Syddansk Universitet, Odense

Det Samfundsvidenskabelige Fakultet

Virksomheders kommercielle behandling af biometriske data efter Databeskyttelsesforordningen

Med fokus på de teknologiske løsninger til brug for behandling af biometriske data, herunder ansigtsgenkendelsessystemer

---

Companies commercial processing of biometric data under the General Data Protection Regulation

Focusing on the technological solutions for the use of biometric data processing, including facial recognition systems

Opgaven er udarbejdet af:	Sara Bech Kamph - 020395
Studieretning:	Cand.merc.jur
Fag:	Persondataret
Juridisk vejleder:	Ayo Næsborg-Andersen
Økonomisk vejleder:	Jesper Kruse Markvart
Afleveringsdato:	2. juni 2020
Antal anslag med mellemrum:	139.922

Tro & Love erklæring

"Det erklæres herved på tro og love, at undertegnet egenhændigt og selvstændigt har udformet denne rapport. Alle citater i teksten er markeret som sådanne, og rapporten eller væsentlige dele af den har ikke tidligere været fremlagt i anden bedømmelsessammenhæng."

Sara Bech Kamph, den 02.06.2020

Abstract

This thesis examines how companies can use the treatment of consumers biometric data commercially in relation to the General Data Protection Regulatory where focus is on technological solutions especially facial recognition systems. The primary legal purpose of this thesis has been to analyze in which extent the treatment of biometric data through verification- and identification systems is legal in relation to the General Data Protection Regulatory.

The thesis is divided into three main parts. The first part (chapter 3 and 4) consists of a description of the technological solutions in use for treatment of biometric data which is the starting point of this thesis. Hereinafter the relevant concepts and sources of law of this thesis' scope will be described concerning companies' treatment of biometric data commercially.

The second part (chapter 5 and 6) consists of a legal and an economic analyze. In chapter 5 the limited case law that exists in the field of a commercially treatment is analyzed. Both case law from The Danish Data Protection Agency and other European Data Protection Agencies are examined. The conclusion of the analyze is that companies' options for treatment of biometric data is limited which makes it difficult to reach an acceptance for the treatment of the biometric data where profiling is performed. The economic analyze in chapter 6 begins with economic reflections that are in relation to theory and shapes**.** In this chapter the impact of companies' implementation of facial recognition systems is examined respectively for the company, the consumers and the society. The examination concludes that the use of facial recognition systems is welfare enhancing for both short and long term why it should be possible for companies to make use of such a system to achieve a more efficient market.

The main results and conclusions of the thesis is presented in chapter 7. The thesis concludes that the scope of treatment options of consumers biometric data is not optimal in relation to economically achieve a more efficient market. The companies are therefore to find other alternative treatment solutions that result in a more efficient market but also complies with the General Data Protection Regulation. In chapter 8 the conclusion leads to an interdisciplinary perspective which results in a presentation of potential welfare enhancing suggestions to companies' options for now and in the future.

Indholdsfortegnelse

Del 1 – Introduktion og rammer for afhandling

1. Indledning

Behandling af biometriske data vækker stor opmærksomhed rundt omkring i verden. Biometri er for alvor blevet en realitet i vores dagligdag, hvor der de seneste år er sket en stigning i anvendelse, opbevaring og formidling af biometriske data i både den private- og offentlige sektor. Den store udvikling inden for ansigtsgenkendelsessystemer og applikationer har medført, at behandling af biometriske data i denne form for teknologi ses mere hyppigt rundt omkring i verden. Den største udvikling ses i Kina, som de seneste år er blevet et overvågningssamfund på meget højt niveau.[1]

Før i tiden var teknologien omkostningskrævende i forhold til at behandle biometriske data, hvilket medførte begrænsede konsekvenser af fysiske personers ret til databeskyttelse. I dag er det blevet mere overkommeligt for de fleste, da teknologien er blevet hurtigere og mindre omkostningskrævende.[2]

Den stigende udvikling vil med stor sandsynlighed skabe en øget efterspørgsel hos virksomheder med et ønske om at benytte teknologien kommercielt, da den giver større mulighed for, at flere forskellige miljøer kan benytte sig af denne form for teknologi.[3]
Virksomheder vil med teknologien have en forhåbning om at spare tid og penge på længere sigt.
Ansigtsgenkendelsessystemer vil for annoncører give mulighed for ikke kun at målrette placeringen af annoncer men tillige deres indhold og hyppighed.
For detailhandlere kan en teknologi, der for eksempel finder frem til den enkelte forbrugers individuelle interesse i en bestemt type produkt, hjælpe med at sælge mere effektivt. Samtidigt kan systemet opbygge stadig mere detaljerede profiler af deres kunder/potentielle kunder og målrette deres markedsføring i højere grad.[4]

[1] https://www.berlingske.dk/virksomheder/kina-saetter-sig-paa-teknologien-til-overvaagning
[2] Artikel 29-gruppen udtalelse: *WP 193*, s. 2
[3] Ibid., s. 16
[4] https://www.taylorwessing.com/download/article-facial-recognition-in-eu.html

Ved behandling af biometriske data stiller Databeskyttelsesforordningen strenge krav. Det ses blandt andet i den dataansvarliges ansvar for at påvise og efterleve reglerne for at opnå et legitimt behandlingsgrundlag.

Afhandlingsområdet er særligt interessant, da behandling af biometriske data med Databeskyttelsesforordningens ikrafttrædelse er omfattet af den særlige kategori af personoplysninger, jf. forordningens art. 9.[5] Området for behandling af den nye form for personoplysning er minimalt, hvilket også afspejles i den begrænsede praksis. Det er derfor interessant at dykke ned i denne behandling for at vurdere virksomheders muligheder og udfordringer ved brug af biometriske data udelukkende ud fra en kommerciel interesse.

1.1. Problemformulering

Afhandlingens fokus er virksomheders mulighed for at bruge forbrugernes biometriske data kommercielt, og hvilke begrænsninger Databeskyttelsesforordningen sætter hertil. Derudover vil afhandlingen behandle de økonomiske konsekvenser for brugen af biometriske data. Kerneområderne for analysen er:

1) *I hvilket omfang kan virksomheder juridisk set i henhold til Databeskyttelsesforordningen benytte forbrugernes biometriske data kommercielt, særligt med fokus på de teknologiske løsninger til brug for behandling af biometriske data, herunder ansigtsgenkendelsessystemer?*
2) *Hvordan er virksomhederne og samfundet stillet økonomisk set ved implementering af teknologierne, med fokus på ansigtsgenkendelsessystemer?*

Ud fra den juridiske og økonomiske analyse er formålet med afhandlingen at vurdere, om Databeskyttelsesforordningens regler er indrettet på en sådan måde, så der kan opnås en efficient tilstand på markedet.

1.2. Struktur for afhandlingen

Indledningsvis foretages der i afsnit 2 en kort introduktion af Databeskyttelsesforordningens (herefter "GDPR" ved henvisning til bestemmelser) historiske baggrund set i en EU-

[5] Betænkning nr. 1565, del 1, bind 1, s. 189-192

retlig kontekst. Formålet med afsnittet er at skabe en forståelse af baggrunden for behandling af de registreredes[6] biometriske data.

Herefter foretages der i afsnit 3 en sondring mellem de forskellige former for teknologier til indsamling af biometriske data, herunder ansigtsgenkendelsessystemer. Formålet med afsnittet er at fastlægge analysens udgangspunkt, førend der foretages en gennemgribende analyse af teknologiernes behandling og omfang i praksis.

I afsnit 4 foretages en behandling af de centrale begreber og retskilder for afhandlingens behandlingsområde, herunder centrale begreber i GDPR art. 4 og relevante retskilder i GDPR art. 5, 6, 9, 21/22 og 35/36. Formålet er her at få fastlagt det relevante retsgrundlag efter Databeskyttelsesforordningen for behandling af biometriske data.

På baggrund af resultaterne frembragt i afsnit 2, 3 og 4 foretages der i afsnit 5 en juridisk analyse. Analysen tager udgangspunkt i de beskrevne teknologier i afsnit 3 for at finde frem til virksomhedernes muligheder for at behandle biometriske data kommercielt.

Herefter vil afsnit 6 omhandle retsøkonomiske betragtninger af implementering af teknologierne, herunder ansigtsgenkendelsessystemer. Formålet er at belyse de mulige gevinster, som virksomheder, forbrugere og samfundet opnår ved virksomhedens implementering af systemet.

Afsnit 7 afrunder analyserne med en samlet konklusion, hvor de enkelte delkonklusioner sammenfattes, og problemformuleringen besvares.

Endeligt vil afsnit 8 omfatte en perspektivering med en retspolitisk vinkel til at foretage en vurdering og give en anbefaling af virksomhedernes muligheder i fremtiden.

1.3. Afgrænsning

Afhandlingen vil koncentrere sig om behandling af biometriske data i teknologiske systemer til kommercielt brug med paralleller til behandling af biometriske data i en

[6] Den registrerede er i GDPR art. 4, nr. 1 defineret som *en identificeret eller identificerbar fysisk person*

samfundsmæssig interesse. Det vil derfor alene være en beskeden behandling af systemernes brug i praksis, da det udelukkende er systemer, som er benyttet ud fra en kommerciel interesse.

Grundet Danmarks nedlukning har det været svært at fremskaffe alt det relevante materiale, hvorfor fodnoter mangler nogle steder. Det drejer sig for eksempel om beskrivelsen i afsnit 1.4.1.3 om den retskildemæssige værdi af Datatilsynets afgørelser og tilladelse inden for området i forhold til afgørelser fra domstolene.

Afhandlingens afsnit 2 er med for at forstå og fortolke rækkevidden af pligter og rettigheder i persondataretten. Det skal her fastlægges, hvilken plads Databeskyttelsesforordningen har i retssystemet samt sammenhængen med anden lovgivning. For forståelsens skyld bliver der foretaget en beskeden behandling af Den Europæiske Menneskerettigheds Konvention (herefter EMRK) og Den Europæiske Unions Charter "Chartret om EU's Grundlæggende Rettigheder" (herefter "chartret" eller "EUC"). Selvom bestemmelserne har en betydning for den registreredes rettigheder, bliver der grundet pladsmangel kun foretaget en begrænset behandling af lovgivningen.

Formålet med afhandlingen er at undersøge virksomheders muligheder for a benytte forbrugers biometriske data ud fra en analyse af retspraksis samt en økonomisk analyse af brugen. Afhandlingen vil derfor kun behandle de definitioner og retskilder i Databeskyttelsesforordningen, som har relevans for afhandlingen.

1.4. Metode og teori

1.4.1. Juridisk metode

1.4.1.1. Den retsdogmatiske metode

Til at beskrive og analysere gældende ret vil den retsdogmatiske metode anvendes[7], med fokus på hvad gældende ret er, også kaldet "de lege lata"[8].

Afhandlingen anvender den retsdogmatiske metode til at fastlægge gældende ret indenfor behandling af biometriske data i Danmark. Der vil være særligt fokus på rækkevidden af

[7] Christian D. Tvarnø og Ruth Nielsen: *Retskilder og retsteorier*, s. 29
[8] http://www.juraplexus.dk/juridisk-leksikon/id.de-lege-lata/i.html

virksomheders behandling af forbrugers biometriske data i forhold til Databeskyttelsesforordningen.

1.4.1.2. Retskilder og deres retskildemæssige værdi

For at fastsætte gældende ret gennem den retsdogmatiske metode er der i afhandlingen anvendt forskellige retskilder[9], der har varierende retskildemæssig værdi.

Afhandlingen inddrager både nationale og EU-retlige regler. EU-retten har en direkte virkning i national ret, hvorfor fortolkningen af nationale regler skal ske i overensstemmelse med EU-retten.[10] Danmark har siden 2000 være forpligtet til at fortolke legaldefinitioner EU-konformt, hvilket blev bekræftet af Domstolen i Google Spain-sagen.[11] Forpligtelsen om konformfortolkning blev skærpet med Databeskyttelsesforordningen grundet et ønske om mere konsekvent og ensartet retsstilling, jf. GDPR præambel 9 og 10. Både EU-Domstolens praksis og vejledninger fra Det Europæiske Databeskyttelsesråd (herefter Databeskyttelsesrådet), tidligere Artikel 29-gruppen, vil spille en afgørende rolle i den EU-konforme fortolkning. Nationale regler vil efter forordningens indtræden fortsat have en vis retskildemæssig værdi, hvis kravet om EU-konform fortolkning opfyldes.[12]

Databeskyttelsesforordningen fastsætter en mulighed for indførelse af specifikationer eller begrænsninger af forordningens regler i national ret. Medlemsstaterne kan indarbejde elementer af forordningen i deres nationale ret, herunder Databeskyttelsesloven (herefter DBL), hvis det er nødvendigt af hensyn til sammenhæng og for at gøre nationale bestemmelser forståelige for de personer, som de finder anvendelse på.[13] DBL vil i afhandlingen behandles, hvor det er nødvendigt som supplement til forordningen.

Vejledninger vil som udgangspunkt tillægges en begrænset værdi retskildemæssigt ved fastlæggelse af gældende ret, da det er en myndigheds fortolkning af lovgivning. I

[9] Christian D. Tvarnø og Ruth Nielsen: *Retskilder og retsteorier,* s. 477 – En retskilde beskrives af den europæiske realistiske retspositivisme som en norm, altså et normativt udsagn om et retsspørgsmål afgivet med en bestemt retlig kompetence.
[10] Ibid., s. 205 ff.
[11] C-131/21 (Google Spain), præmis 32-41
[12] C-6/64 (Flamino Costa mod ENEL)
[13] GDPR præambel 8

afhandlingen vil vejledninger fra Databeskyttelsesrådet og Artikel 29-gruppen benyttes for at få en bedre forståelse af persondataretten, hvor vejledningerne bidrager til en ensartet anvendelse af bestemmelserne inden for området, jf. Persondatadirektivet art. 30, stk. 1, litra a. Med ikrafttrædelse af Databeskyttelsesforordningen blev Artikel 29-gruppen afløst af Databeskyttelsesrådet. Selvom Artikel 29-gruppen formelt er instrueret af Persondatadirektivet, vil gruppens udtalelser og arbejdspapirer stadig tillægges betydning.[14]

Når lovtekster eller praksis ikke giver et klart billede og tydeliggør retstilstanden, er det relevant at søge emnet belyst i den juridiske litteratur. Den juridiske litteratur udgør ikke i sig selv en retskilde grundet forfatterens subjektive fortolkning, men den er med til at give et overblik samt en forståelse af det pågældende emne. Resultater af andre juristers anvendelse af den retsdogmatiske metode vil resultere i den juridiske litteratur, som dermed opnår legitimitet ved at være resultatet af den fælles anerkendte retsdogmatiske metode.

Afhandlingen vil anvende det danske Datatilsyns baggrundsnotat[15] som udgangspunkt for samspillet mellem GDPR art. 6 og 9. Litteratur, vejledninger osv. fra før baggrundsnotatet vil som udgangspunkt ikke være anvendelige, da fortolkningen af reglerne i GDPR art. 6 og 9 er ændret med baggrundsnotatet. Da litteratur og retspraksis fra efter udgivelse af baggrundsnotatet er begrænset, vil litteratur, vejledninger osv. fra før baggrundsnotatet benyttes som belæg for afhandlingens behandlingsområde.

Den begrænsede adgang til litteratur og retspraksis medfører en meget snæver konklusion på afhandlingen. Konklusionen havde haft et bredere fundament og nemmere grundlag for bevarelse af problemformuleringen, hvis omfanget af retspraksis og litteratur havde været større.

[14] Peter Blume: *Den nye persondataret*, s. 52-53
[15] Datatilsynets baggrundsnotat: *j.nr. 2019-20-0004*

1.4.1.3. Udvælgelse af praksis

Retspraksis

Retspraksis betragtes som en egentlig retskilde, hvorfor det er nærliggende at overveje, om retspraksis kan inddrages ved besvarelse af afhandlingens problemformulering.
I søgningen efter relevant dansk retspraksis har det vist sig, at der endnu ikke foreligger dansk retspraksis med relevans for afhandlingens behandlingsområde. I analysen inddrages engelsk retspraksis, da Databeskyttelsesforordningen finder anvendelse på alle andre medlemsstater i EU på lige fod med Danmark, jf. GDPR art. 3, stk. 1. En afgørelse fra en international domstol vil ikke nødvendigvis have retsvirkning i Danmark, hvorfor Danmark som national stat har mulighed for at rette sig efter afgørelsen, uden det er et krav.

Afgørelser fra Datatilsynet

Datatilsynet er en uafhængig myndighed, der fører tilsyn med og vejleder om overholdelse af reglerne om databeskyttelse.[16]
Tilsynets afgørelser inddrages som fundament for afhandlingens juridiske analyse, da der ikke findes retspraksis på området. På baggrund af tilsynets virke og sammensætning, vil afgørelserne tillægges en betydelig værdi i analysen af retstilstanden, især med en betragtning om at der endnu ikke er forelagt lignende sager om behandling af biometriske data til kommercielt brug for domstolene.
Datatilsynets afgørelser betragtes ikke som egentlige retskilder. Såfremt der fremlægges sager ved domstolene omhandlende behandling af biometriske data af kommerciel interesse, vil det muligvis ændre på Datatilsynets afgørelser og dermed retstilstanden.

Det skal bemærkes, at den juridiske analyse behandler afgørelser fra henholdsvis 2003, 2004, 2006, 2008, 2017, 2019 og 2020. Med blot nogle få afgørelser fra efter Databeskyttelsesforordningen trådte i kraft, er det vigtigt at gøre læseren opmærksom på, at der skal tages højde for, at retstilstanden er ændret fra tidspunktet for de historiske afgørelser og til nu. Datatilsynets historiske afgørelser fra før forordningen tager udgangspunkt i den tidligere Persondatalov, som bygger på det tidligere Databeskyttelsesdirektiv. På baggrund af det ændrede retsgrundlag, skal de historiske afgørelser tillægges mindre retskildemæssig værdi.

[16] Se GDPR art. 52 og 57

Den juridiske analyse behandler tillige afgørelser fra andre europæiske datatilsyn, herunder Sverige, Polen og Frankrig. Afgørelserne tager udgangspunkt i Databeskyttelsesforordningen, hvilket giver afgørelserne samme retskildemæssige værdi som nationale afgørelser fra efter forordningens ikrafttrædelse.
Det har ikke været muligt at finde frem til den polske og franske afgørelse, hvorfor analysen foretages ud fra et resumé af afgørelserne. På grund af sprogmæssige begrænsninger har det været svært at finde afgørelser fra andre europæiske lande, og det har været svært at analysere afgørelserne fra henholdsvis Polen og Frankrig. Afgørelserne er fundet på de pågældende Datatilsyns hjemmesider.

1.4.2. Økonomisk metode og teori

1.4.2.1. Retsøkonomisk metode

I retsøkonomien undersøges retten ud fra økonomiske teorier og modeller.[17] Metoden benyttes til at vurdere gældende ret ud fra et mål om økonomisk efficient ressourceallokering. Der er dermed et ønske om at finde frem til, om en domstol vil tillægge den økonomiske effektivitet vægt, og om denne vægt får prioritet over for de andre juridiske argumenter, herunder Databeskyttelsesforordningen. Undersøgelsen sker ud fra et normativt niveau for at finde svaret på, hvilken slags retsregler samfundet bør have for på den måde at finde frem til, hvordan retten skal være. I forlængelse med den retsdogmatiske analyse foretages der en retsøkonomisk analyse for at finde frem til, hvad konsekvenserne ved implementering af teknologiske systemer, herunder ansigtsgenkendelse, har af betydning for virksomheder, forbrugere og samfundet.

