



AALBORG UNIVERSITET

PERSONDATAFORORDNINGEN:

EN ANALYSE AF DE PERSONDATARETLIGE PROBLEMSTILLINGER
I SAGEN OM CAMBRIDGE ANALYTICA



SPECIALEAFHANDLING 2018

DANIEL BRUUN

Titelblad

Emne:	Persondataforordningen: En analyse af de persondataretlige problemstillinger i sagen om Cambridge Analytica
English Title:	The General Data Protection Regulation: An analysis of the problems related to the regulation of personal data in the Cambridge Analytica case
Uddannelsessted:	Aalborg Universitet
Uddannelsesretning:	Cand.merc.jur
Vejleder:	Lektor, ph.d. Marie Jull Sørensen
Projektart:	Specialeafhandling
Retsområde:	Persondataret
Afleveringsdato:	17. maj, 2018
Sideantal:	58
Anslag i alt:	143.185
Antal normalsider:	59,66
Forfatter:	Daniel Bruun

Indholdsfortegnelse

Abstract	- 4 -
Kapitel I. Introduktion	- 5 -
1. Indledning	- 5 -
2. Problemformulering	- 7 -
3. Afgrænsning	- 8 -
4. Metode og retskilder.....	- 9 -
5. Redegørelse af sagen om Cambridge Analytica	- 13 -
Kapitel II. Persondataforordningens anvendelsesområde	- 14 -
1. Beskyttelsesobjektet – Personoplysninger.....	- 14 -
2. Pligtsubjektet – Den dataansvarlige	- 16 -
3. Materiel afgrænsning.....	- 18 -
4. Formel afgrænsning.....	- 19 -
a. Facebook.....	- 20 -
b. Cambridge Analytica.....	- 22 -
Kapitel III. Legaliteten af Cambridge Analytics aktiviteter	- 24 -
1. God databehandlingsskik	- 24 -
2. Selvfølgelig gørelse.....	- 25 -
3. Persondatarettens samtykkebegreb.....	- 26 -
4. Facebooks brugervilkår	- 28 -
5. Cambridge Analytics behandlingsgrundlag	- 31 -
Kapitel IV. Facebooks ansvar og forpligtelser	- 36 -
1. Tilstrækkelig datasikkerhed	- 36 -
2. Underretningspligt	- 39 -
Kapitel V. Sanktionsmuligheder	- 42 -
1. Facebook.....	- 43 -
2. Cambridge Analytica	- 44 -
Kapitel VI. Konklusion	- 47 -
Kapitel VII. Perspektivering	- 49 -
Bibliografi	- 52 -

Abstract

The purpose of this thesis has been to investigate, whether Facebook and Cambridge Analytica have violated the provisions in the EU's General Data Protection Regulation. Furthermore, the thesis similarly explored the possibility that the implicated companies may be sanctioned as a result of their conduct and actions in the recent case.

This study has been completed on the basis of the relevant legal sources and certain news articles, which serves as the factual evidence in the Cambridge Analytica case. Additionally, the study has revolved under the underlying assumption that the legal problems in the case will be decided by the provisions in the new Regulation and not the old Data Protection Directive.

Initially it was explored whether the factual circumstances of the case, satisfies the substantive and territorial requirements of the Regulation. The case pertains to the processing of highly sensitive personal information on 87 million Facebook users, which has been conducted from Cambridge Analytica's office in Britain. It can therefore be concluded that the provisions in the Regulation are applicable in this case.

Subsequently, the study examined the legality of Cambridge Analytica's activities. It could be rejected that the Facebook users had forfeited their data rights by making the information available on Facebook. Furthermore, it was not substantiated that Cambridge Analytica ever held any lawful basis that justifies the alleged activities of the company. Cambridge Analytica has therefore failed to meet the foundational principles that applies to the processing of personal data, which are stated in the Regulation.

The study similarly found that Facebook has failed to honor the obligations, which applies to the data controller. Specifically, the company has not succeeded in securing an adequate level of data security that could have protected the data from being exploited in conjunction with unlawful purposes. Facebook also failed to disclose, to the concerning data subjects and relevant supervisory authority, respectively that it had become aware of a data breach. It could therefore be concluded that Facebook also have failed to meet the basic principles that applies to the data controller as stated in the Regulation.

Lastly, as the case pertains to infringements of the core processing principles in the Regulation, the most burdensome sanction is applicable against both companies. Facebook can therefore receive an administrative fine of 4 % of its total worldwide annual turnover. Cambridge Analytica has begun insolvency procedures which makes it harder to predict the legal ramifications for the company. However, the British Data Protection Agency (ICO) has stated that it currently holds every legal opportunity open, as it continues its investigation of the Cambridge Analytica case.

Kapitel I. Introduktion

1. Indledning

“So whenever you go, and you like something, you are giving me a clue as to who you are as a person. And so all of this can be captured very easily and run through an algorithm that learns who you are. When you go to work - right? - your co-workers only see one side of you. Your friends only see one side of you. But a computer sees all kinds of sides of you. And so we can get better than human level accuracy at predicting your behavior.” – Christopher Wylie¹

Data er blevet beskrevet som det 21. århundredes svar på olie, da adskillige virksomheder efterhånden har øjnet værdien i den mængde data, der befinder sig online.² Det er således estimeret, at 90 % af verdens online data er blevet genereret inden for de seneste to år, hvilket danner grundlag for nye muligheder samt problemstillinger.³ Virksomheder, som Facebook, er eksempelvis i besiddelse af data, der kan angive ret præcist, hvad der kendetegner den enkelte bruger alt afhængigt af, hvor aktiv personen har været på platformen. Dette datamateriale kan derved anvendes til at forudsige konkrete individers handlemønstre, hvilket kan udnyttes til uetiske formål i de forkerte hænder.

Denne problemstilling er eksempelvis illustreret i den aktuelle sag om Cambridge Analytica, der er en dataanalysevirksomhed med speciale i at påvirke valg til politiske institutioner.⁴ Facebook estimerer således selv, at 87 mio. Facebook-brugeres personoplysninger uautoriseret er blevet lækket til Cambridge Analytica.⁵ Disse informationer er angiveligt blevet anvendt til politiske formål i forbindelse med henholdsvis Brexit-afstemningen og Trump-præsidentvalget.⁶ Sagen så først offentlighedens lys, da Christopher Wylie, som havde en instrumental rolle i grundlæggelsen af Cambridge Analytica, stod frem og angav, hvordan virksomheden havde 'høstet' og herefter udnyttet data fra Facebook: *“.. those (Facebook) profiles were used as the basis of the algorithms that became the foundation of Cambridge Analytica itself... we would know what kinds of messaging you'd be susceptible to, including the framing of it, the topics, the content, the tone – whether it's scary or not that kind of thing... and where you're going to consume that and then how many times*

¹ Wylie, 2018: *Cambridge Analytica: Whistleblower reveals data grab of 50 million Facebook profiles*

² Liem & Petropoulos, 2016: *The economic value of personal data for online platforms, firms and consumers*

³ Verhulst & Young, 2018: *How the Data That Internet Companies Collect Can Be Used for the Public Good*

⁴ Cambridge Analytica, 2018: *We find your voters and move them to action*

⁵ Schroepfer, 2018: *An Update on Our Plans to Restrict Data Access on Facebook*

⁶ Cadwalladr & Graham-Harrison, 2018: *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*

we would need to touch you with that, in order to change how you think about something."⁷ Virksomheden har således anvendt en kombination af forskellige metoder, hvilket omfatter data-mining, micro-targeting og psykografisk modellering, til at udlede sammenhænge, der kunne udnyttes til politiske formål.⁸ Hele denne proces skulle angiveligt have fundet sted uden de fleste Facebook-brugeres samtykke eller bevidsthed om, at de var blevet profileret og herefter overvældet med indhold, der skulle skabe sympati for bestemte politiske budskaber.⁹

Sagen har allerede affødt et stort politisk udfald. Facebook CEO, Mark Zuckerberg, har vidnet foran den amerikanske kongres om selskabets håndtering af sagen.¹⁰ Det britiske parlament har ligeledes fremsendt en lignende anmodning, men Zuckerberg har valgt at afvise denne invitation.¹¹ Det forventes ligeledes, at sagen kommer til at have juridiske konsekvenser for de ansvarlige parter. Det britiske datatilsyn (ICO) er eksempelvis, på nuværende tidspunkt, i færd med at foretage en minutiøs undersøgelse af, om Cambridge Analytica og Facebook har handlet i overensstemmelse med de persondataretlige regler.¹² Derimod har det danske datatilsyn indledningsvist besluttet at afvente resultatet af den britiske undersøgelse, før der eventuelt foretages en selvstændig undersøgelse af de omkring 40.000 danske Facebook-brugere, som ligeledes er omfattet af sagen.¹³

På baggrund af denne sag forekommer det indlysende, at det er nødvendigt at have en veludviklet digital infrastruktur, der er i stand til at tage hånd om de skyggesider, der følger med den digitale informationstid, vi lever i. Dette problem relaterer sig dog ikke kun til Facebook. Der opstår således stadig nye digitale platforme og teknologi, hvor forbrugerne, i interaktionen med disse, enten velvidende eller ubevidst afgiver persondata, der kan angive en række vidtrækkende forhold omkring deres personlighed, identitet, privatliv etc. Forbrugerne er muligvis bevidste om, at de betaler for bestemte ydelser med deres informationer, men det kan være vanskeligt for den enkelte at udlede præcist, hvilke data der indsamles, hvordan denne information anvendes, og hvilken betydning informationen kan have for vedkommende i fremtiden.

⁷ Wylie, 2018: *Cambridge Analytica whistleblower: 'We spent \$1m harvesting millions of Facebook profiles'*

⁸ Cadwalladr & Graham-Harrison, 2018: *How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool*

⁹ Cadwalladr & Graham-Harrison, 2018: *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*

¹⁰ Watson, 2018: *The key moments from Mark Zuckerberg's testimony to Congress*

¹¹ Hern & Sabbagh, 2018: *Zuckerberg's refusal to testify before UK MPs 'absolutely astonishing'*

¹² Information Commissioner's Office, 2018: *ICO statement: investigation into data analytics for political purposes*

¹³ Datatilsynet, 2018: *Fælles europæisk reaktion på sagen om Cambridge Analytica og Facebook*

Persondataforordningen¹⁴ er et forsøg på at skabe et retligt fundament, der adresserer en række af de nutidige problemstillinger, som vi står over for. Forordningen er lovfæstet til at blive bragt i anvendelse fra den 25. maj 2018¹⁵, og det er derfor interessant at undersøge, om denne retskilde udgør en tilstrækkelig ramme for den persondataretlige regulering i årene fremover. Formanden for Artikel 29-Gruppen¹⁶, Andrea Jelinek har udtalt følgende om den aktuelle sag, hvilket tjener som en passende overgang til omdrejningspunktet for dette speciale. ”*We reiterate our earlier commitment to assist and fully cooperate with the UK’s Information Commissioner’s Office (ICO) in its investigation of Cambridge Analytica and Facebook... We are at the start of a new era of data protection. The protection of individuals against unlawful use of their personal data on social media platforms will be one of our key priorities.*”¹⁷

2. Problemformulering

Det vil være formålet med dette speciale at besvare følgende overliggende problem, der vil være fokuspunktet for hele fremstillingen:

Har henholdsvis Facebook og Cambridge Analytica handlet i strid med persondataforordningens bestemmelser, og kan de eventuelt sanktioneres som følge af denne sag?

Problemformuleringen vil nedbrydes til følgende specifikt afgrænsede problemstillinger, der vil besvares løbende i projektet. Indledningsvist vil det blive undersøgt, om sagen falder inden for persondataforordningens anvendelsesområde. Derefter vil spørgsmålet om legaliteten af indsamlingen og behandlingen af Facebook-brugernes informationer behandles nærmere. Det vil endvidere blive vurderet, om Facebook har handlet i overensstemmelse med de grundlæggende forpligtelser, der påhviler den dataansvarlige. Afslutningsvist vil det være intentionen at udlede hvilke sanktionsmuligheder, der kan tages i brug som følge af denne sag.

¹⁴ Parlamentets og Rådets forordning 2016/679 (herefter omtalt som persondataforordningen, Forordningen eller GDPR)

¹⁵ GDPR art. 99, stk. 2.

¹⁶ ”The ”Article 29 Working Party” is the short name of the Data Protection Working Party established by Article 29 of Directive 95/46/EC. It provides the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States.” se EDPS, 2018: Glossary

¹⁷ Art. 29-gruppen, 2018: Press Release: ”Sorry is not enough”: WP29 establishes a Social Media Working Group

3. Afgrænsning

Dette speciale er afgrænset til at behandle de persondataretlige problemstillinger, der er væsentlige for Cambridge Analytica-sagen specifikt. Dog vil begrænsningen af fremstillingens omfang betyde, at det ikke er muligt at inddrage samtlige forhold, som ellers er relevante for den afgrænsede hovedproblemstilling. Dette omfatter eksempelvis, hvilke rettigheder de berørte Facebook-brugere besidder som følge af den persondataretlige regulering. Forholdet omkring de registreredes rettigheder vil således kun indgå i fremstillingen, såfremt det er nødvendigt for at vurdere legaliteten af de aktiviteter, der har fundet sted.

Sagens faktuelle omstændigheder kan også berettige en undersøgelse af, hvilke betingelser der gælder for at transportere personoplysninger videre til tredjelande som USA. Denne problemstilling vil dog ikke blive behandlet nærmere i denne fremstilling. Derudover har Cambridge Analytica forsøgt at danne indsigt i vælgeradfærd og derfor må børns særlige persondataretlige status formodes at være irrelevant i belysningen af fremstillingens afgrænsede problem. Derfor bliver disse bestemmelser ikke inddraget i specialet.

En anden nødvendig afgrænsning, angår spørgsmålet om jurisdiktion. Problemet opstår, da både Facebook og Cambridge Analytica ikke kun er aktive i Europa. De faktuelle omstændigheder, der omgiver sagen, trækker således tråde fra lande som fx USA, Indien, Nigeria og flere medlemsstater i EU.¹⁸ Med internettets fremkomst kan der argumenteres for, at fysiske landegrænser har en mindre betydning, da personoplysninger kan svæve rundt på platforme, der er tilgængelige i alle verdenshjørner.¹⁹ Denne fremstilling tager imidlertid udgangspunkt i Forordningen, og denne har, som udgangspunkt, udelukkende retsvirkning i det indre marked. Kerneproblemstillingen vil af denne årsag hovedsageligt betragtes fra et EU-retligt perspektiv. Medlemsstaternes nationale lovgivning vil derfor udelukkende inddrages i det omfang, hvor det er nødvendigt for behandlingen af sagens afledte problemstillinger. Sanktionskapitlet vil desuden kun undersøge de relevante myndigheders mulighed for at sanktionere virksomhederne. Forordningens særlige regler om erstatning vil derfor ikke blive inkluderet, selvom de omfattede Facebook-brugere muligvis har ret til erstatning efter disse bestemmelser.

¹⁸ Taylor, 2018: *Cambridge Analytica's reach went far beyond the U.S. elections* og Cadwalladr, 2018: *Revealed: graphic video used by Cambridge Analytica to influence Nigerian election*

¹⁹ se Tranberg, et al., 2017 s. 98.

4. Metode og retskilder

I forsøget på at besvare afhandlingens problemformulering vil den retsdogmatiske metode blive anvendt. Det vil derfor være målsætningen at udarbejde en fremstilling af gældende ret i forhold til de persondataretlige problemstillinger i sagen om Cambridge Analytica. Dette omfatter en analyse af de relevante retskilder, som vil udgøre det empiriske fundament for denne juridiske undersøgelse.²⁰

Dernæst vil det være hensigtsmæssigt at udlede, hvilke retskilder der kan anvendes til at belyse gældende ret om dette konkrete emne. I flere værker i den juridiske litteratur omtales den såkaldte nordiske retskildeteori.²¹ Det anføres i henhold til denne anskuelse, at de danske retskilder består af fire hovedgrupper; *loven, retspraksis, sædvanen og forholdets natur*. Det vil blive lagt til grund, at disse retskildegrupper anses for ligestillede, hvormed der således ikke eksisterer et egentligt hierarki mellem retskildehovedgrupperne.²² Det vil derfor forudsætte en konkret vurdering for at udlede, hvilken retskilde der skal tillægges afgørende betydning.²³ Dog må det formodes, at det primære grundlag for at fastlægge gældende ret, i dette tilfælde, vil bestå af en analyse af de relevante retsregler og dertilhørende praksis.

I relation til den første hovedgruppe, der betegnes som loven, vil kilder indgå fra forskellige dele af det juridiske kompleks. Dette speciale er centreret om persondataretlige problemstillinger, hvor EU-retten må formodes at have en stor betydning. Det kan kortfattet konstateres, at EU-retten er en del af medlemsstaternes nationale ret.²⁴ EU's Charter om Grundlæggende Rettigheder²⁵ indeholder i art. 8 en række fundamentale rettigheder i relation til fysiske personers personoplysninger. Oplysninger skal således behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet lovfæstet grundlag. Afsluttende anføres det, at enhver har adgang til indsamlede oplysninger, der vedrører personen selv og til en berigtigelse af disse informationer. Rettskildeværdien af Charteret er indskrevet i TEUF²⁶, hvori det er anført, at den har samme juridiske rettskildeværdi som EU's Traktater.²⁷ Den grundlæggende ret til at få beskyttet personoplysninger er ligeledes udtrykt i traktatgrundlaget for den

²⁰ se Evald, 2016: Juridisk Teori, Metode og Videnskab s. 201.

²¹ se Munk-Hansen, 2014: Retsvidenskabsteori s. 192 og Evald, 2000: Retsskilderne og den juridiske metode s. 7.

²² se Blume, 2016: Retssystemet og Juridisk Metode s. 194

²³ se Munk-Hansen, 2017: Den Juridiske Løsning s. 17.

²⁴ se Munk-Hansen, Retsvidenskabsteori, 2014 s. 259.

²⁵ EU's Charter om Grundlæggende Rettigheder - 2000/C 364/01 (herefter omtalt som 'Chartret')

²⁶ Traktaten om Den Europæiske Unions Funktionsmåde, C-326 af 26/10/2012.

²⁷ Jf. TEUF art. 6, stk. 1 og se Sørensen, Nielsen, & Danielsen, 2014 s. 128.

