrer mulighederne for udviklere af kunstig intelligens, da det er hensynet til de registreredes beskyttelsesniveau, der vægtes højere end hensynet til de

¹⁰⁸ EU-forordningen 2016/679, artikel 5, stk. 1, litra e

¹⁰⁹ EU-Domstolens sag: C-77/21, præmis 53

¹¹⁰ EU-Domstolens sag: C-77/21, præmis 58

¹¹¹ Forslag til afgørelse fra generaladvokat P. Pikamäe sag: C-77/21, præmis 62 og heri nævnte retspraksis

¹¹² Forslag til afgørelse fra generaladvokat P. Pikamäe sag: C-77/21, præmis 62

¹¹³ EU-Domstolens sag: C-77/21, præmis 59

dataansvarlige i forhold til opbevaringsbegrænsning. Det er vigtigt at understrege, at denne indsnævring vedrører tidsperioden, hvor personoplysninger opbevares, og ikke behandlingsmulighederne i perioden de er opbevaret. Sidste del af bestemmelsen vedrørende muligheden for at opbevare personoplysninger i længere tid omhandler de samme elementer, som er gennemgået i "Undtagelser til formålsbegrænsning"-afsnittet, og vil derfor ikke blive gentaget her. Der gøres dog opmærksom på, at denne mulighed foreligger.

Gennemgangen ovenfor og inddraget retspraksis fokuserer på selve tidsrammen af opbevaringsbegrænsningsprincippet. Princippet om "*...at det ikke er muligt at identificere de registrerede...*"¹¹⁴ er desværre ikke bestridt i omtalte dom¹¹⁵. Det er dog især ordlyden sammenkoblet med formålet med bestemmelsen i denne henseende, der er interessant for udviklere af kunstig intelligens. Diskussionen vedrørende at identificere den registrerede er som beskrevet i "Anonymisering, pseudonymisering og aggregerede data"-afsnittet uden for dette speciales scope. Det er dog stadig værd at nævne, at opbevaringsbegrænsning er afhængig af muligheden for at identificere de registrerede, og hvis der bruges de tekniske muligheder som anonymisering, pseudonymisering og aggregerede data, vil udviklere af kunstig intelligens ikke være nødsaget til at begrænse tidsperioden, de opbevare dataene. Det understreges dog her, at der skal være tale om, at det ikke er muligt at identificere de registrerede. Det kan udledes, at ordlyden her stemmer overens med måden, hvorpå GDPR tager stilling til anonymiseret data, som beskrevet i "Anonymisering, pseudonymisering og aggregerede data"-afsnittet, da der, hvis der ikke er snak om personoplysninger, selvfølgelig heller ikke gælder en opbevaringsbegrænsning på personoplysningerne.

¹¹⁴ EU-forordningen 2016/679, artikel 5, stk. 1, litra e

¹¹⁵ Forslag til afgørelse fra generaladvokat P. Pikamäe sag: C-77/21, præmis 61, heri refererede fodnote 30

Princippet om integritet og hemmeligholdelse

Artikel 5, stk. 1, litra f omhandler integritet og hemmeligholdelse i form af tilstrækkelig sikkerhed for de pågældende personoplysninger. Ordlyden af artiklen er ”*[Personoplysninger skal] behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger*¹¹⁶”. Det centrale i bestemmelsen er det generelle princip om ’tilstrækkelig’ sikkerhed. Det er ikke klart ud fra bestemmelsen, hvad ’tilstrækkelig’ betyder. Inddrages artikel 32 omhandlende den egentlige sikkerhedsregel i fortolkningen opnås der ikke mere klarhed. Det er altså ikke muligt ud fra fortolkning at fastlægge betydningen, og det er derfor nødvendigt at bruge den mest nærliggende fremgangsmåde: udfyldning. Der blev under direktivet udformet en praksis om datasikkerhed i de enkelte datatilsyn, men den dynamiske udformning af bestemmelsen nødvendiggør, at det vil være situationsbestemt, hvordan ’tilstrækkelig’ sikkerhed skal forstås. Det vil være datatilsynspraksis, som er bestemmende, og det kan anmærkes, at denne praksis kun overordnet er indrammet af GDPR¹¹⁷. Fortolkningen af denne bestemmelse er ikke central for svaret på problemformuleringen i dette speciale, da den i mere figurative ord omhandler ’hvordan’et’ i forbindelse med behandlingen af personoplysninger¹¹⁸. Den er dog inddraget kort, da den er en af de bestemmelser, der er til stede i artikel 5 i GDPR, og er relevant for udviklere af kunstig intelligens at forholde sig til.