1.4.2.2. Nyinstitutionelle økonomi

Afhandlingens økonomiske analyse tager udgangspunkt i den nyinstitutionelle økonomi, som er kendetegnet ved en forudsætning om effektiv og ikke-fuldkommen konkurrence. Aktørerne på markedet er begrænset rationelle og har et ønske om at maksimere deres egne interesser inden for rammerne af den institutionelle ramme.[18] Fælles for både den neoklassiske økonomiske teori og den nyinstitutionelle økonomi er, at analyseniveauet er markedet, og analyseenheden er virksomheden.[19]

---

[17] Kim Østergaard: *Metode på cand.merc.jur. studiet, s. 277*
[18] Ibid.*, s. 273*
[19] Kim Østergaard: *Relevansen af interdisciplinær…,* s. 6

1.4.2.3. Mikroøkonomi

Den økonomiske analyses opstillede modeller, der anvendes til at undersøge den økonomiske gevinst ved behandling af biometriske data i tekniske systemer, herunder ansigtsgenkendelse, er baseret på den mikroøkonomiske teori angående markedets udbud og efterspørgsel. Teorien søger at forklare, hvordan forskellige aktører på markedet agerer, samt hvordan samfundets ressourcer som følge at denne ageren vil allokeres. Traditionelt består teorien af en udbuds- og efterspørgselskurve, som kan anvendes til at undersøge den samlede velfærd, herunder forbrugervelfærden og producentoverskuddet. Derudover vil teorien benyttes til at beskrive en markedssituation med prisdiskrimination. Udbudskurven viser forholdet mellem markedsprisen og den mængde, som en virksomhed er villig til at producere og sælge.[20] Efterspørgselskurven viser den mængde, som forbrugeren efterspørger til en given pris.[21]

1.4.3. Integreret teori og metode

1.4.3.1. Retspolitik

I forhold til den måde hvorpå retten analyseres, vil retspolitikken adskille sig fra retsdogmatikken. Som tidligere nævnt analyserer retsdogmatikken gældende ret, hvor der sker en vurdering af, hvordan retten er. En retspolitisk analyse vurderer, hvordan retten bør være.[22] Retspolitikken giver dermed anbefalinger om, hvordan en regel bør ændres eller udformes.[23]

Afhandlingens integrerede del, herunder afhandlingens perspektivering, vil omfatte en retspolitisk analyse. Formålet er, blandt andet ved hjælp af økonomisk teori og analyse, at foretage en vurdering af, om de nuværende regler om behandling af registreredes biometriske data i teknologiske løsninger, herunder ansigtsgenkendelsessystemer, er optimalt indrettet i forhold til omfanget af Databeskyttelsesforordningen. Dette sker ud fra den samlede konklusion på den juridiske- og økonomiske analyse. Derudover vil analysens formål være at finde frem til forslag til eventuelle alternative behandlingsmuligheder, så virksomhedernes muligheder for at opnå et mere efficient marked bliver større, samtidig med at behandlingen overholder Databeskyttelsesforordningen.

[20] Paul A. Samuelson: *Economics*, s. 51
[21] Ibid., s. 46
[22] Christian D. Tvarnø og Ruth Nielsen: *Retskilder og retsteorier*, s. 445
[23] Ibid., s. 446

1.4.4. Empiri og kildekritik

Artikler udarbejdet af juridiske og økonomiske forfattere bærer en grad af subjektivitet. Når sådanne artikler benyttes, vil de behandles med omhu. En videnskabelig artikel vil antages at udgøre en tilnærmelsesvis verificering af det faglige indhold, hvilket medfører, at forfatternes ståsted grundlæggende vil fungere som genstand for den kritiske tilgang til det persondataretlige område.

De behandlede nyhedsartikler skal benyttes endnu mere varsomt, da værdien af artiklerne ikke er særlig høj. Men grundet det begrænsede omfang af litteratur samt en perspektivering til samfundet, vil artiklerne inddrages i afhandlingen som et supplement til besvarelsen.

2. Databeskyttelsesforordningens historiske baggrund og internationale kontekst

For at kunne forstå og fortolke rækkevidden af de registreredes interesser og rettigheder i persondataretten, er det nødvendigt at forstå Databeskyttelsesforordningens plads i retssystemet og dens sammenhæng med såvel den nationale ret og EU-rettens regler.

2.1. Andre reguleringer af databeskyttelse

EMRK og EUC indeholder bestemmelser om grundlæggende menneskerettigheder, som supplerer reglerne om databeskyttelse, herunder Databeskyttelsesforordningen.[24] EMRK er inkorporeret i dansk ret og kan påberåbes af de danske domstole på linje med anden dansk lov.[25] Chartret er et supplement til EMRK, jf. EUC art. 52, stk. 3, og skal fortolkes i overensstemmelse med EMRK.

I Traktaten om Den Europæiske Union (TEU) findes der et grundlæggende princip om, at Unionen er baseret på principperne om frihed, demokrati, respekt for menneskerettighederne og grundlæggende frihedsrettigheder, jf. TEU art. 6. Da TEU trådte i kraft, fik chartret opnået samme juridiske værdi som traktaterne, dog med det forbehold at der med EUC ikke var tilsigtet en udvidelse af Unionens beføjelser som efter traktaterne, jf. TEU art. 6, stk. 1.

[24] Jonas Christoffersen: *EU's charter om grundlæggende rettigheder med kommentarer*, s. 137

[25] https://menneskeret.dk/om-os/menneskerettigheder/menneskerettigheder-danmark/dansk-lovgivning.

I EMRK art. 8 er der fokus på beskyttelsen af privatlivets fred. I bestemmelsen er der krav om, at et indgreb i privatlivets fred skal være begrundet. Ved at foretage et indgreb efter en legitim interesse, herunder GDPR art. 6, stk. 1, litra f, kræves der dermed en begrundelse for indgrebets nødvendighed.
Som et supplement hertil findes der i EUC art. 8 en ret til selvstændig beskyttelse af personoplysninger. Bestemmelsen fastsætter et krav om et retsgrundlag for behandling af personoplysninger, herunder samtykke eller andet berettiget grundlag.

Med EMRK og EUC skabes der et behov for et tilstrækkeligt retsgrundlag ved behandling af personoplysninger. Med betingelser for retsgrundlaget og krav om nødvendighed heraf vil der ske en styrkelse af betydningen for princippet om lovlighed.
Selvom fokus ved vedtagelse af EMRK ikke er det samme som i dag persondataretligt, bidrager EMRK art. 8 med et godt og vigtigt grundlag for retspraksis, som omhandler databeskyttelsesretten, hvilket blev fastslået af Menneskerettighedsdomstolen i sag nr. 61496/08.[26]

2.2. Fra Persondatadirektiv til Databeskyttelsesforordning

Den store udvikling på det persondataretlige område skabte et ønske om at afløse det hidtidige Persondatadirektiv.[27] Persondatadirektivet blev afløst af Databeskyttelsesforordningen[28], som fik virkning i medlemsstaterne d. 25. maj 2018. Forordningen er i dag udgangspunktet for gældende databeskyttelsesret.
Danmark valgte at supplere forordningen med Databeskyttelsesloven (DBL)[29], som ophævede den hidtidige Persondatalov.[30]

Overgangen fra direktiv til forordning var grundet et ønske om en større grad af harmonisering i medlemsstaterne.[31] Siden Persondatadirektivets vedtagelse i 1995 har den hastige teknologiske udvikling og globalisering skabt nye udfordringer vedrørende

[26] Henrik Udsen: *IT-ret*, s.323-324 - Sagen omhandlede en arbejdsgiver, der gennemgik en af de ansattes private elektroniske kommunikation, uden forudgående at havde informeret den ansatte herom
[27] Direktiv 95/46 EF *om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger*
[28] Forordning 2016/679 *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*
[29] Lov nr. 502 af 23. maj 2018 *om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger*
[30] Henrik Udsen: *IT-ret*, s. 330
[31] Ibid., s. 329

personoplysninger, hvilket har medført et krav om en stærkere og mere sammenhængende databeskyttelsesramme i Unionen.[32]

En vedtagelse af Databeskyttelsesforordningen skabte den tillid, som ville gøre det muligt for den digitale økonomi at udvikle sig på det indre marked, da forordningen forholder sig mere til problemstillinger, som vi kender i dag.[33]

Hensigten med at vælge en forordning er at undgå nationale implementeringslove, hvilket DBL i nogle tilfælde ikke lever op til.[34] Der blev i forordningen indsat regler om, at medlemsstaterne kunne supplere forordningen med egne behandlingsregler, herunder GDPR art. 6, stk. 2 og art. 9, stk. 2, litra a. Medlemsstaterne har mulighed for at vælge nationale regler på nogle specifikke områder. Det ses for eksempel i GDPR art. 8, stk. 1, hvor hovedreglen er, at børn under 16 år ikke kan give samtykke til udbydere af informationstjenester. Medlemsstaterne har her mulighed for at fastsætte en national aldersgrænse helt ned til 13 år, jf. DBL art. 8, stk. 1, 3. pkt.

Som beskrevet ovenfor er Databeskyttelsesforordningen udgangspunktet for databeskyttelsesretten i dag. EMRK og EUC har ikke samme fokus i dag som på vedtagelsestidspunktet, men giver alligevel et godt grundlag for behandling af spørgsmål om rettigheder og behandling af personoplysninger.
På nationalt plan bliver forordningen suppleret med DBL. Ud over DBL findes der andet særlovgivning nationalt, der regulerer behandling af personoplysning, herunder Sundhedsloven og TV-overvågningsloven.

[32] GDPR præambel 6 og 7
[33] GDPR præambel 7
[34] Ibid., Under forhandlingerne om forordningen, havde en række medlemsstater, herunder Danmark, et ønske om at opretholde eksisterende særregler for at have et nationalt råderum.

Del 2 – Tekniske løsninger og centrale begreber og retskilder

I afsnittet vil der foretages en gennemgang af de relevante forudsætninger for afhandlingens analyse.

3. Tekniske løsninger til brug for behandling af biometriske data

Afsnit 3 giver en teoretisk gennemgang af de tekniske løsninger, hvor det er muligt at behandle biometriske data, herunder hvilke former for biometrisk data der anvendes.

3.1. Former for biometriske data

Biometriske data, som defineres senere i opgaven, findes i forskellige former[35], jf. også GDPR art. 4, nr. 14;

1) Ansigtsgenkendelse: måling af de unikke mønstre i et individs ansigt ved en sammenligning og analyse af ansigtskonturer. Det er denne form, som afhandlingen tager udgangspunkt i.

2) Irisgenkendelse: identifikation af de unikke mønstre for et individs iris, som det farverige område i øjet omkring pupillen.

3) Fingeraftryksscanning: registrering af de unikke mønstre af dybderne på fingeren. Denne scanning ses i dag ved mange smartphones og nogle bærbare computere.

4) Stemmegenkendelse: måling af de unikke lydbølger i stemmen, ved at tale til en enhed.

5) Håndgeometri: måling og registrering af længden, tykkelsen, bredden og overfladearealet på et individs hånd.

6) Adfærdsegenskaber: analyse af den måde, hvorpå individet interagerer ved et edb-system.

Systemer, der ikke behandler personoplysninger, vil falde udenfor forordningens anvendelsesområde, hvorfor disse systemer ikke har interesse for afhandlingens område.

[35] https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html

Systemerne nedenfor tager udgangspunkt i ansigtsgenkendelse. Det betyder dog ikke, at måden hvorpå systemerne er bygget op, ikke vil kunne benyttes i situationer, hvor anden form for biometrisk data anvendes.

3.2. Ansigtsgenkendelsessystemer

Teknisk set findes der forskellige former for systemer med ansigtsgenkendelse. Det er derfor vigtigt at fastslå, hvilke former for ansigtsgenkendelsessystemer der findes, og dermed hvilke systemer der vil falde under GDPR art. 9, da systemerne er afhandlingens udgangspunkt.

Begreberne "verifikation" og "identifikation" er benyttet i afhandlingen ud fra Artikel 29-gruppens definitioner i deres udtalelse WP 193[36], hvor "traditionel ansigtsgenkendelse" er udledt af de i afsnittes benyttede artikler.

3.2.1. Traditionel ansigtsgenkendelse

Ved et system med traditionel ansigtsgenkendelse vil softwaren registrere, om der er et ansigt indenfor kameraets området for på den måde at foretage en analyse af ansigtstræk, herunder placering, størrelse og/eller form på ansigtets funktioner og egenskaber, henholdsvis øjne, næse, kæbe, mund osv. Denne form for ansigtsgenkendelsessystem benyttes for eksempel ved Animoji- og Instagram-filtre, hvor kameraet registrerer de definerede funktioner og vartegn. Efter en registrering vil systemet benytte algoritmer (udregnede værdier) til at låse sig fast på ansigtet for på den måde at bestemme, hvilken retning ansigtet ser, om der er en åben mund eller anden for registrering.[37]

En traditionel ansigtsgenkendelse vil foretage en registrering og ikke en identifikation eller et match af den registrerede, som befinder sig indenfor kameraets område. Derudover vil de registrerede ansigtsoplysninger ikke lagres på en ansigtstemplate, hvor der foretages en udregnet værdi af de biometriske data.

3.2.2. Verifikation[38]

Denne form for system foretager en 1:1 sammenligning.[39] Sammenligningen sker ud fra to biometriske skabeloner, som normalt vil antages at tilhøre den samme person, for at

[36] Artikel 29-gruppen udtalelse: *WP 193*
[37] https://www.howtogeek.com/427897/how-does-facial-recognition-work/
[38] Artikel 29-gruppen udtalelse: *WP 193*, s. 6
[39] FRA: *Facial recognition technology: fundamental rights considerations […]*, s. 7

bestemme om personen på de sammenlignelige billeder er den samme. Det sker for eksempel ved konfigurering af Face-ID eller lignende på mobilen eller andre enheder. Den registrerede registrerer sit ansigtsbillede i systemet, hvor der foretages en måling af afstanden mellem ansigtsfunktionerne. Hver gang mobilen skal låses op, vil softwaren anvende kameraet til at måle og bekræfte (verificere) den registreredes identitet. Verifikation kræver ikke nødvendigvis, at de scannede biometriske oplysninger opbevares og lagres i ansigtsgenkendelsessystemet, da der er tale om en 1:1 sammenligning. I stedet vil systemet registrere præcise ansigtsdata ved projicering og analysering af punkter i ansigtet for på den måde at skabe en digital model af den registreredes ansigt. Den digitale model bliver transformeret til et matematisk billede, der ved hjælp af algoritmer sammenlignes med den registreredes ansigtsbillede.[40]

3.2.3. Identifikation[41]

Der findes systemer med ansigtsgenkendelse, hvor der foretages en identifikation af den registrerede blandt mange andre registrerede[42], hvilket i afhandlingen betegnes som et system med identifikation. Systemet svarer til systemer med *verifikation* dog med en større skala af personoplysninger. Algoritmer behandles for at foretage en sammenligning af det scannede ansigt og en omfattende database med ansigter af andre registrerede. Databaser med klare og forud-identificerede ansigtsbilleder er at foretrække, selvom enhver form for database kan benyttes. I sammenligningen vil der aktiveres en beregning af lighederne mellem billederne, der angiver sandsynligheden for, at billederne refererer til det samme individ.[43] Det ses blandt andet ved organisationers ønske om identifikation af ansigter grundet sikkerheds-, reklame- eller politimæssige formål.[44]

Ansigtsgenkendelsessystemer der benyttes ved videoovervågning fungerer ofte som realtidsteknologi, hvor behandlingen foretages med det samme, og hvor videomaterialet ikke optages.[45] I andre situationer er det nødvendigt at opbevare videomaterialet, hvor materialet kun behandles i tilfælde af en hændelse.[46]

---

[40] https://support.apple.com/da-dk/HT208108
[41] Artikel 29-gruppen udtalelse: *WP 193,* s. 5
[42] FRA: *Facial recognition technology: fundamental rights considerations […]*, s. 8
[43] DPIAC: *Privacy recommendations in Connection with the Use of Facial Recognition Technology,* s. 2
[44] https://www.howtogeek.com/427897/how-does-facial-recognition-work/
[45] FRA: *Facial recognition technology: fundamental rights considerations […]*, s. 8
[46] Det Europæiske Databeskyttelsesråds vejledning: *Guidelines 3/2019,* s. 11

3.2.4. Behandling i 2D og 3D

De fleste systemer foretager ofte ansigtsgenkendelse i 2D uden dybde i ansigtet. Uden nogen form for dybde i det scannede ansigt vil systemet mangle identificerende funktioner. Det er muligt for systemet at måle den registreredes afstand mellem pupiller og bredde på munden, men det er ikke muligt af måle længden af næsen eller pandens prominens. 2D er afhængig af et godt lys, hvorfor en 2D scanning ikke er velfungerende i mørke. Forhold som lys, afstand og placering vil dermed kunne begrænse en behandling foretaget i 2D.[47] Af den grund vil en levende form for ansigtsgenkendelsessystem være mere tilbøjelig til at lave fejl, når der skal foretages en sammenligning af ansigtsbillederne i 2D.[48] En tredimensionel ansigtsgenkendelsesteknik i systemet vil kunne løse disse fejl. Teknikken bruger 3D-sensorer til at fange informationer om ansigtets form. Oplysningerne bruges til at identificere karakteristiske træk på overfladen af ansigtet, såsom konturen på næse og hage. Teknikken vil ikke påvirkes af belysningen som en basal 2D-billededannelse, og det vil kunne identificere et ansigt fra flere synsvinkler. Ansigtsgenkendelsesteknikken sender infrarød (IR)-matrix i den registreredes ansigt. Denne matrix reflekteres herefter fra ansigtet og bliver sendt tilbage til et IR-kamera. Kameraet måler, hvor lang tid det tager for hver bit IR-lys at hoppe ud til den registreredes ansigt og tilbage til ansigtsgenkendelsesenheden. Der skabes her et unikt dybdekort over ansigtet, hvorfor brugen af 3D sammen med den basale 2D-billededannelse skaber en større nøjagtighed af systemets behandling.[49]

Kameraer med termisk behandling gør det muligt at foretage ansigtsgenkendelse om natten. Ved termisk behandling sker der registrering af det IR-lys, som den registrerede udsender, hvorfor der er mulighed for at registrere temperaturforskelle på en overflade.[50]

3.2.5. Delkonklusion

Der findes forskellige former for ansigtsgenkendelsessystemer, som alle behandler personoplysninger forskelligt. Der kan i ansigtsgenkendelsessystemer både foretages registrering, verifikation og identifikation af den registrerede. Da ansigtsgenkendelsessystemer kan foretage mange forskellige former for behandling, er det derfor vigtigt at se på

[47] https://www.howtogeek.com/427897/how-does-facial-recognition-work/
[48] FRA: *Facial recognition technology: fundamental rights considerations […]*, s. 8
[49] https://www.howtogeek.com/427897/how-does-facial-recognition-work/
[50] Ibid.

det tekniske setup, herunder funktionalitet og omfang, for at kategorisere systemet i en af de ovenstående kategorier. Verifikation, i nogle tilfælde, og identifikation kræver lagring af skabelonen af det scannede ansigt til brug i en senere sammenligning.

4. Centrale begreber og retskilder

I dette afsnit vil de relevante definitioner og bestemmelser i Databeskyttelsesforordningen, med relevans for afhandlingens område, behandles, herunder GDPR art. 4, 5, 6, 9, 21/22 og 35/36.

4.1. Centrale definitioner (GDPR art. 4)

4.1.1. Personoplysninger

GDPR art. 4 indeholder legaldefinitioner af begreber, som er omfattet af Databeskyttelsesforordningen. Bestemmelsens nr. 1 definerer begrebet ”personoplysninger”:

> ”Enhver form for information om en identificeret eller identificerbar fysisk person (”den registrerede”); ved identificerbar fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.”

Definitionen suppleres af forordningens præambel 26 og 30, hvor der foretages en præcisering af, at pseudonymiserede oplysninger samt onlineidentifikatorer er omfattet af definitionen. Præambel 26 understreger rækkevidden af definitionen ved en præcisering af begrebet ”identificerbar”. Efter præambel 26 bør alle midler tages i betragtning, for at kunne identificere en identificerbar fysisk person, hvis det med rimelighed kan tænkes, at det vil bringes i anvendelse. Hertil bør alle objektive forhold som omkostninger og tid, der er nødvendig for identifikationen, tages i betragtning, under hensyntagen til den tilgængelige teknologi på tidspunktet for behandlingen og den teknologiske udvikling.

Både EU-Domstolen[51] og Datatilsynet[52] har generelt anlagt en bred fortolkning af begrebet, hvilket også var hensigten efter EU-rettens forarbejder.[53] Denne brede fortolkning medfører nye grænsetilfælde grundet den teknologiske udvikling, hvilket blandt andet kan ses i praksis.

Behandling af personoplysninger defineres i GDPR art. 4, nr. 2 med supplering af GDPR præambel 15. Efter præambel 15 er behandlingen efter GDPR teknologineutral, hvorfor både manuelle og digitale behandlinger af personoplysninger er omfattet af forordningen.

4.1.2. Biometriske data

Efter forordningen er der i GDPR art. 9 indsat en ny form for personoplysning kaldet "biometriske data". Biometriske data er en speciel form for data, som i princippet deles på tværs af de fleste hvis ikke hele den menneskelige befolkning. De er stabile, i hvert fald i de betydelige perioder af et menneskes liv, samt karakteristiske, hvis ikke unikke, for det enkelte individ.[54]

Definitionen af biometriske data findes i GDPR art. 4, nr. 14:

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

Bestemmelsen opdeler biometriske data i; 1) fysiske egenskaber (blandt andet ansigtstræk, fingeraftryk og irisegenskaber) og 2) adfærdsegenskaber (blandt andet vaner, handlinger og personlighedstræk). Der skal efter definitionen muliggøres eller bekræftes en entydig identifikation af den registreredes karakteristika, ved at anvende en specifik teknisk behandling, for at der er tale om biometriske data.