Europæiske Union, hvor TEUF art. 16 stipulerer denne grundlæggende ret. Der er således to primære EU-retlige retskilder, der danner hovedrammerne for den persondataretlige regulering i EU.²⁸

Den sekundære EU-ret har dog specificeret essensen af den konkrete persondataretlige regulering siden 1995, hvor databeskyttelsesdirektivet blev vedtaget.²⁹ Dette direktiv blev implementeret i dansk ret med persondataloven³⁰, der dog forventes at overgå til retshistorie, når henholdsvis persondataforordningen og databeskyttelsesloven³¹ træder i kraft fra d. 25. maj 2018.³² Databeskyttelsesloven er dog ikke endeligt vedtaget i Folketinget på tidspunktet for udfærdigelsen af dette speciale.³³ Da både primære og sekundære EU-retskilder har en afgørende betydning i forhold til denne sag, vil det være relevant at undersøge det juridiske forhold mellem EU-retskilderne. EU-domstolen har fastlagt, at den anser traktatgrundlaget som Unionens forfatningsgrundlag, og derfor kan der ikke udstedes sekundære retskilder, der ikke har hjemmel i Traktaterne. Dog er der ingen regel, der stipulerer en bestemt rangering mellem de sekundære EU-retskilder, der er angivet i TEUF art. 288. Denne vurdering vil således forudsætte en konkret vurdering af de relevante retsregler.³⁴

I relation til forholdet mellem EU-lovgivningen og medlemsstaternes interne lovgrundlag, kan det anføres, at denne problemstilling er forholdsvist velafklaret i både retspraksis og den juridiske litteratur. Forrangsprincippet blev i første omgang statueret af EU-domstolen i 60'erne³⁵, hvilket har den retlige konsekvens, at EU-retskilder har forrang over national ret. Dette fortolkningsprincip anerkendes ligeledes af de danske domstole med det forbehold, at Højesteret ikke accepterer den vide fortolkning af forrangsprincippet, der bevirker, at EU-retten ligeledes har forrang i forhold til Grundloven.³⁶

²⁸ se Blume, 2016: Den nye persondataret s. 15.

²⁹ Parlamentets og Rådets direktiv 95/46/EF

³⁰ Lov 2000-05-31 nr. 429 om behandling af personoplysninger (Herefter omtalt som 'PDL') og Lotterup, 2016, Karnovs indledende note til persondataforordningen.

³¹ *L 68 Forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger* (Databeskyttelsesloven)

³² se Holst-Christensen, 2013: *EU-lovteknik* s. 489.

³³ Folketinget, 2018: *Sagsang for behandling af L 68*.

³⁴ se Sørensen, Nielsen, & Danielsen, 2014 s. 113-114.

³⁵ Jf. *Costa v. ENEL*, C-6/64 og se Sørensen, Nielsen, & Danielsen, 2014 s. 174-175.

³⁶ Jf. U1998.800H, præmis 9.2: "*Det kan ikke i medfør af § 20 overlades til en international organisation at udstede retsakter eller træffe afgørelser, som strider mod bestemmelser i grundloven, herunder dennes frihedsrettigheder.*"

Forordninger er karakteriseret ved at være almengyldige og bindende i alle enkeltheder og gældende umiddelbart i hver medlemsstat.³⁷ Forordninger har derfor virkning som en almindelig lov i de enkelte medlemsstater, da de anvendes direkte. I de situationer hvor indholdet i forordningen tillægger medlemsstaterne kompetence til at foretage nationale supplerende bestemmelser, vil forordningen i en vis grad svare til et direktiv.³⁸ Dette er i særdeleshed tilfældet med persondataforordningen, der giver medlemsstaterne adskillige muligheder for at implementere supplerende national lovgivning.³⁹ Det må endvidere konstateres, at persondataforordningens pligtsubjekt er den dataansvarlige.⁴⁰ Den dataansvarlige kan både være en fysisk eller juridisk person, herunder myndigheder.⁴¹ Derfor må det formodes, at Forordningens bestemmelser kan anvendes både vertikalt og horisontalt til at forpligte private og offentlige retssubjekter.⁴²

Det er essentielt at fremhæve, at der kan være reel diskussion i forhold til, om Cambridge Analytica-sagen skal behandles efter det gamle paradigme eller det nye. Dog vil denne fremstilling arbejde ud fra forudsætningen om, at samtlige forhold i sagen skal behandles efter persondataforordningens bestemmelser. Hovedformålet med undersøgelsen er således ikke at forudsige, hvordan sagen præcist vil blive afgjort ved tilsynsmyndighederne eller domstolene. Formålet vil derimod være at udlede, om persondataforordningen sikrer et tilstrækkeligt grundlag for den persondataretlige regulering i årene fremover. Denne vurdering foretages ved at sammenholde det nye retsgrundlag med den aktuelle sag.

Den væsentligste ændring af retstilstanden med den nye Forordning er dog, at der kommer nogle væsentlige strengere håndhævelsesbestemmelser.⁴³ Forordningen viderefører dermed de væsentligste principper fra databeskyttelsesdirektivet. Dette argument understøttes af Justitsministeriets generelle konklusion af indholdet i den nye Forordning: *"Analysearbejdet har vist, at forordningen i vidt omfang svarer til den gældende retstilstand efter persondataloven og databeskyttelsesdirektivet med tilhørende praksis fra bl.a. EU-domstolen og Datatilsynet. Bl.a. svarer forordningens*

³⁷ Jf. TEUF art. 288. Se endvidere s. 487 ff. i Holst-Christensen, 2013: *EU-lovteknik*.

³⁸ se Holst-Christensen, 2013: *EU-lovteknik* s. 487.

³⁹ se Blume, *Den nye persondataret*, 2016 s. 18 *"Det er bemærkelsesværdigt, at der ikke har været større diskussion af brugen af en forordning, men det kan skyldes, at der i forordningen er åbnet mange, vist over 50, muligheder for at fastsætte nationale regler. På denne måde kan forordningen minde om et direktiv."*

⁴⁰ se Blume, 2016: *Den nye persondataret* s. 61.

⁴¹ Jf. GDPR art. 4, nr. 7.

⁴² se Sørensen, Nielsen, & Danielsen, 2014 s. 158.

⁴³ se s. 941 i Justitsministeriets Betænkning nr. 1565 del 1, bind 2. Der gives en redegørelse af strafniveauet under det gamle paradigme. Den mest byrdefulde straf der er pålagt for brud på persondatalovens regler, er således 25.000 kr. Det oplyses endvidere, at private virksomheder normalt blev straffet med 10.000 kr. for at foretage ulovlig behandling af personfølsomme oplysninger.

centrale bestemmelser om anvendelsesområde, definitioner, principper for behandling af personoplysninger, behandlingsregler, de registreredes rettigheder og behandlingssikkerhed i stort omfang til gældende ret efter persondataloven og databeskyttelsesdirektivet.”⁴⁴

Det betyder, at det, som udgangspunkt, kan forudsættes, at den nationale og EU-retlige praksis, i vidt omfang, fortsat er gældende, selvom det knytter sig til det gamle lovgrundlag. Det er dog nødvendigt at foretage en konkret vurdering for at udlede, om den tidligere praksis fortsat er gældende.⁴⁵ Det kan endvidere anføres, at Datatilsynets praksis generelt tillægges en stor betydning inden for det persondataretlige retsområde.⁴⁶ Den store præjudikatsværdi af Datatilsynets praksis er bl.a. begrundet i, at tilsynets afgørelser sjældent ankes til domstolene. De nationale datatilsyn er endvidere gensidigt forpligtet til at sikre en ensartet fortolkning af persondataforordningen.⁴⁷ Dette bevirker, at afgørelsen af den britiske undersøgelse kan vise sig at have betydning for det danske datatilsyn, såfremt der bliver rejst en dansk sag på et senere tidspunkt.

Derudover vil en række ikke-juridiske kilder indgå i specialet. Det er nødvendigt, da afhandlingens problemformulering er centreret omkring en aktuel sag. Mediekilder som fx artikler og interviews vil derfor anvendes til at danne klarhed over de faktuelle omstændigheder i sagen. Dette udgør naturligvis et usikkerhedsmoment. Dog er det relevant at fremhæve, at The Guardians rapportering bygger på vidneudsagn af tidligere ansatte hos Cambridge Analytica, der endvidere er understøttet af andet bevismæssigt materiale i form af kontrakter, korrespondance mv.⁴⁸ Dette giver naturligvis disse mediers udlægning af hændelsesforløbet en udvidet grad af troværdighed. Det må alligevel understreges, at det er vanskeligt at vurdere, hvordan en domstol, eventuelt, vil vurdere validiteten af bevismaterialet. Afslutningsvist vil Facebooks brugervilkår inddrages i undersøgelsen, da de påviser Facebooks oprindelige behandlingsgrundlag. Dette kan eksempelvis have betydning for vurderingen af, om der forelå et fornødent samtykkegrundlag til at videregive de mange Facebook-brugeres informationer til andre interessenter. På tilsvarende vis vil brugervilkårene fra Kogans applikation ligeledes inddrages i fremstillingen, da disse vilkår udgør behandlingsgrundlaget for Cambridge Analyticas aktiviteter.

⁴⁴ se Justitsministeriet, 2017: *Betæknings nr. 1565 om Databeskyttelsesforordningen - og de retlige rammer for dansk lovgivning* s. 15.

⁴⁵ se Blume, 2016: *Den nye persondataret* s. 22.

⁴⁶ se Tranberg, et al., 2017 s. 100.

⁴⁷ Jf. GDPR art. 51, stk. 2.

⁴⁸ Wylie, 2018: *Why I broke the Facebook data story - and what should happen now*

5. Redegørelse af sagen om Cambridge Analytica

Dette afsnit har til formål at give læseren en baggrundsforståelse for det faktiske hændelsesforløb i sagen om Cambridge Analytica. Disse faktiske informationer vil blive anvendt løbende i fremstillingen, mens det undersøges, om virksomhederne har handlet i strid med den persondataretlige regulering. Informationerne i dette afsnit er baseret på The Washington Posts redegørelse af sagen.⁴⁹

Sagen begynder i sommeren 2014 hvor en forsker ved Cambridge University, Aleksandr Kogan, bliver hyret af Cambridge Analytica⁵⁰ til at indsamle informationer på Facebook-brugere. Kogan designer efterfølgende en Facebook app, *This Is Your Digital Life*, hvor ca. 300.000 Facebook-brugere bliver kompenseret med en økonomisk gevinst for at tage appens personlighedstest. I servicevilkårene til appen var det anført, at brugerne gav samtykke til, at den ville indsamle data på de konkrete respondenter og deres Facebook-venner. Ved hjælp af denne metode var Kogan således i stand til at indsamle data på 87 mio. Facebook-brugere, selvom kun 300.000 havde accepteret brugervilkårene.

Fra dette punkt i sagsforløbet har Kogan, Cambridge Analytica og Facebook forskellige opfattelser af, hvad der skete efterfølgende. Kogan anfører, at *“We clearly stated that the users were granting us the right to use the data in broad scope, including selling and licensing the data.”* Facebook mener dog, at Kogan vildledte dem, da de angiveligt antog, at Kogan ville anvende datasættene til forskningsformål. Dog kan det fastlægges med sikkerhed, at Facebook i 2015 beordrer datamaterialet destrueret af alle parter, som har været i besiddelse af dette. Facebook anmoder de omhandlende interessenter om at underskrive en erklæring, hvor de kvitterer for at have slettet materialet. Facebook foretager imidlertid ikke nogen egentlig undersøgelse af, om dette faktisk effektueres. Der er dog stærke indicier for, at datamaterialet ikke blev slettet af alle de relevante parter og at det derfor stadigvæk eksisterer helt eller delvist.

Dette bliver det foreløbige punktum i sagen, indtil marts 2018 hvor Christopher Wylie afslører, at informationerne er blevet udnyttet til kommercielle samt politiske formål.

⁴⁹ Riley, Frier, & Baker, 2018: *Understanding the Facebook-Cambridge Analytica Story: QuickTake*

⁵⁰ Indledningsvist bliver Kogan hyret af SCL Elections, der dog er et beslægtet selskab til Cambridge Analytica. Sidstnævnte blev dog først etableret efter, at Facebook-informationerne blev høstet.

Kapitel II. Persondataforordningens anvendelsesområde

I dette afsnit vil Forordningen kortfattet blive introduceret. Dernæst vil Forordningens beskyttelsesobjekt og pligtsubjekt blive udledt for at skitsere, hvordan Cambridge Analytica-sagen er relevant i en persondataretlig kontekst. Derudover vil det blive undersøgt, om sagens faktum opfylder de materielle samt formelle betingelser for at være underlagt Forordningens jurisdiktion.

Som en pendant til artikel 8 i EU's Charter om Grundlæggende Rettigheder er beskyttelse af personoplysninger ligeledes implementeret i traktatgrundlaget for Den Europæiske Union. Det er således anført i TEUF art. 16, at enhver har ret til beskyttelse af personoplysninger om vedkommende selv. Det er endvidere bestemt, at Parlamentet og Rådet skal fastsætte regler, der har til hensigt at beskytte fysiske personers personoplysninger. Det snarligt forældede databeskyttelsesdirektiv og den nye Forordning skal således anses som et udtryk for at efterleve denne hensigt, som er erklæret i traktatbestemmelsen. Det må lægges til grund, at Forordningen forstærker den generelle grad af harmonisering i det indre marked i forhold til det gamle retsgrundlag, selvom medlemsstaterne fortsat tillægges muligheder for at fastsætte nationale regler.⁵¹

1. Beskyttelsesobjektet – Personoplysninger

Forordningen opererer med 26 legaldefinitioner, der udgør en stor del af persondatarettens grundlæggende terminologi.⁵² Det mest centrale begreb er persondatarettens beskyttelsesobjekt - *personoplysninger*. Det er således angivet, at begrebet skal forstås som enhver form for information, der henviser til en identificeret eller identificerbar fysisk person.⁵³ Den identificerede person betegnes som 'den registrerede' med persondataretlig terminologi. Ved *identificeret* eller *identificerbar person* menes der en fysisk person, som kan identificeres direkte eller indirekte som følge af en identifikator som fx navn, identifikationsnummer, lokaliseringsdata eller en online identifikator. Derudover kan øvrige elementer, som er kendetegnende for personens fysiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet ligeledes udgøre en personhenførbare oplysning.⁵⁴

Da personoplysninger omfatter enhver information, der kan knyttes til en identificerbar person, må begrebet skulle fortolkes ekstensivt.⁵⁵ Derudover kan

⁵¹ Se Blume, 2016: Den nye persondataret s. 19-20.

⁵² se Tranberg, et al., 2017 s. 112 og GDPR art 4.

⁵³ Jf. GDPR art. 4, nr. 1.

⁵⁴ Jf. GDPR art. 4, nr. 1. og se endvidere Tranberg, et al., 2017 s. 112.

⁵⁵ se Blume, 2016: Den nye persondataret s. 59.

personoplysningsbegrebet generelt opdeles i almindelige og personfølsomme oplysninger.⁵⁶ Persondataforordningen afgrænser almindelige oplysninger negativt ved at foretage en positiv opregning af alle personfølsomme oplysninger. ”*Behandling af personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering er forbudt.*”⁵⁷ Den fundamentale forskel i vurderingen af disse to typer af personoplysninger består i, at behandlingskravet skærpes, når der er tale om personfølsomme oplysninger.⁵⁸ Disse konkrete behandlingskrav vil blive undersøgt nærmere senere i fremstillingen.

Sagen om Cambridge Analytica er bemærkelsesværdig i en persondataretlig kontekst, da 87 mio. Facebook-brugeres personoplysninger angiveligt er blevet behandlet.⁵⁹ For at påvise Forordningens anvendelighed i den konkrete sag, må det først undersøges, om de konkrete oplysninger kan betragtes som *personoplysninger* i Forordningens forstand. I denne vurdering er det indledningsvist nødvendigt at aflede, hvilke konkrete oplysninger som Cambridge Analytica har behandlet.⁶⁰ Dernæst skal det også vurderes, om disse oplysninger kan henføres til en identificerbar person, før de to led i begrebet er opfyldt. ”*The algorithm at the heart of the Facebook data breach sounds almost too dystopian to be real. It trawls through the most apparently trivial, throwaway postings -the ‘likes’ users dole out as they browse the site – to gather sensitive personal information about sexual orientation, race, gender, even intelligence and childhood trauma. A few dozen ‘likes’ can give a strong prediction of which party a user will vote for...*”⁶¹ Baseret på dette citat kan det konstateres, at Cambridge Analytica specifikt har forsøgt at behandle personfølsomme oplysninger. Derudover må det forudsætte en konkret vurdering at udlede, om et konkret Facebook ’like’ kan udgøre en personfølsom oplysning. Hvis en Facebook-bruger eksempelvis ’liker’ et politisk opslag, må denne information kunne anvendes til at sige noget om den registreredes politiske overbevisning. Dog må de ’likes’, som ikke er følsomme oplysninger, behandles som almindelige

⁵⁶ Persondataforordningen opererer med betegnelsen ’særlige kategorier af oplysninger’, jf. art. 9.

⁵⁷ Jf. GDPR art. 9, stk. 1

⁵⁸ se Blume, 2016: Den nye persondataret s. 82.

⁵⁹ Schroepfer, 2018: *An Update on Our Plans to Restrict Data Access on Facebook*

⁶⁰ BBC har udarbejdet en god redegørelse af, hvordan Facebook-oplysningerne blev udnyttet af Cambridge Analytica. Se ’BBC, 2018: *Facebook data: How it was used by Cambridge Analytica*’

⁶¹ Cadwalladr & Graham-Harrison, 2018: *How Cambridge Analytica turned Facebook ‘likes’ into a lucrative political tool*

personoplysninger.⁶² Business Insider har endvidere foretaget en undersøgelse af hvilke oplysninger, som Facebook-værktøjet 'API', hypotetisk set, kunne høste fra Facebook-plattformen i 2014.⁶³ Dette værktøj er det selvsamme, som blev anvendt af Kogan til at høste Facebook-brugernes oplysninger i denne sag. Baseret på undersøgelsen kan det kortfattet anføres, at værktøjet var i stand til at høste enhver oplysning, der knytter sig til en Facebook-profil. Dette var endvidere tilfældet uagtet af den enkelte brugers privatindstillinger. Der må således foreligge en stærk formodning om, at Cambridge Analytica har været i besiddelse af Facebook-data, der indeholder personoplysninger, der både kan karakteriseres som almindelige og følsomme.

Det er dernæst også nødvendigt at undersøge, om Facebook-oplysningerne ligeledes kan henføres til en identificerbar person. Der er grundlæggende flere forhold, der bevirker, at en person nemt kan identificeres direkte eller indirekte på et medie som Facebook. En Facebook-bruger kan, hypotetisk set, identificeres ved navn, adresse, telefonnummer, billeder etc. Det må derfor konkluderes, at denne betingelse ligeledes er opfyldt. Dette argument er ligeledes underbygget af, at Channel 4 News har været i stand til at identificere bestemte Facebook-brugere på baggrund af en delmængde af det høstede datamateriale.⁶⁴

Det vil dermed blive lagt til grund for den videre undersøgelse, at det lækkede datamateriale opfylder betingelserne for at blive anset som *personoplysninger* i Forordningens forstand.⁶⁵ Det kan endvidere konstateres, at Cambridge Analytica skal dokumentere, at der foreligger et lovligt behandlingsgrundlag efter art. 6 og 9, da datamaterialet både omfatter almindelige og personfølsomme oplysninger. Dette vil blive undersøgt nærmere i kapitel III.

