INSTITUT FOR MENNESKE RETTIGHEDER

TECH-GIGANTERNE, YTRINGS-FRIHEDEN OG PRIVATLIVET

TECH-GIGANTERNE, YTRINGS-FRIHEDEN OG PRIVATLIVET

Rikke Frank Jørgensen & Marya Akhtar

Wilders Plads 8K
1403 København K
Telefon 3269 8888
www.menneskeret.dk

Vi tilstræber, at vores udgivelser bliver så tilgængelige som muligt. Vi bruger fx store typer, korte linjer, få orddelinger, løs bagkant og stærke kontraster. Læs mere om tilgængelighed på www.menneskeret.dk/tilgaengelighed

INDHOLD

1 SAMMENFATNING

Tech-giganterne spiller en **stadig større rolle i samfundet**, fordi de kontrollerer de platforme og tjenester, hvor kommunikation, informationssøgning, offentlig debat, mv., udfolder sig. Samtidig opererer virksomhederne (i større eller mindre grad) ud fra en forretningsmodel, der er baseret på at indsamle og analysere så mange oplysninger om borgerne som muligt.

Tech-giganterne har en hidtil uhørt mulighed for at påvirke menneskerettigheder og demokratiske processer for millioner af borgere samtidig med, at de agerer uden for demokratisk kontrol.

Virksomhederne har således væsentlig indflydelse på den enkeltes rettigheder, samtidig med at de på flere områder opererer i et **reguleringsmæssigt tomrum**. Det har i høj grad været op til virksomhederne selv at sikre, at de respekterer menneskeretten.

Denne rapport beskriver de væsentligste menneskeretlige problemer med særligt fokus på:

- **Ytringsfriheden**, herunder de gråzoner, der aktuelt eksisterer for beskyttelse af ytringsfriheden på digitale platforme.
- **Retten til privatliv og beskyttelsen af personoplysninger**, herunder platformenes indsamling og kommercielle brug af oplysningerne.
- **Effektiv håndhævelse** af rettighederne.

Når tech-giganterne fjerner indhold på internettet, kan det ske af mange forskellige grunde. Det kan være, fordi en stat konkret har givet påbud til platformen om at fjerne indholdet, eller fordi platformen selv har besluttet, at visse typer indhold ikke skal være synlige på deres platforme. Indholdet kan også blive fjernet, fordi staten har opfordret til det, eller fordi platformen har indgået en frivillig aftale med staten om at fjerne indholdet. De mange forskellige grunde til, at indhold bliver fjernet, indebærer, at **statens ansvar for at beskytte ytringsfriheden er uklart**.

Tech-giganterne forventes i praksis at vurdere store mængder indhold for at fjerne det ulovlige indhold. Dette skaber en risiko for **overregulering**, således at mere indhold end nødvendigt fjernes. Overregulering af indhold kan medføre en *chilling effect* på ytrings- og informationsfriheden.

Advarslen mod at lade private aktører forestå vurderingen af ulovligt indhold intensiveres, når vurderingen foretages via **automatiserede indholdsfiltre**.

Tech-giganternes omfattende indsamling og brug af personoplysninger er blevet beskrevet som **overvågningskapitalisme**. **Overvågningskapitalismen har skabt nye produkter og markeder**, der er baseret på muligheden for at kunne forudsige og påvirke borgeres adfærd.

Markedets nuværende struktur indebærer, at oplysninger om den enkelte borger deles og bruges af en lang række aktører, som borgeren ikke kender til. De uigennemsigtige relationer aktørerne imellem medfører blandt andet, at **borgeren ikke ved, hvem en klage skal rettes imod**.

Det uigennemsigtige samspil mellem de mange aktører på markedet fører til **et rettighedstab**. Forretningsmodellen udfordrer tillige flere centrale persondataretlige principper: krav til **dataminimering, formålsbestemthed, (oplyst) samtykke og indsigt.**

2 INDLEDNING

Tech-giganter som Google, Apple, Amazon, Microsoft og Facebook har som private virksomheder et stort frirum til at definere vilkår og grænser for brug af deres tjenester. I takt med, at de har fået en stadig mere **dominerende rolle i samfundet**, er der kommet øget fokus på, hvordan deres platforme og tjenester griber ind i samfundets demokratiske liv og i menneskerettigheder.