Princippet om ansvarlighed

Artikel 5, stk. 2 angiver princippet om ansvarlighed og lyder som følger: ”*Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes*”¹¹⁹. Princippet om ansvarlighed er interessant, da det ikke er nok, at dataansvarlige overholder stk. 1, men også skal påvise/dokumentere overholdelsen. Det er ikke kun i denne bestemmelse, princippet kommer til udtryk i GDPR. Princippet er bekræftet i artikel 24, stk. 1, der ifølge bestemmelsen pålægger dataansvarlige at implementere passende tekniske og organisatoriske foranstaltninger og være i stand til at påvise, at behandlingen er i overensstemmelse med GDPR. Foranstaltningerne skal tage

¹¹⁶ EU-forordningen 2016/679, artikel 5, stk. 1, litra f

¹¹⁷ Blume, Peter – *Persondatarettens kilder og metoder*, side 98

¹¹⁸ Forslag til afgørelse fra generaladvokat M. Szpunar sag: C-439/19, præmis 100

¹¹⁹ EU-forordningen 2016/679, artikel 5, stk. 2

hensyn til behandlingens omfang, karakter, sammenhæng og formål, samt risici for varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder¹²⁰. Hvis det står i rimeligt forhold til behandlingsaktiviteterne, skal foranstaltningerne indeholde passende databeskyttelsespolitikker¹²¹. Det er ikke kun i artikel 24, at ansvarlighedsprincippet kommer til udtryk i GDPR. Der foreligger kravet om 'fortegnelser' over behandlingsaktiviteter i artikel 30, konsekvensanalyse vedrørende databeskyttelse i artikel 35, forudgående høring ved høj risiko i forhold til mangel af foranstaltninger i artikel 36, udpegelse af databeskyttelsesrådgiver i artikel 37 og databeskyttelse gennem design og standardindstillinger i artikel 25¹²².

I forhold til kunstig intelligens er der, som beskrevet igennem kapitlet, allerede nogle udfordringer for udviklere af kunstig intelligens i forhold til overholdelse af artikel 5, stk. 1 af GDPR.

Gennemgangen i kapitlet har vist, hvordan den korrekte regelforståelse af principperne er en svær disciplin i sig selv, og det gør det ikke mindre kompliceret, at de også skal påvise/dokumentere overholdelsen af alle principperne. En af de større udfordringer, som vil blive gennemgået mere i dybden i kapitel 4, er sammenhængen med gennemsigtighed og forklarlighed og Black Box problematikken, som beskrevet i Black Box-afsnittet.

¹²⁰ EU-forordningen 2016/679, artikel 24, stk. 1

¹²¹ EU-forordningen 2016/679, artikel 24, stk. 2

¹²² Trzaskowski, Jan: *Your Privacy Is Important to US! – Restoring Human Dignity in Data-Driven Marketing*, side 51f

Kapitel 4 – Gennemsigtighed og forklarlighed

Dette kapitel ser nærmere på gennemsigtigheds- og forklarlighedskravene i GDPR, og prøver at belyse, hvordan udviklere af kunstig intelligens kan overholde disse i relation til beslutningsprocesserne, der er grundlaget for AI's output. Kapitlet bygger videre på gennemsigtighedsprincippet fra artikel 5, stk. 1, litra a gennemgået i kapitel 3 og Black Box problematikken introduceret i "Black Box"-afsnittet. Kapitlet introducerer kort 'symbolsk tilgang', en anden disciplin inden for kunstig intelligens, der vil blive inddraget i analysen af forklarlighedsproblemet bag kunstig intelligens' behandlingsprocessor. Gennemsigtighed er uløseligt forbundet med princippet om rimelighed og ansvarlighed beskrevet i kapitel 3. De praktiske informationskrav er beskrevet i artikel 12-14 i GDPR¹²³. Gennemsigtighedsprincippet er omfattende, og det ligger uden for rammerne af dette speciale at beskrive alle elementerne vedrørende princippet. Det vil i stedet fokusere på en af de centrale overvejelser vedrørende princippet, som artikel 29-arbejdsgruppen præsenterer i deres retningslinjer for gennemsigtighed i henhold til GDPR. Denne tilgang er valgt, da Black Box-problematikken er en særlig udfordring for udviklere af kunstig intelligens. Især i lyset af den konstante udvikling og voksende kompleksitet, kunstig intelligens gennemgår, og uklarhederne ved behandlingsprocesserne bag deres beslutninger. Dette skaber ikke kun et teknisk problem, men også juridiske udfordringer, når fokus sættes på de registrerede, grundlæggende rettigheder og beskyttelse af deres personoplysninger.