2. Pligtssubjektet – Den dataansvarlige

Det kan generelt anføres, at persondatarettens pligtssubjekt er den dataansvarlige.⁶⁶ Dette betyder, at den dataansvarlige er det subjekt, som de fleste regler i Forordningen knytter sig til. Dette afsnit har derfor til formål at udlede, hvem der bærer ansvaret som dataansvarlig i den omhandlede sag. Begrebet defineres som

⁶² Jf. GDPR art. 6.

⁶³ Hartmans, 2018: *It's impossible to know exactly what data Cambridge Analytica scraped from Facebook — but here's the kind of information apps could access in 2014*

⁶⁴ Channel 4 News, 2018 *Revealed: Cambridge Analytica data on thousands of Facebook users still not deleted*

⁶⁵ Jf. GDPR art. 4, nr. 1.

⁶⁶ se Blume, 2016: Den nye persondataret s. 60-61.

*”en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger”.*⁶⁷ Der er grundlæggende tre subjekter, som kan have erhvervet status som dataansvarlig i Cambridge Analytica-sagen. Dette inkluderer Facebook, Cambridge Analytica og Aleksandr Kogan.

Det kan forholdsvist sikkert konkluderes, at Facebook-oplysningerne er blevet behandlet af dem alle tre i løbet af sagsforløbet.⁶⁸ Derved kan det udledes, at de enten kan have status som dataansvarlig eller databehandler. En databehandler er defineret som en fysisk eller juridisk person, der udfører databehandlingen på vegne af den dataansvarlige.⁶⁹ Der kan ikke antages at være en af de omfattede subjekter, som kan have udført databehandlingen på vegne af den dataansvarlige. Derfor må det modsætningsvist lægges til grund, at alle tre parter er dataansvarlige. Det må dog afvises, at de har erhvervet et fælles ansvar som dataansvarlige, som det er beskrevet i Forordningen.⁷⁰ Det beskrives således, at de dataansvarlige skal have udformet formålene med databehandlingen i fællesskab. Dog er der ikke grundlag for at anføre, at Facebook har været med til at udforme formålene bag den databehandling, som Cambridge Analytica har udført. Dog kan dette fælles ansvar godt foreligge mellem Kogan og Cambridge Analytica, da de udformede en skriftlig kontrakt, hvor formålet med indsamlingen af Facebook-data blev anført.⁷¹ Dog må vurderingen af, om der foreligger et fælles eller separat ansvar, formodes at have en mindre betydning, da parterne alligevel er underlagt de samme pligter og juridiske ansvar. Det vil dermed forudsætningsvist blive lagt til grund, at Facebook, Cambridge Analytica og Kogan er pligtsubjekterne i denne sag.

Kortfattet kan det anføres, at den dataansvarliges generelle ansvar omfatter at være i stand til at påvise, at den konkrete behandling er i overensstemmelse med Forordningen.⁷² Derudover pålægges den dataansvarlige også et generelt princip om ansvarlighed.⁷³ Den dataansvarliges konkrete forpligtelser vil blive behandlet mere indgående i kapitel III og IV.

⁶⁷ Jf. GDPR art. 4, nr. 7.

⁶⁸ Cadwalladr, 2018 ‘I made Steve Bannon’s psychological warfare tool’: meet the data war whistleblower

⁶⁹ Jf. GDPR art. 4, nr. 8.

⁷⁰ Jf. GDPR art. 26, stk. 1.

⁷¹ Appendix II, 2014: Aftale mellem GSR (Kogan) og SCL Elections (Cambridge Analytica) afsnit 1 og 6.

⁷² Jf. GDPR art. 24, stk. 1.

⁷³ Jf. GDPR art. 5, stk. 2. Se endvidere Tranberg, et al., 2017 s. 106.

3. Materiel afgrænsning

Den materielle vurdering angår spørgsmålet om, hvilke former for aktiviteter, der er reguleret i Forordningen. ”Denne forordning finder anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling”.⁷⁴ Begrebet *automatisk* må formodes at være synonym med digital databehandling i denne sammenhæng.⁷⁵

Det er allerede udledt tidligere i specialet, at der er tale om personoplysninger i Forordningens forstand. Dette afsnit vil derfor forsøge at udlede, hvorvidt Cambridge Analytics aktiviteter ligeledes opfylder det sidste led i den materielle vurdering. Dette led angår selve behandlingsbegrebet. Ved udtrykket ’*behandling*’ er enhver form for databehandling af personoplysninger omfattet af Forordningens bestemmelser.⁷⁶ Der stilles dermed ikke store minimumskrav til hvilke former for behandling, der er omfattet af Forordningen.

Den specifikke form for databehandling som Cambridge Analytica har benyttet, er positivt angivet under betegnelsen *profilering*.⁷⁷ Profilering er beskrevet som behandling af personoplysninger, der har til formål at evaluere bestemte personlige forhold med henblik på at analysere eller forudsige elementer vedrørende den fysiske persons arbejdsindsats, økonomiske situation, helbred, personlige præferencer, interesser, pålidelighed, adfærd, geografiske position eller bevægelser.⁷⁸ Det kan generelt anføres, at profilering er blevet aktuelt med ankomsten af fænomenet *Big Data*. Med udviklingen i teknologi er det således blevet muligt at indsamle og behandle meget store datamængder. Disse datamængder kan herefter mikroanalyseres ved brug af datamining⁷⁹, hvorved der kan påvises komplicerede sammenhænge om bestemte personers adfærdsmønstre i forskellige situationer.⁸⁰ Denne viden kan efterfølgende udnyttes til at forudse fysiske personers fremtidige adfærd, da de bliver profilet på baggrund af de modeller, der udledes ved hjælp af datamining-processen.

Det må konkluderes, at Cambridge Analytics behandlingsmetoder er omfattet af persondatarettens vide behandlingsbegreb, og derfor er Forordningen anvendelig,

⁷⁴ Jf. GDPR art. 2, stk. 1.

⁷⁵ se Blume, 2016: *Den nye persondataret* s. 49.

⁷⁶ se Tranberg, et al., 2017 s. 103.

⁷⁷ Wade, 2018: *Psychographics: the behavioural analysis that helped Cambridge Analytica know voters' minds*

⁷⁸ Jf. GDPR art 4, nr. 4.

⁷⁹ ”Data mining is the process of analysing inter-data relationships – connecting the dots and finding hidden meanings and relationships that can provide startling new insights.” - Khan, 2014: *Explainer: what is big data?*

⁸⁰ se Blume, 2016: *Den nye persondataret* s. 59-60.

såfremt de formelle betingelser ligeledes er opfyldt. Det må derimod afvises, at det specielle forbud om at gøre personer genstand for automatisk profilering finder anvendelse i denne sag.⁸¹ Forbuddet har virkning, såfremt den registrerede gøres til genstand for en afgørelse ”som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende.” Hvilke former for afgørelser der er omfattet af bestemmelsen uddybes i betragtning 71: ’... såsom et automatisk afslag på en onlineansøgning om kredit eller e-rekrutteringsprocedurer uden nogen menneskelig indgriben.” Selvom det muligvis kan argumenteres, at Trump og Brexit kan have en betydelig påvirkning for den pågældende, må det alligevel konkluderes, at den afledte effekt er for indirekte i forhold til de eksempler, der anføres i betragtningen.

4. Formel afgrænsning

Dette afsnit behandler Forordningens territoriale rækkevidde. Denne afgrænsning er nødvendig for at påvise Forordningens anvendelighed i forhold Facebook og Cambridge Analytica respektivt. Udgangspunktet for denne vurdering anføres i art. 3, hvor det er beskrevet, at *’forordningen finder anvendelse på behandling af personoplysninger, der foretages i led med aktiviteter, der udføres af en dataansvarlig eller databehandler, som er etableret i Unionen, uanset om behandlingen finder sted i Unionen eller ej.*⁸² Der er adskillige forhold i formuleringen, som allerede er blevet udledt i undersøgelsen. Det er tidligere konstateret, at både Facebook og Cambridge Analytica er dataansvarlige i denne sag. Derudover er det også påvist, at de konkrete aktiviteter ligeledes er omfattet af Forordningens materielle rækkevidde.

Den territoriale afgrænsning af Forordningen er det forhold, som kan give anledning til vanskeligheder i den praktiske verden. En personoplysning kan være offentliggjort af en dansk person på Facebook og efterfølgende være genstand for databehandling i USA. Udgangspunktet for denne vurdering er, at den dataansvarlige skal være etableret i Unionen for at være underlagt Forordningens bestemmelser. Etableringsbegrebet specificeres i betragtning 22, hvor det anføres, at *’etablering indebærer effektiv og faktisk udøvelse af aktivitet gennem en mere permanent struktur*’.⁸³ Derudover er etableringsbegrebet også nærmere beskrevet i EU-domstolens praksis, hvorved *enhver, selv minimal, reel og faktisk aktivitet, der udøves via en permanent struktur* anses for at opfylde det persondataretlige etableringsbegreb.⁸⁴ Domstolen har endvidere udtalt, at det var muligt at retsforfølge

⁸¹ Jf. GDPR art. 22, stk. 1.

⁸² GPDR art. 3, stk. 1.

⁸³ Jf. GDPR betragtning 22.

⁸⁴ Jf. C-230/14, Weltimmo, præmis 30.

Google for at handle i strid med de persondataretlige bestemmelser gennem et europæisk datterselskab, som virksomheden havde etableret i forsøget på at sælge reklameannoncer i en medlemsstat.⁸⁵ ”En registeransvarlig, som er etableret på flere medlemsstats områder, især i form af datterselskaber, skal, navnlig for at undgå omgåelse, sikre sig, at hver enkelt struktur opfylder kravene i den gældende nationale lovgivning.” Selskabet, som var aktivt i EU, havde således en forpligtelse til at handle i overensstemmelse med den nationale og EU-retlige lovgivning, herunder de persondataretlige bestemmelser.

Forordningen indeholder endvidere en skærpelse af retstilstanden i forhold til det snarligt forældede retsgrundlag:⁸⁶ ”Denne forordning finder anvendelse på behandling af personoplysninger om registrerede, der er i Unionen, og som foretages af en dataansvarlig eller databehandler, der ikke er etableret i Unionen, hvis behandlingsaktiviteterne vedrører:

- a) udbud af varer eller tjenester til sådanne registrerede i Unionen, uanset om betaling fra den registrerede er påkrævet eller
- b) overvågning af sådanne registreredes adfærd, for så vidt deres adfærd finder sted i Unionen.”⁸⁷

Det må således udledes af stk. 2, at virksomheder kan være omfattede af persondataforordningen, selvom selskabet muligvis ikke opfylder tilknytningskravet til etableringen, som udledes af stk. 1.⁸⁸

a. Facebook

Indledningsvist kan det konstateres, at Facebook udbyder deres tjenester til de registrerede inden for EU's geografiske område. Efter ordlyden i artikel 3(2)(a) kan der således ikke være nogen tvivl om, at Forordningen, teoretisk set, vil være anvendelig i Facebooks tilfælde. Bestemmelsen har den afledte retsvirkning, at Forordningen beskytter fysiske personer, som befinder sig inden for EU's grænser, uanset om den konkrete databehandling finder anvendelse i EU eller ej.⁸⁹ Fortsætter Facebook derfor med at gøre deres tjenester tilgængelige i EU, må det formodes, at virksomheden vil være et pligtsubjekt under Forordningen. Det er imidlertid uvist, hvordan man kan gennemføre et retskrav mod et selskab, der kun er omfattet af

⁸⁵ Jf. C-131/12, Google Spain.

⁸⁶ Jf. GDPR art. 3, stk. 2, litra a-b.

⁸⁷ Jf. GDPR art. 3, stk. 2, litra a-b.

⁸⁸ se Tranberg, et al., 2017 s. 104.

⁸⁹ Lotterup, 2016: Karnovs note 26 til GDPR.

Forordningen efter artikel 3(2). Der kan således være en praktisk problemstilling, der relaterer til, hvordan denne bestemmelse kan håndhæves. Det må eksempelvis anses som usandsynligt, at de europæiske domstole kan tvinge en amerikansk domstol til at håndhæve en afgørelse, der knytter sig til denne bestemmelse.

Facebook har imidlertid etableret et selskab i Irland⁹⁰, der formodentligt opfylder etableringsbetingelserne i artikel 3(1).⁹¹ Det er ikke mange informationer, der kan findes om Facebooks irske virksomhed på internettet, dog må denne entitet formodes at opfylde etableringskravet, da denne blot skulle udøve en *minimal aktivitet*. Derudover angives det ligeledes i Google Spain-afgørelsen, at det persondataretlige retsgrundlag finder anvendelse, hvis det etablerede selskab har til formål at sælge reklameannoncer, der er målrettet mod indbyggere inden for Unionens område. Det kan ikke med sikkerhed fastsættes, at den irske virksomhed er oprettet med dette formål, men det må alligevel anses som værende sandsynligt, at dette, koblet med skatteretlige hensyn, er bagtanken med denne selskabsmæssige indretning. Alle disse forhold indikerer således, at Facebook risikerer et juridisk ansvar, hvis virksomheden har handlet i strid med Forordningens bestemmelser.

Der er dog en række praktiske forhold, som giver anledning til tvivl i forhold til Forordningens territoriale rækkevidde. Facebook har eksempelvis allerede bekendtgjort, at virksomheden ændrer sine brugervilkår således, at 1.5 mia. Facebook-brugere nu overgår fra at være i et kontraktforhold med deres irske selskab til moderselskabet⁹² i Californien.⁹³ Denne ændring skulle angiveligt være motiveret i et ønske om at omgå den europæiske regulering; *"The previously unreported move, which Facebook confirmed to Reuters on Tuesday, shows the world's largest online social network is keen to reduce its exposure to GDPR, which allows European regulators to fine companies for collecting or using personal data without users' consent."*⁹⁴ Facebook har annonceret disse ændringer cirka en måned, før Forordningen skal anvendes, hvilket underbygger den mistanke, som fremføres i citatet.

Den foreløbige redegørelse af Forordningens anvendelsesområde har vist, at de Facebook-brugere, som opholder sig i EU, fortsat er omfattet af retskildens territoriale anvendelsesområde på trods af Facebooks ændring.⁹⁵ Vælger Facebook

⁹⁰ Virksomheden skulle være etableret i Dublin under *Facebook Ireland Ltd.*

⁹¹ Se endvidere Larsen, 2017: *De sociale mediers brugervilkår del II – værnetinget*, om relationen mellem sociale medieplatformes fysiske placering og vernetingsproblemstillingen.

⁹² Etableret i Californien som *Facebook Inc.*

⁹³ Hern, 2018: *Facebook moves 1.5bn users out of reach of new European privacy law*

⁹⁴ Ingram, 2018: *Exclusive: Facebook to put 1.5 billion users out of reach of new EU privacy law*

⁹⁵ Jf. GDPR art 3, stk. 2, C-230/14, Weltimmo, præmis 30 og C-131/12, Google Spain.

derimod at nedlægge det irske selskab og fortsætte med at udbyde deres tjenester til EU fra selskabets domicil i USA, vil dette formodentligt besværliggøre muligheden for at retsforfølge virksomheden for lovbrud. Peter Blume understøtter ligeledes dette synspunkt ved at anføre, at *”Det ikke helt åbenbart, om bestemmelsen fuldt ud er i overensstemmelse med de almindelige principper i international ret, og dermed om en domstol i et tredjeland på dette grundlag vil lægge forordningen til grund, men det må forventes at være tilfældet i EU.”*⁹⁶ Det er derved sandsynligt, at der kan opstå en situation, hvor artikel 3(2) ikke kan håndhæves i praksis, så det bliver interessant at følge, hvordan denne problemstilling vil blive håndteret af de relevante myndigheder på sigt.

Hvis det viser sig, at disse teoretiske overvejelser er korrekte, vil virksomheder som Facebook og Google således have et stærkt incitament til at sikre, at de ikke risikerer et juridisk ansvar i jurisdiktioner, hvor der er en skærpet persondataretlig regulering. I USA er der eksempelvis ikke nogen persondataretlig regulering.⁹⁷ Amerikanske virksomheder er derfor underlagt en jurisdiktion, hvor de på nuværende tidspunkt ikke kan retsforfølges for at behandle persondata på en måde, der vil være uforeneligt med principperne i Forordningen. En online virksomhed, som Facebook, har udelukkende en ren økonomisk interesse i at etablere en fysisk entitet inden for EU's jurisdiktion. Der er således ikke nogen praktiske forhold, der bevirker, at virksomheden skal have et fysisk link i Europa for at levere deres tjenester til indbyggerne i EU-lande. Derved forstærker det formodningen om, at der kan opstå en situation, hvor flere af disse virksomheder vil begynde at spekulere i at indrette sig på en måde, der vil begrænse deres juridiske ansvar i EU.

b. Cambridge Analytica

Den territoriale problemstilling er forholdsvis enkel at udrede i forhold til Cambridge Analytica. Selskabets moderselskab er etableret i den amerikanske stat Delaware, der er kendt for at have en meget lempelig selskabsretlig regulering.⁹⁸ Dog er denne entitet angiveligt et skuffeselskab, der blot har til formål at eje IPR-rettighederne til Cambridge Analyticas psykografiske modeller.⁹⁹ Derimod skulle virksomhedens reelle aktiviteter og ledelse være placeret i London. Der kan dermed ikke være nogen tvivl om, at Cambridge Analytica er omfattet af Forordningens formelle rækkevidde

⁹⁶ Se Blume, 2016: *Den nye persondataret* s. 55.

⁹⁷ Jolly, 2017: *Data protection in the United States: overview*

⁹⁸ se fx Sørensen, Nielsen, & Danielsen, 2014 s. 617 om den såkaldte *Delaware-effekt*.

⁹⁹ Rosenberg, 2018: *Cambridge Analytica, Trump-Tied Political Firm, Offered to Entrap Politicians* og Cadwalladr & Graham-Harrison, 2018: *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*

efter hovedreglen i artikel 3(1). Virksomhedens aktiviteter i Brexit-kampagnen skaber også en formodning om, at de vil være omfattet af artikel 3(2).¹⁰⁰ Dette har imidlertid ingen praktisk betydning, eftersom virksomheden utvivlsomt har fornøden tilknytning efter hovedreglen.