Formålet med denne rapport er at give et overblik over de **menneskeretlige problemstillinger**, der opstår, når tech-giganterne indtager en stadig større rolle i samfundet. Notatet fokuserer på to centrale rettigheder: **ytrings- og informationsfriheden samt retten til respekt for privatlivet**.

Den rolle, tech-giganterne spiller for ytringsfriheden, skyldes navnlig to forhold:

1. staterne gør brug af regulering for at begrænse **ytringer med ulovligt indhold**, herunder ved at pålægge virksomhederne et ansvar for at fjerne ulovlige ytringer.
2. virksomhederne gennemfører selv indholdsregulering, der begrænser ytringer med **lovligt indhold**.

Tech-giganternes rolle udfordrer også privatlivet og beskyttelsen af personoplysninger, da indsamling, analyse og deling af store mængder oplysninger om borgerne skaber grundlag for nye former for overvågning og kontrol, foretaget af både stater og virksomheder.[1]

Der er imidlertid også **andre rettigheder**, der kan være berørt, men som ikke behandles i denne rapport. For eksempel har FN's specialrapportør for forenings- og forsamlingsfrihed fremhævet, at virksomhedernes adfærd også har indflydelse på forsamlingsfriheden.[2] Herudover har der været rejst spørgsmål om, hvorvidt personligt målrettede annoncer, herunder boligannoncer og jobannoncer, kan være i strid med diskriminationsforbuddet.[3] Mere overordnet har spørgsmålet om tech-giganternes rolle i demokratiet været genstand for debat, blandt andet i forhold til spørgsmål om disinformation, politiske kampagner og tonen på de sociale medier.[4]

Resten af notatet er struktureret på følgende måde: I **afsnit 3** forklares begrebet "tech-gigant", og i **afsnit 4** gennemgås den del af menneskerettighederne, som

notatet har fokus på (ytrings- og informationsfriheden samt beskyttelsen af privatliv og personoplysninger). I **afsnit 5** fremhæves de væsentligste menneskeretlige problemstillinger, som opstår i mødet mellem staterne, virksomhederne og borgerne.

KAPITEL 3

HVAD ER EN TECH-GIGANT?

Tech-gigant er ikke et juridisk begreb, men bruges om teknologivirksomheder, der har opnået en markedsdominerende position gennem udbredelsen af deres platforme og tjenester.

Tech-giganterne er kommet i fokus, fordi der i takt med udviklingen af det digitale samfund er sket en markedskoncentration, hvor relativt få virksomheder har fået stadig større indflydelse på den enkeltes muligheder for at udøve sine menneskerettigheder. Dette skyldes, at virksomhederne kontrollerer de platforme og tjenester, hvor kommunikation, informationssøgning, offentlig debat, mv., udfolder sig.

I en europæisk kontekst omtaler man typisk Apple, Amazon, Google, Facebook og Microsoft som tech-giganter. Virksomhederne tilbyder en række tjenester og platforme inden for en bred vifte af aktiviteter, såsom markedspladser, søgemaskiner, sociale medier, distributionsplatforme for applikationer, betalingssystemer og platforme til deleøkonomi.[5]

I denne rapport bruges tech-giganter som et samlebegreb for teknologivirksomheder, hvis størrelse og position i markedet aktualiserer særlige menneskeretlige problemstillinger.

Nogle af de rettigheder, der særligt påvirkes, er ytringsfriheden, informationsfriheden, privatlivet og beskyttelsen af personoplysninger. Eksempelvis beslutter virksomhederne, hvilke samtaler de vil tillade, hvilket indhold der bliver fjernet, hvilke informationer den enkelte præsenteres for, og hvordan de anvender den store mængde oplysninger, som de opsamler om hver enkelt bruger af platformen.[6]

Virksomhedernes forretningsmodel baserer sig på indsamling, analyse og brug af oplysninger, herunder personoplysninger om brugere af platformen. Oplysningerne bruges kommercielt af virksomhederne og udveksles også med stater, blandt andet som led i efterforskning og efterretningsvirksomhed.