En central overvejelse i forbindelse med gennemsigtighedsprincippet er, at den registrerede på forhånd har mulighed for at fastlægge både omfanget og konsekvenserne af behandlingen af deres personoplysninger. Der bør ikke opstå overraskelser senere hen vedrørende, hvordan deres personoplysninger er blevet anvendt. Dette knytter sig også til rimelighedsprincippet fra artikel 5, stk. 1, litra a af GDPR og præambelbetragtning 39, der fastsætter, at *"fysiske personer bør gøres bekendt med risici, regler, garantier og rettigheder i forbindelse med behandling af personoplysninger"*¹²⁴. Artikel 29-arbejdsgruppen nævner, at det navnlig er i forbindelse med tekniske, komplekse eller uventet databehandling, at de dataansvarlige, udover at efterleve de praktiske informationskrav i artikel 13-14, også helt utvetydigt og særskilt bør præcisere, hvad de

¹²³ Artikel 29-arbejdsgruppens *retningslinjer for gennemsigtighed i henhold til forordning 2016/679*, side 5f

¹²⁴ Artikel 29-arbejdsgruppens *retningslinjer for gennemsigtighed i henhold til forordning 2016/679*, side 8

vigtigste konsekvenser af behandlingen bliver¹²⁵. Det må konkluderes, at kunstig intelligens og dens behandlingsproces, selvom det ikke nævnes direkte, vil kategoriseres som kompleks og teknisk og i nogle tilfælde uventet databehandling. Komplexiteten og det tekniske aspekt er især til stede, når det er Deep Learning algoritmer, den kunstige intelligens er bygget på. Det er, som beskrevet i "Black Box"-afsnittet, lige præcis dette høje niveau af kompleksitet, der i flere situationer umuliggør selv for de dataansvarlige at kunne forklare behandlingsprocessen. Alt andet lige, hvis det er umuligt for de dataansvarlige selv at forstå behandlingsprocessen, eller ikke at kunne forklare behandlingsprocessen, så vil det også være meget svært for de registrerede at fastlægge omfanget og konsekvenserne ved behandlingen. Som beskrevet ovenfor i afsnittet, er gennemsigtighedsprincippet uløseligt knyttet til ansvarlighedsprincippet i artikel 5, stk. 2. Her vil Black Box problematikken og manglende forklarlighed også medføre besværligheder for udviklere af kunstig intelligens i at påvise overholdelsen i artikel 5, stk. 1 af GDPR.

Fundamentalt ligger problemet i forklarlighedsgraden af selve behandlingsprocessen, da udviklere af kunstig intelligens ville kunne skabe gennemsigtighed ved at forklare de registrerede, hvordan behandlingsprocessen foregår og problematikken bag Black Box. Essensen er så, hvorvidt de registrerede, hvis de er i en position, hvor de er blevet informeret om Black Box problematikken, rent faktisk er i stand til at kunne afgøre hvad omfanget og konsekvenserne af behandlingen indebærer. Gennemsigtighedsprincippet er uløseligt forbundet med rimelighedsprincippet, der sammenkoblet med præambelbetragtning 39 foreskriver, at "*Personoplysninger bør kun behandles, hvis formålet med behandlingen ikke med rimelighed kan opfyldes på anden måde*"¹²⁶. Black Box-problematikken er, som nævnt ovenfor, en udfordring for udviklere af kunstig intelligens i forhold til gennemsigtighedsprincippet, men forbindelsen med rimelighedsprincippet ovenfor kan vise sig at være en endnu større udfordring at efterleve. Det er vigtigt at understrege, uden det bliver en teknisk gennemgang, at Black Box-problemet kun opstår ved Deep Learning algoritmer. Med andre ord, hvis der vælges en anden form for kunstig intelligens, vil den ikke have det samme forklaringsproblem.