Forordningens præambel angiver endvidere, at fysiske personer erhverver beskyttelse efter loven uanset deres nationalitet eller bopæl.¹⁰¹ De persondatarelige rettigheder som udledes af Forordningen, er dermed ikke kun gældende for unionsborgere eller fysiske personer med bopæl inden for Unionen. Forordningens bestemmelser kan således finde anvendelse, såfremt en dataansvarlig, med fornøden tilknytning til EU, behandler tredjelandsborgeres personoplysninger. Hypotetisk set, vil Forordningen dermed beskytte samtlige personer, der er omfattet af den aktuelle sag, da Cambridge Analyticas databehandling har fundet sted i Storbritannien.¹⁰² Dette er bestemt ikke uvæsentligt, eftersom amerikanske statsborgere alene, ifølge Facebooks egen redegørelse, udgør over 80 % af de personer, som er omfattet af sagen.¹⁰³ Baseret på ordlyden i betragtning 14 i Forordningen, må det derfor formodes, at samtlige tredjelandsborgere ligeledes erhverver beskyttelse efter Forordningen. Denne formodning underbygges endvidere af den omstændighed, at ICO har beordret Cambridge Analytica til at videregive de informationer, som de har på amerikanske borgere.¹⁰⁴ Dette påbud er opstået efter, at en amerikansk statsborger har forsøgt at anvende de persondatarelige rettigheder, der udledes af de europæiske retskilder.

Det vil derfor forudsætningsvist lægges til grund, at alle omfattede Facebook-brugere, uanset nationalitet, vil erhverve beskyttelse efter Forordningen, da Cambridge Analytica foretog deres databehandling inden for Unionens område.¹⁰⁵

¹⁰⁰ Cadwalladr & Graham-Harrison, 2018: *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*

¹⁰¹ Jf. GDPR betragtning 14.

¹⁰² Wylie, 2018: *Christopher Wylie: Why I broke the Facebook data story – and what should happen now*

¹⁰³ Schroepfer, 2018: *An Update on Our Plans to Restrict Data Access on Facebook*

¹⁰⁴ ICO, 2018: *ICO serves Enforcement Notice on SCL Elections Ltd over inadequate response to subject access request*

¹⁰⁵ Jf. GDPR art 3, stk. 1 og betragtning 14.

Kapitel III. Legaliteten af Cambridge Analytics aktiviteter

I denne del af specialet vil det blive undersøgt, om Cambridge Analytica har handlet i overensstemmelse med den persondatarelige regulering. I forsøget på at udrede, om selskabets databehandling hviler på et lovligt grundlag, vil det indledningsvist blive afklaret hvilken overordnet ramme, den dataansvarlige skal holde sig inden for.

Det blev tidligere konstateret, at Cambridge Analytica har behandlet datamateriale, der indeholder personfølsomme oplysninger. Derfor vil det blive undersøgt, om der er grundlag for at antage, at behandlingsforbuddet i artikel 9(1) kan fraviges i den konkrete sag. Der er to konkrete undtagelsesbestemmelser, som muligvis kan legitimere virksomhedens aktiviteter. Det vil derfor blive undersøgt, om de omfattede Facebook-brugere har givet afkald på den persondatarelige beskyttelse ved at offentliggøre deres personoplysninger på Facebook. Dernæst vil det afklares, om databehandlingen kan begrundes ved, at Facebook-brugerne har givet et fornødent samtykke.

1. God databehandlingsskik

I persondatalovens § 5 er det anført, at personoplysninger skal behandles i overensstemmelse med *god databehandlingsskik*. Formuleringen 'god databehandlingsskik' er en dansk tilføjelse, der blev indført med implementeringen af databeskyttelsesdirektivet. Direktivet angiver, at personoplysninger skal behandles *rimeligt* og *lovligt*.¹⁰⁶ Disse to grundlæggende behandlingsprincipper er ligeledes videreført i Forordningen, hvor der endvidere tilføjes et princip om *gennemsigtighed*.¹⁰⁷ Det er således bestemt, at personoplysninger skal behandles *lovligt*, *rimeligt* og *gennemsigtigt* i forhold til den registrerede. Dog er det uvist, om selve formuleringen 'god databehandlingsskik' vil blive anvendt fremadrettet, eftersom begrebet ikke længere fremgår af det gældende lovgrundlag. Denne afvigelse kan dog ikke antages at have en semantisk betydning for bestemmelsens juridiske indhold. Af denne årsag vil fremstillingen anvende begrebet 'god databehandlingsskik' som en samlebetegnelse for de tre grundlæggende behandlingsprincipper, der fremgår af Forordningen.

Disse tre hovedprincipper udgør således den ydre ramme, som enhver databehandling skal holde sig inden for.¹⁰⁸ Håndterer den dataansvarlige eksempelvis data på en måde, som er uforeneligt med disse principper, vil der være

¹⁰⁶ Jf. Databeskyttelsesdirektivets art. 6, stk. 1, litra a og se Tranberg, et al., 2017 s. 119.

¹⁰⁷ Jf. GDPR art. 5, stk. 1.

¹⁰⁸ se Tranberg, et al., 2017 s. 119.

tale om en situation, hvor den dataansvarlige ikke har udvist *god databehandlingsskik*. Disse generelle behandlingsprincipper finder anvendelse, uanset om der er tale om følsomme eller almindelige personoplysninger.¹⁰⁹

Lovlighedskravet angiver, at databehandlingen af personoplysninger udelukkende må finde sted, såfremt den er lovlig. Den dataansvarlige har således en forpligtelse til at sikre, at den konkrete databehandling er lovlig i henhold til EU-lovgivningen samt den nationale lovgivning i de relevante medlemsstater.¹¹⁰

Rimelighedskravet indebærer, at den konkrete databehandling skal være i overensstemmelse med den grundtanke, som udgør fundamentet for Forordningens beskyttelsesinteresse.¹¹¹ Det danske datatilsyn har anvendt denne betingelse som en generalklausul.¹¹² Kravet kan således anvendes til at opsætte betingelser eller direkte afvise, at en konkret behandling må finde sted, selvom den dataansvarlige ellers opfylder Forordningens øvrige behandlingsprincipper.

Transparenskravet skaber en forpligtelse for den dataansvarlige, hvormed de databehandlinger der foretages skal overskueliggøres.¹¹³ Dette krav er implementeret som et nyt forhold i Forordningen, da gennemsigtighed selvsagt er en nødvendig forudsætning for at føre tilstrækkelig kontrol over, om den persondataretlige lovgivning bliver overholdt.

2. Selvoffentliggørelse

Det anføres således i artikel 9(2)(e), at forbuddet mod at behandle personfølsomme oplysninger ophæves, såfremt den registrerede tydeligvis har offentliggjort de omhandlende informationer selv. Spørgsmålet er således, hvad der skal til, før en Facebook-bruger har givet afkald på den beskyttelse, som er angivet i Forordningen. Denne konkrete problemstilling er forelagt for Folketingets Ombudsmand i 2011.¹¹⁴ I sagen brugte en medarbejder fra SKAT en kvindes Facebook-profil til at indsamle oplysninger om kvinden. Da kvinden havde en åben profil, der var tilgængelig for enhver, mente Folketingets Ombudsmand, at hun havde givet opgivet retten til at få disse informationer beskyttet. Det var endvidere ombudsmandens opfattelse, at en

¹⁰⁹ Jf. GDPR art. 5, stk. 2 og se endvidere Blume, 2016: *Den nye persondataret* s. 69.

¹¹⁰ se Blume, 2016: *Den nye persondataret* s. 69-70.

¹¹¹ se Blume, 2016: *Den nye persondataret* s. 70.

¹¹² se Blume, 2016: *Den nye persondataret* s. 70.

¹¹³ Dele af transparenskravet er ligeledes kodificeret ind i forordningen som konkrete forpligtelser, jf. fx art. 12 og 13,

¹¹⁴ Folketingets Ombudsmand afgørelse: *J.nr. 2011-2657-2091*

Facebook-profil ligeledes er offentligt tilgængelig, hvis den konkrete bruger har et stort antal 'venner' i sit Facebook-netværk.

Det forekommer dog ualmindeligt byrdefuldt, hvis en Facebook-profil kan miste dens persondataretlige beskyttelse, fordi personen har mange venner i sit netværk. Selv i situationen hvor Facebook-profilen er helt åben, virker det som en barsk konsekvens. Dette argument begrundes i det faktum, at de fleste Facebook-brugere sandsynligvis ikke er bekendte med indstillingsmulighederne samt hvilke afledte konsekvenser en åben profil kan have for vedkommende. Det er imidlertid mere forståeligt, at beskyttelsen ophæves, hvis profilen er helt åben, da enhver person eller virksomhed således kan tilgå informationen. Alligevel understøttes det førnævnte synspunkt i den konkrete sag, da kvinden jo ikke ønskede at give samtykke til, at myndighederne kunne anvende oplysningerne til dette konkrete formål.

Det må alligevel udledes, at det er muligt for virksomheder, som Cambridge Analytica, at behandle data fra 'åbne profiler' og profiler med et stort antal venner uden nogen begrænsninger.¹¹⁵ Dette argument forudsætter dog, at de relevante judicielle myndigheder vælger at bakke op om Ombudsmandens vurdering.¹¹⁶ Det lækkede datamateriale består af 87 mio. af Facebook-brugeres informationer. Der må således være en klar formodning om, at et ukendt antal af profilerne må være 'åbne' eller have et stort antal af Facebook-venner. Dog er der ingen indikationer, der antyder, at Cambridge Analytica har forsøgt at begrænse deres undersøgelse til disse profiler. Derudover blev også omtalt tidligere i fremstillingen, at det konkrete værktøj, som Kogan brugte, var i stand til at høste data på brugere, som har en lukket profil. Det må derfor generelt afvises, at undtagelsen kan påberåbes i denne sammenhæng.¹¹⁷

3. Persondatarettens samtykkebegreb

En anden undtagelsesmulighed til forbuddet i artikel 9(1) mod at behandle følsomme personoplysninger er, såfremt den registrerede har givet samtykke til at gøre de konkrete oplysninger genstand for databehandling. Det er i denne sammenhæng vigtigt at anføre, at disse bestemmelser er præceptive og derved ikke kan fraviges ved aftale.¹¹⁸ Persondatarettens samtykkebegreb er indledningsvist beskrevet som

¹¹⁵ Jf. GDPR art. 9, stk. 2, litra e.

¹¹⁶ Ombudsmandens udtalelser har ikke bindende juridisk virkning, men domstolene kan vælge at støtte sig til denne udtalelse. Se fx Munk-Hansen, 2014: *Retsvidenskabsteori* s. 342.

¹¹⁷ Hartmans, 2018: *It's impossible to know exactly what data Cambridge Analytica scraped from Facebook — but here's the kind of information apps could access in 2014*

¹¹⁸ se Blume, 2016: *Den nye persondataret* s. 64.

”enhver frivillig, specifik, informeret, og utvetydig viljestilkendegivelse fra den registrerede, hvorved den registrerede ved erklæring eller klar bekræftelse indvilger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling”.¹¹⁹ Denne bestemmelse opsætter de grundlæggende rammer for, hvad der helt konkret menes ved et gyldigt samtykke.¹²⁰ Forordningen har dog en række særlige bestemmelser, der finder anvendelse, når der behandles følsomme oplysninger. Det angives således, at den registrerede skal have givet udtrykkeligt samtykke til at lade sådanne oplysninger behandle til et eller flere specifikke formål.¹²¹ Det må således udledes, at retsstillingen ikke ændres betydeligt, når der er tale om følsomme oplysninger i forhold til samtykkeproblemstillingen.

Den første betingelse om, at samtykket skal være givet frit er uddybet i artikel 7(4). Det er således angivet i bestemmelsen, at der skal tages hensyn til, om opfyldelsen af en kontrakt eller tjenesteydelse er gjort betinget af et samtykke til at behandle personoplysninger, som ikke har nogen relevans for den konkrete kontrakt. Den anden betingelse bestemmer, at samtykket skal være givet til et eller flere specifikke formål. Dette krav præciserer således, at den registrerede ikke kan afgive et generelt samtykke til at gøre personoplysninger tilgængelig for enhver form for behandling. Det må ligeledes udledes, at bestemmelsen opsætter et princip om formålsbestemthed, før der kan antages at foreligge et gyldigt samtykke.¹²² Artikel 29-gruppen har angivet en række eksempler, der sandsynligvis ikke opfylder betingelsen: *”For these reasons, a purpose that is vague or general, such as for instance ‘improving users’ experience’, ‘marketing purposes’, ‘IT-security purposes’ or ‘future research’ will - without more detail - usually not meet the criteria of being ‘specific’”*.¹²³ Betingelsen om formålsbestemthed er også essentiel for afvejningen af finalité-princippet, der sætter en retlig ramme for den lovlige databehandling.¹²⁴

Den tredje betingelse om informeret samtykke betyder, at den registrerede skal være tilstrækkeligt bevidst om, hvad der begrunder den konkrete behandling af personoplysninger. Hvis der gives samtykke i en skriftlig erklæring, som tilfældet jo ofte er digitalt, så skal anmodningen forelægges på en måde, der gør det klart, letforståeligt og lettilgængeligt for den registrerede at skelne, hvad der præcist gives samtykke til.¹²⁵ Det fjerde krav der angiver, at samtykket skal være utvetydigt eller

¹¹⁹ Jf. GDPR art. 4, nr. 11.

¹²⁰ se Blume, 2016: *Den nye persondataret* s. 64.

¹²¹ Jf. GDPR art. 9, stk. 2, litra a.

¹²² se endvidere Blume, 2016: *Formålsbestemthed*

¹²³ se Artikel 29-Gruppen, 2013: *Opinion 03/2013 on purpose limitation* s. 16.

¹²⁴ Jf. GDPR art. 5, stk. 1, litra b.

¹²⁵ Jf. GDPR art. 7, stk. 2.

udtrykkeligt må formodes at tilsige, at der ikke må foreligge tvivl, om der er givet samtykke eller ej.¹²⁶ Såfremt der er afgivet et samtykke, som ikke opfylder disse grundlæggende krav, vil det være ugyldigt. I denne situation vil retsvirkningen af det ugyldige samtykke være, at den dataansvarliges behandling er retsstridig, medmindre en af de andre undtagelser finder anvendelse.¹²⁷ Under det gamle paradigme i dansk ret, har den dataansvarlige været forpligtet til at kunne dokumentere, at den registrerede har afgivet et gyldigt samtykke, hvis retmæssigheden af den konkrete behandling hviler på dette grundlag.¹²⁸ Derved foreligger der en omvendt bevisbyrde for den dataansvarlige. Dette krav bliver dog først harmoniseret til at være retstilstanden i det indre marked fra Forordningens anvendelsesdato.¹²⁹

I de to følgende afsnit vil det blive vurderet, om der foreligger et lovligt behandlingsgrundlag, der kan legitimere Cambridge Analyticas aktiviteter. Indledningsvist vil Facebooks brugervilkår inddrages for at udlede, hvad det oprindelige behandlingsgrundlag var for at indsamle de omhandlende personoplysninger. Dernæst vil brugervilkårene fra Kogans applikation også blive analyseret, da disse vilkår giver en generel forståelse af grundlaget for den viderebehandling, som efterfølgende fandt sted.

4. Facebooks brugervilkår

I det digitale informationssamfund vi lever i, må det antages at være en begrænset andel af forbrugerne, som læser indholdet i brugervilkårene, før de accepterer at anvende en online tjenesteydelse på udbyderens vilkår.¹³⁰ Dette er i sig selv ikke bemærkelsesværdigt, da selv jurister kan have vanskeligheder ved at udlede, hvad der helt præcist gives samtykke til. I oprettelsesfasen af den konkrete brugerprofil vil det sociale medie således påstå, at der er indgået en bindende aftale mellem brugeren og virksomheden, hvor personen har indvilget i at oprette brugeren under de angivne vilkår.¹³¹ Dette udgangspunkt kan rejse adskillige juridiske problemstillinger, hvilket bl.a. omfatter en række forhold, som er relevante i et persondataretligt perspektiv. For kan man overhovedet påstå, at der kan foreligge et informeret samtykke, hvis der

¹²⁶ se Blume, 2016: *Den nye persondataret* s. 64-65.

¹²⁷ Jf. bl.a. forbuddet i GDPR art. 9, stk. 1.

¹²⁸ Lotterup, 2016: Karnovs note 69 til GDPR.

¹²⁹ Jf. GDPR art. 7, stk. 1 og art 99, stk. 2.

¹³⁰ Berreby, 2017: *Click to agree with what? No one reads terms of service, studies confirm*

¹³¹ Se Larsen & Feldthusen, 2016: *De sociale mediers brugervilkår del I - aftalen*

er en stærk formodning om, at forbrugerne ikke læser eller har mulighed for at forstå brugervilkårene?

Denne problemstilling er i særdeleshed relevant i forhold til Facebook. På Facebook er brugerne produktet og de reelle kunder er de virksomheder, som køber reklameannoncer for at nå ud til brugerne. Forbrugerne har derved ikke kendskab til, hvordan Facebook anvender deres personoplysninger i forsøget på at skabe den perfekte marketingsplatform.¹³² Det er således muligt, at visse forbrugere ville genoverveje deres beslutning om at oprette deres Facebook-profiler, hvis de var blevet tilstrækkeligt informeret om de omkostninger, der følger med adgangen til kerneydelsen. Problemet bliver ikke mindre kompliceret, eftersom der ikke eksisterer et reelt alternativ til Facebook.¹³³ Det er således en buffet, hvor forbrugeren enten accepterer samtlige Facebooks vilkår eller må vælge at leve uden en Facebook-profil. Det må således konkluderes, at styrkeforholdet mellem Facebook og forbrugerne er særdeles skævt. Forbrugerne har ingen mulighed for at forhandle de konkrete brugervilkår, og derfor er den persondataretlige regulering en af de juridiske forhold, der kan begrænse Facebooks dominans.

Facebook har foretaget en række ændringer til deres brugervilkår de seneste måneder. Det er nærliggende at antage, at Facebook foretager disse ændringer i forsøget på at komme i 'compliance' med persondataforordningens bestemmelser inden skæringsdatoen den 25. maj 2018. I deres snarligt forældede generelle brugervilkår¹³⁴ har Facebook dog formuleret en vidtgående fuldmagt til dem selv:

"Our goal is to deliver advertising and other commercial or sponsored content that is valuable to our users and advertisers. In order to help us do that, you agree to the following:

- 1. You give us permission to use your name, profile picture, content and information in connection with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information, without any compensation to you. If you have selected a specific audience for your content or information, we will respect your choice when we use it.*

¹³² Hull, 2018: *The internet is designed for corporations, not people*

¹³³ Statista, 2018: *Most popular social networks worldwide as of April 2018, ranked by number of active users*

¹³⁴ Apendix I, 2018: *Terms of Service* (findes også på dansk, men den engelske version har forrang, jf. aftalen)

2. *We do not give your content or information to advertisers without your consent.*¹³⁵

Det kan udledes på baggrund af ovenstående uddrag fra brugervilkårene, at forbrugerne nærmest giver Facebook en blankocheck til at udnytte deres personoplysninger og IP-beskyttede værker kommercielt. Den enkelte Facebook-bruger skal således acceptere, at enhver information, som virksomheden har på vedkommende, kan anvendes til reklamekampagner og andre kommercielle formål af Facebook. Det angives dog til sidst, at Facebook ikke giver brugernes informationer videre til tredjeparter, medmindre brugeren giver samtykke til dette. Dette er essentielt, da sagen netop omhandler en tredjepart, Cambridge Analytica, som er kommet i besiddelse af Facebook-data. Dette bliver undersøgt nærmere i næste afsnit i relation til at udlede, om der forelå et sådan samtykkegrundlag.