---

[51] F.eks. De forenede sager C-92/09 og C-93/09 (om selskabsnavn for personligt ejede selskaber, præmis 53 og 54); C-342/12 (om arbejdstageres tidsregistreringer, præmis 18-22) samt C-434/16 (om eksamensbesvarelse alene påført eksamensnr.)
[52] F.eks. afgørelse nr. 2004-219-0208 (om fingeraftryk), nr. 2007-631-0020 (om billeder) samt nr. 2015-631-0122 (om nummerplader).
[53] Artikel 29-gruppen udtalelse: *WP 136*, s. 4
[54] Peter Blume: *Ret, privatliv og teknologi*, s. 208

Efter GDPR præambel 51 falder almindelige fotografier udenfor definitionen af biometriske data:

> ” […] Behandling af fotografier bør ikke systematisk anses for at være behandling af særlige kategorier af personoplysninger, eftersom de kun vil være omfattet af definitionen af biometriske data, når de behandles ved en specifik teknisk fremgangsmåde, der muliggør entydig identifikation eller autentifikation af en fysisk person […]”

Ved et specifikt ansigtsgenkendelsessystem er det afgørende, om der sker identifikation af fysiske personer. Hvis systemet ikke muliggør identifikation af de registrerede, vil ansigtsgenkendelsessystemet falde udenfor definitionen af biometriske data, jf. GDPR art. 4, nr. 14, og dermed GDPR art. 9, herunder den traditionelle ansigtsgenkendelse i afsnit 3.2.1. Det samme gør sig gældende ved fotografier eller videooptagelser uden en særlig teknisk mulighed for et match eller sammenligning af andre identifikationsoplysninger. En behandling af personoplysninger, som falder udenfor GDPR art. 9, vil i stedet for være omfattet af GDPR art. 6, om almindelige personoplysninger.

4.1.3. Profilering

Profilering defineres i GDPR art. 4, nr. 4 som:

> ”enhver form for automatisk behandling af personoplysninger, der består i at anvende personoplysninger til at evaluere bestemte personlige forhold vedrørende en fysisk person, navnlig for at analysere eller forudsige forhold vedrørende den fysiske persons […], personlige præferencer, interesser, pålidelighed, adfærd, geografiske position eller bevægelser”

Profilering er en moderne teknologi, hvor der sker en automatiseret brug, gennem onlineidentifikatorer, af personoplysninger, der gør det muligt at profilere og identificere de registrerede og på den måde evaluere personlige træk, jf. GDPR præambel 30. Det er med teknologien muligt at forudsige fremtidig adfærd, for eksempel i købssituationen, eller afdække personlige interesser eller præferencer.

Profilering kan anvendes på tre måder: 1) generel profilering, 2) afgørelser baseret på profilering og 3) afgørelser, der alene er baseret på automatisk behandling, herunder profilering, som har retsvirkning eller betydeligt har påvirket den registrerede, efter GDPR art. 22, stk. 1.[55] Forskellen på 2) og 3) er, at der i 2) er en personlig indblanding i profileringen, hvor profileringen i 3) sker ud fra algoritmer og dermed alene er baseret på en automatisk behandling.

Automatiske afgørelser, der alene baseres på automatisk behandling, er evnen til at træffe en afgørelse teknologisk uden menneskelig indgriben. Ikke alle automatiske afgørelser omfatter profilering af den registrerede, men de kan delvist overlappe med eller være resultatet af profilering.[56] En simpel klassificering af den registrerede baseret på karakteristika som køn, alder og højde, vil ikke nødvendigvis indebære profilering. Det afhænger af formålet med den pågældende klassificering.
Ved at benytte ansigtsgenkendelsessystemer, og dermed foretage en automatisk behandling, herunder traditionel ansigtsgenkendelse, verifikation eller identifikation, se afsnit 3, betyder det ikke som udgangspunkt, at der sker en profilering af den registrerede. Der skal her ses på formålet med behandlingen og det tekniske setup af den automatiske behandling, for at finde frem til, om systemet foretager en profilering.

Der vil kunne foretages profilering og træffes automatisk afgørelse, hvis de grundlæggende behandlingsprincipper er opfyldt, jf. GDPR art. 5, og der er et retligt grundlag for behandlingen efter GDPR art. 9 og 6.

4.2. Relevante regler i GDPR

Ovenfor er de vigtigste legaldefinitioner for brugen af biometriske data defineret. Lige så vigtigt er det at fastlægge de relevante regler i Databeskyttelsesforordningen for behandling af biometriske data. De generelle principper i GDPR art. 5, stk. 1, litra a-f går igennem hele forordningen som røde tråde. Principperne skaber et grundlæggende fundament for lovligheden af persondatabehandling og angiver derfor de grundlæggende rammer for virksomheden. Når principperne er opfyldt, kan den videre behandling af personoplysninger foretages.

[55] Artikel 29-gruppens vejledning: *WP 251,* s. 9
[56] Ibid., s. 8

4.2.1. Art. 5.

4.2.1.1. Ansvarlighed

For alle de grundlæggende principper i GDPR art. 5, stk. 1 gælder der et fælles ansvarlighedsprincip, jf. GDPR art. 5, stk. 2. Ansvarlighedsprincippet er en af de mest fundamentale forpligtelser i forordningen. Den dataansvarlige, som efter GDPR art. 4, nr. 7 defineres som; "en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger", er ansvarlig for og skal kunne påvise, at behandlingsprincipperne i stk. 1 overholdes. Ansvaret hos den dataansvarlige findes i GDPR art. 24, hvor ansvaret medfører en gennemførelse af tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandlingen sker i overensstemmelse med forordningens regler, jf. GDPR art. 24, stk. 1. Denne sikring og påvisning sker ved på forhånd at have designet og indrettet en sikring for behandlingen, jf. GDPR art. 25, stk. 1 (databeskyttelse gennem design) samt ved at justere standardindstillinger, jf. GDPR art. 25, stk. 2 (databeskyttelse gennem standardindstillinger), for på den måde at fremme databeskyttelsen. Formålet med for eksempel videoovervågning skal dokumenteres skriftligt og specificeres for hvert overvågningskamera, medmindre kameraerne bruges til det samme formål af en enkelt dataansvarlig, da behandlingen kan have forskellig karakter og omfang for hvert kamera.[57]

4.2.1.2. Relevante behandlingsprincipper

Ud fra ovenstående er det den dataansvarlige, der er ansvarlig for, at de grundlæggende behandlingsprincipper overholdes for enhver behandling af personoplysninger. I dette afsnit vil de mest relevante principper i GDPR art. 5, stk. 1 for behandling af biometriske data efter afhandlingens område beskrives.

<u>*God behandlingsskik*</u>

God behandlingskik er kravet om *lovlig, rimelig og gennemsigtig* behandling af personoplysninger, jf. GDPR art. 5, stk. 1, litra a. Kravet om *lovlighed* fastslår, at behandlingen skal overholde forordningens beskyttelsesinteresse samt tilhørende lovgivning.[58] Den dataansvarlige skal med kravet om *rimelighed* opføre sig retfærdigt og loyalt ved at drage

[57] Det Europæiske Databeskyttelsesråd vejledning: *Guidelines 3/2019.,* s. 9
[58] Bent Ole Gram Mortensen (red.): *Dansk persondataret*., s. 59

omsorg for de personoplysninger, der behandles.[59] Den registrerede skal være fuldt ud informeret om behandlingen af vedkommendes personoplysninger før, der gives samtykke til behandlingen, hvilket også fremgår af GDPR art. 7.[60] Kravet om *gennemsigtighed* fastslår, at den registrerede skal have mulighed for at kunne overskue behandlingen af vedkommendes personoplysninger, jf. GDPR præambel 39.[61]

Dataminimering

Personoplysninger skal være "tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles", jf. GDPR art. 5, stk. 1, litra c, hvilket også kaldes proportionalitetsprincippet.

Som et supplement til bestemmelsen findes der i GDPR præambel 39 et krav om, at perioden for opbevaring af personoplysninger ikke må være længere end strengt nødvendigt. Oplysninger, som både er relevante og tilstrækkelige, skal derfor også opfylde kravet om *nødvendighed*. Det er op til den dataansvarlige at vurdere, om realisering af formålet gør det nødvendigt at have oplysningerne i en sådan form, så den registrerede kan identificeres.[62]

Duplikerer oplysningerne andre informationer, eller er oplysningerne overflødige, vil de ikke opfylde kravet om nødvendighed.[63] Der skal kun indsamles oplysninger nok til, at det oprindelige formål kan opnås efter kravet om dataminimering.[64] Behandlingsformålet må derfor ikke kunne opfyldes med mindre indgribende midler, hvorfor der skal være sammenhæng mellem behandlingsformen og det ønskede formål.

Opsummerende omfatter proportionalitetsprincippet en vurdering af nedenstående punkter:

1. Hvorvidt det benyttede system er nødvendigt for at opfylde behandlingens formål, eller om systemet alene er benyttet til f.eks. at finde en nemmere og billigere løsning?
2. Er det valgte system effektivt og velegnet til behandlingens formål?

[59] Personoplysninger tilhører den registrerede, hvorfor de behandlede oplysninger kun er til låns, jf. GDPR præambel 7, 2. pkt.
[60] Bent Ole Gram Mortensen (red.): *Dansk persondataret*., s. 60
[61] Kommunikationen om behandlingen skal anvende et klart, enkelt og forståeligt sprog, ses GDPR art. 12, stk. 1.
[62] Bent Ole Gram Mortensen (red.): *Dansk persondataret*, s. 92
[63] Det kan nogle gange være nok at bruge pseudonymiserede eller anonymiserede oplysninger.
[64] Bent Ole Gram Mortensen (red.): *Dansk persondataret*, s. 91

3. Står et resulteret tab af privatliv i rimeligt forhold til virksomhedens forventede fordele? En praktisk fordel eller en mindre økonomisk besparelse vil ikke anses som en hensigtsmæssig behandling.
4. Kan et middel, der griber mindre ind i privatlivets fred, opfylde formålet? [65]

4.2.2. Art. 6 og 9

I forordningen skelnes der mellem almindelige og særlige kategorier af personoplysninger (følsomme personoplysninger) i henholdsvis GDPR art. 6 og 9.

4.2.2.1. Særlige kategorier af personoplysninger

I GDPR art. 9 er der en udtømmende liste over, hvilke personoplysninger der anses som særlige kategorier af personoplysninger. Det betyder, at almindelige personoplysninger efter GDPR art. 6 omfatter de personoplysninger, som ikke er oplistet i GDPR art. 9 og art. 10 om strafbare forhold.

GDPR art. 9, stk. 1 fastsætter et forbud mod at behandle følsomme personoplysninger, da oplysningerne kræver en særlig beskyttelse. Det følger af ordlyden i GDPR art. 9, stk. 1, at biometriske data kun er omfattet af forbuddet, hvis formålet er at identificere en fysisk person:

> "Behandling af personoplysninger om […] samt behandling af genetiske data, biometriske data med et formål entydigt at identificere en fysisk person […]

I GDPR art. 9, stk. 2 findes der behandlingsmuligheder for de forbud, der findes i bestemmelsens stk. 1, om behandling af følsomme personoplysninger.

4.2.2.2. Almindelige personoplysninger

Som beskrevet ovenfor omfatter GDPR art. 6 de almindelige personoplysninger. Bestemmelsen er vigtig for forordningens kernefunktion, da enhver personoplysning, selvom denne er triviel, kun må behandles med hjemmel i lov.[66] Ved behandling af almindelige

[65] De 4 vurderingstrin er defineret af Artikel 29-gruppen i: *WP 193,* s. 8
[66] Peter Blume: *Den nye persondataret*, s. 95

personoplysninger skal mindst én af betingelserne i GDPR art. 6, stk. 1, litra a-f opfyldes af den dataansvarlige.

4.2.2.3. Samspillet mellem art. 6 og 9

Tidligere var der et selvstændigt behandlingsgrundlag i GDPR art. 9, stk. 2, hvis behandlingen omhandlede følsomme personoplysninger. Kravet var, at der alene skulle findes et behandlingsgrundlag i GDPR art. 9, stk. 2 til forbuddet i GDPR art. 9, stk. 1 ved behandling af følsomme personoplysninger.[67]

Den 7. november 2019 valgte Det danske Datatilsyn at udgive et notat med en ny fortolkning af bestemmelserne i GDPR art. 6 og 9. Fremadrettet skal den dataansvarlige, som behandler følsomme oplysninger omfattet af forbuddet i GDPR art. 9, stk. 1, finde en relevant undtagelse i GDPR art. 9, stk. 2 til forbuddet samt et lovligt behandlingsgrundlag i GDPR art. 6, stk. 1. Hertil kommer de grundlæggende principper for behandling af personoplysninger i GDPR art. 5, der altid skal være opfyldt ved behandlinger omfattet af forordningen.[68]

Grundet den høje integritetsbeskyttelse, som findes i GDPR art. 9, stk. 2, må det vurderes, at behandlingsbetingelserne i GDPR art. 6, stk. 1 sædvanligvis vil være opfyldt, hvis der kan findes en undtagelse til forbuddet i GDPR art. 9, stk. 2. Hvis en behandling foretages efter samtykke fra den registrerede, er der forskel på, om der er tale om samtykke efter GDPR art. 9, stk. 2, litra a og art. 6, stk. 1, litra a. Der skal efter GDPR art. 9, stk. 2, litra a være givet en udtrykkelig samtykkeerklæring og ikke blot en utvetydig viljeserklæring til behandlingen. Kravene til samtykket er dermed større i art. 9 end i art. 6, hvorfor GDPR art. 6, stk. 1, litra a, altid vil være opfyldt ved brug af behandlingsbetingelsen i GDPR art. 9, stk. 2, litra a.

Baggrundsnotatet har givet en ny måde at fortolke GDPR art. 6 og 9 på. Der er indført et større krav til behandling af følsomme personoplysninger grundet kravet om særlig beskyttelse. Ændringen giver i praksis den registrerede mulighed for at gøre indsigelse efter GDPR art. 21, mod behandling af følsomme personoplysninger efter GDPR art. 9, i de tilfælde hvor behandlingen, foruden at opfylde en undtagelse i GDPR art. 9, stk. 2, tillige

[67] Datatilsynets baggrundsnotat: *j.nr. 2019-20-0004,* s. 3
[68] Ibid., s. 6

sker på grundlag af GDPR art. 6, stk. 1, litra e eller f.[69] Der vil med den nye fortolkning ske en ændring i betydningen for vurderingen af, og muligheden for, indsigelser efter GDPR art. 21.

Det er nødvendigt, at der findes et behandlingsgrundlag i GDPR art. 9, stk. 2 og derefter et lovligt behandlingsgrundlag i GDPR art. 6, stk. 1, når virksomheder ønsker at behandle biometriske data i en kommerciel interesse.

4.2.3. Art. 21 og 22

4.2.3.1. Ret til indsigelse

Selvom der findes et lovligt behandlingsgrundlag i GDPR art. 9 og 6, vil den registrerede til enhver tid have ret til at gøre indsigelse mod en ellers lovlig behandling af vedkommendes personoplysninger, baseret på behandlingsgrundlaget i GDPR art. 6, stk. 1, litra e eller litra f, jf. GDPR art. 21, stk. 1. Det er nu muligt at gøre indsigelse mod behandling af følsomme personoplysninger, hvis behandlingen tillige er baseret på behandlingsbetingelsen om samfundets interesse, jf. GDPR art. 6, stk. 1, litra e, eller behandlingsbetingelsen i GDPR art. 6, stk. 1, litra f, om legitim interesse, herunder profilering baseret på disse bestemmelser.[70]

Ved at den registrerede gør indsigelse mod behandlingen, vil behandlingen af den registreredes personoplysninger ikke kunne fortsætte medmindre, at den dataansvarlige kan påvise, at den legitime eller samfundsmæssige interesse går forud for interessen hos den registrerede.

4.2.3.2. Behandling alene baseret på automatisk behandling

Den registrerede har ret til ikke at være genstand for en afgørelse eller profilering, der alene er baseret på automatisk behandling, jf. GDPR art. 22, stk. 1. Afgørelser eller profilering, der har retsvirkning for eller påvirker den registrerede betydeligt, eller indebærer en evaluering af den registreredes personlige forhold, må derfor som udgangspunkt ikke behandles. Da afhandlingen omhandler den tekniske behandling af biometriske data, er der tale om automatisk behandling. Hvis den registrerede påberåber sig rettigheden efter

[69] Datatilsynets baggrundsnotat: *j.nr. 2019-20-0004*, s. 7
[70] Ibid., s. 7

GDPR art. 22, stk. 1, vil behandlingen af den registreredes biometriske data ikke kunne foretages grundet brugen af automatisk behandling.
Efter GDPR art. 22, stk. 4 åbnes der en mulighed for alligevel at kunne foretage behandling af biometriske data. Det fremgår af bestemmelsen, at afgørelser, der er omfattet af listen i stk. 2, herunder samtykke fra den registrerede, som udgangspunkt ikke må behandles på særlige kategorier af personoplysninger. Undtagelsen hertil er, at hvis den registrerede har givet sit udtrykkelige samtykke, jf. GDPR art. 9, stk. 2, litra a, eller hvis behandlingen er nødvendig af hensyn til væsentlige samfundsmæssige interesser, jf. GDPR art. 9, stk. 2, litra g, må behandlingen gerne foretages alligevel. Som et yderligere krav skal der indføres passende foranstaltninger til beskyttelse af den registreredes interesser og rettigheder.

4.2.4. Art. 35 og 36

Inden der skal foretages en behandling, navnlig ved brug af en ny teknologi, skal det analyseres, om den påtænkte behandlingsaktivitet har konsekvenser for beskyttelsen af personoplysninger, jf. GDPR art. 35, stk. 1, hvilket den dataansvarlige er ansvarlig for. Et eksempel på en ny teknologi vil være behandling af biometriske data, herunder kunstig intelligens og ansigtsgenkendelse. Der er tale om en ny teknologi i de tilfælde, hvor de eksisterende biometriske teknologier anvendes på en ny måde.[71]
Analysen har til formål først at vurdere risiciene for de fysiske personers rettigheder og frihedsrettigheder og derefter fastlægge de foranstaltninger, der vil kunne afhjælpe de fundne risici. Pligten til at foretage en konsekvensanalyse findes i de tilfælde, hvor der sandsynligvis vil være en høj risiko for de fysiske personers rettigheder og frihedsrettigheder. Der er i GDPR art. 35, stk. 7 fastsat et minimum for, hvad analysen skal omfatte. En konsekvensanalyse er særligt påkrævet ved; 1) systematisk og omfattende vurdering af personlige forhold baseret på automatisk behandling, herunder profilering, 2) behandling af særlige kategorier af følsomme personoplysninger i et stort omfang, jf. GDPR art. 9, stk. 1 og 3) systematisk overvågning af et offentligt tilgængeligt område i et stort omfang, jf. GDPR art. 35, stk. 3.
Hvis risikoen stadig er høj efter indførelse af passende foranstaltninger, og det derfor ikke har været muligt at begrænse de påviste risici, skal der ske forudgående høring hos Datatilsynet, jf. GDPR art. 36.

[71] Datatilsynets vejledning: *Konsekvensanalyse*, s. 6

4.3. Samtykke-reglens anvendelse på brugen af ansigtsgenkendelse

Samtykke skal ses som én behandlingsbetingelse blandt flere mulige behandlingsbetingelser. Selvom samtykke som behandlingsbetingelse er oplistet som den første behandlingsbetingelse i GDPR art. 9, stk. 2, litra a og art. 6, stk. 1, litra a, betyder det ikke nødvendigvis, at den dataansvarlige først skal undersøge, om den registrerede ønsker at give sit samtykke til behandlingen.

Et samtykke fra den registrerede er "enhver frivillig, specifik, informeret og utvetydigt viljestilkendegivet fra den registrerede" jf. GDPR art. 4, nr. 11.
At samtykket skal være *frivilligt*, betyder, at den registrerede har en reel bestemmelsesret og kontrol over sit samtykke[72], jf. også GDPR præambel 42. Når der ikke gives samtykke til behandling, skal der ikke være en risiko for vildledning, intimidering, tvang eller væsentlige negative konsekvenser fra den datasansvarlige side. I et afhængighedsforhold, herunder forholdet mellem elev og skole, er det usandsynligt, at den registrerede kan afvise at give et samtykke uden frygt eller risiko for, at det vil være til skade for den registrerede.[73]
Et samtykke skal tillige være *specifikt*. Her er det et krav, at formålet er klart og præcist, så der ikke er i tvivl om hvilket formål, der gives samtykke til.[74] I forlængelse heraf skal samtykket være *informeret* og dermed opfylde kravet om gennemsigtighed, jf. GDPR art. 5, stk. 1, litra a. Denne bestemmelse stiller et krav til den dataansvarlige om, at vedkommende skal informere den registrerede om behandlingens elementer.[75]
At der ved samtykke skal være en *utvetydig viljeserklæring* fra den registrerede, betyder, at den registrerede ved en erklæring eller en klar bekræftelse indvilliger i behandling af vedkommendes personoplysninger, jf. GDPR art. 4, nr. 11. Den registrerede skal derfor foretage en forsætlig handling for at give sit samtykke til behandlingen.[76]

Ved behandling af følsomme personoplysninger er det muligt at bruge samtykke som behandlingsgrundlag, hvis samtykket er givet udtrykkeligt, jf. GDPR art. 9, stk. 2, litra a. Ved et udtrykkeligt samtykke skal der være et aktivt svar fra den registrerede tilstede, hvor der ikke vil herske tvivl om, at der er givet et samtykke. En skriftlig

[72] Artikel 29-gruppen vejledning: *WP 259*, s. 13-14
[73] Ibid., s. 8
[74] Ibid., s. 13
[75] Datatilsynets vejledning: *Samtykke*, s. 10
[76] Artikel 29-gruppen vejledning: *WP 259*, s. 17

samtykkeerklæring gør det nemmere at bevise, at det udtrykkelige samtykke er afgivet.[77] Et udtrykkeligt samtykke åbner op for muligheden for at foretage afgørelser, der alene er baseret på automatisk behandling af følsomme personoplysninger, herunder afhandlingens område om biometriske data, jf. GDPR art. 22, stk. 4.