Der er i kapitel 2 introduceret Machine Learning og Deep Learning, der er karakteriseret ved behovet for store mængder data og læring gennem korrelationer. Der findes dog også en anden

¹²⁵ Artikel 29-arbejdsgruppens *retningslinjer for gennemsigtighed i henhold til forordning 2016/679*, side 8

¹²⁶ EU-forordningen 2016/679, præambel 39

disciplin inden for kunstig intelligens, kaldet symbolsk tilgang, hvor mennesker fastsætter regler direkte. Symbolsk AI's primære tilgang er at bruge logikbaseret programmering, der allerede er defineret af et menneske. Den fungerer kun optimalt i de situationer, hvor der er veldefineret data. Et eksempel er inden for medicin, hvor algoritmen skal vurdere, om en patient har lungebetændelse. Her vil en prædefineret regel eksempelvis være, at hvis patienten har 3 scenarier opfyldt, såsom, feber, hoste og svært ved at trække vejret, kan patienten have lungebetændelse. Dette skaber også en ligefrem forklarlighed, da udviklerne af den kunstige intelligens nemt kan tjekke, hvorfor og hvordan algoritmen er kommet frem til sit resultat. Ydermere skaber det også en nemmere tilgang til at forbedre og opdatere algoritmen, hvis ny information skulle blive tilgængelig¹²⁷.

Black Box og forklarlighedsproblemet vil, som beskrevet ovenfor, ikke være til stede ved den symbolske tilgang. Alt andet lige vil dette også betyde, at formålet med rimelighed kan opnås på anden måde. Det er dog situationsbestemt, da symbolsk tilgang ikke altid kan løse de samme tekniske udfordringer og formål, som Deep Learning kan og formålet vil derfor ikke kunne opnås på anden måde. Det vil være en konkret vurdering i forhold til formålet, men det kan konkluderes, at udviklere af kunstig intelligens i nogle situationer vil have svært ved at overholde rimelighedsprincippet og forklare brugen af Deep Learning fremfor eksempelvis symbolsk tilgang. Det er også vigtigt at understrege, at det er en helhedsvurdering, hvor det er hensynet til de dataansvarlige og samfundet vægtet op imod de registreredes grundlæggende garanti for forudsigelighed og retssikkerhed, der overordnet set tages i betragtning i de konkrete situationer. Der foreligger ikke klare retningslinjer, der angiver, hvilken vej vægtskålen vil pege, men Europa Kommissionen angiver i *Hvidbog om kunstig intelligens – en europæisk tilgang til ekspertise og tillid*, at "*Ved at kombinere symbolske tankelove med dybe neurale net kan vi opnå kunstig intelligens med bedre forklarlighed*"¹²⁸. Værd at nævne her er, at specialet ikke beskæftiger sig med retspolitiske problemstillinger og hvidbogens formål er at opstille politiske løsningsmodeller¹²⁹.

¹²⁷ DataCamp Team, *What is Symbolic AI?*, <https://www.datacamp.com/blog/what-is-symbolic-ai>, besøgt d. 15 november 2023

¹²⁸ Europa Kommissionen, COM(2020) 65 final, *Hvidbog om kunstig intelligens – en europæisk tilgang til ekspertise og tillid*, side 5

¹²⁹ Europa Kommissionen, COM(2020) 65 final, *Hvidbog om kunstig intelligens – en europæisk tilgang til ekspertise og tillid*, side 2

Gennemgangen i dette afsnit viser, hvordan der foreligger nogle fundamentale problemstillinger i forhold til forklarlighed og gennemsigtighed i kunstig intelligens' behandling af personoplysninger. Det er dog ikke muligt direkte at udlede nogen retningslinjer for udviklere af kunstig intelligens i forhold til denne problematik, da retslandskabet vedrørende denne problemstilling ikke er afklaret. Gennemgangen i dette kapitel belyser dog, hvordan valget af kunstig intelligens og teknisk løsning i konkrete situationer kan have betydning for overholdelsen af GDPR.