I forhold til de betingelser som blev gennemgået i det foregående afsnit vedrørende samtykkevurderingen, må det konstateres, at der generelt er flere forhold ved Facebooks vilkår, der giver anledning til nærmere overvejelser. Først kan det konstateres, at kravet om formålsbestemthed sandsynligvis bevirker, at vilkårene allerede fejler testen.¹³⁶ Dette argument er understøttet af Artikel 29-gruppens eksempler, der angiver, at formuleringer som fx 'til marketingsformål' vil fejle testen. Dette konkrete vilkår fremgår direkte af formuleringen sammen med andre forhold. Facebook kan således anvende dette led til at begrunde en databehandling, der tager afsæt i en politisk eller kommerciel markedsføringskampagne, uden at den registrerede vil have mulighed for at tage eksplicit stilling til dette. Derudover forudsætter oprettelsen af en Facebook-profil ikke, at den konkrete bruger har været inde og 'scrolle' ned over brugerbetingelserne.¹³⁷ Derved åbnes muligheden endvidere for, at brugervilkårene kan være i strid med kravet om utvetydig viljeserklæring fra den registrerede.

Det danske forbrugerråd har i flere omgange forsøgt at få Datatilsynet til at tage stilling til legaliteten af Facebooks brugervilkår.¹³⁸ Dog har det danske datatilsyn hævdet, at det er de irske myndigheder, som bærer ansvaret for at undersøge, om Facebook overholder de persondataretlige regler. En tysk domstol har imidlertid i februar 2018, afsagt kendelse i en sag, der netop omhandler Facebooks generelle brugervilkår.¹³⁹ I afgørelsen bestemte den tyske domstol, at Facebook ikke afgiver

¹³⁵ Appendix I, 2018: *Terms of Service*, pkt. 9.

¹³⁶ Jf. bl.a. GDPR art. 5, stk. 1, litra b og artikel 9, stk. 2, litra a.

¹³⁷ Larsen & Feldthusen, 2016: *De sociale mediers brugervilkår del I - aftalen*

¹³⁸ Ritzau, 2018: *Datatilsynet får kritik for at afvise Facebook-sag*

¹³⁹ Hern, 2018: *Facebook personal data use and privacy settings ruled illegal by German court*

nok informationer, der påviser, at der kan foreligge et gyldigt samtykke. Den tyske domstol tog endvidere stilling til adskillige forhold i brugervilkårene og tilkendegav endvidere, at det ikke er foreneligt med persondatalovgivningen, at Facebook forbeholder sig retten til at føre brugernes data til tredjelande som USA.¹⁴⁰ Afgørelsen kan have betydning for retstilstanden i EU, da datatilsynene samt de nationale domstole har en forpligtelse til at iagttage hinandens praksis og forsøge at ensarte fortolkningen af bl.a. Forordningen.¹⁴¹

Det må generelt konstateres, at Facebooks brugervilkår sandsynligvis krænker persondatarettens samtykkebegreb i forhold til kravene om en informeret, formålsbestemt samt utvetydig viljeserklæring. Derudover kan det endvidere udledes, at Facebook ikke forbeholder sig retten til at videregive oplysninger til tredjeparter, medmindre der foreligger et specifikt samtykkegrundlag for at foretage denne handling. Som en afsluttende bemærkning til dette afsnit, kan det endvidere anføres, at Facebook ikke foretager de store ændringer til de forhold, som er blevet kritiseret i dette afsnit, i deres opdaterede vilkår. Ordlyden af de tilsvarende bestemmelser er blevet marginalt ændret, hvorved formuleringen er en anelse mere specifik. Dog må det stadig konkluderes, at brugervilkårene sandsynligvis fortsat er i konflikt med persondatarettens samtykkebegreb.

5. Cambridge Analyticas behandlingsgrundlag

I dette afsnit vil legaliteten af Cambridge Analyticas handlinger endeligt blive vurderet. Det vil således blive udledt, om virksomheden har været i besiddelse af et legitimt behandlingsgrundlag, der fraviger forbuddet i artikel 9(1). For at undersøge legaliteten af Cambridge Analyticas aktiviteter, er det først nødvendigt at tage udgangspunkt i mellemmanden Aleksandr Kogan. Kogan er i 2014 ansat som forsker ved The University of Cambridge. Samme år bliver han kontaktet af virksomheden SCL Elections¹⁴², der er et beslægtet selskab til Cambridge Analytica. De ønsker således at indlede et samarbejde om at høste informationer fra Facebook. SCL tilbyder at betale kompensationen til de Facebook-brugere, som deltager i undersøgelsen. Som kompensation for deres ydelse ønsker de at få autorisation til at behandle datasættene til kommercielle formål.¹⁴³ Kogan accepterer disse vilkår,

¹⁴⁰ Se Facebooks vilkår I Appendix I, 2018, afsnit I6. Se også C-362/14, Safe Harbour-afgørelsen.

¹⁴¹ Jf. bl.a. princippet om EU-konform fortolkning og GDPR art 51, stk. 1-2.

¹⁴² SCL Elections er et beslægtet selskab til Cambridge Analytica. Før høstelsen af Facebook-data eksisterede Cambridge Analytica ikke. Derfor var det SCL Elections der indgik den indledede aftale med Kogan.

¹⁴³ Stahl, 2018: *Aleksandr Kogan: The link between Cambridge Analytica and Facebook*

hvilket fremgår af kontrakten mellem Kogan og SCL. Dette er vedhæftet som Appendix II.¹⁴⁴ Kogan udvikler herefter applikationen 'This Is Your Digital Life', som bliver startskuddet for den kontroversielle del af nærværende sag. Applikationens brugervilkår fremgår af Appendix III.¹⁴⁵

I det følgende vil det blive lagt til grund, at de registrerede havde læst brugervilkårene. Punkt 3 i vilkårene angiver formålet med indsamlingen af data: "We use this application as a part of our research on understanding how people's Facebook data can predict different aspects of their lives. Your contribution and data will help us better understand relationships between human psychology and online behavior." Det kan indledningsvist noteres, at disse data blev udnyttet til to forskellige formål af henholdsvis Kogan og Cambridge Analytica. Det er formodentligt korrekt, at Kogan ville anvende informationerne til sin forskning, hvilket imidlertid anføres som applikationens eneste formål.

Det fremgår af aftalen mellem Kogan og SCL, at begge parter vidste, at informationerne også ville blive udnyttet til kommercielle og politiske formål.¹⁴⁶ Denne antagelse underbygges endvidere af et interview foretaget af 60 Minutes, hvor Kogan erkender at have været bevidst om, at SCL Elections ville anvende informationerne til kommercielle samt politiske formål.¹⁴⁷ Cambridge Analytica bliver umiddelbart herefter grundlagt med ambitionen om at udlede metoder, hvorved disse informationer kunne udnyttes politisk.¹⁴⁸ Formuleringen 'as a part of our research', i det ovenfor indsatte citat, angiver ikke entydigt, at personoplysninger udelukkende skulle anvendes til akademisk forskning. Dog vil dette argument, under alle omstændigheder, ikke kunne opretholdes. Det fremgår indledningsvist af vilkårene, at modtageren af undersøgelsens resultater er et fakultet, som er underlagt the University of Cambridge. Dermed må der have forelagt en klar formodning om, at informationerne udelukkende skulle bruges til akademisk forskning.¹⁴⁹

En af den dataansvarliges forpligtelser er at fastlægge formålene bag den konkrete databehandling.¹⁵⁰ I det omfang hvor personoplysninger behandles udover det, som er angives som de konkrete formål, foreligger der *viderebehandling*.¹⁵¹ Denne situation vil som udgangspunkt være i strid med persondatarettens finalité-princip,

¹⁴⁴ Appendix II, 2014: *Aftale mellem Kogan og SCL pkt. 1-3.*

¹⁴⁵ Appendix III, 2014 – Terms and Conditions for Kogan app.

¹⁴⁶ Appendix II, 2014: *Aftale mellem Kogan og SCL, Afsnit 1 og 6.*

¹⁴⁷ Stahl, 2018: *Alexandr Kogan: The Link Between Cambridge Analytica And Facebook*

¹⁴⁸ Wylie, 2018: *Cambridge Analytica: Whistleblower reveals data grab of 50 million Facebook profiles*

¹⁴⁹ "...its registered office based at Magdalene College, Cambridge." Appendix III, 2014 pkt. 1.

¹⁵⁰ Jf. GDPR art. 4, nr. 7.

¹⁵¹ Jf. GDPR art. 5, stk. 1, litra b.

der opsætter en retlig grænse for muligheden om at viderebehandle personoplysninger. Er viderebehandlingen dog i samfundets interesse, til videnskabelige eller historiske forskningsformål eller statistiske formål, vil forbuddet undtagelsesvist ophæves. Disse undtagelser kan ikke antages at finde anvendelse her. Det kan således allerede konkluderes, at Cambridge Analytica ulovligt har databehandlet Facebook-brugernes oplysninger.¹⁵²

Indtil nu er problemstillingen vedrørende legaliteten af Cambridge Analyticas handlinger udelukkende blevet anskuet ud fra forudsætningen om, at alle omfattede Facebook-brugere har læst brugervilkårene. Dette er særdeles tvivlsomt, da brugerne af Kogans applikation sandsynligvis kun havde anledning til at tro, at der var tale om en simpel personlighedstest. I det tidligere refererede interview anerkender Kogan, at applikationens eneste formål var at få testpersonerne til at logge ind med deres Facebook-login, så man kunne få autorisation til at indhente brugerens oplysninger. Kogan beskriver processen således: *"So I create this app where people sign up to do a study. And when they sign up to do the study, we would give them a survey. And in the survey we would have just this Facebook log-in button. And they would click the button, authorize us.... To collect certain data. We would collect things like their location, their gender, their birthday, their page "likes" and similar information for their friends."*¹⁵³ Såfremt testpersonerne skulle have haft en reel mulighed for at udlede, hvad de faktisk blev kompenseret for, skulle personen have læst følgende brugervilkår og tilmed forestået rækkevidden af formuleringen.

*"We collect any information that you choose to share with us by using the Application. This may include, inter alia, the name demographics, status updates and Facebooks likes of your profile and your network. If you click "OKAY" or otherwise use the Application or accept payment, you permit GSR to edit, copy, disseminate, publish, transfer, append or merge with other databases, sell, licence (by whatever means and on whatever terms) and archive your contribution and data."*¹⁵⁴ Dette brugervilkår giver konkret GSR (Kogans virksomhed) retten til at udnytte brugernes informationer uden begrænsninger. Det må formodes, at et vilkår af denne karakter efter almindelig dansk aftaleret vil kunne betegnes som et særligt byrdefuldt vilkår. I henhold til koncipistreglen må betingelsen kunne tilsidesættes.¹⁵⁵ Det forekommer endvidere indlysende, at der ikke kan antages at foreligge et gyldigt samtykke efter

¹⁵² Jf. GDPR art. 5, stk. 1, litra a.

¹⁵³ Stahl, 2018: *Alexandr Kogan: The Link Between Cambridge Analytica And Facebook*

¹⁵⁴ Appendix III, 2014: Kogan app vilkår pkt 6-7.

¹⁵⁵ Se Larsen & Feldthusen, 2016: *De sociale mediers brugervilkår del I - aftalen*

de persondataretlige bestemmelser. Det blev tillige anført tidligere i fremstillingen, at kravet om samtykke ikke kan fraviges ved aftale.¹⁵⁶

Applikationens brugervilkår kan ligeledes kritiseres under de samme forhold, som blevet gennemgået i afsnittet med Facebooks brugervilkår. I dette tilfælde er der blot tale om en mere 'grov' udgave. Sagen bliver alligevel løftet til et andet niveau, når der tages udgangspunkt i de personer, som ikke har haft kendskab til applikationen. Det er således estimeret, at 300.000 brugere har taget testen, hvorimod de resterende 87 mio. Facebook-brugere ikke har haft mulighed for at vide, at deres informationer var blevet høstet og derefter behandlet. Dette har været muligt, fordi Facebook-platformen har givet app-udviklere autorisation til at høste data fra venner til brugere, som havde godkendt en bestemt applikation. Dette er direkte i modstrid med pkt. 2 i Facebooks brugervilkår, der blev citeret i det foregående afsnit. Facebook har således givet tilladelse til, at tredjeparter har tilegnet sig adgang til brugeres informationer uden, at brugeren har givet særligt samtykke til dette.

Kogan har også svært ved at retfærdiggøre dette aspekt af sagen, da han bliver spurgt til indsamlingen af Facebook-vennernes informationer. "*So they didn't opt-in explicitly*"¹⁵⁷ Det er uvist, hvad Kogan forsøger at gøre gældende med denne bemærkning. Det kan umiddelbart godt tolkes som om, at han mener, at venner indirekte havde bemyndiget deres Facebook-venner til at give samtykke på deres vegne. Forordningen forhindrer ikke, at en fuldmægtig kan give samtykke på vegne af fuldmagtsgiveren, dog skal dette stadig ske i overensstemmelse med de almindelige regler.¹⁵⁸ Dette argument vil således knytte sig til en påstand om, at en Facebook-bruger automatisk afgiver en fuldmagt til personer i deres vennekreds. Disse Facebook-venner kan således afgive et gyldigt samtykke på hinandens vegne. Det må konkluderes, at dette argument ikke vil blive accepteret af de relevante judicielle myndigheder.

Det må dermed generelt udledes, at der ikke er nogen indikationer, der peger i retningen af, at Cambridge Analyticas databehandling er baseret på et lovligt grundlag. På baggrund af resultaterne i det foregående afsnit kan det udledes, at videregivelsen af Facebook-brugernes informationer var i strid med Facebooks egne vilkår. Hovedparten af de omfattede brugere er ikke blevet forelagt muligheden for at give samtykke til, at deres informationer blev videregivet til Kogan og derefter Cambridge Analytica.

¹⁵⁶ se Blume, 2016 Den nye persondataret s. 64.

¹⁵⁷ Stahl, 2018: *Alexandr Kogan: The Link Between Cambridge Analytica And Facebook*

¹⁵⁸ se Blume, 2016: Den nye persondataret s. 64.

Det må endvidere afvises, at der er påvist nogen formildende omstændigheder i forhold til virksomhedens aktiviteter. Alle indikationer er således, at disse begivenheder har fundet sted forsætligt. Cambridge Analytica har derfor handlet i strid med persondatarettens grundprincipper på en måde, der kan betegnes som særligt groft.¹⁵⁹ Dette gælder både for de 300.000 brugere, som aktivt tog testen samt de omtrent 87 mio. brugere, der ikke havde kendskab til Kogans applikation.

¹⁵⁹ Jf. GDPR art. 5, stk. 1, litra a og art. 83, stk. 2.

Kapitel IV. Facebooks ansvar og forpligtelser

Det vil i dette afsnit blive undersøgt, om Facebook har handlet i overensstemmelse med de generelle forpligtelser, der gælder for den dataansvarlige. Denne redegørelse vil endvidere tage udgangspunkt i andre forhold, end dem som blev udledt i afsnittet om Facebooks brugervilkår. Det er således påvist, at Facebook sandsynligvis ikke opfylder persondatarettens bestemmelser vedrørende gyldigt samtykke.

De problematiske forhold omkring Facebooks brugervilkår er dog kendetegnende for virksomheden generelt. Dette har således ikke nødvendigvis nogen særlig tilknytning til Cambridge Analytica-sagen. Der er imidlertid også en række specifikke forhold vedrørende Facebooks håndtering af sagen, der medfører, at selskabet muligvis ikke har udvist adfærd, der kan karakteriseres som god databehandlingsskik efter principperne i artikel 5(1)(a). Selve datalækket af 87 mio. brugeres informationer er et forhold, som bør undersøges nærmere. Denne generelle problemstilling rummer flere problematiske forhold set fra et juridisk perspektiv. Det kan indledningsvist betvivles, om Facebook har overholdt deres forpligtelse til at tilvejebringe en tilstrækkeligt virkende datasikkerhed om de oplysninger, som de har indsamlet på platformen. Derudover er det også tvivlsomt, om virksomheden har handlet i overensstemmelse med den underretningspligt, der påhviler den dataansvarlige, når der foreligger et sikkerhedsbrud. Disse to kerneproblemstillinger er omdrejningspunktet for de to følgende underafsnit.

1. Tilstrækkelig datasikkerhed

Det er beskrevet i artikel 32(1), at den dataansvarlige skal foretage passende tekniske og organisatoriske foranstaltninger for at sikre et tilstrækkeligt sikkerhedsniveau. Hvad der konkret konstituerer et tilstrækkeligt sikkerhedsniveau er generelt beskrevet i bestemmelsen. Det skal således vurderes efter den konkrete behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder.¹⁶⁰ Formålet med denne bestemmelse er, at den skal forebygge mod angreb og derved forhindre uautoriseret viderebehandling af de oplysninger, der søges beskyttet.¹⁶¹

Forordningen forholder sig kun generelt til hvilke generelle hensyn, der skal inddrages i denne vurdering. Denne realitet kan besværliggøre vurderingen af, hvornår en dataansvarlig har foretaget tilstrækkelige sikkerhedsforanstaltninger, der er i overensstemmelse med bestemmelsens ordlyd. Derudover opererer

¹⁶⁰ Jf. GDPR art. 32, stk. 1.

¹⁶¹ se Blume, 2016: Den nye persondataret s. 118-119

Forordningen ligeledes ud fra et generelt princip om integritet og fortrolighed.¹⁶² Dette indebærer, at den dataansvarlige skal behandle personoplysninger på en måde, hvorved der sikres en tilstrækkelig sikkerhed, der beskytter oplysningerne fra at blive genstand for uautoriseret eller ulovlig behandling.¹⁶³ Spørgsmålet er således, hvorvidt Facebook har taget passende tiltag i brug for at sikre, at deres platform ikke kunne udnyttes til uautoriseret eller ulovlig databehandling.

Det kan allerede betvivles på det foreliggende grundlag, at Facebook har handlet i overensstemmelse med disse generelle forskrifter. Indledningsvist kan det konstateres, at de omtalte hensyn om behandlingens karakter, omfang, sammenhæng og formål, understøtter påstanden om, at Facebook burde have taget effektive midler i brug for at beskytte de informationer, der er på platformen. Facebook har i øjeblikket 2.2 mia. brugere og de konkrete oplysninger kan, som tidligere beskrevet, udlede en række meget vidtrækkende forhold om disse fysiske personer. Der er således flere forhold, der antyder, at Facebook er en af de virksomheder i verden, som vil have det strengeste ansvar efter bestemmelsen. De er den sociale medieplatform, som har flest brugere, og de besidder tilmed meget følsomt datamateriale på disse personer.¹⁶⁴ Det er allerede udledt, at Kogan var i stand til at høste data på 87 mio. brugere, fordi platformen tillod, at han kunne indhente informationer på hver respondents Facebook-venner. Dette er allerede en meget alvorlig omstændighed. Derefter bliver spørgsmålet, om Facebook har været bevidst om disse problemstillinger angående den manglende datasikkerhed.