Ved at indhente et samtykke fra den registrerede medfører det ikke, at den dataansvarliges forpligtelser efter GDPR art. 5 forsvinder. I en situation med behandling af biometriske data, hvor den dataansvarlige kan opnå et legitimt behandlingsgrundlag ved den registreredes samtykke, vil det for eksempel ikke berettige en indsamling og behandling af personoplysninger, der står i misforhold til formålet.[78]

I forordningen er der indsat en bestemmelse i GDPR art. 7 med en præcisering af betingelserne for samtykke. Den dataansvarlige skal efter GDPR art. 7, stk. 1 kunne påvise, at den registrerede har givet sit samtykke til behandlingen.
Behandling af børns personoplysninger kræver en særlig beskyttelse, jf. GDPR præambel 38, hvor de særlige krav i GDPR art. 8 tillige skal opfyldes.

Kravet om kontrol findes også i GDPR art. 7, stk. 3, om den registreredes ret til, til enhver tid, at trække sit samtykke tilbage. Ved behandling af biometriske data i et teknisk system er det et krav, at den dataansvarlige implementerer tekniske midler, som effektivt kan fjerne alle identitetsforbindelser, der er oprettet i systemet, hvis den registrerede trækker sit samtykke tilbage.[79]

Ved at opfylde kravene om samtykke, jf. GDPR art. 4 og art. 7, er det muligt for den dataansvarlige at benytte samtykke som behandlingsgrundlag efter GDPR art. 6, stk. 1, litra a, og GDPR art. 9, stk. 2, litra a. Det strengere krav om et udtrykkeligt samtykke i GDPR art. 9 medfører, at der ved brug af behandlingsbetingelsen i GDPR art. 9, stk. 2, litra a tillige vil opstå en opfyldelse af betingelserne for samtykke efter GDPR art. 6, stk. 1, litra a, se også beskrivelsen i afsnit 4.2.2.1.

[77] Datatilsynets vejledning: *Samtykke*, s. 13
[78] Artikel 29-gruppen: *WP 187,* s. 8
[79] Artikel 29-gruppen: *WP 193,* s. 12

4.4. Delkonklusion

Helt overordnet er det den dataansvarliges ansvar at sikre sig, at en behandling af personoplysninger har et lovligt grundlag. At den dataansvarlige finder et behandlingsgrundlag i GDPR art. 9 og derefter art. 6, ved behandling af biometriske data, er ikke nok til et legitimt behandlingsgrundlag. Det er derudover vigtigt, at den dataansvarlige iagttager, om de grundlæggende behandlingsprincipper i GDPR art. 5 er opfyldt.
Det er kun de ansigtsgenkendelsessystemer, hvor der sker en identifikation af den registrerede, der er omfattet af definitionen på biometriske data.

Del 3 – Analyse

5. Juridisk analyse – brug af teknologier i praksis

5.1. Indledende bemærkninger

Afhandlingens analyse af praksis inddeles i de forskellige former for tekniske løsninger til brug for behandling af biometriske data, som er defineret i afsnit 3. Denne inddeling foretages, når det skal udledes, hvad Datatilsynet hidtil har lagt vægt på i vurderingen af behandlingens opfyldelse af proportionalitetsprincippet, jf. GDPR art. 5, stk. 1, litra c. Brugen af de tekniske løsninger i praksis vil tage udgangspunkt i opfyldelsen af proportionalitetsprincippet ud fra opsummeringspunkterne fra afsnit 4.2.1.2:

1. Hvorvidt det benyttede system er nødvendigt for at opfylde behandlingens formål?
2. Er det valgte system effektivt og velegnet til behandlingens formål?
3. Står et resulteret tab af privatliv i rimeligt forhold til virksomhedens forventede fordele?
4. Kan et middel, der griber mindre ind i privatlivets fred, opfylde formålet?[80]

Det er vigtigt at læseren er opmærksom på den retskildemæssige værdi af de analyserede historiske afgørelser. Selvom værdien ikke er lige så høj som ved afgørelser med udgangspunkt i Databeskyttelsesforordningen, vil de være med til at give et indblik i virksomhedernes behandlingsmuligheder kommercielt, da praksis på området er begrænset. Analysen behandler tillige afgørelser fra andre europæiske datatilsyn. Disse afgørelser vil

[80] Artikel 29-gruppen udtalelse: *WP 193,* s. 8

tillægges betydelig værdi, da Databeskyttelsesforordningen gælder for alle EU-lande, hvorfor retsgrundlaget er det samme.

Da praksis for kommercielt brug er begrænset, vil kravene til opfyldelse af proportionalitetsprincippet tillige søges i afgørelser med et andet behandlingsgrundlag, herunder GDPR art. 9, stk. 2, litra g og GDPR art. 6, stk. 1, litra e.

Alle afgørelser i analysen omfatter behandling af følsomme personoplysninger efter GDPR art. 9, hvorfor alle afgørelserne falder under Databeskyttelsesforordningens anvendelsesområde.

5.2. Traditionel ansigtsgenkendelse

Som beskrevet i afsnit 3.2.1 er der her tale om systemer, som udelukkende registrerer, om der er et ansigt indenfor kameraets område, hvorfor der ikke foretages identifikation af den registrerede. Som allerede fastlagt i afsnit 4.1.2., vil den traditionelle ansigtsgenkendelse falde uden for definitionen af biometriske data, jf. GDPR art. 4, nr. 14 og præambel 51. Systemets behandling vil dermed falde uden for behandling af følsomme personoplysninger efter GDPR art. 9, da kravet om identifikation ikke er opfyldt. For at være omfattet af forordningen, skal der foretages en behandling af personoplysninger, hvilket er beskrevet i afsnit 4.1.1. Da et traditionelt ansigtsgenkendelsessystem ikke behandler oplysninger om identificerede eller identificerbare fysiske personer, vil en behandling i denne form for system falde helt uden for forordningens anvendelsesområde. På den baggrund, vil der i afhandlingen ikke foretages en analyse af praksis med udgangspunkt i en traditionel ansigtsgenkendelse.

5.3. Verifikation

Brugen af verifikationssystemer i praksis tager udgangspunkt i Datatilsynets afgørelser, om behandling af fingeraftryk, fra før og efter Databeskyttelsesforordningen ikrafttrædelse. Verifikationssystemer foretager en 1:1 sammenligning af den registreredes personoplysninger, som beskrevet i afsnit 3.2.2.

5.3.1. Dansk praksis

Datatilsynets afgørelse fra 2003, *Fingeraftryk på Bornholmerkort*[81], drejer sig om brugen af fingeraftryk til identifikation i forbindelse med indførelse af nyt id-kort.

Er behandlingen nødvendig for at opfylde formålet? Formålet med behandlingen er et ønske om *entydig identifikation*, hvilket efter Datatilsynets vurdering anses som en berettiget interesse. For at der kan foretages en behandling af den registreredes biometriske data, herunder fingeraftryk, er det i afgørelsen et krav, at den registrerede har givet sit udtrykkelige og frivillige samtykke, jf. GDPR art. 9, stk. 2, litra a og art. 6, stk. 1, litra a[82]. Nødvendigheden er i denne situation tilstede, da behandlingen bliver nødvendig ud fra den registreredes udtrykkelige samtykke, for at kunne opfylde kontrakten med den registrerede om erhvervelse af et id-kort.

Er verifikationssystemet effektivt og velegnet til formålet? Ved behandling af den registreredes fingeraftryk bliver der alene lagret en udregnet værdi af det biometriske rådata på en template. Lagringen af den udregnede værdi sker på et id-kort, som den registrerede selv har kontrol over. Udover den udregnede værdi, bliver den registreredes kundenummer lagret på id-kortet. Der er her tale om et 2-faktorsystem, hvor der først skal findes et match af kundenummeret i bookingsystemet og dernæst en sammenligning af den lagrede værdi og scanningen af den registreredes fingeraftryk. For at få adgang, i dette tilfælde til BornholmsTrafikkens færge, er det et krav, at der findes et match i to-faktorsystemets sammenligninger. Ved et match mellem den lagrerede værdi på id-kortet og scanningen af den registreredes fingeraftryk sker der en overførsel af de behandlede oplysninger til id-kortet. Da overførslen sker i krypteret form som en ekstra sikkerhed for, at oplysningerne ikke misbruges af udefrakommende, vil denne overførsel anses som værende i overensstemmelse med behandlingsprincipperne i GDPR art. 5.

Behandlingen er effektiv og velegnet til formålet, da den registrerede selv har kontrol over de lagrede værdier, som udelukkende lagres på den registreredes id-kort, samtidig med at der er foretaget sikkerhedsforanstaltninger ved kryptering og behandling af de udregnede værdier.

Er behandlingen rimelig i forhold til den registreredes rettigheder? Formålet om at sikre en entydig identifikation anses som en berettiget interesse og vægtes derfor højere end den registreredes interesse i, at behandlingen ikke foretages. Den registrerede har

[81] Datatilsynets afgørelse nr. 2003-212-0143
[82] Før Persondataloven § 6, stk. 1, nr. 1

mulighed for selv at vælge, om behandlingen skal foretages, ved at vedkommende giver sit udtrykkelige samtykke.
Da oplysningerne forbliver i den registreredes varetægt, er det svært at forestille sig, at formålet kan opnås ved mindre indgribende midler. Proportionalitetsprincippets 4 punkter vil dermed være opfyldt, hvorfor behandlingen er i overensstemmelse med princippet, jf. GDPR art. 5, stk. 1, litra c.[83]

I en anden af Datatilsynets afgørelser fra 2006, *Anvendelse af biometri ved indcheckning af bagage*[84], er formålet også et ønske om *entydig identifikation* af den registrerede, hvilket i dette tilfælde er grundet en specifik forordning på området med krav om sikring af, at de rigtige personer er med på rejserne.
Som ved afgørelsen fra 2003 vil nødvendigheden af behandlingen være tilstede, da behandlingen udelukkende sker ud fra den registreredes udtrykkelige samtykke.
Kravet om effektivitet og velegnethed opfyldes i denne afgørelse, da der ved en scanning af et fingeraftryk udregnes en værdi, som bliver lagret på en central database i en begrænset periode, hvilket her er indtil tidspunktet for ombordstigning på det pågældende fly.
I forhold til den registrerede har vedkommende ikke mulighed for at føre kontrol som i afgørelsen fra 2003, da den registrerede ikke har adgang til den centrale database. Forskellen mellem denne afgørelse og afgørelsen fra 2003 er, at der her er tale om en verificering af, om bagagen kan kobles til en specifik person og dermed ikke en egentlig identificering af den registrerede. Den registrerede har derudover selv mulighed for at vælge behandlingen til ud fra det udtrykkelige samtykke. Flyselskabet har her givet den registrerede en alternativ løsning til behandlingen igennem en manuel id-kontrol. Selskabet har på tidspunktet for oplysning om den alternative løsning samtidig oplyst om den biometriske behandling, hvorfor den registrerede er vidende om, hvad behandlingen omhandler.
Da behandlingen alene omfatter udregnede værdier lagret i en begrænset periode, vil systemet kun behandle de nødvendige oplysninger til opfyldelse af formålet om entydig identifikation, hvorfor proportionalitetsprincippet er opfyldt, jf. GDPR art. 5, stk. 1, litra c.

[83] Før Persondataloven § 5, stk. 3
[84] Datatilsynets afgørelse nr. 2006-2019-0370

Der findes også et eksempel fra praksis, hvor proportionalitetsprincippet ikke opfyldes ved brug af et verifikationssystem. Eksemplet findes i Datatilsynets afgørelse fra 2017, *Brug af fingeraftryk ved bloddonation*[85]. Som ved afgørelserne fra 2003 og 2006 er formålet her også at sikre en *entydig identifikation*. I afgørelsen fra 2017 sker behandlingen ud fra en sikkerhed om, at den registrerede rent faktisk er den, som personalet forventer. Forskellen fra de andre afgørelser er, at den registrerede i dette tilfælde ikke har mulighed for at samtykke til behandlingen, hvorfor behandlingen ikke kan anses som værende frivillig. Derudover bliver behandlingen foretaget ud fra den registreredes fingeraftryk, altså rådata, hvor et billede af fingeraftrykket lagres på en central database sammen med den registreredes personnummer. Det, at der sker lagring af to former for personoplysninger samme sted, udelukkende som rådata, øger risikoen for misbrug af den registreredes personoplysninger. Derudover lagres oplysningerne i minimum 30 år, hvilket ikke kan anses som nødvendigt i forhold til formålet.
Som det fremhæves af afgørelserne fra 2003 og 2006, er behandlingen tilstrækkelig og nødvendig, hvis behandlingen foretages ud fra den registreredes udtrykkelige samtykke. Datatilsynets afgørelse fra 2017 er betydeligt mere indgribende overfor den registrerede, end hvad der kan kræves til at opfylde formålet om entydig identifikation, da der sker behandling af rådata. Behandlingen er derfor ikke nødvendig efter proportionalitetsprincippet, og formålet kan derfor opfyldes med mindre indgribende midler.

5.3.2. Delkonklusion

Det kan konkluderes, at proportionalitetsprincippet ved behandling af biometriske data i verifikationssystemer er opfyldt, hvis: i) formålet er en sikring af en entydig identifikation, ii) der alene sker behandling af udregnede værdier, iii) de udregnede værdier lagres i en begrænset periode på et id-kort eller på en central database, iv) behandlingen sker på baggrund af den registreredes udtrykkelig samtykke og v) den dataansvarlige har lavet sikkerhedsforanstaltninger ud fra en risiko- og konsekvensanalyse som sikring for den registreredes rettigheder.

5.4. Identifikation

Eksemplerne fra praksis på brugen af identifikationssystemer, defineret i afsnit 3.2.3., tager udgangspunkt i to historiske afgørelser fra Datatilsynet og en afgørelse fra

[85] Datatilsynets afgørelse nr. 2014-632-0081

henholdsvis det svenske, polske og franske datatilsyn. I Datatilsynets afgørelse fra 2008 tages der udelukkende stilling til proportionalitetsprincippets opfyldelse ved den del af behandlingen, som omhandler biometriske data, herunder fingeraftryk.

5.4.1. Dansk praksis

I Datatilsynets afgørelse fra 2004, *Adgangssystem til motionscenter baseret på fingeraftryk*[86], er formålet med behandlingen en nemmere form for adgangskontrol ved scanning af fingeraftryk.

I den pågældende afgørelse vil behandlingen udelukkende finde sted, hvis den registrerede har givet sit udtrykkelige samtykke hertil, og behandlingen dermed opfylder behandlingsgrundlaget i GDPR art. 9, stk. 2, litra a og art. 6, stk. 1, litra a.

Når den registreredes fingeraftryk scannes, findes der en udregnet værdi af det biometriske rådata, som derefter sammenlignes med motionscenterets centrale database. De udregnede værdier bliver lagret i systemet i krypteret form, hvor det ikke er muligt at eksportere data fra systemet. Oplysningerne bliver lagret i systemet indtil medlemskabet ophører. Hvis scanningen af fingeraftrykket ikke finder et match i systemet, vil oplysningerne slettes med det samme.

Ved at oplysningerne lagres på en central database, har den registrerede ikke mulighed for at føre kontrol med sine personoplysninger.

Sammenholdt med Datatilsynets afgørelse fra 2003, *Fingeraftryk på Bornholmerkort*[87], er der en lighed i den frivillig aftale med den registrerede ud fra vedkommendes udtrykkeligt samtykke. Forskellen fra 2003-afgørelsen er, at der her sker lagring af personoplysninger på en central database og ikke på et id-kort. Problemet med den pågældende behandling skal derfor findes i lagringen af oplysningerne, da den registrerede ikke kan føre kontrol med sine personoplysninger på en central database.

Den registreredes rettigheder og interesse går forud for formålet om en nemmere form for adgangskontrol, selvom den registrerede har samtykket til behandlingen, og der er foretaget sikkerhedsforanstaltninger forud for behandlingen, da behandlingen er for indgribende i forhold til formålet. Behandlingens nødvendighed er derfor ikke tilstede.

De 4 vurderingspunkter kan dermed ikke anses for opfyldt, hvorfor proportionalitetsprincippet ikke er opfyldt, jf. GDPR art. 5, stk. 1, litra c.

[86] Datatilsynets afgørelse nr. 2004-219-0208
[87] Datatilsynets afgørelse nr. 2003-212-0143

Det bør i dette tilfælde overvejes, om der i stedet skal udstedes et id-kort, som ved afgørelsen fra 2003, hvor de udregnede værdier alene lagres på kortet og matches med resultatet af det scannede fingeraftryk i et verifikationssystem.

Som et andet eksempel på Datatilsynets praksis findes afgørelsen fra 2008, *Adgangskontrol på diskoteker og førelse af intern karantæneliste.*[88] Som ved afgørelsen fra 2004 er der tale om en behandling af udregnede værdier, der bliver lagret på en central database, som alene kan foretages ud fra den registreredes udtrykkelige samtykke. Som en ekstra sikkerhed for, at der er tale om den rigtige person, bliver der i systemet lagret et billede af den registrerede. Den udregnede værdi af fingeraftrykket vil automatisk blive slettet efter 90 dage, hvis den registrerede ikke har besøgt diskoteker indenfor denne periode, hvorfor opbevaringsperioden er afgrænset.
Afgørelsen fra 2008 adskiller sig fra 2004-afgørelsen ved, at der her er tale om et formål om at sikre en ensartet kontrol af diskotekets gæster ud fra et hovedformål om at sikre et trygt og sikkert natteliv indenfor en afgrænset periode samt at undgå køer uden for diskoteket. Et formål om en ensartet kontrol og ikke blot en nemmere løsning til adgangskontrol, som var tilfældet ved afgørelsen fra 2004, vil opfylde kravet om et sagligt og nødvendigt behandlingsformål. Behandlingen anses ikke som værende for indgribende i forhold til den registrerede, da der alene kan ske behandling, hvis den registrerede giver sit udtrykkelige og frivillige samtykke. Behandlingen opfylder, ud fra formålet og den registreredes samtykke, proportionalitetsprincippet.

5.4.2. Udenlandsk praksis

Afgørelserne fra de andre europæiske datatilsyn omhandler skolers brug af identifikationssystemer med behandling af biometriske data, herunder fingeraftryk og ansigtsgenkendelse.