Kapitel 5 – Konklusion

Dette speciale har haft til formål at undersøge gældende ret for brugen af personoplysninger i udviklingen af kunstig intelligens i overensstemmelse med EU-forordningen 2016/679 om databeskyttelse. Det har fokuseret på de retlige standarder og generelle principper præsenteret i artikel 5 i GDPR, især kompleksiteten i at opfylde kravene om formålsbegrænsning, dataminimering samt sikring af gennemsigtighed og forklarlighed i beslutningsprocesserne for kunstig intelligens. Disse retlige standarder angiver ikke fuldt ud en specifik regel, men derimod mere en retningspil for tilrettelæggelsen af persondatabehandlingen. Manglen på præcision kan skabe en vis usikkerhed om fortolkningen af principperne i de konkrete situationer. Ved dybdegående gennemgang af GDPR har specialet belyst den nuværende regelforståelse af de retlige standarder og bestemmelser og derved klarlagt fortolkningen og forståelsen af de enkelte bestemmelser. Det fremgår dog klart af Analysen, at regelforståelsen og regelefterlevelsen er situationsbestemt og altid vil være en konkret vurdering af den enkelte situation. De retlige standarders sammenhæng med reguleringens dynamiske karakter viser dog også, hvordan specialet ikke præsenterer en overordnet anvendelig løsning, men derimod belyser, hvilken betydning bestemmelserne har for udviklere af kunstig intelligens.

Det er i specialet blevet analyseret, hvordan de retlige standarder i artikel 5, stk. 1, litra a bliver understøttet eller konkretiseret af de efterfølgende bestemmelser, samt hvordan de også har en determinerende indflydelse på, hvorvidt udviklere af kunstig intelligens overholder de enkelte bestemmelser. Fortolkningen af legitime formål i artikel 5, stk. 1, litra b er et eksempel på, hvordan den retlige standard lovlighed konkretiseres i forhold til formål. Det er ikke nok, at selve behandlingen af personoplysninger følger princippet om lovlighed, hvoraf GDPRs forhold for lovlig behandling i artikel 6 og alt andet regulering respekteres, men formålet skal også følge de samme standarder. Specialet belyser, hvordan konsekvensen af dette for udviklere af kunstig intelligens er, at det ikke er nok at have lovligt belæg i henhold til GDPR, men at alt andet regulering i henhold til beskyttelse af den registrerede også skal overholdes, såsom EU-chartret.

I forhold til formålsbegrænsning er det ikke nok, at indsamling af personoplysninger har legitime formål. De skal også være udtrykkelig angivne formål. Dette nødvendiggør, at formål er saglig og velbegrundet i henhold til de konkrete omstændigheder, samt præcist nok defineret, så den

registrerede er i stand til på et oplyst grundlag at forstå databehandlingen og tage et informeret valg. Graden af præcision afhænger af de konkrete omstændigheder, men for udviklere af kunstig intelligens, der bruger Deep Learning og Big Data, vil der være behov for en større grad af præcision af formål. Det vil ikke være nok at definere formål vagt og overordnet, som 'kunstig intelligens-relaterede formål', da præcisionskravet kræver, at formuleringen skal give den samme forståelse hos de registrerede og udviklerne af kunstig intelligens. Formål er i GDPR defineret i flertal, da det vil være muligt for udviklere af kunstig intelligens at have flere sammenlignelige formål i forhold til hovedformålet, men præcisionskravet nødvendiggør stadig, at de registrerede skal kunne tage informerede valg på et oplyst grundlag.

Artikel 5, stk. 1, litra b angiver, at viderebehandling af de førnævnte formål ikke må være uforenelig. Ordlyden af viderebehandling ligger klart i retspraksis, da viderebehandling udgør enhver behandling af personoplysninger, der sker efter den oprindelige behandling. Specialets analyse klarlægger, hvordan bestemmelsen definerer 'ikke viderebehandling af uforenelig formål,' og hvilken betydning det har, at bestemmelsen er udformet på den måde fremfor at definere, at viderebehandling skal være forenelig med de oprindelige formål. Fortolkningen af forenelighed bygger på 5 hensyn, som EU-Domstolen bruger i retspraksis, samt fremgår af artikel 6, stk. 4, litra a-e i GDPR. Relevansen af hver enkelt hensyn og vægtningen af den er afhængig af udviklingen inden for teknologi og samfund. Hensynene er kumulative, og det er en overordnet konkret vurdering, hvor hver enkelt hensyn inddrages, eller udelades, samt vægtes i forhold til relevans, der danner baggrund for viderebehandlingens forenelighed. Det er en helhedsvurdering ved hjælp af de 5 hensyn i den konkrete situation, der angiver forståelsen for, hvordan de overordnede hensyn til dataansvarlige og samfundet vægtes op imod de registreredes grundlæggende garanti for forudsigelighed og retssikkerhed skal vurderes.