Det er i den forbindelse særegent for den digitale tidsalder, at **infrastrukturerne** for ytringsfrihed og informationsfrihed samt for overvågning fra myndigheder eller private, forenes i de samme få og store virksomheder**.[7] De kanaler, som borgerne er afhængige af for at kunne kommunikere, er de samme, som staten (og virksomhederne) bruger til at overvåge borgerne.**

Tech-giganterne har en enestående kommerciel magt og innovationsstyrke på markedet samtidig med, at de har indflydelse på demokrati og meningsudveksling og kan skabe detaljerede profiler om borgerne.[8]

Denne udvikling betyder, at tech-giganterne har en uhørt mulighed for at påvirke menneskerettigheder og demokratiske processer for millioner af borgere samtidig med, at de agerer uden for demokratisk kontrol. Virksomhedernes kontrol over digitale platforme og tjenester har ligeledes betydet, at stater skal gå via dem, når de vil kontrollere indhold på internettet, for eksempel når de vil have fjernet ulovlige ytringer.

Denne særlige position i samfundet benævnes **"gatekeeper"**.[9] Heri ligger, at virksomhederne på grund af deres særlige position i markedet udøver væsentlig kontrol over adgangen til en central samfundsressource. En gatekeeperposition rejser spørgsmål om virksomhedens retlige og/eller sociale **forpligtelser** i samfundet på grund af deres markedsposition, status og/eller indflydelse på demokratiet.[10] Det spiller for eksempel ind, om borgeren har andre og tilsvarende muligheder for at deltage i den offentlige debat.

Det er blevet fremhævet, at tech-giganterne besidder **en ny form for magt** i forhold til nyhedsformidling, demokratiske processer, adgangen for borgere til at forene sig kollektivt samt informationssøgning og formidling af synspunkter, herunder holdninger, der dissentierer fra magthaverne.[11]

Man taler om, at tech-giganternes platforme og tjenester er blevet grundlæggende for det moderne samfund og for, hvordan mennesker interagerer med hinanden.[12]

Denne dominerende rolle i samfundet gør det essentielt at sikre, at den enkeltes rettigheder er beskyttet på de platforme, hvor de udleves. Dette er ikke tilfældet i dag, som vi skal se i det følgende.

KAPITEL 4

DEN MENNESKERETLIGE RAMME

Menneskeretten binder de stater, der har underskrevet de internationale konventioner, hvorimod virksomheder – fordi de er private aktører – ikke er **direkte forpligtede** af menneskeretten.

Staten har pligt til at beskytte individet mod krænkelser fra virksomheder (dette kaldes en **positiv forpligtelse**). Rækkevidden af statens positive forpligtelser afhænger af de konkrete omstændigheder (se nedenfor afsnit 4.2.1). I det omfang, staten vælger at regulere virksomhedernes adfærd, skal virksomhederne overholde de fastsatte regler, hvorved de bliver **indirekte forpligtede** af menneskeretten.

EU-retten kan binde private aktører direkte til at overholde visse rettigheder. For eksempel er både private og offentlige aktører forpligtet til at beskytte personoplysninger efter databeskyttelsesforordningen (se nedenfor afsnit 4.3.1).

I det følgende gives et overblik over de væsentligste menneskeretlige kilder til vurdering af tech-giganternes adfærd.

4.1 FN

4.1.1 BINDENDE REGLER

FN's Konvention om Borgerlige og Politiske Rettigheder beskytter ytrings- og informationsfriheden (artikel 19) og **retten til respekt for privatlivet** (artikel 17). Bestemmelserne forpligter staterne til at respektere rettighederne. Bestemmelserne retter sig derimod ikke mod private virksomheder, og tech-giganterne er dermed *ikke* omfattet.

Retten til privatliv er tæt knyttet til de øvrige frihedsrettigheder såsom ytringsfrihed, og **den fulde effekt af begge rettigheder er gensidigt betinget af hinanden.**[13]

Staten har mulighed for at gribe ind i ytrings- og informationsfriheden samt i retten til respekt for privatlivet. For at et indgreb skal være foreneligt med

menneskeretten, skal det have hjemmel i lov, forfølge et legitimt formål og være nødvendigt (herunder proportionalt). Staten kan således regulere ytringsfriheden og indgreb i privatlivet.