Det svenske datatilsyn, Datainspektionen, har i 2019 foretaget en afgørelse om en skoles behandling af biometriske data med det formål af registrere og kontrollere elevernes deltagelse i undervisningen. Systemet skal gøre processen mere enkel og effektiv.[89] Der er tale om en forsøgsordning på 3 uger med kontrol af 22 elever, hvor der forud for forsøget

[88] Datatilsynets afgørelse nr. 2008-42-0742
[89] Svenske datatilsyn afgørelse nr. DI-2019-2221, s. 3

er indsamlet samtykkeerklæringer fra de myndige elever samt de ikke-myndige elevers forældre.
Ansigtsgenkendelsessystemet foretager behandling af eleverne, når de bevæger sig ind i klasselokalet. De biometriske data i form af ansigtsbilleder bliver sammenlignet med systemets lagrede billeder af de deltagende elever. Lagringen sker på en central database på en computer uden adgang til internettet.[90]
Allerede efter første vurderingspunkt, om behandlingens nødvendighed i forhold til formålet, vil denne behandling skabe problemer. Der er tale om behandling af mindreåriges biometriske data, hvilket kræver en større beskyttelse, jf. GDPR art. 8 og præambel 38. Derudover er der tale om et afhængighedsforhold mellem eleverne og skolen, da eleverne anses som værende afhængige af skolen i forhold til karakterer, studiefinansiering, uddannelse og muligheden for fremtidigt arbejde og videre studie.[91] Eleverne har ikke mulighed for frivilligt at give deres udtrykkelige samtykke til behandlingen, da den ensidige kontrolforanstaltning indeholder et betydeligt ulige forhold mellem eleverne og skolen. Gymnasiet har derfor et retligt grundlag for at administrere de studerendes deltagelse i undervisningen, men de vil ikke have juridisk støtte til at behandle elevernes følsomme personoplysninger, da kravene om et frivilligt samtykke ikke er opfyldt.
Identifikationssystemet kan ikke anses som effektivt og velegnet til formålet, da der i dette tilfælde ikke er udarbejdet en forudgående konsekvensanalyse, jf. GDPR art. 35. Behandlingen medfører derfor en for stor risiko for krænkelse af den registreredes rettigheder, hvorfor behandlingen anses som værende for indgribende i forhold til det angivne formål.
Behandlingen står ikke i et rimeligt forhold til den registreredes rettigheder, da formålet alene er at finde en nemmere løsning, herunder en besparelse af den tid som skolen ellers ville bruge på at kontrollere elevernes deltagelse i undervisningen.
Behandlingen opfylder ikke proportionalitetsprincippet, hvorfor der er et krav om, at der skal findes mindre indgribende midler til opfyldelse af formålet.[92]

Det franske datatilsyn, CNIL, foretog i 2019 en tilsvarende afgørelse om franske gymnasiers brug af ansigtsgenkendelse. Formålet med behandlingen er fundet ud fra et ønske

[90] Svenske datatilsyn afgørelse nr. DI-2019-2221, s. 3
[91] Ibid., s. 5
[92] Ibid., s. 12

om en nemmere kontrolløsning ved adgangene til gymnasierne og et ønske om at forhindre uønsket indtrængen og identitetstyveri.[93]
Systemet fungerer på samme måde som i den svenske afgørelse ved en automatisk sammenligning af elevens ansigtsbillede og en lagring af en liste over alle elevernes ansigter i systemet. Behandlingen foretages alene ud fra et udtrykkeligt samtykke fra den myndige elev eller forældrene.
Som ved den svenske afgørelse vil der her blive slået ned på afhængighedsforholdet mellem skolen og eleverne og behandlingen af mindreåriges biometriske data, jf. GDPR art. 8 og præambel 38. Behandlingen bliver derfor anset som værende for indgribende i forhold til den registreredes rettigheder.
Da et samtykke i et afhængighedsforhold ikke kan anses som værende givet frivilligt, vil det ikke være muligt at bruge samtykke som behandlingsgrundlag efter GDPR art. 9, stk. 2, litra a og art. 6, stk. 1, litra a.
Behandlingen efter den franske afgørelse vil derfor heller ikke anses som nødvendig og stå i et rimeligt forhold til formålet om en lettere og mere sikker adgangskontrol, hvorfor proportionalitetsprincippet ikke er opfyldt.

Endnu et tilfælde af skolers brug af elevers biometriske data findes i det polske datatilsyns, UODO, afgørelse fra 2020. Den polske afgørelse omhandler en skoles brug af elevers biometriske data, herunder fingeraftryk, til at identificere de elever, der modtager måltider fra kantinen for på den måde at verificere betaling af måltidsgebyret.[94]
Som det er tilfældet ved både den svenske og franske afgørelse, er der her tale om en lagring af udregnede værdier af de biometriske data, som bliver sammenlignet med elevens scannede fingeraftryk. Det er kun muligt at modtage måltider, hvis den enkelte elev bliver identificeret ved et match i systemet.[95]
Der er igen tale om en situation, hvor en skole ønsker at foretage behandlingen ud fra elevernes forældres frivillige og udtrykkelige samtykke[96], hvilket ikke er muligt grundet afhængighedsforholdet mellem skolen og eleverne.
Efter proportionalitetsprincippet vil en behandling af biometriske data være for indgribende i dette tilfælde, når behandlingen foretages for at opfylde formålet om

[93] https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position
[94] Polske datatilsyns afgørelse nr. ZSZZS.440.768.2018
[95] Ibid. s. 2, pkt. 3
[96] Ibid., s. 2, pkt. 1

identificering af elever for at verificere et måltidsgebyr, da behandlingen skaber en større risiko for krænkelse af den registreredes rettigheder. Derudover understreges behandlingens unødvendighed igen ved det særlige krav om beskyttelse, når der er tale om behandling af mindreåriges personoplysninger.

Som det er beskrevet i afsnit 4.3., må det ikke skabe negative konsekvenser, hvis den registrerede ikke ønsker at samtykke til behandlingen. Den polske skole vælger i dette tilfælde at stille alternative løsninger til rådighed, herunder brug af elektroniske kort eller kontrol baseret på navn eller elevnummer, hvis forældrene ikke ønsker at samtykke til behandling af elevernes biometriske data. Som udgangspunkt opfylder de alternative løsninger kravene for samtykke og kravet om behandlingens proportionalitet. Problemet ved afgørelsen er, at de elever, som benytter de ovenstående alternativer, er nødsaget til at vente med at få adgang til kantinen, indtil alle elever med biometrisk identifikation har modtaget måltider.[97] Det skaber en forskelsbehandling af eleverne, hvilket er en uberettiget fordeling fra skolens side.

Ud fra ovenstående vil hverken kravene til et udtrykkeligt samtykke, jf. GDPR art. 9, stk. 2, stk. a eller proportionalitetsprincippet i GDPR art. 5, stk. 1, litra c være opfyldt.

5.4.3. Delkonklusion

Det kan konkluderes, at proportionalitetsprincippet, ved behandling af biometriske data i identifikationssystemer alene er opfyldt, hvor formålet er en sikring af ensartet kontrol. Da hovedformålet i 2008-afgørelsen er at sikre et trygt og sikkert natteliv, vil identifikationssystemet formentlig ikke kunne anvendes alene til et kommercielt formål.

5.5. Proportionalitetsvurdering efter andre behandlingsgrundlag

Med den begrænsede praksis på behandling af biometriske data kommercielt, vil der drages mulige paralleller til behandling efter GDPR art. 9, stk. 2, litra g og art. 6, stk. 1, litra e, om væsentlige samfundsmæssige interesser eller offentlig myndighedsudøvelse. Ved hjælp af praksis på området, vil det her udledes, hvornår en behandling af biometriske data i dette tilfælde opfylder proportionalitetsprincippet, med udgangspunkt i punkterne oplistet i afsnit 5.1.

[97] Polske datatilsyns afgørelse nr. ZSZZS.440.768.2018, s. 2, pkt. 6.

Analysen tager udgangspunkt i en tilladelse[98] fra Datatilsynet[99] og en afgørelse fra Landsretten for England og Wales[100], som begge er fra 2019. Som udgangspunkt vil både tilladelsen og afgørelsen ikke have en høj retskildemæssig værdi, men da det er det eneste praksis på området, vil de alligevel tillægges en betydelig værdi for analysen.

Af begge eksemplerne på praksis fremgår der et formål om sikkerhed igennem en entydig identifikation af de fysiske personer, i et ansigtsgenkendelsessystem med identifikation, omfattet af afsnit 3.2.3., ved offentlige begivenheder.

5.5.1. Dansk praksis

I den danske tilladelse fra Datatilsynet bliver den automatiske ansigtsgenkendelse med identifikation benyttet som adgangskontrol. Læseren skal være opmærksom på, at tilladelsen er givet ud fra en forventning om, at de analyserede punkter nedenfor opfyldes.

Efter tilladelsen er proportionalitetsprincippets krav om behandlingens nødvendighed efter Datatilsynets opfattelse opfyldt, hvis formålet omfatter et ønske om at skabe ro og sikkerhed ved offentlige begivenheder. Denne sikkerhed skabes for Brøndby Stadion ved at identificere den registrerede ud fra en intern karantæneliste. På listen findes der oplysninger om andre registrerede, der har karantæne fra Brøndby Stadions kampe grundet tidligere uroligheder. Systemet hjælper med at finde frem til de personer, som skal nægtes adgang fra området. Det antages, at karantænerne er givet ud fra et proportionalt og sagligt grundlag, herunder overtrædelse af et ordensreglement.[101]
Om behandlingen er effektiv og velegnet til formålet, skal besvares ud fra systemets tekniske setup. For at behandlingen kan stå i et rimeligt forhold til formålet, skal der alene lagres oplysninger om den registrerede, hvis der findes et match. Lagringen skal udelukkende ske i en begrænset periode, hvilket i dette tilfælde er indtil de pågældende kampe er afviklet.[102] Det betyder, at oplysninger, som ikke resulterer i et match, skal slettes med

[98] Når en privat virksomhed ønsker at foretage behandling af følsomme personoplysninger, skal Datatilsynet give tilladelse hertil, jf. DBL § 7, stk. 4
[99] Datatilsynets tilladelse: *Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion*
[100] Afgørelse nr. CO/4085/2018
[101] Datatilsynets tilladelse: *Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion,* pkt. 2
[102] Ibid.*,* pkt. 4

det samme og dermed ikke lagres i systemet.[103] De lagrede oplysninger skal alene omfatte udregnede værdier af de indsamlede biometriske data. Det betyder, at den registreredes rådata alene benyttes til at skabe de udregnede værdier og dermed ikke benyttes til den egentlig behandling.[104] Dermed vil selve behandlingen af den registreredes biometriske data foretages automatisk gennem ansigtsgenkendelsessystemet. Den endelige beslutningsproces, i forhold til at nægte de registrerede adgang, må ikke alene foretages ud fra systemets automatiserede setup. Ved et match er det i sidste ende op til en uddannet sikkerhedsperson at tage stilling til, om den registrerede skal nægtes adgang til området.[105] Med andre ord skal der foretages en to-faktor-godkendelse, så der er en sikkerhed for, at systemet ikke har foretaget et fejlmatch.

Ved at opfylde ovenstående punkter, vil behandlingen anses som effektiv og velegnet til formålet.

På den anden side skal behandlingens gyldighed ses i forhold til den registrerede. Det er vigtigt, at den registrerede bliver opmærksom på, at behandlingen foretages. Det kan ske ved, at Brøndby Stadion ved skiltning eller på anden måde tydeliggør, at der foretages denne specielle form for adgangskontrol.[106] Derudover er det et krav, at der efter GDPR art. 35 er foretaget en risiko- og konsekvensanalyse, da der er tale om en ny form for teknologi. Set i forhold til den registreredes rettigheder, vil en behandling i et ansigtsgenkendelsessystem stå i rimeligt forhold til virksomhedens forventede fordele, da fordelen kommer ved at skabe en højere grad af sikkerhed. Virksomhedens behandling går derfor forud for den registreredes rettigheder og interesse i, at behandlingen ikke foretages. Med det ovenstående i mente, er det svært at finde mindre indgribende midler til opnåelse af formålet, hvorfor proportionalitetsprincippet er opfyldt.

5.5.2. Udenlandsk retspraksis

Det eneste eksempel på retspraksis på området findes i den engelske afgørelse om South Wales politis behandling af biometriske data i overvågningssystemer. I afgørelsen lægges der stor vægt på opfyldelse af proportionalitetsprincippet, som også er tilfældet efter dansk praksis.

---

[103] Datatilsynets tilladelse: *Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion,* pkt. 3
[104] Ibid., pkt. 6
[105] Ibid., pkt. 8
[106] Ibid., pkt. 5

Der er tale om overvågningssystemer, som er implementeret ved omkring 50 store offentlige begivenheder. Systemerne fungerer i realtid, hvorfor behandlingen foretages med det samme, når fysiske personer træder ind i kameraernes område.
Der skal igen foretages en undersøgelse af behandlingens nødvendighed i forhold til formålet. At formålet er en interesse i at forhindre uroligheder ved konkrete begivenheder, skaber en nødvendighed og tilstrækkelighed for at behandlingen foretages.[107]
Det tekniske setup er udgangspunktet for vurderingen af behandlingens effektivitet og velegnethed. Som ved eksemplet på dansk praksis er behandlingen i dette tilfælde alene foretaget ud fra udregnede værdier af den registreredes biometriske data ved en sammenligning af oplysninger om registrerede på de interne overvågningslister.[108] Listerne inkluderer udelukkende oplysninger om; personer, mistænkt for at have begået en forbrydelse, personer med brug for beskyttelse, personer, hvis tilstedeværelse ved en bestemt begivenhed ville skabe særlig bekymring og personer af interesse for politiet. De udregnede værdier lagres alene, når der sker et match i systemet. Hvis systemet ikke finder et match, skal oplysningerne slettes med det samme uden nogen form for lagring. Et match skal alene lagre de udregnede værdier i en begrænset periode, hvilket i dette tilfælde gælder en lagring i op til 24 timer og formentlig allerede efter begivenheden er afsluttet.[109]
Som ved Datatilsynets tilladelse, hvor der er et krav om en to-faktor-godkendelse, er der i denne sag tale om en sikkerhedsperson, som tjekker for mulige systemfejl, når systemet finder et match. Beslutningsprocessen vil dermed ikke anses som fuldt automatiseret.[110]
Som resultat af den engelske afgørelse, vil politiets interesse gå forud for den registreredes rettigheder, selvom en overvågning i det offentlige rum kan anses som værende krænkende overfor den registrerede. Grundlaget herfor er formålet om forhindring af uroligheder sammen med politiets sikkerhedsforanstaltninger. Ansigtsgenkendelsessystemet er benyttet på en åben og gennemsigtig måde, hvor der alene foretages en behandling, hvis den registrerede befinder sig på en af overvågningslisterne.[111] Der er i dette tilfælde foretaget en aktiv handling for, at en krænkelse af den registreredes rettigheder mindskes ved at have klare juridiske rammer for, hvorvidt, hvornår og hvordan systemet benyttes, hvilket fremgår af de interne politikker og procedurer.[112]

[107] Afgørelse nr. CO/4085/2018, afsnit F, pkt. 127
[108] Ibid., afsnit C, pkt. 24
[109] Ibid., afsnit D, pkt. 37-38
[110] Ibid., afsnit F., afsnit D, pkt. 33
[111] Ibid., afsnit E2, pkt. 83
[112] Ibid., annex "A", pkt. 40-42

Ud fra de ovenstående betragtninger er det ikke muligt at opfylde formålet ved mindre indgribende midler, hvorfor proportionalitetsprincippet er opfyldt.

5.5.3. Delkonklusion

Det kan ud fra praksis konkluderes, at proportionalitetsprincippet ved behandling med et formål om sikkerhed er opfyldt, hvis: i) der alene sker behandling af udregnede værdier, ii) de udregnede værdier lagres i en begrænset periode, hvis systemet finder et match, iii) sletning sker med det samme, hvis systemet ikke finder et match iv) den endelige beslutningsprocessen er hos en sikkerhedsperson, som kan tjekke for systemfejl og v) den dataansvarlige har lavet sikkerhedsforanstaltninger ud fra en risiko- og konsekvensanalyse som sikring for den registreredes rettigheder.

5.6. Samlet konklusion på den juridiske analyse

Det kan på baggrund af ovenstående analyse konkluderes, at virksomheder efter Databeskyttelsesforordningen kun i et meget begrænset omfang har mulighed for at behandle forbrugeres biometriske data kommercielt.
Hvis virksomheder har et ønske om at identificere forbrugerne, er det kun muligt at behandle biometriske data, hvis behandlingen foregår i et verifikationssystem. Kravene til brugen af systemet er, at der alene sker behandling af udregnede værdier og ikke rådata af den registreredes biometriske data, og at lagringen af værdierne sker på en form for idkort, så den registrerede har mulighed for at føre kontrol med sine oplysninger.

Det kan tillige konkluderes, at det alene er muligt at foretage en behandling af biometriske data kommercielt, hvis forbrugerne samtykker til behandlingen og dermed opfylder behandlingsgrundlaget i GDPR art. 9, stk. 2, litra a og art. 6, stk. 1, litra a.

Proportionalitetsprincippet er særligt vigtigt i vurderingen af behandlingens nødvendighed og tilstrækkelighed i forhold til det angivende formål. Artikel 29-gruppens 4 vurderingstrin er et nyttigt værktøj, når den dataansvarlige, herunder virksomheder, skal vurdere, hvorvidt en behandling af biometriske data i et verifikations- eller identifikationssystem er i overensstemmelse med de grundlæggende behandlingsprincipper, med særligt fokus på proportionalitetsprincippet. De 4 trin kan tillige benyttes i vurderingen af, hvilke tiltag der kan mindske behandlingens indgriben overfor den registreredes rettigheder.

Ud fra formålet med behandlingerne og de tekniske setups kan det konkluderes, at der endnu ikke er praksis på området, som omhandler profilering, jf. GDPR art. 4, nr. 4. Da der ved profilering sker analysering eller forudsigelse af forhold vedrørende den registrerede, vil profileringen formentlig anses som mere indgribende end de behandlinger, som allerede findes i praksis. Ud fra den betragtning vil profilering ikke anses som nødvendig og tilstrækkelig, hvis behandlingen af biometriske data sker ud fra en kommerciel interesse.

6. Økonomisk analyse - Retsøkonomiske overvejelser

Som resultat af den juridiske analyse i afsnit 5 har virksomheder efter Databeskyttelsesforordningens regler kun begrænsede muligheder for at behandle den registrerede, herefter forbrugerens, biometriske data kommercielt.
Et ansigtsgenkendelsessystem giver virksomheder mulighed for at sælge mere effektivt. Virksomheder kan benytte systemet både online og i fysiske butikker. Ved online brug er det muligt at udarbejde skræddersyede reklamer og annoncer til den enkelte forbruger, da systemet hjælper med at lave detaljerede profiler af den enkelte ud fra forskellige karakteristika.[113] Systemet kan også benyttes i fysiske butikker, hvor ansigtsgenkendelsessystemet kan guide og hjælpe den enkelte forbruger hen til de produkter, som har en interesse. Hjælpen sker på baggrund af de informationer, som scanningen giver, hvilket beskrives yderligere i analysen nedenfor.

Det bliver i analysen relevant at se på de økonomiske påvirkninger af virksomheder, forbrugere og samfundet på kort og lang sigt ved implementering af ansigtsgenkendelsessystemet. Det skal undersøges, om det kan give en økonomisk gevinst at benytte systemet, selvom forordningen sætter diverse begrænsninger.
Her bliver blandt andet behandlet forhold som prisdiskrimination, patent, velfærd samt forbrugerens præferencer og købsbeslutningsproces. Kapitlet indledes med en kort gennemgang af de økonomiske overvejelser, som ligger bag afhandlingens økonomiske analyse.

[113] https://www.taylorwessing.com/download/article-facial-recognition-in-eu.html

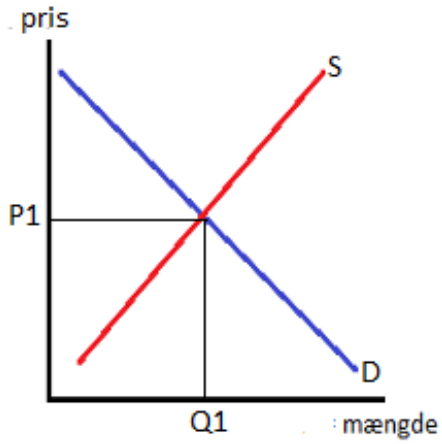
6.1. Økonomiske overvejelser

Inden den økonomiske analyse kan foretages, er det relevant at få fastlagt de økonomiske overvejelser, der ligger bag analysens opstillede modeller, herunder hvordan markedsstrukturen skal defineres, hvordan det er muligt at benytte prisdiskrimination, og hvordan købsbeslutningsprocessen skal defineres.