I forlængelse af forenelighed har specialet bearbejdet 2 af de 4 undtagelser til forenelighed, der fremgår af ordlyden af artikel 5, stk. 1, litra b, hvilke har mest relevans for udviklere af kunstig intelligens. Det konkluderes i denne sammenhæng, at udviklere af kunstig intelligens, hvis det er disse formål udviklingen har, vil være i stand til at levere de fornødne garantier i overensstemmelse med GDPRs artikel 89, stk. 1 og dermed være fritaget for forenelighedstesten. Det vil dog være en konkret helhedsvurdering af, hvorvidt de kan levere de nødvendige tekniske og organisatoriske foranstaltninger, der sikrer de registreredes rettigheder.

I forhold til dataminimeringsprincippet i artikel 5, stk. 1, litra c konkluderes det ud fra EU-Domstolens retspraksis, at princippet er et udtryk for proportionalitetsprincippet. Artiklen skal fortolkes ud fra egnethed og nødvendighed, som forstået i proportionalitetsprincippet. Fortolkningen af nødvendighedsbegrebet foretages ud fra, hvorvidt det er nødvendigt at efterprøve om, under hensyn til alvoren af det indgreb i retten til beskyttelse af personoplysninger, er begrundet og navnlig forholdsmæssig, med henblik på at nå de forfulgte mål. Den kontekst, hvori nødvendighed skal fortolkes i henhold til artiklen, ligger i det overordnede proportionalitetsprincip og i de retlige standarder angivet i artikel 5, stk. 1, litra a. Proportionalitetsprincippet i sammenkobling med rimelighed og lovlighed udgør forståelsen af nødvendighed i artiklen, og i sidste ende også regelforståelsen af dataminimering. I forlængelse af fortolkningen af nødvendighed i forhold til dataminimering, konkluderes det også, at opbevaringsbegrænsningsprincippet i artikel 5, stk. 1, litra e er denne samme fortolkning EU-Domstolen ligger til grund for regelforståelsen. Dog er det vigtigt at fastslå, at formålene, nødvendighed fortolkes ud fra, er forskellige. Opbevaringsbegrænsning er også afhængig af de samme undtagelser nævnt under forenelighed, der muliggør en længere opbevaringsperiode. Opbevaringsbegrænsning kan også helt undgås at skulle vurderes af udviklere af kunstig intelligens, hvis det ikke længere er muligt at identificere de registrerede, hvilket afhænger af, hvilke fornødne garantier, der er valgt.

Den dybdegående gennemgang og analyse af GDPR retlige standarder viser, hvordan det for det andet afhænger af, hvilken form for kunstig intelligens, udviklere ønsker at udvikle, da det skaber forskellige juridiske komplikationer i henhold til overholdelse af GDPR. Datakvalitet i artikel 5, stk. 1, litra d og integritet og fortrolighed i artikel 5, stk. 1, litra f vil især have forskellige konsekvenser for udviklere af kunstig intelligens i forhold til, hvilken algoritme, de vælger at udvikle, og hvilke sikkerhedsmekanismer, der bruges. Valget af kunstig intelligens spiller også en væsentlig rolle i forhold til overholdelse af gennemsigtighedsprincippet og forklarlighed. Specialet konkluderer, at regelforståelsen af disse principper i henhold til Deep Learning og Black Box problematikken, og hvilke konsekvenser, det vil have for udviklere af kunstig intelligens, er uklare. Det udledes dog, at udviklere af kunstig intelligens skal have fokus på en særlig præcision af formål, da de arbejder med tekniske og komplekse behandlingsprocessor, der giver den registrerede mulighed for på

forhånd at fastlægge både omfanget og konsekvenserne af behandlingen af deres personoplysninger.