Følgende udsagn fra Sandy Parakilas, der har arbejdet for Facebook, som manager for virksomhedens databeskyttelsesteam, giver et indblik i, hvordan organisationen håndterede spørgsmålet datasikkerhed, mens han var ansat der. *"Well they didn't want to know in the sense that if they didn't know, then they could say they didn't know and they weren't liable, whereas if they knew they would actually have to do something about it. And one of the things that I was concerned about was that applications or developers of applications would receive all of this Facebook data, and that once they received it, there was no insight, Facebook had no control or view over what they were doing with the data."*¹⁶⁵ Dette citat skaber således en stærk formodning om, at Facebook har været bevidst om de potentielle sikkerhedsproblemer, der senere blev udnyttet af Kogan og Cambridge Analytica. Derudover var de ligeledes bevidste om, at virksomheden ikke kunne kontrollere, hvad personoplysningerne blev brugt til,

¹⁶² se GDPR art 5, stk. 1, litra f.

¹⁶³ Se Tranberg, et al., 2017 s. 127.

¹⁶⁴ Statista, 2018: *Most popular social networks worldwide as of April 2018, ranked by number of active users*

¹⁶⁵ Stahl, 2018: *Aleksandr Kogan: The link between Cambridge Analytica and Facebook*

hvis informationerne blev hentet ned fra platformen. Alligevel udarbejdede Facebook adskillige værktøjer for app-udviklere, der gjorde det enkelt at hente store mængder data ned.¹⁶⁶ I det allerede refererede interview med 60 Minutes forklarer Kogan, hvor simpel processen var i forhold til at hente informationerne ned fra Facebook. *"And it seems crazy now. But this was a core feature of the Facebook platform for years. This was not a special permission you had to get. This was just something that was available to anybody who wanted it who was a developer."*

Det kan således påvises, at Facebook har indrettet deres platform på en måde, hvorved denne var utrolig sårbar over for uautoriseret viderebehandling af Facebook-brugernes informationer. Der er endvidere stærke indicier, der antyder, at virksomheden har være bekendte med disse forhold i adskillige år. Det kan derfor ikke betvivles, at Facebook bærer en stor del af ansvaret for, at datalekket af 87 mio. brugeres informationer blev lækket til en tredjepart, som derefter behandlede disse data ulovligt.

Zuckerberg erkendte ligeledes, i en vis udstrækning, den mangelfulde sikkerhed ved høringen i den amerikanske kongres. *"For the first 10 or 12 years of the company, I viewed our responsibility as primarily building tools that, if we could put those tools in people's hands, then that would empower people to do good things... It's not enough to just build tools. We need to make sure that they're used for good. And that means that we need to now take a more active view in policing the ecosystem and in watching and kind of looking out and making sure that all of the members in our community are using these tools in a way that's going to be good and healthy."*¹⁶⁷ Det kan udledes af dette citat, at Zuckerberg erkender virksomhedens begrænsede prioritering af datasikkerhed. Herunder at Facebook udviklede værktøjer, der kunne misbruges til at komprimere den generelle grad af datasikkerhed på platformen.

Derudover angår en stor del af kritikken omkring Cambridge Analytica-sagen det faktum, at Kogans applikation blev gjort tilgængelig for Facebook-brugerne i første omgang. Det er kun Facebook, der kan overvåge om de apps, der kan anvendes i sammenhæng med virksomhedens tjenester kan anvendes til skade for forbrugerne. Som Kogan anførte i det ovenfor indsatte citat, var det ikke nødvendigt at indhente specielle tilladelser, før han fik ubegrænset adgang til at hente data ned fra Facebook-platformen. Derudover fremgik det specifikt af de vilkår, som han havde skrevet til Facebook, at han bl.a. forbeholdte sig retten til at udnytte informationerne

¹⁶⁶ Hartmans, 2018: *It's impossible to know exactly what data Cambridge Analytica scraped from Facebook — but here's the kind of information apps could access in 2014*

¹⁶⁷ Bloomberg Government, 2018: *Transcript of Mark Zuckerberg's Senate hearing*

kommercielt.¹⁶⁸ Dette er i strid med Facebooks egne brugervilkår, der dikterer, at virksomheden ikke videregiver brugernes informationer til tredjeparter, medmindre der foreligger et særligt samtykkegrundlag, som begrundet denne handling. Mike Schroepfer, der er ansat hos Facebook som *chief technology officer*, har erkendt, at der ikke var nogen medarbejdere hos Facebook, som læste Kogans brugervilkår igennem, før applikationen blev gjort tilgængelig for brugerne på platformen.¹⁶⁹

Der er således flere selvforårsagede forhold, der bevirker, at Facebook ikke var i stand til at afværge denne situation, før skaden indtraf. Facebook har bevidst åbnet platformen, hvorved app-udviklere uden videre fik autorisation til at hente data ned på virksomhedens brugere. Det kan således ikke lægges til grund, at Facebook har foretaget passende tiltag, der kunne sikre, at personoplysningerne på platformen ikke kunne viderebehandles på en måde, der ville være uforeneligt med persondatarettens grundlæggende behandlingsprincipper. Det blev endvidere indledningsvist konstateret, at det forventes af Facebook, på grund af omfanget af platformens brugere samt karakteren af de oplysninger, som de er i besiddelse af, at de generelt fastholdes til en høj sikkerhedsmæssig standard.¹⁷⁰ Det er derfor meget sandsynligt, at virksomheden kan blive sanktioneret på baggrund af de oplysninger, der er blevet udledt i dette afsnit.

2. Underretningspligt

Det blev i det foregående afsnit udledt, at Facebook ikke har overholdt deres forpligtelse til at sikre en tilstrækkelig grad af sikkerhed på platformen. I dette afsnit vil det blive undersøgt, om virksomheden har handlet i strid med bestemmelserne om underretningspligt efter, at de blev opmærksomme på datalækket.

Forordningen indeholder en underretningsforpligtelse for den dataansvarlige, såfremt der foreligger et sikkerhedsbrud, der indebærer en høj risiko for, at den registreredes rettigheder kan blive krænket.¹⁷¹ Denne forpligtelse skal udføres uden unødigt forsinkelse. Derudover er der en tilsvarende underretningspligt til de relevante tilsynsmyndigheder.¹⁷² Det angives, at den dataansvarlige ved brud på persondatasikkerheden har en forpligtelse til at underrette myndigheden uden unødigt forsinkelse og om muligt inden for senest 72 timer efter, at den dataansvarlige bliver bekendt med forholdet. Denne konkrete forpligtelse fremgik

¹⁶⁸ Appendix III, 2014: Kogans app vilkår pkt. 7.

¹⁶⁹ Romm, 2018: *Facebook didn't read the terms and conditions for the app behind Cambridge Analytica*

¹⁷⁰ Jf. GDPR art. 31, stk. 1.

¹⁷¹ Jf. GDPR art. 34, stk. 1.

¹⁷² Jf. GDPR art. 33, stk. 1.

ikke direkte af lovgrundlaget under det gamle paradigme. Bestemmelsen er dog en kodificering af en tilsvarende underretningsforpligtelse, der tidligere blev udledt af den retlige standard, som er angivet i persondatalovens § 5 om god databehandlingskik.¹⁷³

Forordningen angiver i artikel 4(12), hvad der kan statuere et *brud* på persondatasikkerheden. ”*et brud på sikkerheden, der fører til hædelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet*”.¹⁷⁴ I den konkrete sag er der tale om uautoriseret videregivelse og adgang til personoplysninger, der blev opbevaret på Facebook-plattformen. Det kan derved udledes, at der foreligger et brud på sikkerheden efter Forordningens definition. Spørgsmålet er dernæst, om Facebook havde kendskab til datalækket, hvorved de således burde have underrettet de relevante parter.

Facebook har erkendt, at de indledningsvist blev bekendte med datalækket i 2015, da The Guardian giver dem besked om, at Cambridge Analytica er kommet i besiddelse af datamaterialet.¹⁷⁵ Facebook er således på dette tidspunkt bevidste om, at en uautoriseret tredjepart havde tilegnet sig adgang til en forholdsvis stor mængde af Facebook-data. Facebook fjerner derefter Kogans applikation, men der gives ingen underretning til de relevante parter. Dette finder først sted efter, at historien bliver bragt af diverse nyhedsmedier i marts 2018.¹⁷⁶ Det må således udledes, at Facebook har afholdt offentligheden fra at få kendskab til sagen i omtrent tre år. Derudover fremgår det ligeledes af et brev, som Facebook har sendt til Christopher Wylie i 2016, at virksomheden havde kendskab til, at disse informationer var blevet udnyttet på en måde, der havde krænket de registreredes persondataretlige rettigheder.¹⁷⁷ Derved foreligger der allerede et tilstrækkeligt grundlag til at antage, at Facebook skulle have givet denne underretning.

Facebook fastholdte indledningsvist, at de ikke indberettede sikkerhedsbruddet, fordi de ikke mente, at man var forpligtet til at give denne underretning.¹⁷⁸ Denne forklaring bliver dog ændret, da Zuckerberg afgav forklaring til den amerikanske kongres. ”*When we learned in 2015 that Cambridge Analytica had bought data from*

¹⁷³ se Tranberg, et al., 2017 s. 152.

¹⁷⁴ Jf. GDPR art. 4, nr. 12.

¹⁷⁵ Cadwalladr & Graham-Harrison, 2018: *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*

¹⁷⁶ Schroepfer, 2018: *An Update on Our Plans to Restrict Data Access on Facebook*

¹⁷⁷ Wylie, 2018: *Christopher Wylie: Why I broke the Facebook data story – and what should happen now*

¹⁷⁸ Cadwalladr & Graham-Harrison, 2018: *How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool*

*an app developer on Facebook that people had shared it with, we did take action. We took down the app, and we demanded that both the app developer and Cambridge Analytica delete and stop using any data that they had. They told us that they did this. In retrospect, it was clearly a mistake to believe them... Senator, when we heard back from Cambridge Analytica that they had told us that they weren't using the data and had deleted it, we considered it a closed case. In retrospect, that was clearly a mistake.*¹⁷⁹

Zuckerberg erkender således, at Facebook har begået fejl i forbindelse med håndteringen af denne sag. Dog kommer denne erkendelse først adskillige år efter, at virksomheden fik kendskab til sagen. Hvis disse omstændigheder ikke er skærpende nok i sig selv, så anfører journalisterne bag den oprindelige historie om Cambridge Analytica, at Facebook brugte store mængder af ressourcer på at modarbejde publikationen af denne historie til det sidste.¹⁸⁰ I dette lys fremstår Zuckerbergs undskyldning i april utroværdig. Det må ligeledes antages, at den adfærd som virksomheden har udvist, er direkte i modstrid med det generelle princip om transparens i artikel 5(1). Det må derfor samlet set konkluderes, at Facebooks ageren, i denne sag, har været særdeles kritisabel og i strid med god databehandlingskik.

¹⁷⁹ Bloomberg Government, 2018: *Transcript of Mark Zuckerberg's Senate hearing*

¹⁸⁰ Adams, 2018: *Facebook's week of shame: the Cambridge Analytica fallout*

Kapitel V. Sanktionsmuligheder

Formålet med dette kapitel vil være at udlede, om Cambridge Analytica og Facebook kan sanktioneres for de lovovertrædelser, der er blevet udledt i de tidligere afsnit. Indledningsvist vil der redegøres for de konkrete sanktionsmuligheder og hvordan disse skal udmåles. Derefter vil virksomhedernes konkrete strafansvar vil blive vurderet. Det blev beskrevet tidligt i fremstillingen, at det største problem under det gamle paradigme var manglen på effektive håndhævelsesmuligheder.¹⁸¹

Den eneste sanktionsmulighed der er fuldt ud harmoniseret i Forordningen, vedrører den administrative bødestraf.¹⁸² Det retsstridige forhold skal dog have en vis grovhed, før den administrative bødestraf kan tages i brug.¹⁸³ Der er endvidere hjemmel i Forordningen til, at medlemsstaterne kan indføre andre sanktionsmuligheder, men disse vil således variere alt efter, hvilken kurs den enkelte medlemsstat ønsker at gå.¹⁸⁴ Det fremgår eksempelvis af lovforslaget til den danske databeskyttelseslov, at diverse lovovertrædelser af Forordningens bestemmelser kan straffes med bøde eller fængsel op til 6 måneder.¹⁸⁵

Det angives i Forordningen, at tilsynsmyndighederne skal sikre, at der uddeles administrative bøder, såfremt bestemmelserne krænkes.¹⁸⁶ Disse sanktioner skal være *effektive, rimelige* i forhold til *overtrædelserne* og have *afskrækkende virkning*. Når selve strafudmålingen skal foretages, vil dette bero på de hensyn, som er angivet i artikel 83(2)(a-k):

- a. *”overtrædelsens karakter, alvor og varighed under hensyntagen til pågældende behandlings karakter, omfang eller formål samt antal registrerede, der er berørt, og omfanget af den skade, som de har lidt*
- b. *hvorvidt overtrædelserne blev begået forsætligt eller uagtsomt*
- c. *eventuelle foranstaltninger, der er truffet af den dataansvarlige eller databehandleren for at begrænse den skade, som den registrerede har lidt”*¹⁸⁷

Disse hensyn udgør således en række af de momenter, der kan anvendes i udmålingen af bødestraffen. Bestemmelsen opstiller flere hensyn, men de anførte er de mest relevante for denne fremstilling. Forordningen opsætter ligeledes konkrete

¹⁸¹ se eksempelvis Blume, 2016: Den nye persondataret s. 162.

¹⁸² Jf. GDPR art. 83, stk. 1.

¹⁸³ se Blume, 2016: Den nye persondataret s. 162.

¹⁸⁴ Jf. GDPR art. 84, stk. 1. Se herved L68 (2017-2018) om den danske implementering.

¹⁸⁵ Jf. § 41 i L68 – Forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)

¹⁸⁶ Jf. GDPR art. 83, stk. 1.

¹⁸⁷ Jf. GDPR art. 83, stk. 2, litra a-c.

sanktionsniveauer, hvilket betyder, at dette forhold bliver harmoniseret fremadrettet i EU.

Den mest betydningsfulde ændring af retstillingen, med Forordningens ankomst, er det voldsomme spring i bødesatserne. Under det gamle paradigme ville en grov sag blive sanktioneret med en bøde på 25.000 kr. i Danmark.¹⁸⁸ Derimod kan alle overtrædelser af Forordningens bestemmelser straffes med administrative bøder på op til 10.000.000 EUR eller 2 % af en virksomheds globale omsætning, såfremt denne er højere.¹⁸⁹ Vedrører lovovertrædelsen bl.a. de grundlæggende behandlingsprincipper i artikel 5, 6, 7 og 9, bliver den mest byrdefulde bødestraf aktiveret.¹⁹⁰ Den dataansvarlige kan i denne situation straffes med 20.000.000 EUR eller 4 % af den globale årlige omsætning, såfremt denne er højere.¹⁹¹

1. Facebook

Det kan indledningsvist konstateres, at det er besværligt at udlede nogen forhold i sagen, der kan betragtes som formildende omstændigheder. Undersøgelsen har derimod frembragt adskillige forhold, der kan anses som skærpene omstændigheder. Det er påvist, at oplysninger som Facebook har været ansvarlig for, er blevet viderebehandlet på en måde, som er uforenelig med de grundlæggende behandlingsprincipper i artikel 5(1-2). Derudover er der tale om særdeles personfølsomme informationer, der er beskyttet efter artikel 9. Det er beskrevet i artikel 83(5)(a), at den strengeste sanktionsmulighed i Forordningen bliver aktiveret, såfremt der er tale om overtrædelser af de grundlæggende principper for behandling, herunder betingelserne for samtykke i artikel 5, 6, 7 og 9. Det kan således allerede på det foreliggende grundlag udledes, at Forordningens strengeste sanktionsmulighed er anvendelig.

Det angives indledningsvist i artikel 83(1), at sanktionen skal være rimelig i forhold til overtrædelsen. Derudover må den specifikke udmåling af bødestrafen bero på de momenter, som er angivet i artikel 83(2). Det er vanskeligt at udlede, hvordan sagens faktum kan være mere alvorlig i et persondataretligt perspektiv, end tilfældet er her. Facebook er en virksomhed, der er ansvarlig for 2.2 mia. Facebook-brugeres følsomme datamateriale. Virksomheden indsamler personoplysningerne for at udnytte den kommercielle værdi af disse informationer. Selskabet har dog udviklet

¹⁸⁸ se s. 941 i Justitsministeriets Betænkning nr. 1565 del 1, bind 2.

¹⁸⁹ Jf. GDPR art. 83, stk. 4.

¹⁹⁰ Jf. GDPR art. 83, stk. 5, litra a.

¹⁹¹ Jf. GDPR art. 83, stk. 5, litra a-e.

værktøjer, der har gjort disse oplysninger sårbare over for angreb samt ulovlig databehandling. Som en konsekvens af virksomhedens manglende prioritering af datasikkerhed er 87 mio. Facebook-brugeres personoplysninger blevet lækket til en uautoriseret tredjepart.

Facebook har således været bevidste om, at Cambridge Analytica databehandlede personoplysninger, der var blevet lækket fra deres platform. Virksomheden har også været klar over, at Cambridge Analytica viderebehandlede disse oplysninger til politiske og kommercielle formål, hvilket ligeledes er i strid med Facebooks egne generelle tjenestevilkår. Alligevel har Facebook forholdt sig passivt i forhold til at underrette de relevante tilsynsmyndigheder samt omfattede brugere. Til sidst forsøgte virksomheden ligeledes at mørklægge sagen, selvom Facebook allerede havde holdt de faktuelle omstændigheder i sagen hemmelige i tre år. Det må derfor lægges til grund, at der er en reel sandsynlighed for, at Facebook bliver idømt den strengeste administrative bødestraf, som Forordningen tillader. Dette bygger stadig på den forudgående antagelse om, at sagens faktum bliver afgjort efter bestemmelserne i Forordningen. Håndhævelsen vil dog forudsætte, at Facebook fastholder sit irske selskab. Bliver det europæiske datterselskab nedlagt, er det svært at udlede, hvilke retsmidler der kan gennemtvinge et juridisk krav mod Facebook, der således udelukkende vil være etableret i USA.