Læseren skal forestille sig, at når den første virksomhed implementerer et ansigtsgenkendelsessystem, gennemgår virksomheden to faser. De to faser skyldes, at der er tale om et nyt system, som virksomheder tidligere kun har haft en begrænset mulighed for at anvende kommercielt. Der er her tale om systemets påvirkninger på kort og lang sigt.
Fase 1 beskriver den situation, hvor det første ansigtsgenkendelsessystem implementeres på markedet. I fase 1 er der tale om et marked med ikke-fuldkommen konkurrence, da en virksomhed som first-mover er den eneste, der har implementeret et ansigtsgenkendelsessystem. Ved ikke-fuldkommen konkurrence har den enkelte virksomhed gennem en markeds- eller monopolmagt mulighed for at påvirke prisen på deres produkter og dermed prissætte over ligevægtsprisen.[114]
Fase 2 beskriver den situation, hvor der på lang sigt er flere virksomheder på markedet, som implementerer ansigtsgenkendelsessystemer, hvis det første implementerede ansigtsgenkendelsessystem anses som en succes. Konkurrencesituationen flytter sig på lang sigt tættere på en fuldkommen konkurrence, da virksomheden som first-mover ikke længere har den samme status på markedet grundet de konkurrerende virksomheders implementering af ansigtsgenkendelsessystemer.[115]

Som beskrevet i metodeafsnittet tager den økonomiske analyse udgangspunkt i den mikroøkonomiske teori. I figur 1 nedenfor illustreres udbuds- og efterspørgselsdiagrammet, hvor ligevægten defineres som den situation på markedet, hvor den udbudte mængde S er lig med den efterspurgte mængde D, også kaldet ligevægtsbetingelsen.[116]

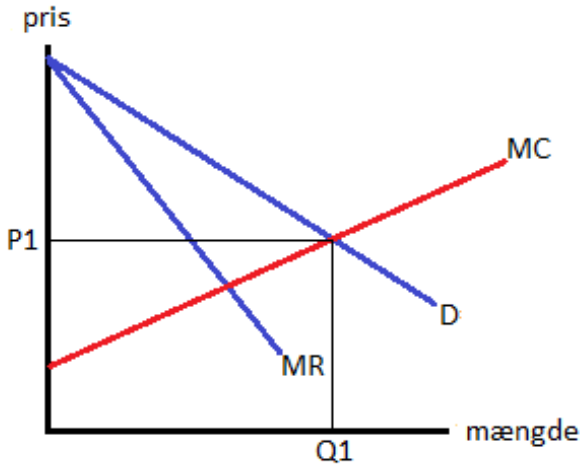
[114] Paul A. Samuelson: *Economics*, s. 170
[115] Ibid., s. 150
[116] Jeffery M. Perloff: *Microeconomics with Calculus,* s. 42-43



Figur 1: Udbud- og efterspørgselsdiagram[117]

6.1.1. Prisdiskrimination

Med udgangspunkt i figur 2, vil følgende gælde for en situation uden prisdiskrimination. Hvis en virksomhed befinder sig på et marked, hvor det ikke er muligt at prisdiskriminere, vil det kræve en pris på P1, hvis virksomheden ønsker at afsætte mængden Q1. Her skelnes der ikke mellem forbrugerne, men der ses alene på, hvad forbrugeren, der køber den sidste enhed, er villig til at betale.[118] MR illustrerer virksomhedens marginalindtjening ved salg af det pågældende produkt, og MC angiver stigningen i omkostningerne, når produktionen øges med én.[119]



Figur 2: Situation uden prisdiskrimination[120]

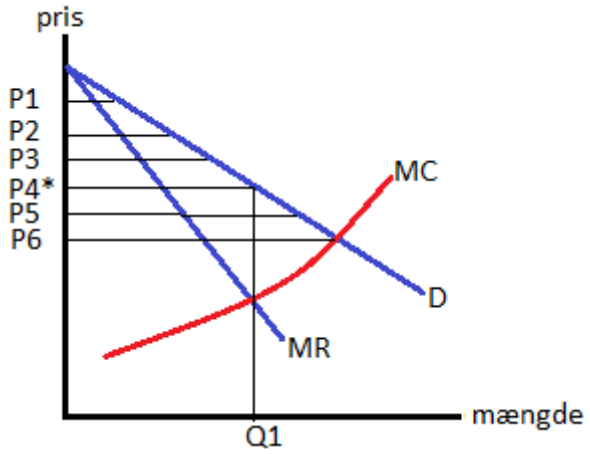
[117] Eget arbejde
[118] Robert S. Pindyck: *Microeconomics,* s. 408
[119] Ibid., s. 292
[120] Eget arbejde

Ved prisdiskrimination er det muligt for virksomheden at påvirke prisen på produkterne ved at sælge det samme produkt eller den samme serviceydelse til forskellige grupper af forbrugere til forskellige fastsatte priser.[121] Prisdiskrimination er relevant for virksomhedens fase 1, om påvirkningen af ansigtsgenkendelsessystemet på kort sigt, da det er en forudsætning for benyttelse af prisdiskrimination, at den pågældende virksomhed har opnået en monopolstatus på markedet.
Ved en prisfastsættelse afhænger den valgte pris af, hvilken pris den enkelte forbruger er villig til at betale for produktet også kendetegnet som "den rationelle købsmodel".[122] En forbruger har en maksimumpris, som vedkommende er villig til at betale. Forbrugeren tager beslutning om købet ved at se på forskellen mellem maksimumprisen og den pris, som forbrugeren reelt set skal betale for produktet[123], også kaldet forbrugervelfærd.[124] Ved flere valgmuligheder vil forbrugeren vælge det produkt, hvor vedkommende opnår den største forbrugervelfærd.

Der findes forskellige former for prisdiskrimination: 1) Forskellig pris til hver enkelt forbruger, 2) Prissætning på baggrund af mængde og 3) Forskellig pris ud fra observationer hos grupper af forbrugere.[125]

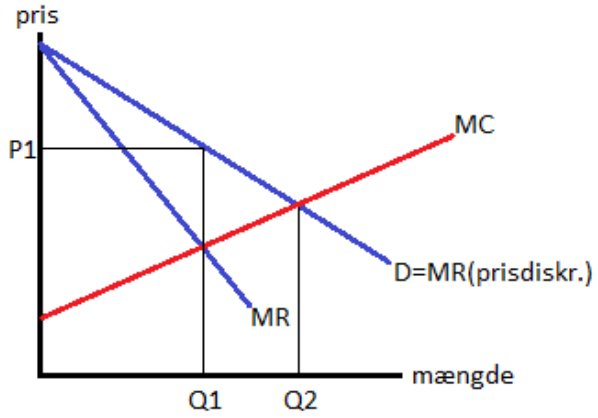
1. grads prisdiskrimination, også kaldet "perfekt prisdiskrimination", dækker over den situation, hvor enhederne af et produkt sælges enkeltvis til den højst mulige pris, som en forbruger er villig til at betale. Det er her et krav, at virksomheden kender de enkelte forbrugeres marginale betalingsvillighed for alle enheder af produktet. Prisfastsættelsen er illustreret i figur 3 nedenfor.

[121] Rakesh V. Vohra: *Principles of Pricing,* s. 106
[122] Ibid.*,* s. 7
[123] Ibid.
[124] Paul A. Samuelson: *Economics*, s. 96
[125] Rakesh V. Vohra: *Principles of Pricing,* s. 108



Figur 3: Prisfastsættelse ved 1. grads prisdiskrimination[126]

En 1. grads prisdiskrimination vil ændre på MR, som i denne situation bliver lig efterspørgselskurven, da der nøjagtigt kræves den pris, som den enkelte forbruger er villig til at betale. MC vil være uændret, og da profitten maksimeres ved at sælge produkterne, indtil MR er lig MC, vil mængden ændre sig til Q2. Ved at fastsætte en individuel pris til alle forbrugere vil virksomhedens totale omsætning bestå af hele området under efterspørgselskurven. Forbrugervelfærden, som var tilstede før prisdiskriminationen, vil tilegnes af virksomheden, hvorfor den samlede producentvelfærd i denne situation er maksimeret. Situationen med 1. grads prisdiskrimination er illustreret i figur 4 nedenfor.



Figur 4: Situation med 1. grads prisdiskrimination[127]

[126] Eget arbejde
[127] Ibid.

Ved 2. grads prisdiskrimination foretages prisdiskriminationen på baggrund af mængde. Forskellige mængder sælges her til forskellige priser.[128] Som eksempler herpå findes "versionering" og "bundling". Versionering definerer den situation, hvor en virksomhed laver forskellige versioner af det samme produkt, som er tilpasset til forskellige købssegmenter.[129] Bundling definerer den situation, hvor en virksomhed sælger en samlet pakke af forskellige produkter eller serviceydelser.[130]

Ved 3. grads prisdiskrimination kan monopolisten adskille forbrugerne i grupper ud fra observerbare kendetegn for eksempel demografi og lokation.[131] Ud over prisdiskriminationens fælles krav om virksomhedens monopolstatus er der ved 3. grads prisdiskrimination krav om, at forbrugerne kan inddeles i grupper med forskellig efterspørgsel, samt at grupperne kan differentieres fra hinanden.[132] Der skal findes et optimum, hvor MC er den samme for hver gruppe, og hvor hver gruppe har en individuel MR. Den samlede MR for markederne skal dog være lig MC, hvis optimalitetsbetingelsen, MC=MR, skal opfyldes.[133]

Som udgangspunkt vil en 1. grads prisdiskrimination være svær at benytte i praksis, da det er umuligt for virksomheden at vide alt om forbrugerne.[134] Det interessante er her, at det ved hjælp at et ansigtsgenkendelsessystem er muligt at identificere den enkelte forbruger. Her er det muligt at indsamle nok oplysninger til at lave en profil af hver enkelt forbruger, se afsnit 4.1.3. Ud fra en profil af den enkelte forbruger vil det være muligt for virksomheden at udarbejde en specifik reklame og pris til den enkelte ved at kende til præferencer og villigheden til at betale for produktet eller serviceydelsen. Det vil være svært at nå til en informationsgrad på 100%, men ansigtsgenkendelsessystemets mange muligheder gør det muligt at indsamle meget mere information i dag, end hvad der har været muligt førhen. Systemet vil derfor gøre det muligt at gøre brug af en 1. grads prisdiskrimination, hvorfor analysen tager udgangspunkt i denne form.

[128] Robert S. Pindyck: *Microeconomics,* s. 412
[129] Rakesh V. Vohra: *Principles of Pricing,* s. 111-112
[130] Ibid., s. 116
[131] Ibid., s. 108-111
[132] Jeffery M. Perloff: *Microeconomics with Calculus,* s. 430-431
[133] Robert S. Pindyck: *Microeconomics,* s. 414
[134] Ibid., s. 410-411

6.1.2. Købsbeslutningsproces

I fase 2 foretages en undersøgelse af de faser den enkelte forbruger gennemgår i købsbeslutningsprocessen.[135]

Afhængig af produktets betydning for forbrugeren, vil beslutningsprocessen variere. For at finde frem til graden af produktets betydning for den enkelte forbruger er faktorer som i) produktets vigtighed og ii) risikoen ved at købe produktet relevante.[136]

Den længste beslutningsproces med en høj grad af vigtighed samt høj risiko ved købet vil gennemgå fem steps[137]:

1. Erkendelse af et problem
2. Informationssøgning
3. Vurdering af alternativer
4. Beslutning om køb
5. Evaluering efter køb

En virksomhed har mulighed for at påvirke forbrugerens beslutningsproces, hvilket beskrives i SOR-modellen. Modellen omfatter "stimuli", som er virksomhedens påvirkning gennem blandt andet reklame og marketing-tiltag, "organisme", som er den påvirkede forbruger, og "respons", som er den reaktion, forbrugeren har på virksomhedens stimuli.[138]

Forbrugerens beslutningsproces er relevant for fase 2, da virksomheden på lang sigt mister sin monopolstatus, hvorfor virksomheden skal finde alternative løsninger til at differentiere sig fra konkurrenterne. Det kan blandt andet ske ved at påvirke beslutningsprocessen ved hjælp af rabatter og forenkling/forkortelse af processen.

6.2. Fase 1 – På kort sigt

Først undersøges det, hvordan en virksomheds implementering af ansigtsgenkendelsessystemer vil påvirke henholdsvis virksomheder, forbrugere og samfundet på kort sigt.

[135] Svend Hollesen: *Marketing management,* s. 121-124
[136] Ibid., s. 120
[137] Ibid., s. 121-124
[138] Ibid., s. 119-120

6.2.1. First-mover

Med et ansigtsgenkendelsessystem, som endnu ikke er implementeret på markedet til virksomheders kommercielle brug, vil der på kort sigt være en virksomhed "first-mover", som er den første til at implementere systemet. Ved implementering af systemet, er der et ønske fra virksomheden om at opnå en økonomisk fordel.
At være first-mover på et marked medfører en markeds- eller monopolmagt. First-mover kan ved hjælp af systemets mange muligheder yde en bedre service til forbrugerne.[139]

Der er økonomiske fordele forbundet med at være first-mover. Ved at være den eneste på markedet med et ansigtsgenkendelsessystem har virksomheden mulighed for at definere markedet i sin status som markedsleder. Da der endnu ikke er nogen konkurrenter til virksomhedens nye ansigtsgenkendelsessystem, er virksomheden prissætter og kan dermed fastsætte den pris, som vedkommende mener er realistisk grundet det højere serviceniveau.[140]
Virksomheden opnår med sin status et teknologisk førerskab grundet den læring og de oplevelser, som det nye system giver. First-mover opnår desuden et læringsforspring og dermed mulighed for at lære systemet bedre at kende, inden konkurrenterne på markedet vælger at implementere et lignende system. Virksomheden får mulighed for at være på forkant med forebyggende investeringer i udstyr til ansigtsgenkendelsessystemet, så systemet fortsat er førende på markedet ved hele tiden at følge den teknologiske udvikling.
En anden fordele skal findes hos forbrugerne. Hvis forbrugerne opnår en tryghed ved den service, som first-mover kan give grundet ansigtsgenkendelsessystemet, er det svært for virksomhedens konkurrenter at få forbrugerne til at købe produkter eller serviceydelser hos dem i stedet.[141] Forbrugerne ved, hvilken service de får hos first-mover, hvorfor der for mange forbrugere vil være en for stor usikkerhed i at skifte over til en af de konkurrerende virksomheder, selvom de benytter lignende ansigtsgenkendelsessystemer.

Der er også negative sider forbundet med at være first-mover. First-mover skal skabe et nyt marked med brug af ansigtsgenkendelsessystemer, hvilket har store omkostninger forbundet med sig. Før implementeringen har virksomheden x antal omkostninger og en

[139] Robert S. Pindyck: *Microeconomics,* s. 365-366
[140] Jeffery M. Perloff: *Microeconomics with Calculus,* s. 386
[141] Marvin B. Lieberman: *First-mover (dis)advantages: Retrospective and link with the resource-based view,* s. 1112-1113

pris fastsat til y kr. Efter implementeringen stiger omkostningerne grundet de høje implementeringsomkostninger, da der skal investeres penge i systemet samt bruges penge på at udvikle infrastrukturen på det nye marked.
Selvom der ved implementeringen er store omkostninger, vil virksomheden have et håb om, at systemets mange muligheder på længere sigt vil skabe en profit for virksomheden. First-mover har mulighed for at prissætte en pris over ligevægtsprisen, grundet sin status som prissætter, hvilket kan hjælpe med at tjene det stigende antal omkostninger ind. De omkostninger, som first-mover bruger til udvikling af infrastrukturen, er med til at give virksomheden og tillige forbrugerne et bedre kendskab til det nye implementerede system.

Som first-mover er der en større risiko for at begå fejl. På implementeringstidspunktet er der endnu ikke andre på markedet, som har implementeret en form for ansigtsgenkendelsessystem, hvorfor first-mover er nødt til at prøve sig frem. Ved at prøve sig frem lærer virksomheden mere om systemet, som beskrevet ovenfor, men der er tillige en større risiko for, at der igennem læringen sker fejl. Konkurrerende virksomheder kan lære af fejlene og dermed være bedre stillet ved implementering af lignende systemer.
Den forbedrede serviceydelse, som ansigtsgenkendelsessystemet giver, vil være ny for forbrugerne, hvilket vil skabe en usikkerhed. Indtil det tidspunkt hvor der er skabt en tryghed hos forbrugerne ved systemets behandling, vil de have en begrænset viden om systemet og den nye form for service, hvilket gør det svært at trække forbrugerne til.[142]

Som beskrevet i dette afsnit vil det at være den første på markedet, som implementerer et ansigtsgenkendelsessystem, typisk have store omkostninger forbundet med sig. En sådan virksomhed tager en stor og bekostelig risiko, da der ikke er sikring for, at det nye system bliver en succes, samtidig med at andre virksomheder på markedet har mulighed for at duplikere virksomhedens innovative idé. En løsning her kan være at få et patent på det implementerede ansigtsgenkendelsessystem. Et patent er virksomhedens mulighed for at sikre sig sin status som monopolejer af systemet i en periode, hvor andre virksomheder ikke vil kunne duplikere teknologien grundet denne indgangsbarriere.[143]

[142] Constantinos C. Markides: *Fast second,* s. 19
[143] Jeffery M. Perloff: *Microeconomics with Calculus,* s. 407-408

Sikringen skaber en stigende lyst til innovation, da first-mover ved, at de bekostelige nye og innovative idéer er sikret gennem et patent.

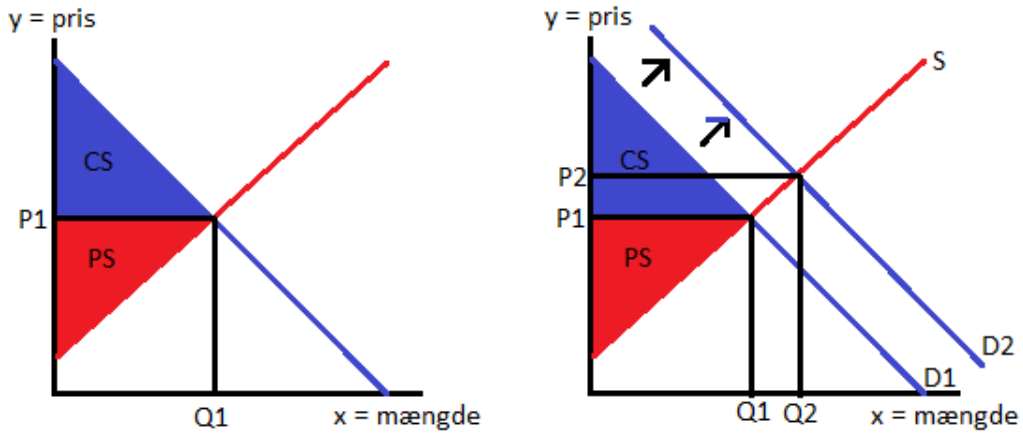
6.2.2. Prisdiskrimination og forbrugernes villighed

Som beskrevet tidligere i analysen kan virksomheden ved brug af et ansigtsgenkendelsessystem have et ønske om at udarbejde en specifik reklame med en specifik pris til den enkelte forbruger ud fra profiler om personlige forhold, herunder præferencer, interesser og adfærd. Ved at virksomheden kan yde et højere serviceniveau, vil det tillige give virksomheden mulighed for at prissætte til et højere niveau.

Som beskrevet i de økonomiske overvejelser i afsnit 6.1.1. er det ved hjælp af et ansigtsgenkendelsessystem muligt for virksomheden at foretage en 1. grads prisdiskrimination og dermed fastsætte en individuel pris til den enkelte forbruger. Det er her vigtigt, at virksomheden ser på forbrugernes villighed til at betale for produktet ud fra det nye fastsatte prisniveau.

For de gamle og loyale forbrugere vil et højere serviceniveau medføre en større nytteværdi. Det at forbrugerne ved, at ansigtsgenkendelsessystemet kan hjælpe med at skræddersy en reklame til den enkelte og dermed skabe en bedre oplevelse ved køb af et produkt, vil det skabe en større villighed hos forbrugerne til at betale en højere pris. Derudover vil villigheden hos de forbrugere, som endnu ikke handler hos first-mover, formentlig også stige i denne situation, da de kan se, at det nye ansigtsgenkendelsessystem giver dem en bedre og mere effektiv service. På den måde får virksomheden mulighed for at lokke nye forbrugere til, når de finder ud af, at deres nytte stiger ved at handle hos den pågældende virksomhed. Grundet den større nytteværdi og den større betalingsvillighed hos forbrugerne vil der ske en stigning i efterspørgslen, hvilket skaber en stigning i den samlede velfærd.

Situationen er illustreret i figur 5 nedenfor. Figuren til venstre viser udgangspunktet fra før virksomhedens implementering af ansigtsgenkendelsessystemet, hvor der er en ligevægt ved P1 og Q1. Når virksomheden implementerer et ansigtsgenkendelsessystem, som forhøjer serviceniveauet og betalingsvilligheden, vil det medføre en stigning i efterspørgslen, hvilket er illustreret i figuren til højre i figur 5. Med en stigning i efterspørgslen vil der opstå en ny ligevægt, som i figuren til højre illustreres som skæringen ved P2 og Q2.



Figur 5: Situationen før og efter en implementering af et ansigtsgenkendelsessystem[144]

I dette tilfælde vil virksomheden foretage en 1. grads prisdiskrimination, da det er muligt gennem de oplysninger, som ansigtsgenkendelsessystemet kan indsamle. Ved at prisdiskriminere forsvinder forbrugervelfærden CS, da virksomheden har mulighed for at fastsætte den pris, som den enkelte forbruger som maksimum er villig til at betale. Der vil dermed ikke være en forskel mellem forbrugerens maksimumpris og den pris, som forbrugeren betaler, hvilket ellers er den forskel, der skaber forbrugervelfærden. Ved at virksomheden kan fjerne forbrugervelfærden, vil den stigende efterspørgsel i stedet skabe et maksimeret producentoverskud PS, hvilket samlet set giver en stigning i den samlede velfærd.

Der vil på det pågældende marked befinde sig en gruppe af forbrugere, som vægter deres rettigheder højere end en behandling af deres biometriske data. Denne gruppe af forbrugere vil formentlig have en lavere villighed til at betale den højere fastsatte pris for produktet, da et højere serviceniveau ikke giver den samme nytte for disse forbrugere. Virksomheden er her nødt til, gennem sin 1. grads prisdiskrimination, at fastsætte en pris under den nye ligevægtspris, P2 og Q2, for at sikre, at forbrugerne fortsat ønsker at købe produkter hos virksomheden, selvom de biometriske data behandles i ansigtsgenkendelsessystemet. Selvom virksomhedens indtjening for salget til denne gruppe af forbrugere vil ligge under den nye ligevægt, vil den højere indtjening hos de forbrugere, hvor der er en høj betalingsvillighed, sikre virksomheden profit.