Litteraturliste

Love og forordninger

- Europa-Parlamentets og Rådets Forordning – Om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens) og om ændring af visse af unionens lovgivningsmæssige retsakter – COM(2021) 206 final
- Europa-Parlamentets og Rådets forordning af 2016-04-27 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) (2016/679)

Vejledninger

- Artikel 29-arbejdsgruppens udtalelse nr. 03/2013 on *purpose limitation*, adopted 2 April 2013
- Europa Kommissionen udtalelse nr. COM(2020) 65 final, *Hvidbog om kunstig intelligens – en europæisk tilgang til ekspertise og tillid*, adopted 19.2.2020
- Artikel 29-arbejdsgruppens *retningslinjer for gennemsigtighed i henhold til forordning 2016/679*, wp 260 rev. 01, senest revideret og vedtaget den 11. april 2018
- Artikel 29-arbejdsgruppens udtalelse nr. 4/2007 on *the concept of personal data*, wp 136, adopted 20 juni

Domme og afgørelser

- EU-Domstolens sag C-60/22: UZ mod Bundesrepublik Deutschland
- Forslag til afgørelse fra generaladvokat P. Pikamäe sag: C-77/21: Digi Távközlési és Szolgáltató Kft. Mod Nemzeti Adatvédelmi és Információszabadság Hatóság
- EU-Domstolens sag: C-77/21: Digi Távközlési és Szolgáltató Kft. Mod Nemzeti Adatvédelmi és Információszabadság Hatóság
- Forslag til afgørelse fra generaladvokat M. Szpunar sag: C-439/19: (anmodning om præjudiciel afgørelse indgivet af Satversmes tiesa (forfatningsdomstolen, Letland))
- EU-Domstolens sag 439/19: angående en anmodning om præjudiciel afgørelse i henhold til artikel 267 TEUF, indgivet af Latvijas Republikas Satversmes tiesa (Republikken Letlands forfatningsdomstol)

Bøger

- Munk-Hansen, Carsten: *Den juridiske løsning*, 1. udgave, 2. oplag, Jurist- og Økonomforbundets Forlag, 2017
- Høilund, Dorte: *Persondataret*, 4. udgave, 1. oplag, Hans Reitzels Forlag, 2022
- Blume, Peter: *Persondatarettens kilder og metode*, 1. udgave, 1. oplag, Djøf Forlag, 2020
- Blume, Peter: *Den nye persondatarets aktører*, 1. udgave, 1. oplag, Jurist- og Økonomforbundets Forlag, 2018
- Trzaskowski, Jan: *Your Privacy Is Important to U\$! – Restoring Human Dignity in Data-Driven Marketing*, 1. udgave, Ex Tuto Publishing, 2021

Internetkilder

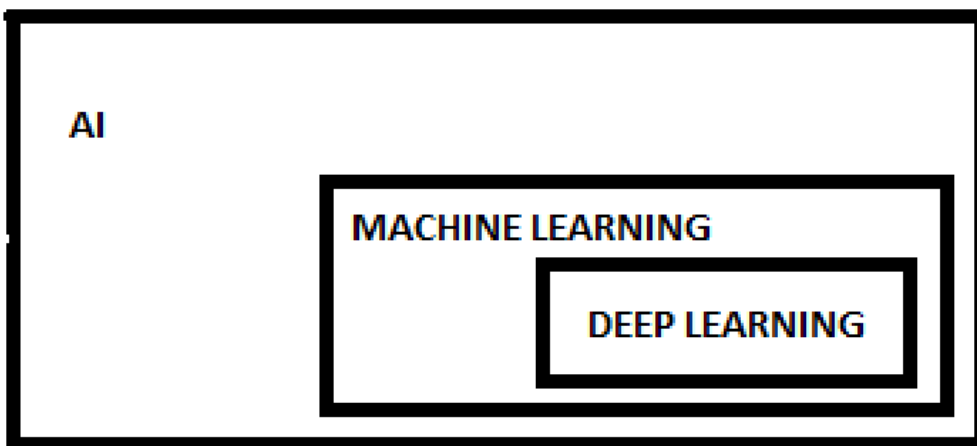
- Danmarks Statistik, *Hver fjerde virksomhed bruger kunstig intelligens*.
<https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=31880>
- OpenAI, Blog: *Introducing GPTs*, 6 november 2023
<https://openai.com/blog/introducing-gpts#OpenAI>
- Datatilsynet, *Hvad er personoplysninger?*
<https://www.datatilsynet.dk/hvad-siger-reglerne/grundlaeggende-begreber/hvad-er-personoplysninger>
- IBM Data and AI Team, juli 6, 2023, *AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the difference?*.
<https://www.ibm.com/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks/>
- Brown, Sara, april 21, 2021, *Machine Learning, Explained*.
<https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained>
- IBM, *What is artificial intelligence (AI)?*.
<https://www.ibm.com/topics/artificial-intelligence>
- IBM, *What is machine learning?*
<https://www.ibm.com/topics/machine-learning>
- Bolander, Thomas, 21. august, 2018, *Hvad er kunstig intelligens (AI) egentlig?*
<https://videnskab.dk/teknologi/hvad-er-kunstig-intelligens-ai-egentlig/>
- IBM, *What is deep learning?*