2. Cambridge Analytica

Det blev i kapitel III konkluderet, at Cambridge Analytica fuldstændigt havde ignoreret de persondataretlige regler i forbindelse med deres databehandling. Der kan således ikke være nogen tvivl om, at virksomheden har handlet i strid med de almindelige behandlingsprincipper i artikel 5, 6 og 9. Af denne årsag risikerer Cambridge Analytica ligeledes at modtage den strengeste administrative bødestraf efter 83(5). Dog er problemstillingen vedrørende effektiv retshåndhævelse blevet mere kompliceret, eftersom virksomheden har indgivet en konkursbegæring d. 2. maj 2018.¹⁹²

Derudover er selskabet 'SCL Elections', der indgik den oprindelige aftale med Kogan, ligeledes omfattet af konkursen. Det er uvist på nuværende tidspunkt, om beslutningstagerne i koncernen 'SCL Group' har til hensigt at lukke alle selskaberne eller om enkelte forbliver aktive. Det efterlader spørgsmålet om, hvorvidt der

¹⁹² Cambridge Analytica, 2018: *Cambridge Analytica and Scl Elections Commence Insolvency Proceedings and Release Results of Independent Investigation into Recent Allegations*

overhovedet er et retssubjekt, som kan holdes ansvarlig for Cambridge Analytics aktiviteter efter de specifikke bestemmelser i det persondataretlige retsgrundlag.

En række britiske og amerikanske advokater har rejst påstand om at holde Facebook og koncernen SCL Group ansvarlige for de konkrete aktiviteter. De har dermed oprettet et gruppesøgsmål mod Facebook og SCL Group i USA.¹⁹³ Forordningen hverken hjemler eller forbyder muligheden for at foretage et gruppesøgsmål.¹⁹⁴ Det er derfor de nationale regler, der regulerer dette forhold. Der er dog reel bekymring om, at opløsningen har til formål at hindre den britiske efterforskning af sagen. Dette er ikke uden betydning, da Cambridge Analytics forhenværende ledelse allerede skulle have etableret sig i en anden entitet, Emerdata.¹⁹⁵ Der kan endvidere være en formodning om, at disse individer fortsat er i besiddelse af det ulovlige datamateriale, da det er umuligt at spore datamateriale af denne karakter.

Det er efter Forordningen den dataansvarlige, som bærer ansvaret for behandlingen af personoplysninger.¹⁹⁶ Efter formuleringen i art 4(7) kan fysiske personer godt bære dette ansvar, dog vil virksomheder eller organisationer som helhed bære dette ansvar, hvis det er muligt. Dette synspunkt underbygges endvidere af følgende beskrivelse af afgrænsningen i forhold til det relevante pligtsubjekt: *"Den dataansvarlige er ikke en bestemt person i myndigheden eller virksomheden mv., men derimod selve myndigheden eller virksomheden."*¹⁹⁷ I manglen af praksis der kan angive, hvordan dette forhold skal afgøres, er det svært at nå en definitiv konklusion. Det er således uvist på nuværende tidspunkt om denne 'finte' succesfuldt kan anvendes til at omgå Forordningens sanktionsmuligheder. Den britiske tilsynsmyndighed har dog afgivet følgende udtalelse efter konkursbegæringen: *"The ICO will continue its civil and criminal investigations and will seek to pursue individuals and directors, as appropriate and necessary even where companies may no longer be operating. We will also monitor closely any successor companies using our powers to audit and inspect, to ensure the public is safeguarded."*¹⁹⁸ Baseret på denne udmelding kan det udledes, at ICO holder alle muligheder åbne og tiden vil vise, hvilke sanktionsmuligheder myndigheden vil tage i brug.

Viser det sig, at der ikke er hjemmel til at sanktionere Cambridge Analytica og den ansvarlige ledelse for disse lovovertrædelser, vil dette udgøre et alvorligt problem på

¹⁹³ Bowcott & Hern, 2018: *Facebook and Cambridge Analytica face class action lawsuit*

¹⁹⁴ se Blume, 2016: *Den nye persondataret* s. 160.

¹⁹⁵ Cadwalladr, 2018: *Cambridge Analytica has gone. But what has it left in its wake?*

¹⁹⁶ Jf. GDPR art. 4, nr. 7.

¹⁹⁷ Se Lotterup, 2016: *Karnovs note 31 til GDPR*.

¹⁹⁸ Information Commissioner's Office, 2018: *ICO statement: investigation into data analytics for political purposes*

sigt. Det har aldrig været formålet med Cambridge Analytica at skabe en profitabel forretning. Målet har derimod fra starten været at sikre politisk indflydelse.¹⁹⁹ Derfor vil det være nødvendigt at sikre et effektivt rettsværn overfor denne form for aktivitet uanset udfaldet af denne sag.

¹⁹⁹ Cadwalladr, 2018: *'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower*

Kapitel VI. Konklusion

Formålet med denne fremstilling har været at besvare følgende overliggende problemstilling: *'Har henholdsvis Facebook og Cambridge Analytica handlet i strid med persondataforordningens bestemmelser, og kan de eventuelt sanktioneres som følge af denne sag?'*

I bestræbelserne på at besvare denne problemstilling blev det indledningsvist vurderet, hvorvidt sagens faktum opfylder Forordningens materielle samt formelle betingelser. Forordningen afgrænses materielt ved, at den finder anvendelse ved enhver databehandling af personoplysninger.²⁰⁰ Behandlingskriteriet kunne påvises at være opfyldt i sagen, da Cambridge Analytica har anvendt profileringsmetoden til at udlede sammenhænge om vælgergrupper.²⁰¹ Derudover kunne det også udledes, at Facebook-profiler indeholder informationer, der både kan betegnes som almindelige samt følsomme personoplysninger. Det kan således påvises, at begge led i den materielle vurdering er opfyldt. Derudover kan det konstateres, at begge virksomheders aktiviteter skal vurderes efter den skærpende bestemmelse artikel 9, da datamaterialet indeholder personfølsomme oplysninger. Dernæst har det været nødvendigt at påvise, at Cambridge Analytica og Facebook er pligtsubjekter i nærværende sag. Det kunne således påvises, at disse virksomheder besidder ansvaret som dataansvarlig i sagen.²⁰² Facebook og Cambridge Analytica er ligeledes begge omfattet af Forordningens territoriale afgrænsning, da begge virksomheder er etableret inden for Unionens område.²⁰³ Det kan således konstateres, at Forordningen er anvendelig i denne sag.

Dernæst har det været nødvendigt at undersøge, hvorvidt Facebook og Cambridge Analytica har handlet i overensstemmelse med Forordningens bestemmelser. Indledningsvist blev det afvist, at de 87 mio. Facebook-brugere har opgivet den persondataretlige beskyttelse ved at offentliggøre oplysningerne på Facebook.²⁰⁴ En sådan opgivelse må dog antages at foreligge, såfremt Facebook-brugeren har en 'åben' profil eller et stort antal af Facebook-venner, hvilket ikke kunne antages at være tilfældet for samtlige 87 mio. profiler. Dernæst viste den konkrete undersøgelse af Cambridge Analyticas aktiviteter, at virksomheden ikke har tilegnet sig et lovligt behandlingsgrundlag, der kan begrunde den konkrete databehandling. Virksomheden har derved handlet i strid med persondatarettens grundlæggende

²⁰⁰ Jf. GDPR art. 2, stk. 1.

²⁰¹ Jf. GDPR art. 4, nr. 4.

²⁰² Jf. GDPR art. 4, nr. 7.

²⁰³ Jf. GDPR art. 3, stk. 1.

²⁰⁴ Jf. GDPR art. 9, stk. 2, litra e.

behandlingsprincipper.²⁰⁵ Dette er både tilfældet for de brugere, der anvendte Kogans applikation og de Facebook-venner, som ligeledes blev opslugt i indsamlingsprocessen af Facebook-data.

Undersøgelsen har ligeledes vist, at Facebook har handlet i strid med persondataforordningens forskrifter. I den konkrete sag har virksomheden fejlet i at sikre et passende sikkerhedsniveau, hvorved brugernes personoplysninger har været underlagt en vis grad af datasikkerhed.²⁰⁶ Dette mangelfulde sikkerhedsniveau er hovedårsagen til, at Cambridge Analytica har været i stand til at komme i besiddelse af data på 87 mio. brugere. Derudover blev det ligeledes påvist, at virksomheden også fejlede i at give underretning efter, at den fik kendskab til den ulovlige viderebehandling.²⁰⁷ Denne ulovlige viderebehandling er endvidere i strid med Facebooks egne brugervilkår, der angiver, at virksomheden ikke videregiver brugernes informationer uden deres specifikke samtykke. Dermed har Facebook ligeledes misligholdt den kontrakt, der er indgået med de omfattede brugere. Facebook har også forsøgt at mørklægge sagen, hvorved det ligeledes må konkluderes, at de har handlet i strid med persondataforordningens generelle krav om transparens.²⁰⁸

Afslutningsvist blev det vurderet, om virksomhederne risikerer at blive sanktioneret som følge af sagen. Det kan således udledes, at begge virksomheders aktiviteter udløser den mest byrdefulde sanktion i Forordningen.²⁰⁹ Den aktiveres i den situation, hvor lovovertrædelsen er positivt opregnet i bestemmelsen. I denne situation har både Facebook og Cambridge Analytica handlet i strid med de grundlæggende behandlingsprincipper i Forordningen. Forordningen angiver ligeledes, hvilke momenter der skal inddrages i udmålingen af en administrativ bødestrafs størrelse. I denne vurdering må det udledes, at undersøgelsen udelukkende har belyst forhold, der kan betragtes som skærpende omstændigheder. Sagens omfang og generelle karakter må således skabe en formodning om, at den videste sanktionsmulighed er en reel mulighed. Dog skaber Cambridge Analyticas konkurs en række tvivlsspørgsmål i forhold til, hvordan personerne bag de ulovlige aktiviteter fortsat kan sanktioneres. Dette kan ikke besvares entydigt i denne fremstilling, og derfor vil det blive interessant at følge de relevante tilsynsmyndigheders behandling af sagen, som den skrider frem.

²⁰⁵ Jf. GDPR art. 5, stk. 1-2, art. 6 og art. 9.

²⁰⁶ Jf. GDPR art. 32.

²⁰⁷ Jf. GDPR art. 33-34 og art. 5, stk. 2.

²⁰⁸ Jf. GDPR art. 5, stk. 1.

²⁰⁹ Jf. GDPR art. 83, stk. 5.

Kapitel VII. Perspektivering

I dette afsluttende kapitel vil der kommenteres på en række af de generelle problemstillinger, der er blevet observeret i løbet af udfærdigelsen af dette speciale. Indledningsvist skal det dog bemærkes, at persondataforordningen utvivlsomt må betragtes som et skridt i den rigtige retning i forsøget på at skabe en nogenlunde regulering af det persondataretlige retsområde. Det er dog fortsat vigtigt at videreudvikle den ramme, der nu er skabt.

Først og fremmest kan det diskuteres, om det overhovedet er ønskværdigt, at data-mining processen må anvendes til politiske formål. Cambridge Analytica-sagen belyser den alvorlige natur af disse bestræbelser, såfremt processerne rettes mod vores demokratiske institutioner.²¹⁰ Det indbyggede grænseoverskridende element i problematikken vedrørende behandling af personoplysninger bevirker, at det ikke kan overlades til hver enkelt medlemsstat at forbyde denne særlige behandlingsform. Det vil således være ideelt, hvis et eventuelt forbud vedtages på EU-niveau. Alternativt vil der opstå en situation, hvor der kan 'shoppes' efter de mest gunstige vilkår. Derved vil dette forhold blive en konkurrenceparameter, der kan drage den næste Cambridge Analytica til en medlemsstat med en lempelig regulering. I takt med at den kunstige intelligens bliver mere sofistikeret, bliver denne overliggende problemstilling tilsvarende mere relevant og derved øges beskyttelsesbehovet for en skærpet regulering. Det britiske datatilsyn 'ICO' lader til at dele denne vurdering. Tilsynsmyndigheden har således allerede bekendtgjort, at der indledes en bredere efterforskning, der har til formål at afdække, hvordan dataanalysevirksomheder anvender personoplysninger til politiske formål.²¹¹

Afsluttende er der forholdet om den manglende transparens, der besværliggør tilsynsmyndighedernes muligheder for at føre tilsyn med de dataansvarlige. I bestræbelserne på at komme nogen af disse generelle problemstillinger til livs, kan det ud fra et virkningssynspunkt være hensigtsmæssigt at skabe mere effektive redskaber, der kan forbedre den generelle grad af gennemsigtighed. I den omhandlende sag lykkedes det Facebook og Cambridge Analytica at mørklægge datalekket og den ulovlige behandling i flere år, før tilsynsmyndighederne fik kendskab til sagen. Forordningen indfører adskillige tiltag, der har til formål at øge den dataansvarliges incitament til at handle i overensstemmelse med de pålagte pligter. Eksempelvis gælder der et præsumptionsansvar i række tilfælde, hvor den dataansvarlige skal kunne dokumentere, at der foreligger et lovligt grundlag, der

²¹⁰ Hinsliff, 2018: *Cambridge Analytica may be guilty of hype. But data mining poisons our politics*

²¹¹ Information Commissioner's Office, 2018: *ICO statement: investigation into data analytics for political purposes*

begrunder den konkrete databehandling.²¹² Dette er sandsynligvis det rette udgangspunkt. Dette kan fortsat suppleres af andre forhold, der kan forhindre misbrug. Ligesom det er udviklingen i teknologi, der har skabt en række af disse problemstillinger, kan teknologien ligeledes anvendes til at skabe de tilstræbte løsninger.

Blockchain nævnes som en særdeles lovende og revolutionerende teknologi, der har potentialet til at være i stand til at adressere en række af disse identificerede problemstillinger. De fleste personer har sandsynligvis kun hørt om Blockchain-teknologien i spekulationsøjemed, da det er blevet et fænomen at investere i kryptovalutaer som eksempelvis bitcoin.²¹³ Teknologien rummer dog en række særdeles interessante muligheder, der ligeledes er tiltrækkende i et juridisk perspektiv.²¹⁴ *”Put simply, a blockchain is a transaction-recording computer database that’s stored in many different places at once. In a sense, it’s like a public bulletin board where people can post notices of transactions. Each post must be accompanied by a digital signature, and can never be changed or deleted.”*²¹⁵ Der er grundlag for at formode, at Blockchain-teknologien har potentialet til at forebygge mod misbrug ved at forbedre den generelle grad af transparens. Hvis vi eksempelvis forudsætter, at personoplysninger kun befinder sig i en database, der knytter sig til denne teknologi, vil enhver transaktion eller behandling af denne information kunne spores. *”Blockchain rummer så mange muligheder, at det er vigtigt ikke at se teknologien i et ensidigt perspektiv. Teknologien kan hjælpe især den offentlige sektor, til at sætte de mange data-registreringer ind i et effektivt system, som vil kunne afsløre misbrug mv.”*²¹⁶

Hvis de principper som er kendetegnende for Blockchain-teknologien kan overføres til at beskytte personoplysninger på platforme som Facebook, vil dette sandsynligvis løse en række af de mest alvorlige praktiske problemer i det nuværende persondataretlige økosystem. Det er ikke nemt at beskrive det fulde potentiale i Blockchain-teknologien, da det hurtigt bliver meget teknisk og kompliceret. Dog kan man forestille sig en situation, hvor Facebook er forpligtet til at programmere enhver personoplysning, der er på platformen efter beskyttelsesbehovet udtrykt i de relevante retskilder. I denne situation kan systemet øjeblikket ’notificere’, hvis en konkret part uautoriseret eller ulovligt behandler den konkrete oplysning. Systemet

²¹² Jf. fx GDPR art. 7, stk. 1.

²¹³ Alam & Kendall, 2017: *Now that bitcoins are worth more than their weight in gold, is it time for central banks to make their own?*

²¹⁴ Hall, 2016: *How Blockchain could help us take back control of our privacy*

²¹⁵ Kshetri, 2018: *Using blockchain to secure the ‘internet of things’*

²¹⁶ se Haarup, 2018: *Blockchain - Den digitale disruption af revisionsbranchen?*

vil således kunne vurdere, om der foreligger et tilstrækkeligt samtykke til, at den konkrete databehandler må tilgå informationen. Såfremt subjektet ulovligt behandler oplysningen, vil tilsynsmyndighederne næsten øjeblikkeligt tilegne sig kendskab til dette faktum.

Afslutningsvist må det dog konstateres, at der fortsat er lang vej, før teknologien er moden nok til at overføre dette perspektiv til den praktiske virkelighed. På sigt kan perspektiverne i denne teknologi imidlertid sikre et særdeles effektivt retsværn i kampen mod misbrug af data.