[144] Eget arbejde

Ved at virksomheden gennem en 1. grads prisdiskrimination kan prissætte ud fra den enkelte forbrugers villighed til at betale, vil virksomheden sikre en stigende forbrugertilfredshed. Hvis den enkelte forbruger mener, at den service som virksomheden tilbyder stemmer overens med den fastsatte pris på det pågældende produkt, vil tilfredsheden alt andet lige stige, hvorfor forbrugeren har en større villighed til at handle hos first-mover i stedet for andre virksomheder på markedet.

6.3. Fase 2 – På lang sigt

I fase 2 undersøges de økonomiske konsekvenser ved brugen af ansigtsgenkendelsessystemer på lang sigt for henholdsvis virksomheder, forbrugere og samfundet.

For at analysen på lang sigt kan foretages, skal læseren forestille sig, at ansigtsgenkendelsessystemet er blevet en succes for first-mover. På lang sigt vil et succesfuldt ansigtsgenkendelsessystemet medføre, at alle andre virksomheder på markedet viser en større interesse i at implementere et lignende system.

6.3.1. Ændring på patentområdet

Som beskrevet i afsnit 6.2.1., har en first-mover på kort sigt mulighed for at få et patent på ansigtsgenkendelsessystemet. I patentperioden har andre virksomheder ikke mulighed for at duplikere systemet, hvorfor first-mover er sikret i denne periode. Det betyder ikke, at virksomheden kan læne sig tilbage i patentperioden, hvis virksomheden på lang sigt stadig har et ønske om at være førende på markedet.

Andre virksomheder har mulighed for at skabe et konkurrerende system og dermed opnå et konkurrerende patent. Kravene til de konkurrerende patenter er, at patentet skal omfatte et originalt system, og patentet må ikke krænke allerede eksisterende patenter. Hvis kravene til det konkurrerende patent opfyldes, er det muligt for de konkurrerende virksomheder at implementere lignende systemer, hvilket vil være i konkurrence med first-movers oprindelige system.[145]

Ved konkurrerende systemer på markedet vil markedsstrukturen ændre sig, da first-mover ikke længere har mulighed for at foretage en 1. grads prisdiskrimination. De konkurrerende virksomheder har ligesom first-mover et ønske om at fastsætte en højere pris på

[145] http://paguidelines.dkpto.dk/aa/danske-patenter/indlevering-af-nationale-patentansoegninger/krav.aspx

deres produkter grundet det højere serviceniveau, som skabes gennem ansigtsgenkendelsessystemet. Det medfører, at prisen hos first-mover og prisen hos konkurrenterne vil ligge på det samme niveau, som er ligevægten illustrereret til højre i figur 5 ovenfor.
Ved at konkurrenterne implementerer ansigtsgenkendelsessystemet vil konkurrencen på markedet rykke sig tættere på en fuldkommen konkurrence, da first-mover ikke længere vil have en monopolstatus på markedet.

På det tidspunkt hvor first-movers patent udløber, er det muligt for andre virksomheder at duplikere systemet, hvilket fjerner virksomhedens førende status på markedet. For at virksomheden kan sikre sin position på markedet, er det nødvendigt at vurdere, hvilke andre muligheder virksomheden har for at differentiere sig fra konkurrenterne. Forhold som i) produktets levetid og ii) tidspunktet for fald i profit er vigtige i vurderingen. Der kommer et tidspunkt, hvor profitten på det oprindelige system falder, hvis virksomheden ikke udvikler systemet. Det er derfor vigtigt for virksomheden at vurdere, hvor længe virksomheden regner med at kunne få noget ud af systemet.

Når forbrugerne gennem deres betalingsvillighed og deres højere nytteniveau har valgt at handle hos first-mover på kort sigt, må det forventes, at der på lang sigt er skabt en tryghed hos forbrugerne i forhold til brugen af ansigtsgenkendelsessystemet. Forbrugerne ved hvilket service- og prisniveau, de får hos first-mover. Trygheden vil hos forbrugerne give en usikkerhed i forhold til at skifte over til en af de konkurrerende virksomheder, da de ikke er sikre på, om de vil få det samme service- og prisniveau hos disse virksomheder. Denne usikkerhed hos forbrugerne er positiv for first-mover, da first-mover ved, at forbrugerne vil fastholde salget til vedkommende. Hvis first-mover ikke løbende udvikler på ansigtsgenkendelsessystemet eller giver forbrugerne en yderligere service, risikerer virksomheden, at forbrugerne på sigt vælger at handle hos en af konkurrenterne i stedet.

6.3.2. Forbrugernes købsbeslutningsproces

Som beskrevet tidligere vil andre virksomheder på markedet, der vælger at implementere et ansigtsgenkendelsessystem, lade deres prisniveau stige med den nye ligevægt i P2 og Q2.
First-mover vil dermed ikke have den samme mulighed for at differentiere sig på pris som på kort sigt. På kort sigt var der særligt fokus på forbrugernes rettigheder, hvor prisen

blev fastsat ud fra dette. Men hvis forbrugerne på lang sigt skal betale den samme pris hos alle virksomheder på markedet, skal forbrugeren vindes ud fra andre præferencer.
For at first-mover kan differentiere sig fra konkurrenterne på lang sigt, skal vedkommende finde alternative differentieringsstrategier. I vurderingen af en alternativ differentieringsstrategi tages der udgangspunkt i forbrugerens købsbeslutningsproces, som er defineret i afsnit 6.1.3.

Ud fra de 5 steps, som er oplistet i afsnit 6.1.3., vil der i starten af virksomhedens brug af ansigtsgenkendelsessystemet være mulighed for i punkt 4 at ændre på tiden for beslutning om køb. Som beskrevet i afsnit 6.2. gør systemer det muligt at kende forbrugerne bedre, da der ved hjælp af identificering og profilering kan findes frem til den enkelte forbrugers præferencer. Ud fra karaktertræk som køn, alder, adfærd, interesser og bevægelighed, som indsamles ved hjælp af ansigtsgenkendelsessystemet, er det muligt for den enkelte virksomhed at skræddersy markedsføring og reklame til den enkelte forbruger. En skræddersyet reklame vil fange forbrugerens opmærksomhed, da reklamen udelukkende indeholder oplysninger om produkter, som forbrugeren søger, og dermed spares den enkelte forbruger for irrelevant information. Denne skræddersyede service findes også i situationen, hvor systemet hjælper med at guide forbrugeren rundt i en butik ved at hjælpe forbrugeren hen til de produkter, som er relevant for vedkommende.
Efter noget tid vil virksomheden have en meget specifik profil af forbrugerne ud fra en længere overvågningsperiode, hvilket påvirker processen endnu bedre. Da virksomheden for eksempel ved, hvilke produkter forbrugeren typisk går efter, vil det resultere i en kortere og mere effektiv beslutningsproces og dermed minimere den tid, som forbrugeren ellers ville bruge på informationssøgning i processens punkt 2. For forbrugeren bliver dette en personlig berigelse.[146]
Den forbedrede beslutningsproces vil også påvirke den enkelte virksomhed. Med virksomhedens bedre muligheder for at hjælpe og guide forbrugerne hen til de relevante produkter, vil det formentlig skabe en større forbrugertilfredshed, da serviceniveauet stiger. Jo mere tilfredse forbrugerne er med servicen, jo større chance er der for, at forbrugerne vender tilbage til den pågældende virksomhed. Forbrugerne vil ved hjælp af et ansigtsgenkendelsessystem komme hurtigere igennem deres købsbeslutningsproces, hvilket giver en positiv indvirkning på den samlede købsoplevelse.

[146] Svend Hollesen: *Marketing management,* s. 125-126

Hvis alle markedets ansigtsgenkendelsessystemer på en eller anden måde har mulighed for at give den enkelte forbruger en bedre købsoplevelse, er det nødvendigt at den enkelte virksomhed igennem yderligere tiltag kan sikre sig, at forbrugerne vælger virksomheden frem for konkurrenterne.

En virksomhed har mulighed for at påvirke forbrugernes købsbeslutningsproces gennem forskellige former for stimuli.
Et eksempel på en differentieringsstrategi er rabatter. Hvis first-mover ved, at de konkurrerende virksomheder fastsætter den samme pris på produkterne, som first-mover, har first-mover mulighed for at prisdiskriminere ved at yde rabatter til forbrugerne. Ved at give den enkelte forbruger en rabat, når vedkommende foretager en handel hos first-mover, skabes der en yderligere stigning i forbrugerens nytteværdi. Den højere nytteværdi medfører, at forbrugeren forsat ønsker at handle hos first-mover i stedet for hos konkurrenterne, da rabatterne giver en yderligere service.
Denne differentiering kan lade sig gøre indtil det tidspunkt, hvor de konkurrerende virksomheder er blevet opmærksomme på rabatterne. For at virksomhederne ikke mister forbrugerne, vil de ligesom first-mover begynde at give rabatter til forbrugerne. Dette vil igen sætte first-mover i en situation, hvor vedkommende ikke differentierer sig fra konkurrenterne i forhold til service og pris.

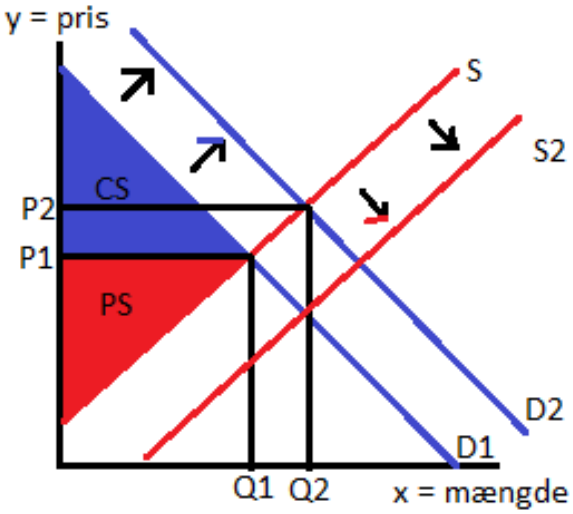
En anden måde, hvorpå first-mover kan differentiere sig fra konkurrenterne, er ved at påvirke beslutningsprocessen tidsmæssigt.
Som beskrevet i afsnit 6.2.1. vil first-mover have en førende viden indenfor brugen af ansigtsgenkendelsessystemer. Hvis first-mover har et ønske om fortsat at have en førende status på markedet, er virksomheden nødt til at foretage nogle løbende forbedringer af systemet. Ved løbende at forbedre det oprindelige ansigtsgenkendelsessystem, gennem systemopdateringer og udvikling, vil det medføre, at virksomhedens system vil være foran konkurrenternes ansigtsgenkendelsessystemer, da first-mover har en større viden inden for den teknologiske udvikling. Ved at first-mover er på forkant, er det muligt for virksomheden at tilbyde et nyere og hurtigere ansigtsgenkendelsessystem til forbrugerne. Hvis forbrugerne ved, at first-movers nyere og hurtigere ansigtsgenkendelsessystem kan mindske deres beslutningsproces yderligere, vil det formentlig resultere i, at forbrugerne fortsat vælger first-mover frem for konkurrenterne.

Punkt 3 i forbrugerens beslutningsproces, om vurdering af alternativer, vil formentlig mindskes eller helt forsvinde, hvis first-mover gennem sit videreudviklede og opdaterede ansigtsgenkendelsessystem kan gøre beslutningsprocessen og servicen endnu bedre end konkurrenternes. En tidsmæssig forbedret service skaber en stigende forbrugertilfredshed, samtidig med at forbrugernes opbyggede loyalitet forbliver uændret, da de kender til serviceniveauet og er i god tro om, at virksomheden hele tiden ønsker at forbedre niveauet.

Selvom der på lang sigt er flere virksomheder på markedet, der benytter sig af ansigtsgenkendelsessystemer, vil first-mover sikre sig sin førende status på markedet ved at give forbrugerne rabatter og forbedre beslutningsprocessen tidsmæssigt. På den måde sikrer first-mover, at forbrugerne fastholder deres køb hos vedkommende, samtidig med at virksomheden med et nyere og opdaterede system vil opnå profit i en længere periode.

6.3.3. Velfærden

På kort sigt steg den samlede velfærd grundet det højere efterspørgselsniveau, se figur 5. På lang sigt vil antallet af udbydere på markedet være steget, da der på dette tidspunkt er flere virksomheder, der har implementeret et ansigtsgenkendelsessystem. Et stigende antal udbydere vil medføre en stigning i udbuddet på markedet, hvilket flytter udbuddet S til højre, hvilket er illustreret i figur 6 nedenfor. Det højere serviceniveau, gennem ansigtsgenkendelsessystemer, må forventes at holde efterspørgslen på samme niveau som på kort sigt eller muligvis medføre en stigning på lang sigt. Grunden til dette er, at forbrugerne på lang sigt er blevet mere trygge ved ansigtsgenkendelsessystemets behandling, hvorfor de vil være mere åbne og trygge i forhold til den nye behandlingsform. Med en efterspørgsel på enten samme niveau eller et højere niveau på lang sigt, samtidig med en stigning i udbuddet, vil der ske en stigning i den samlede velfærd på lang sigt.



Figur 6: Ændring i den samlede velfærd på lang sigt[147]

6.4. Samlet konklusion på den økonomiske analyse

Det kan på baggrund af ovenstående analyser konkluderes, at anvendelsen af ansigtsgenkendelsessystemer har en væsentlig betydning for virksomheder, forbrugere og samfundet.

Fase 1 viser, at en implementering af et ansigtsgenkendelsessystem på kort sigt skaber muligheder for first-mover. Systemet kan hjælpe med at identificere og profilere forbrugerne, så virksomheden kan skræddersy reklame til den enkelte forbruger og dermed skabe større forbrugertilfredshed. First-mover opnår her fordele ved at definere markedet og prissætte, som vedkommende mener er bedst. Prisfastsættelsen vil ved hjælp af et ansigtsgenkendelsessystem ske gennem 1. grads prisdiskrimination, så alle forbrugere betaler den pris for produktet, som den enkelte er villig til at betale. First-mover har tillige et teknologisk forspring og mulighed for patent. Selv med de negative konsekvenser ved implementeringen, vil den samlede velfærd stige grundet en stigende efterspørgsel ud fra forbrugernes højere betalingsvillighed.

Fase 2 viser, at en implementering af et ansigtsgenkendelsessystem på lang sigt skaber muligheder for first-mover og de andre virksomheder, som har valgt at implementere et lignende system. Som udgangspunkt kan alle virksomheder, som implementerer

[147] Eget arbejde

systemet, påvirke forbrugernes købsbeslutningsproces ved at afkorte processen med en skræddersyet reklame til den enkelte.
For at first-mover kan beholde sin førende status på markedet og fortsat være forbrugernes foretrukne valg, er virksomheden nødt til at finde alternative differentieringsstrategier, herunder rabatter samt udvikling og opdatering af systemet. Det skaber en hurtigere og mere effektiv proces. En løbende udvikling skaber større omkostninger, men vil på sigt gavne virksomheden, da udviklingen gør det muligt at fastholde forbrugerne og fastholde en profit i en længere periode.
Velfærden vil tillige stige på lang sigt, da der sker en stigning i udbyderne på markedet.

Samlet set vil den samlede velfærd stige ved brugen af denne form for system grundet det stigende antal udbydere samtidig med en stigende tilfredshed og betalingsvillighed hos forbrugerne. Det højere serviceniveau vil både medfører en stigning i efterspørgslen og udbuddet på markedet. Et ansigtsgenkendelsessystem vil økonomisk set både stille virksomheder, forbrugere og samfundet bedre.
Virksomhederne skal dog være opmærksom på de kritiske forbrugere, som mener, at systemet krænker deres rettigheder. Virksomhederne skal her gøre noget ekstra for, at denne gruppe af forbrugere får en god oplevelse med den nye behandlingsform.

Del 4 – Konklusion, perspektivering og litteratur- og kildefortegnelse

7. Konklusion

Afhandlingens formål er at vurdere, hvorvidt de nuværende regler om behandling af biometriske data i teknologiske løsninger, herunder ansigtsgenkendelsessystemer, efter Databeskyttelsesforordningen er optimalt indrettet, så der skabes en efficient tilstand på markedet.

I relation til kommerciel behandling af biometriske data i teknologiske løsninger har den juridiske analyse vist, at der kun er begrænsede muligheder for at foretage behandlingen grundet en beskyttelse af den registreredes interesser. Det er kun muligt at foretage behandling af biometriske data, hvis behandlingen foregår i et verifikationssystem. Yderligere krav til behandlingen er, at den alene kan ske ud fra udregnede værdier af de

biometriske data, og lagringen af oplysningerne skal foretages, så den registrerede har mulighed for at føre kontrol med oplysningerne. Forordningen forbyder derfor ikke enhver form for behandling af biometriske data, men det kræves, at der foretages en afvejning af behandlingens formål og nødvendighed. De begrænsede muligheder for behandlingen gør det svært for virksomheder at gøre profilering gældende grundet den mere indgribende form for behandling.
Behandlingsformen er i praksis alene accepteret med samtykke som behandlingsgrundlag, jf. GDPR art. 9, stk. 2, litra a og art. 6, stk. 1, litra a. For at anse behandlingen som tilstrækkelig og nødvendig er den altovervejende hovedregel, at proportionalitetsprincippet overholdes, jf. GDPR art. 5, stk. 1, litra c.

Den økonomiske analyse har vist, at virksomheders brug af ansigtsgenkendelsessystemer både vil påvirke virksomheder, forbrugere og samfundet positivt. Analysen viser, at Databeskyttelsesforordningen begrænser muligheden for en stigning i den samlede velfærd, hvorfor den mere efficiente tilstand på markedet ikke er mulig.

På baggrund af den juridiske og økonomiske analyse vurderes det, at Databeskyttelsesforordningens nuværende regler ikke er indrettet på en sådan måde, så der kan opnås en efficient tilstand på markedet gennem brugen af ansigtsgenkendelsessystemer. Det juridiske og økonomiske syn på behandlingen modstrider i dette tilfælde hinanden. Juridiske set er alle begrænsninger for behandling lavet med særlig fokus på beskyttelse af forbrugerne, hvilket skaber begrænsninger for virksomhederne. Den økonomiske synsvinkel har fokus på virksomhederne og viser, at brugen af den nye form for system tillige vil påvirke forbrugerne positivt.

Virksomhederne er derfor nødt til at finde andre alternativer til behandling af biometriske data, som kan skabe et mere efficient markedet, men som samtidig overholder Databeskyttelsesforordningens regler.

8. Perspektivering

Afsnit 8 omhandler virksomheders behandlingsmuligheder i dag og i fremtiden. Til den videre undersøgelse af afhandlingens behandlingsområde vil politiske synsvinkler og andre aspekter fra samfundet vurderes.

8.1. Behandlingsmuligheder i dag

Som afhandlingen konkluderer, er der begrænsede muligheder for virksomheder til at behandle biometriske data ud fra en kommerciel interesse grundet forholdet til den registreredes rettigheder. Det er derfor ud fra den juridiske praksis vurderet, at det ikke er muligt at foretage profilering af de registrerede ud fra en kommerciel behandling af biometriske data.

Begrænsningerne sætter en stopper for virksomhederne i forhold til at skabe et mere efficient marked ved brug af ansigtsgenkendelsessystemer. Som reglerne ser ud i dag, er virksomheder nødt til at finde alternative behandlingsmuligheder, hvis de skal have mulighed for at skabe et mere efficient marked.

Hvis virksomheder ønsker at lave markedsføring til den enkelte forbruger, er det på internettet allerede muligt gennem cookies. Cookies er små datafiler, der indsamler digitale fodspor om forbrugeren, når de færdes online.[148] Ud fra et kommercielt henseende kan virksomheder benytte sig af markedsføringscookies, hvor der indsamles oplysninger ved at følge den enkelte forbruger rundt på de enkelte hjemmesider. På den måde kan virksomhederne skabe et overblik over forbrugernes interesser, vaner og aktiviteter for på den måde at vise relevante annoncer for produkter, som den enkelte forbruger tidligere har søgt efter. Kravet for at kunne benytte markedsføringscookies er, at forbrugeren har givet sit samtykke til behandlingen, da der ved behandlingen er en mulighed for at identificere den enkelte forbruger.[149]

Hvis det i stedet omhandler en mere effektiv handel i virksomheders fysiske butikker, kan virksomheder for eksempel tilbyde forbrugerne kundefordele. Det kan ske ved, at forbrugeren vælger at blive kunde i butikken for på den måde at modtage et medlemskort. Med et medlemskort har virksomheden mulighed for at give forbrugerne forskellige fordele som for eksempel rabatdage, kundeaftener osv. Denne behandling er allerede benyttet af for eksempel Matas[150] og Magasin[151]. Det er en vurdering, at det efter Databeskyttelsesforordningen er muligt at videreudvikle det allerede eksisterende medlemskort, hvis behandlingen ikke er mere indgribende end de opstillede krav i afhandlingens afsnit 5.6.