<https://www.ibm.com/topics/deep-learning>

- Gillis S., Alexander, 07 august, 2023, *4 main types of artificial intelligence: Explained*
<https://www.techtarget.com/searchenterpriseai/tip/4-main-types-of-AI-explained>
- Bahrynovska, Tanya, maj 29, 2023, *Exploring the intersection of Big Data and AI: Unlocking Insights and Driving Innovation*
<https://forbytes.com/blog/big-data-and-ai/>
- Oracle, *What is Big Data?*
<https://www.oracle.com/big-data/what-is-big-data/>
- Blouin, Lou, marts 6, 2023, *AI's mysterious 'black box' problem, explained*
<https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained>
- DataCamp Team, may 2023, *What is Symbolic AI?*
<https://www.datacamp.com/blog/what-is-symbolic-ai>

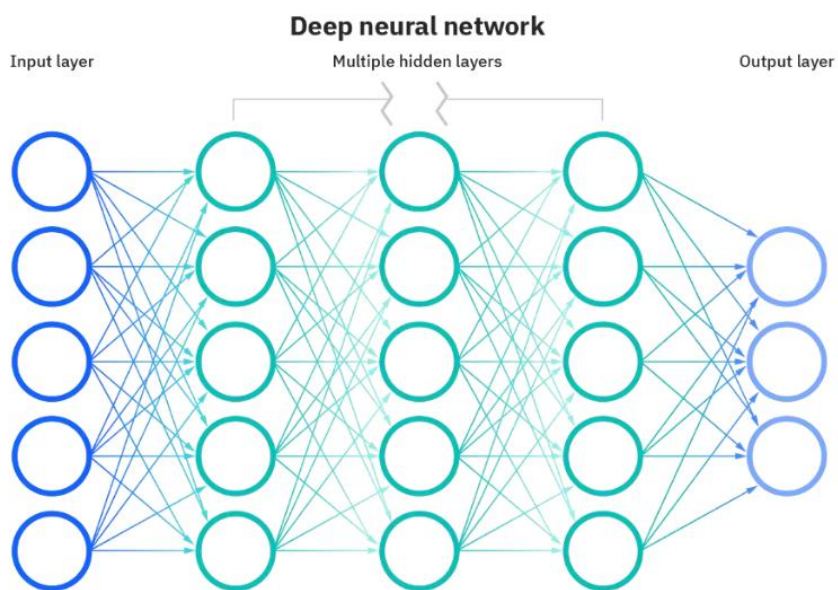
Figuroversigt

Figur 1 – Egen tilvirkning. Viser forholdet mellem AI, Machine Learning og Deep Learning



Kilde: Egen tilvirkning.

Figur 2 – Viser et Deep neuralt netværk



Kilde: <https://www.ibm.com/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks>

Forside:



Kilde: <https://oecd.ai/en/work/increasing-legal-cases>

Antal anslag:

Ordoptælling

?

×

Statistik:

Sider	54
Ord	16.871
Tegn (uden mellemrum)	100.020
Tegn (med mellemrum)	116.693
Afsnit	143
Linjer	1.319

☐ Medtag tekstfelter, fodnoter og slutnoter

Luk