Bibliografi

Litteratur

- Adams, T. (24. Marts 2018). *Facebook's week of shame: the Cambridge Analytica fallout*. Hentet fra The Guardian: <https://www.theguardian.com/technology/2018/mar/24/facebook-week-of-shame-data-breach-observer-revelations-zuckerberg-silence>
- Alam, N., & Kendall, G. (9. Marts 2017). *Now that bitcoins are worth more than their weight in gold, is it time for central banks to make their own?* Hentet fra The Conversation : <https://theconversation.com/now-that-bitcoins-are-worth-more-than-their-weight-in-gold-is-it-time-for-central-banks-to-make-their-own-73984>
- Appendix I. (2018). *General Terms of Usage*. Facebook.
- Appendix II. (4. Juni 2014). *Aftale mellem Kogan og SCL (Cambridge Analytica)*.
- Appendix III. (2014). *Terms and Conditions - Kogan App*.
- Artikel 29-Gruppen. (Marts 2013). *Opinion 03/2013 on purpose limitation*.
- Artikel 29-Gruppen. (11. April 2018). *Press release on Facebook*. Hentet fra http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=621779
- Batchelor, O., & Nissen, M. (6. April 2018). *Datatilsynet overlader "høst" af danske facebook-profiler til britiske kolleger*. Hentet fra DR: <https://www.dr.dk/nyheder/penge/datatilsynet-overlader-hoest-af-danske-facebook-profiler-til-britiske-kolleger>
- BBC. (9. April 2018). *Facebook data: How it was used by Cambridge Analytica*. Hentet fra <http://www.bbc.com/news/av/technology-43674480/facebook-data-how-it-was-used-by-cambridge-analytica>
- Berreby, D. (3. Marts 2017). *Click to agree with what? No one reads terms of service, studies confirm*. Hentet fra The Guardian: <https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print>
- Bloomberg Government. (10. April 2018). *Transcript of Mark Zuckerberg's Senate hearing*. Hentet fra The Washington Post: https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.372c6d2763b7
- Blume, P. (2016). *Den nye persondataret* (1. udg.). Jurist- og Økonomforbundets Forlag.
- Blume, P. (2016). Formålsbestemthed. *Ugeskrift for Retsvæsen*, s. U.2016B.338.
- Blume, P. (2016). *Retssystemet og Juridisk Metode* (3 udg.). Jurist- og Økonomforbundets Forlag.
- Bowcott, O., & Hern, A. (10. April 2018). *Facebook and Cambridge Analytica face class action lawsuit* . Hentet fra The Guardian: <https://www.theguardian.com/news/2018/apr/10/cambridge-analytica-and-facebook-face-class-action-lawsuit>
- Cadwalladr, C. (18. Marts 2018). *'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower*. Hentet fra The Observer : <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>
- Cadwalladr, C. (6. Maj 2018). *Cambridge Analytica has gone. But what has it left in its wake?* . Hentet fra The Observer : <https://www.theguardian.com/uk-news/2018/may/06/cambridge-analytica-gone-what-has-it-left-in-its-wake>

- Cadwalladr, C. (22. Marts 2018). Cambridge Analytica, Facebook and democracy – Politics Weekly podcast. (T. Guardian, Interviewer)
- Cadwalladr, C. (4. April 2018). *Revealed: graphic video used by Cambridge Analytica to influence Nigerian election*. Hentet fra The Guardian : <https://www.theguardian.com/uk-news/2018/apr/04/cambridge-analytica-used-violent-video-to-try-to-influence-nigerian-election>
- Cadwalladr, C. (5. Maj 2018). *UK regulator orders Cambridge Analytica to release data on US voter*. Hentet fra The Guardian: <https://www.theguardian.com/uk-news/2018/may/05/cambridge-analytica-uk-regulator-release-data-us-voter-david-carroll>
- Cadwalladr, C., & Graham-Harrison, E. (17. Marts 2018). *How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool*. Hentet fra The Guardian: <https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm>
- Cadwalladr, C., & Graham-Harrison, E. (17. Marts 2018). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. Hentet fra The Guardian: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- Cambridge Analytica. (2. Maj 2018). *Cambridge Analytica and Scl Elections Commence Insolvency Proceedings and Release Results of Independent Investigation into Recent Allegations*. Hentet fra <https://ca-commercial.com/news/cambridge-analytica-and-scl-elections-commence-insolvency-proceedings-and-release-results-3>
- Cambridge Analytica. (14. April 2018). *We find your voters and move them to action*. Hentet fra Cambridge Analytica, Political : https://ca-political.com/?__hstc=163013475.171c12aad48ce40fdbf5flc620f03276.1523699889182.1523699889182.1523699889182.1&__hssc=163013475.1.1523699889185&__hsfp=2431616790
- Cook, T. (28. Marts 2018). Apple CEO Tim Cook Slams Facebook's Mark Zuckerberg: I Wouldn't Be In This Situation. (MSNBC, Interviewer)
- Datatilsynet. (14. November 2016). *Artikel 29-gruppen*. Hentet fra <https://www.datatilsynet.dk/om-datatilsynet/internationalt/artikel-29-gruppen/>
- Datatilsynet. (13. April 2018). *Fælles europæisk reaktion på sagen om Cambridge Analytica og Facebook*. Hentet fra <https://www.datatilsynet.dk/nyheder/nyhed/artikel/faelles-europaisk-reaktion-paa-sagen-om-cambridge-analytica-og-facebook/>
- EDPS. (2018). *Glossary* . Hentet fra https://edps.europa.eu/data-protection/data-protection/glossary/a_en
- Erhvervsstyrelsen. (April 2018). *Corporate Governance*. Hentet fra <https://corporategovernance.dk/corporate-governance>
- Evald, J. (2000). *Retskilderne og den juridiske metode* (2 udg.). Jurist- og Økonomforbundets Forlag.
- Evald, J. (2016). *Juridisk Teori, Metode og Videnskab* (1 udg.). Jurist- og Økonomforbundets Forlag.
- Facebook. (2. Maj 2018). *Facebook's commitment & preparation for GDPR*. Hentet fra <https://www.facebook.com/business/gdpr>
- Facebook. (19. April 2018). *Hvordan beslutter Facebook, hvilke annoncer jeg skal se, og hvordan kan jeg bestemme, hvilke annoncer jeg ser?* Hentet fra Facebook Annoncepræferencer : <https://www.facebook.com/help/562973647153813?helpref=related>

- Farrell, H., & Newman, A. (12. April 2018). *Forget Congress. Facebook's real problem is in Europe*. Hentet fra The Washington Post : https://www.washingtonpost.com/news/monkey-cage/wp/2018/04/12/forget-congress-facebooks-real-problem-is-in-europe/?utm_term=.ef93a09c5f13
- Finans. (13. Oktober 2008). *Datatilsynet: Nej til kulegravning af Facebook-vilkår*. Hentet fra <https://finans.dk/artikel/ECE4055250/Datatilsynet:-Nej-til-kulegravning-af-Facebook-vilk%C3%A5r/?ctxref=ext>
- Folketinget. (3. Maj 2018). *L 68 Forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger*. Hentet fra <http://www.ft.dk/samling/20171/lovforslag/168/index.htm>
- Hall, J. (21. Marts 2016). *How Blockchain could help us take back control of our privacy*. Hentet fra The Guardian: <https://www.theguardian.com/commentisfree/2018/mar/21/blockchain-privacy-data-protection-cambridge-analytica>
- Hartmans, A. (22. Marts 2018). *It's impossible to know exactly what data Cambridge Analytica scraped from Facebook — but here's the kind of information apps could access in 2014*. Hentet fra Business Insider : <http://nordic.businessinsider.com/what-data-did-cambridge-analytica-have-access-to-from-facebook-2018-3>
- Hern, A. (16. April 2018). *Cambridge Analytica scandal 'highlights need for AI regulation'*. Hentet fra The Guardian : <https://www.theguardian.com/technology/2018/apr/16/cambridge-analytica-scandal-highlights-need-for-ai-regulation>
- Hern, A. (19. April 2018). *Facebook moves 1.5bn users out of reach of new European privacy law*. Hentet fra The Guardian : <https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law>
- Hern, A. (12. Februar 2018). *Facebook personal data use and privacy settings ruled illegal by German court*. Hentet fra The Guardian : <https://www.theguardian.com/technology/2018/feb/12/facebook-personal-data-privacy-settings-ruled-illegal-german-court>
- Hern, A., & Cadwalladr, C. (13. April 2018). *Revealed: Aleksandr Kogan collected Facebook users' direct messages*. Hentet fra The Guardian : <https://www.theguardian.com/uk-news/2018/apr/13/revealed-aleksandr-kogan-collected-facebook-users-direct-messages>
- Hern, A., & Sabbagh, D. (27. Marts 2018). *Zuckerberg's refusal to testify before UK MPs 'absolutely astonishing'*. Hentet fra The Guardian : <https://www.theguardian.com/technology/2018/mar/27/facebook-mark-zuckerberg-declines-to-appear-before-uk-fake-news-inquiry-mps>
- Hinsliff, G. (20. Marts 2018). *Cambridge Analytica may be guilty of hype. But data mining poisons our politics*. Hentet fra The Guardian : <https://www.theguardian.com/commentisfree/2018/mar/20/cambridge-analytica-data-mining-democracy-channel-4>
- Holst-Christensen, N. (2013). *Skriftlig Jura - Den Juridiske Fremstilling*. Ex Tuto Publishing .
- Hull, G. (27. April 2018). *The internet is designed for corporations, not people*. Hentet fra The Conversation : <https://theconversation.com/the-internet-is-designed-for-corporations-not-people-95030>
- Haarup, N. (2. Maj 2018). *Blockchain - Den digitale disruption af revisionsbranchen? Revision & Regnskabsvæsen*, s. RR.5.2018.50.

- ICO. (5. Maj 2018). *ICO serves Enforcement Notice on SCL Elections Ltd over inadequate response to subject access request*. Hentet fra <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/ico-serves-enforcement-notice-on-scl-elections-ltd/>
- Information Commissioner's Office. (2. Maj 2018). *ICO statement: investigation into data analytics for political purposes*. Hentet fra ICO: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/ico-statement-investigation-into-data-analytics-for-political-purposes/>
- Ingram, D. (19. April 2018). *Exclusive: Facebook to put 1.5 billion users out of reach of new EU privacy law*. Hentet fra Reuters : <https://www.reuters.com/article/us-facebook-privacy-eu-exclusive/exclusive-facebook-to-put-1-5-billion-users-out-of-reach-of-new-eu-privacy-law-idUSKBN1HQooP>
- Jolly, L. (1. Juli 2017). *Data protection in the United States: overview*. Hentet fra Thomsom Reuters - Pratical Law : [https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?originationContext=document&transitionType=DocumentItem&contextData=\(sc.Default\)#co_anchor_a233354](https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)#co_anchor_a233354)
- Joseph, S. (2. April 2018). *Why the business model of social media giants like Facebook is incompatible with human rights*. Hentet fra The Conversation : <https://theconversation.com/why-the-business-model-of-social-media-giants-like-facebook-is-incompatible-with-human-rights-94016>
- Justitsministeriet. (2017). *Betækning nr. 1565 om Databeskyttelsesforordningen - og de retlige rammer for dansk lovgivning* .
- Khan, A. (26. Januar 2014). *Explainer: what is big data?* Hentet fra The Conversation : <https://theconversation.com/explainer-what-is-big-data-13780>
- Kshetri, N. (7. Marts 2018). *Using blockchain to secure the 'internet of things'*. Hentet fra The Conversation : <https://theconversation.com/using-blockchain-to-secure-the-internet-of-things-90002>
- Larsen, T. B. (3. April 2017). De sociale mediers brugervilkår del II - værnetinget. *Erhvervsjuridisk Tidsskrift*, s. ET.2017.142.
- Larsen, T. B., & Feldthusen, R. K. (26. September 2016). De sociale mediers brugervilkår del I - aftalen. *Erhvervsjuridisk Tidsskrift*, s. ET.2016.266.
- Liem, C., & Petropoulos, G. (14. Januar 2016). *The economic value of personal data for online platforms, firms and consumers*. Hentet fra bruegel.org: bruegel.org/2016/01/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers/
- Lotterup, A. (27. April 2016). Europa-Parlamentets og Rådets forordning af 2016-04-27. *Karnovs Noter*.
- McNamee, R. (29. Januar 2017). *Why not regulate social media like tobacco or alcohol?* Hentet fra The Guardian: <https://www.theguardian.com/media/2018/jan/29/social-media-tobacco-facebook-google>
- Munk-Hansen, C. (2014). *Retsvidenskabsteori* (1 udg.). Jurist- og Økonomforbundets Forlag.
- Munk-Hansen, C. (2017). *Den Juridiske Løsning* (1 udg.). Jurist- og Økonomforbundets Forlag.
- Nissen, M., & Lehmann, C. (4. April 2018). *Cambridge Analytica kan have "høstet" 41.820 danskeres facebook-profil*. Hentet fra DR: <https://www.dr.dk/nyheder/viden/teknologi/cambridge-analytica-kan-have-hoestet-41820-danskeres-facebook-profil>
- Osborne, H. (18. Marts 2018). *What is Cambridge Analytica? The firm at the centre of Facebook's data breach*. Hentet fra The Guardian : <https://www.theguardian.com/news/2018/mar/18/what-is-cambridge-analytica-firm-at-centre-of-facebook-data-breach>

- (28. Marts 2018). Revealed: Cambridge Analytica data on thousands of Facebook users still not deleted. (Channel 4 News, Interviewer)
- Riley, M., Frier, S., & Baker, S. (9. April 2018). *Understanding the Facebook-Cambridge Analytica Story: QuickTake*. Hentet fra The Washington Post: https://www.washingtonpost.com/business/understanding-the-facebook-cambridge-analytica-story-quicktake/2018/04/09/0f18d91c-3c1c-11e8-955b-7d2e19b79966_story.html?noredirect=on&utm_term=.bc05051fee3d
- Ritzau. (22. Februar 2018). *Datatilsynet får kritik for at afvise Facebook-sag*. Hentet fra DR: <https://www.dr.dk/nyheder/viden/tech/datatilsynet-far-kritik-afvise-facebook-sag>
- Romm, T. (26. April 2018). *Facebook didn't read the terms and conditions for the app behind Cambridge Analytica*. Hentet fra The Washington Post : https://www.washingtonpost.com/news/the-switch/wp/2018/04/26/facebook-didnt-read-the-terms-and-conditions-for-the-app-behind-cambridge-analytica/?utm_term=.c3665b450d09
- Rosenberg, M. (19. Marts 2018). *Cambridge Analytica, Trump-Tied Political Firm, Offered to Entrap Politicians*. Hentet fra The New York Times : <https://www.nytimes.com/2018/03/19/us/cambridge-analytica-alexander-nix.html>
- Schroepfer, M. (4. April 2018). *An Update on Our Plans to Restrict Data Access on Facebook*. Hentet fra newsroom.fb.com: <https://newsroom.fb.com/news/2018/04/restricting-data-access/>
- Siegelman, W. (5. Maj 2018). *Cambridge Analytica is dead – but its obscure network is alive and well*. Hentet fra The Guardian: <https://www.theguardian.com/uk-news/2018/may/05/cambridge-analytica-scl-group-new-companies-names>
- Sinnreich, A., & Romzek, B. (11. April 2018). *To serve a free society, social media must evolve beyond data mining*. Hentet fra The Conversation: <https://theconversation.com/to-serve-a-free-society-social-media-must-evolve-beyond-data-mining-94704>
- Solon, O. (19. April 2018). *How Europe's 'breakthrough' privacy law takes on Facebook and Google*. Hentet fra The Guardian: <https://www.theguardian.com/technology/2018/apr/19/gdpr-facebook-google-amazon-data-privacy-regulation>
- Solon, O., & Laughland, O. (2. Maj 2018). *Cambridge Analytica closing after Facebook data harvesting scandal*. Hentet fra The Guardian: <https://www.theguardian.com/uk-news/2018/may/02/cambridge-analytica-closing-down-after-facebook-row-reports-say>
- Stahl, L. (22. April 2018). *Aleksandr Kogan: The link between Cambridge Analytica and Facebook*. Hentet fra 60 Minutes: <https://www.cbsnews.com/news/aleksandr-kogan-the-link-between-cambridge-analytica-and-facebook/>
- Statista. (Marts 2017). *Number of apps available in leading app stores as of March 2017*. Hentet fra <https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/>
- Statista. (2018). *Facebook's annual revenue and net income from 2007 to 2017 (in million U.S. dollars)*. Hentet fra <https://www.statista.com/statistics/277229/facebooks-annual-revenue-and-net-income/>
- Statista. (April 2018). *Most popular social networks worldwide as of April 2018, ranked by number of active users*. Hentet fra <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>
- Stewart, E. (11. April 2018). *The privacy question Mark Zuckerberg kept dodging*. Hentet fra Vox : <https://www.vox.com/policy-and-politics/2018/4/11/17225518/mark-zuckerberg-testimony-facebook-privacy-settings-sharing>

- Sørensen, K. E., Nielsen, P. R., & Danielsen, J. H. (2014). *EU-retten* (6 udg.). Jurist- og Økonomforbundets Forlag.
- Taylor, A. (21. Marts 2018). *Cambridge Analytica's reach went far beyond the U.S. elections*. Hentet fra The Washington Post : https://www.washingtonpost.com/news/worldviews/wp/2018/03/20/cambridge-analyticas-reach-went-far-beyond-the-u-s-elections/?utm_term=.ad6ede23b871
- The Guardian. (20. Marts 2018). *What is the Cambridge Analytica scandal?* Hentet fra The Guardian : <https://www.youtube.com/watch?v=Q9InvbJSmS4&feature=youtu.be>
- The Observer. (24. Marts 2018). *Democracy dies without transparency and fairness*. Hentet fra The Guardian: <https://www.theguardian.com/commentisfree/2018/mar/24/cambridge-analytica-brexit-vote-leave>
- Tranberg, C. B., Trzaskowski, J., Jakobsen, S. S., Karstoft, S., Kirk, H., Langsted, L. B., . . . Gudmundsdottir, H. L. (2017). *Internetretten* (3. udg.). Ex Tuto Publishing A/S.
- Verhulst, S. G., & Young, A. (23. Januar 2018). *How the Data That Internet Companies Collect Can Be Used for the Public Good*. Hentet fra Harvard Business Review : <https://hbr.org/2018/01/how-the-data-that-internet-companies-collect-can-be-used-for-the-public-good>
- Wade, M. (21. Marts 2018). *Psychographics: the behavioural analysis that helped Cambridge Analytica know voters' minds*. Hentet fra The Conversation: <https://theconversation.com/psychographics-the-behavioural-analysis-that-helped-cambridge-analytica-know-voters-minds-93675>
- Watson, C. (11. April 2018). *The key moments from Mark Zuckerberg's testimony to Congress*. Hentet fra The Guardian : <https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments>
- Weaver, M. (24. April 2018). *Cambridge University rejected Facebook study over 'deceptive' privacy standards*. Hentet fra The Guardian : <https://www.theguardian.com/technology/2018/apr/24/cambridge-university-rejected-facebook-study-over-deceptive-privacy-standards>
- Weaver, M. (21. Marts 2018). *Facebook scandal: I am being used as scapegoat – academic who mined data*. Hentet fra The Guardian : <https://www.theguardian.com/uk-news/2018/mar/21/facebook-row-i-am-being-used-as-scapegoat-says-academic-aleksandr-kogan-cambridge-analytica>
- Wong, J. C., Lewis, P., & Davies, H. (24. April 2018). *How academic at centre of Facebook scandal tried – and failed – to spin personal data into gold*. Hentet fra The Guardian: <https://www.theguardian.com/news/2018/apr/24/aleksandr-kogan-cambridge-analytica-facebook-data-business-ventures>
- Wylie, C. (17. Marts 2018). *Cambridge Analytica whistleblower: 'We spent \$1m harvesting millions of Facebook profiles'*. (T. Guardian, Interviewer)
- Wylie, C. (17. Marts 2018). *Cambridge Analytica: Whistleblower reveals data grab of 50 million Facebook profiles*. (Channel 4 News, Interviewer)
- Wylie, C. (7. April 2018). *Christopher Wylie: Why I broke the Facebook data story – and what should happen now*. Hentet fra The Guardian : <https://www.theguardian.com/uk-news/2018/apr/07/christopher-wylie-why-i-broke-the-facebook-data-story-and-what-should-happen-now>

Retskilder

Love

EU's Charter om Grundlæggende Rettigheder - 2000/C 364/01 (Chartret)

L 68 Forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (Databeskyttelsesloven)

Lov 2000-05-31 nr. 429 om behandling af personoplysninger (PDL)

Parlamentets og Rådets direktiv 95/46/EF (Databeskyttelsesdirektivet)

Parlamentets og Rådets forordning 2016/679 (Persondataforordningen, Forordningen eller GDPR)

Traktaten om Den Europæiske Unions Funktionsmåde, C-326 af 26/10/2012. (TEUF)

Praksis

C-6/64, Costa v. ENEL

C-131/12, Google Spain

C-230/14, Weltimmo

C-362/14, Safe Harbour

Folketingets Ombudsmand afgørelse: J.nr. 2011-2657-2091

UI998.800H – Maastricht-dommen

Betænkninger

Justitsministeriets Betænkning nr. 1565 bind 1-3