Instituttet har udarbejdet et overblik over den menneskeretlige beskyttelse af privatliv og databeskyttelse her. Der henvises desuden til afsnit 4.2.1 for en nærmere gennemgang af de to rettigheder.

I særlige tilfælde er **staten menneskeretligt forpligtet til at indskrænke** ytringsfriheden og kriminalisere ytringer for at undgå vold, had og overgreb. Det følger således af konventionens artikel 20, stk. 2, at enhver tilskyndelse til nationalt had, racehad eller religiøst had, som ophidser til forskelsbehandling, fjendtlighed eller vold, skal være forbudt ved lov. Staten er også forpligtet til at sikre borgere en effektiv beskyttelse mod diskrimination efter artikel 26. Som led i denne beskyttelse har mange stater vedtaget lovgivning rettet mod hadefuld tale.

FN's Racediskriminationskonventions artikel 4 og 5 forpligter også staterne til at træffe foranstaltninger til at bekæmpe enhver tilskyndelse til eller udøvelse af racediskrimination. Staterne er forpligtet til at kriminalisere udbredelsen af ideer, der hviler på forestillinger om racemæssig overlegenhed eller racehad, tilskyndelse til diskrimination, voldshandlinger og tilskyndelse til voldshandlinger imod personer af en anden etnisk oprindelse.

Forholdet mellem artikel 19 og 20 i Konventionen om Borgerlige og Politiske Rettigheder og artikel 4 i Racediskriminationskonventionen er senest blevet behandlet af FN's specialrapportør for ytringsfrihed, som fremhæver, at de to typer af rettigheder kræver fortolkning og konkret afvejning.[14]

Racediskriminationskomiteen har anført, at kriminalisering af racistiske ytringer efter artikel 4 bør forbeholdes de mest alvorlige sager.[15]

Der henvises i øvrigt til instituttets rapport om hadefulde ytringer i den offentlige debat, der indeholder en gennemgang af den menneskeretlige regulering af hadefuld tale. Rapporten er tilgængelig her.

4.1.2 RETNINGSLINJER OG ANBEFALINGER

I 2011 vedtog FN et sæt retningslinjer **for menneskerettigheder og erhverv**, der omfatter både staters forpligtelser og virksomheders ansvar.[16] **Retningslinjerne er ikke bindende**, men er baseret på, at virksomheder selv tager skridt til at indrette deres forretning, så de respekterer menneskerettighederne.

Retningslinjerne repræsenterer en global standard for forventet adfærd og omfatter alle virksomheder. Blandt andet forventes virksomhederne at udvise menneskeretlig *due diligence* (rettidig omhu) som en integreret del af deres forretning, herunder ved at gennemføre menneskeretlige konsekvensanalyser.[17]

FACEBOOK I MYANMAR

Et eksempel på gennemførelsen af en menneskeretlig konsekvensanalyse er Facebooks analyse af Myanmar og Facebooks rolle i spredningen af hadefuld tale.[18] I 2014 ekspanderede Facebook til Myanmar, og i løbet af tre år voksede antallet af Facebookbrugere fra to til tredive millioner.[19] Sideløbende eskalerede konflikten mellem Rohingya-mindretallet og Myanmars militær, hvilket førte til en omfattende etnisk udrensning af Rohingyaerne. Ifølge en FN-rapport fungerede Facebook som et nyttigt instrument for dem, der ønskede at sprede had i landet.[20] Beskeder og kommentarer, som Facebook ifølge sine egne retningslinjer burde have fjernet, blev i mange tilfælde ikke fjernet, blandt andet fordi Facebook ikke havde nok ansatte, som kunne sproget i Myanmar.

I 2012 fastslog FN for første gang, at menneskerettighederne gælder såvel **online** som **offline**. Siden da er forholdet mellem teknologi og menneskerettigheder blevet adresseret i en række ikke-bindende standarder og anbefalinger.

For et overblik over FN´s standarder på området henvises til instituttets faktaark, der er tilgængeligt her.

I de seneste år har flere af FN's specialrapportører haft fokus på tech-giganternes adfærd.