[148] https://erhvervsstyrelsen.dk/vaerd-at-vide-om-cookies
[149] https://erhvervsstyrelsen.dk/mod-de-vaesentligste-cookietyper
[150] https://www.matas.dk/clubmatas/om-club-matas
[151] https://www.magasin.dk/sider/om-magasin/services/pages_goodie_benefits_1.html

Det kan for eksempel være at give forbrugeren en ekstra oplevelse, når vedkommende træder ind i butikken og scanner sit medlemskort på en skærm ved indgangen. På kortet er der for eksempel lagret oplysninger om forbrugerens tidligere køb, hvorfor systemet kan give vedkommende personlige rabatter ud fra denne historisk. Det er også muligt gennem systemet at guide forbrugerne rundt i butikken. Ved hurtigt at blive guidet hen til de produkter, som forbrugeren ønsker, vil vedkommende spare den tid, som normalt bruges på at finde en ledig ekspedient i butikken. Samtidig vil det formentlig medføre, at der kommer et større salg grundet den hurtigere beslutningsproces, hvilket er positivt for virksomheden. Hvis det forudsættes, at forbrugeren har givet sit samtykke til behandlingen, er det muligt for virksomhederne at indføre denne mere personlige behandling i de fysiske butikker, da den registrerede samtidig har mulighed for at føre kontrol med oplysningerne på det personlige kundekort.

8.2. Fremtiden

Ansigtsgenkendelsessystemer går skridtet videre i forhold til ovenstående behandlingsmuligheder. En fordel ved ansigtsgenkendelsessystemer er, at der kan gives skræddersyede kundeoplevelser både på internettet og i butikker, da systemet gør det muligt at kende den enkelte forbruger bedre.[152] Men selvom der er fordele ved brugen af systemet, kan en sådan databehandling også få negative reaktioner fra befolkningen. Et eksempel på dette ses i Kina, hvor befolkningen demonstrerer over brugen. Kina er blevet et overvågningssamfund i meget højere grad end Danmark, og dele af befolkningen føler sig overvåget og begrænset i det offentlige rum. Regeringens og politiets behandling af befolkningens personoplysninger skaber frygt og usikkerhed, hvilket har ført til demonstrationer. Deltagerne i demonstrationerne vælger at tildække deres ansigter, blokere eller ødelægge overvågningskameraer samt kommunikere via krypterede apps for at skjule deres identitet.[153]

Befolkningens frygt og usikkerhed for behandling af deres biometriske data ses også hos den amerikanske befolkning ved virksomheders brug af ansigtsgenkendelsessystemer. Det er for eksempel tilfældet ved Clearview AIs levering af ansigtstemplates til politiet. Billederne, som befinder sig på de solgte templates, er indsamlet på sociale medier som

[152] https://www.etik.dk/etik.dk/hvor-gaar-graensen-mellem-skraeddersyede-kundeoplevelser-og-overvaagning?
[153] https://www.buzzfeednews.com/article/rosalindadams/hong-kong-protests-paranoia-facial-recognition-lasers

Facebook og Twitter. Det er endnu ikke afgjort, om Clearview har handlet i strid med lovgivningen, men befolkningen mener, at behandlingen krænker deres rettigheder.[154]

Direktøren af Radr, Preben Mejer har udtalt: "Medmindre du har lyst til at gå med en stor plastiksæk over hovedet eller på anden måde maskere dig i det offentlige rum, bliver det i fremtiden svært ikke at opleve en eller anden form for ansigtsgenkendelse i din hverdag".[155] Udtalelsen viser, at befolkningen i fremtiden er nødt til at acceptere, at der sker en større grad af behandling af deres personoplysninger grundet den teknologiske udvikling.

Den Europæiske Kommission har tillige udtalt sig om emnet i deres rapport om brug af kunstig intelligens; "Den digitale teknologi bliver en stadig mere central del af menneskers liv på alle fronter, så derfor bør folk kunne stole på den."[156] Rapporten er også interessant for brugen af ansigtsgenkendelsessystemer, da kunstig intelligens og ansigtsgenkendelse er komplementære teknologier, som også kan eksistere uden hinanden.[157] Problemet er, at der ved alle nye former for teknologi er en stor usikkerhed ved brugen. Befolkningen frygter at blive magtesløse i at forsvare deres rettigheder og sikkerhed, når behandlingen foregår i et elektronisk system, og virksomheder er bekymrede over manglende retssikkerhed.[158] Det vurderes, at jo længere tid en form for teknologi er blevet benyttet i samfundet, jo mere tryghed skabes der hos befolkningen, medmindre teknologien skaber store fejl eller giver store chancer for misbrug. Ved at skabe tryghed vil der formentlig komme flere muligheder for at benytte teknologier som ansigtsgenkendelsessystemer og kunstig intelligens i fremtiden, da befolkningen vil være mere villige til at acceptere behandlingen.

I Kommissionens rapport om kunstig intelligens bliver den nuværende lovgivningsramme diskuteret. Efter Kommissionens mening bør lovgivningsrammen give plads til yderligere udvikling på markedet, da området for teknologi er i hastig udvikling.[159] Denne hastige udvikling indenfor teknologi er blevet præsenteret af forsknings- og rådgivningsvirksomheden Gartner. Gartner præsenterede på et webinar deres forudsigelser af digitale trends

[154] https://www.mediapost.com/publications/article/346620/clearview-ai-slammed-with-new-lawsuit-over-facepri.htm
[155] https://www.etik.dk/etik.dk/hvor-gaar-graensen-mellem-skraeddersyede-kundeoplevelser-og-overvaagning?
[156] Hvidbog, afsnit 1, s. 1
[157] Blog: *AI and Facial Recognition: Challenges and Opportunities*
[158] Hvidbog, afsnit 5, s. 10
[159] Ibid., afsnit 5, s. 11

fra 2020 og frem. Et interessant område er her teknologiens mulighed for at tracke folks følelser samt levere indhold og produkter skræddersyet hertil. Ved at bruge teknologien på denne måde, er det muligt at fremme virksomheders resultater, hvilket udelukkende er muligt grundet den teknologiske udvikling.[160]

Da de nye teknologier på markedet er omfattet af den nuværende lovgivningsramme om databeskyttelse, herunder Databeskyttelsesforordningen, er der en forventning hos forbrugerne om, at beskyttelsesniveauet ved den nye teknologi er den samme som ved alt andet behandling af personoplysninger.[161] Spørgsmålet er, om den nuværende lovgivning er i stand til at håndtere de nye former for risici, der er forbundet med nye teknologier, herunder kunstig intelligens og ansigtsgenkendelse. Hvis den nuværende lovgivning ikke er i stand til dette, er det nødvendigt at se på behovet for en tilpasning af den nuværende lovgivning eller behovet for en helt ny lovgivning, som tager stilling til de nye risici. Flere medlemslande, herunder Danmark, er allerede i gang med at undersøge mulighederne for en national lovgivning, der kan imødekomme de nye udfordringer.[162] Dog mener Kommissionen, at forskelligartede nationale regler vil være med til at skabe hindringer for de europæiske virksomheder. Med en fælles og solid Europæisk lovgivningsramme giver det virksomhederne adgang til det indre marked uhindret, hvilket kan styrke deres konkurrenceevne.[163] Derudover vil den nye lovgivningsramme mindske usikkerheden hos forbrugerne, da den nye lovgivning vil give en bedre beskyttelse af rettigheder ved brug af nye former for teknologi som ansigtsgenkendelse og kunstig intelligens.[164]

Afslutningsvis kan det vurderes, at ud fra ovenstående undersøgelse er det tydeligt, at behandlingen af biometriske data i kommerciel sammenhæng har et stort potentiale. I en videre undersøgelse af feltet kunne det være yderst interessant at følge den nye udvikling af de kommercielle retningslinjer. Undersøgelsen kunne fokusere på, om vægtningen af forbrugerne over virksomhederne, som viste sig i indeværende undersøgelse, ville ændre sig, eller om ikke andet blive mere ligevægtig.

Med en ny lovgivningsramme, hvor virksomheder i højere grad tilgodeses, vil virksomheder være i stand til at udnytte den teknologiske udvikling og dermed benytte teknologi som ansigtsgenkendelse i et større omfang. Ved at give virksomheder denne mulighed vil

[160] Gartner: *The Gartner Top Strategic Prediction for 2020 and Beyond*
[161] Hvidbog, afsnit 5, s. 11
[162] Ibid.
[163] Ibid., afsnit 5B, s. 16
[164] Ibid., afsnit 5, s. 11

det tillige skabe et mere efficient marked, hvilket vil påvirke den samlede velfærd positivt.

9. Litteratur- og kildefortegnelse

9.1. Lovgivning

Traktater

- Traktaten om den Europæiske Union (Refereret i afhandlingen: **TEU)**

Charter

- Den Europæiske Unions Charter 2000/ C 364/01 *om grundlæggende rettigheder* (Refereret i afhandlingen: **Charter** eller **EUC)**

Konventioner

- Europæiske Menneskerettighedskonvention af 4. november 1950 ”*Konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder”* (Refereret i afhandlingen: **EMRK)**

Forordninger

- Europa-Parlamentets og Rådets forordning (EU) nr. 2016/679 af. 7. april 2016 *om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF* (Refereret i afhandlingen: **Databeskyttelsesforordningen**)

Direktiver

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

National lovgivning

- Lov nr. 502 af 23. maj. 2018 *om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger* (Refereret i afhandlingen: **Databeskyttelsesloven**)

9.2. Vejledninger, udtalelser, betænkninger og bemærkninger

Artikel 29-gruppen

- **Vejledninger**
    - ***WP 251:*** *Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679*, WP 251 rev. 01, 3. oktober 2017, senest revideret og vedtaget d. 6. februar 2018
    - ***WP 259****: Retningslinjer vedrørende samtykke I henhold til forordning 2016/670*, WP 259 rev. 01, 28. november 2017, senest revideret og vedtaget d. 10. april 2018

- **Udtalelser**
    - ***WP 136****: Udtalelse nr. 4/2007 om begrebet personoplysninger*, WP 136, 20. juni 2007
    - ***WP 187****: Udtalelse 15/2011 om definitionen af samtykke,* WP 187, 13. juli 2011
    - ***WP 193:*** *Udtalelse 3/2012 om udviklingen inden for biometriske teknologier*, WP 193, 27. april 2012

Det danske Datatilsyn

- **Vejledninger**
    - *Konsekvensanalyse,* marts 2018
    - *Samtykke*, september 2019

- **Baggrundsnotat**
    - ***J.nr. 2019-20-0004****: Baggrundsnotat om betydningen af databeskyttelsesforordningens artikel 6 ved behandling af særlige kategorier af personoplysninger (følsomme personoplysninger) omfattet af forordningens artikel 9*, j.nr. 2019-20-0004, 7. november 2019

Justitsministeriet

- **Betænkning**
    - *Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning*, bind 1, nr. 1565, 2017

Det Europæiske Databeskyttelsesråd

- **Vejledninger**
    - ***Guidelines 3/2019:*** *Guidelines 3/2019 on processing of personal data through video devices*, version 2.1, 29. januar 2020
        - Tilgængelig på: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en.pdf

9.3. Retspraksis og andet praksis

- **Danmark**
    - **Datatilsynets afgørelser**
        - **2003-212-0143**: Afgørelse af 4. marts 2003 – *Fingeraftryk på Bornholmerkort* – j.nr. 2003-212-0143
        - **2004-219-0208**: Afgørelse af 26. november 2004 – *Adgangssystem til motionscenter baseret på fingeraftryk* – j.nr. 2004-219-0208
        - **2006-291-0370**: Afgørelse af 23. maj 2006 – *Anvendelse af biometri ved indcheckning af bagage* – j.nr. 2006-291-0370
        - **2008-42-0742**: Afgørelse af 20. juni 2008 – *Adgangskontrol på diskoteker of førelse af intern karantæneliste* – j.nr. 2008-42-0742
        - **2015-631-0122**: Afgørelse af 8. april 2015 – *Registrering af nummerplader ved parkering* – j.nr. 2015-631-0122
        - **2014-632-0081**: Afgørelse af 22. juni 2017 – *Brug af fingeraftryk ved bloddonation* – j.nr. 2014-632-0081

    - **Datatilsynets tilladelser**
        - Tilladelse af 24. maj 2019 – *Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgangen til Brøndby Stadion*

- **EU-Domstolen**
    - C-6/64, af 15. juli 1964 – *Flamino Costa mod ENEL*
    - C-92/09 og C-93/09 af 9. november 2010 – *Volker und Markus Schecke GbR and Hartmut Eifert mod Land Hessen*

- C-342/12 af 30. maj 2013 – *Worten – Equipamentos para o Lar SA mod Autoridade para as Condições de Trabalho (ACT)*
- C-131/21 af 13. maj 2014 – *Google Spain SL, Google Inc. Mod Agencia Española de Protección de Datos (AEPD), Mario Costeja González*
- C-434/16 af 20. december 2017 – *Peter Nowak mod Data Protection Commissioner*

- **Frankrig**
  - **Datatilsynets afgørelser**
    - Resumé af afgørelse af 17. oktober 2019 – *Eksperimentering med ansigtsgenkendelse på to gymnasier*
      - Tilgængelig her: https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

- **Polen**
  - **Datatilsynets afgørelser**
    - **ZSZZS.440.768.2018**: Afgørelse af 18. februar 2020 – *Skole pålagt bøde for behandling af elevernes fingeraftryk* - j.nr. ZSZZS.440.768.2018
      - Tilgængelig på: https://uodo.gov.pl/de-cyzje/ZSZZS.440.768.2018

- **Storbritannien**
  - **Landsretten – High Court of Justice of England and Wales**
    - **CO/4085/2018**: Afgørelse af d. 4. september 2019 – *R (Bridges) v. CCSWP and SSHD* - nr. CO/4085/2018
      - Tilgængelig på: https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf

- **Sverige**
    - **Datatilsynets afgørelser**
        - **DI-2019-2221**: Afgørelse af 20. august 2019 - *Tillsyn enligt EU:s dataskyddsförordning 2016/679 – ansiktsigenkänning för närvarokontroll av elever* – j.nr. DI-2019-2221
            - Tilgængelig på: https://www.datainspektionen.se/global-assets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf

9.4. Litteratur

- Blume, Peter: *Den nye persondataret*, 2. udgave, Jurist- og Økonomforbundets Forlag, 2018
- Blume, Peter og Janne Rothmar Herrmann: *Ret, privatliv og teknologi*, Jurist- og Økonomforbundets Forlag, 2018
- Christoffersen, Jonas: *EU's charter om grundlæggende rettigheder med kommentarer*, 2. udgave, Juridisk- og Økonomforbundets Forlag, 2018
- Hollesen, Svend: *Marketing management – a relationship approach*, 3. udgave, Pearson, 2014
- Mortensen, Bent Ole Gram (red.), Carina Risvig Hamer, Daniel Hartfield-Traun, Lisa Hjerrild, Kent Kristensen, Jesper Kruse Martvart, Helene Arensbak Mørk, Jesper Løffler Nielsen, Ayo Næsborg-Andersen, Sten Schaumburg-Müller, Christian Højer Schjøler, Peter Straup, Jørn Ullits og Frederik Waage: *Dansk persondataret*, 1. udgave, Ex Tuto Publishing A/S, 2020
- Markides, Constantinos C. og Paul A. Geroski; *Fast second – how smart companies bypass radical innovation to enter and dominate new markets*, Jossey-Bass, 2005
- Perloff, Jeffery M.: *Microeconomics with calculus*, global edition, 3. udgave, Pearson, 2014
- Pindyck, Robert S. og Daniel Rubinfeld: *Microeconomics*, global edition, 8. udgave, Pearson, 2015
- Samuelson, Paul A. og William D. Nordhaus: *Economics*, 19. udgave, McGraw-Hill Irwin, 2009

- Tvarnø, Christian D. og Ruth Nielsen: *Retskilder og retsteorier*, 5. udgave, Jurist- og Økonomforbundets Forlag, 2017
- Udsen, Henrik: *IT-ret*, 4. udgave, Ex Tuto Publishing A/S, 2019
- Vohra, Rakesh V. og Lakshman Krishnamurthi: *Principles of pricing*, Cambridge University Press, 2012

9.5. Artikler

- **Nyhedsartikler**
  - *Facial recognition technology in the EU: does GDPR spell the end,* af Debbie Heywood, TaylorWessing, juli 2018: https://www.taylorwessing.com/download/article-facial-recognition-in-eu.html (set 25.05.2020)
  - *Clearview AI slammed with new lawsuit over 'faceprint' sales*, af Wendy Davis, Mediapost, 4. februar 2020: https://www.mediapost.com/publications/article/346620/clearview-ai-slammed-with-new-lawsuit-over-face-pri.htm (set 25.05.2020)
  - *Hong Kong protesters are worried about facial recognition technology. But there are many other ways they're being watched,* af Rosalind Adams, BuzzFeed News, 17. august 2019: https://www.buzzfeednews.com/article/rosalindadams/hong-kong-protests-paranoia-facial-recognition-lasers (set 25.05.2020)
  - *Hvor går grænsen mellem skræddersyede kundeoplevelser og overvågning?*, af Julie Høgholm, Kristeligt Dagblad, 24. november 2017: https://www.etik.dk/etik.dk/hvor-gaar-graensen-mellem-skraeddersyede-kundeoplevelser-og-overvaagning? (set d. 25.05.2020)
  - *How does facial recognition work?,* af Andrew Heinzman, How-To Geek, 11. Juli 2019: https://www.howtogeek.com/427897/how-does-facial-recognition-work/ (set 23.03.2020)
  - *Kina sætter sig på teknologien til overvågning*, af Thomas Breinstrup, Berlingske, 27. december 2019: https://www.berlingske.dk/virksomheder/kina-saetter-sig-paa-teknologien-til-overvaagning (set 27.04.2020)

- **Videnskabelige artikler**
    - Lieberman, Marvin B. og David B. Montgomery: *First-mover (dis)advantages: retrospective and link with the resource-based view*, strategic management journal s. 1111-1125, 1998
    - Østergaard, Kim: *Metode på cand.merc.jur. studiet*, Jurist- og Økonomiforbundets Forlag, s. 269-285, 2003
    - Østergaard, Kim: *Relevansen af interdisciplinær forskning og empiri i samfundsvidenskaben,* Retfærd årgang 37 nr. 3/136, 2014

9.6. Rapporter

- Department of Homeland Security: *Report 2019-01 of the DHS Data Privacy and Integrity Advisory Committee (DPIAC): Privacy Recommendation in Connection with the Use of Facial Recognition Technology,* offentliggjort d. 26. februar 2019
    - Tilgængelig her: https://www.dhs.gov/sites/default/files/publications/Report%202019-01_Use%20of%20Facial%20Recognition%20Technology_02%2026%202019.pdf
- European Union Agency For Fundamental Rights (FRA): *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019
    - Tilgængelig her: https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

9.7. Hjemmesider

- Apple
    - https://support.apple.com/da-dk/HT208108
- Erhvervsstyrelsen – Regler for cookies
    - https://erhvervsstyrelsen.dk/vaerd-at-vide-om-cookies
    - https://erhvervsstyrelsen.dk/mod-de-vaesentligste-cookietyper
- Institut for menneskerettigheder
    - https://menneskeret.dk/om-os/menneskerettigheder/menneskerettigheder-danmark/dansk-lovgivning

- Juraplexus
    - http://www.juraplexus.dk/juridisk-leksikon/id.de-lege-lata/i.html
- Magasin
    - https://www.magasin.dk/sider/om-magasin/services/pages_goodie_benefits_1.html
- Matas
    - https://www.matas.dk/clubmatas/om-club-matas
- Norton
    - https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html
- Patient- og Varemærkestyrelsen
    - http://paguidelines.dkpto.dk/aa/danske-patenter/indlevering-af-nationale-patentansoegninger/krav.aspx

9.8. Andet

- **Blog**
    - European Data Protection Supervisor: *AI and Facial Recognition: Challenges and Opportunities*
        - Tilgængelig her: https://edps.europa.eu/press-publications/press-news/blog/ai-and-facial-recognition-challenges-and-opportunities_en

- **Webinar**
    - Gartner: *The Gartner Top Strategic Prediction for 2020 and Beyond,* 10. marts 2020 (set 26.05.2020)
        - Tilgængelig her: https://www.gartner.com/en/webinars/52391/top-strategic-predictions-for-2020-and-beyond

- **Hvidbog**
    - Den Europæiske Kommission: *Om kunstig intelligens – en europæisk tilgang til ekspertise og tillid***,** 19. februar 2020
        - Tilgængelig her: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_da.pdf