FN's specialrapportør for ytringsfrihed har i en rapport fra 2018 identificeret to centrale udfordringer i forhold til regulering af indhold på sociale medier mv. Den første er, at **stater i øget omfang indfører lovgivning, der begrænser borgerens adgang til at ytre sig på digitale platforme**, herunder via et øget pres på virksomhederne for at få dem til at begrænse visse former for indhold. Den anden er, at **virksomhedernes regulering af indhold er uigennemsigtig og inkonsekvent**. Med hensyn til sidstnævnte problemstilling tager specialrapportøren afsæt i FN's retningslinjer for menneskerettigheder og erhverv.[21]

FN's specialrapportør for privatliv har ligeledes fremhævet den digitale tidsalders menneskeretlige udfordringer med afsæt i FN's retningslinjer. Rapportøren anbefaler blandt andet, at virksomhederne i højere grad indarbejder FN's retningslinjer i deres forretning, at de sikrer en høj grad af sikkerhed og fortrolighed i borgernes kommunikation, samt at de sikrer størst mulig transparens i de politikker og praksisser, der har indvirkning på borgernes ret til privatliv.[22]

4.2 EUROPARÅDET OG DEN EUROPÆISKE MENNESKERETTIGHEDSDOMSTOL

4.2.1 BINDENDE REGLER

Den **Europæiske Menneskerettighedskonvention beskytter ytrings- og informationsfriheden** (artikel 10) og **retten til respekt for privatliv** (artikel 8). Som nævnt under afsnit 4.1.1 skal begrænsninger i ytringsfrihed og privatliv have hjemmel i lov, forfølge et legitimt formål og være nødvendige (herunder proportionale).

Konventionens artikel 13 indebærer, at enhver, hvis rettigheder krænkes, skal have adgang til effektive retsmidler ved en national myndighed, uanset om krænkelsen er begået af staten eller af private.

Europarådets Konvention om Cyberkriminalitet fra 2001 og tillægsprotokollen fra 2003 regulerer hadefulde ytringer motiveret af racisme og xenofobi.

Tillægsprotokollen pålægger medlemsstaterne at kriminalisere racistiske eller xenofobiske udtalelser på internettet.

4.2.1.1 Ytrings- og informationsfriheden

Ytrings- og informationsfriheden indeholder både retten til at ytre sig og til at afstå fra at ytre sig såvel som retten til at søge, modtage, viderebringe og få adgang til information. Ytringsfriheden omfatter ikke kun ord, men også billeder og lyd.

Den Europæiske Menneskerettighedsdomstol har ikke eksplicit taget stilling til tech-giganternes betydning for ytringsfriheden (eller øvrige menneskerettigheder), men har mere generelt anført, at adgangen til internettet spiller en stor rolle for offentlighedens adgang til information, debat, nyheder og udbredelsen af informationer i øvrigt.[23]

I **Delfi mod Estland** tog Den Europæiske Menneskerettighedsdomstol for første gang stilling til en platforms ansvar for at fjerne ulovligt indhold. Sagen handlede om hadefuld tale på en nyhedsportal (Delfi), og om Delfi hurtigt nok havde fjernet et hadefuldt indlæg. Domstolen vurderede, at Delfi *ikke* hurtigt nok havde fjernet det ulovlige indhold, efter de blev opmærksomme på det, og at det *ikke* stred mod ytringsfriheden at pålægge dem et ansvar for at handle hurtigt. Afgørelsen lagde vægt på Delfis kommercielle interesse i at dele brugergenereret indhold, og at de var landets største nyhedsplatform og ikke et socialt medie.[24] En nærmere gennemgang af dommen kan ses i instituttets EU-studie om ICT og menneskerettigheder (FRAME), der er tilgængeligt her.

Den Europæiske Menneskerettighedsdomstol har i sin praksis anført, at statens forpligtelse til at respektere artikel 10 også indeholder visse **positive forpligtelser**. Omfanget af statens positive forpligtelser indebærer en vurdering af, hvilke ytringer der er tale om, ytringernes evne til at bidrage til den offentlige debat, arten og omfanget af de pågældende begrænsninger, alternative adgange til at ytre sig, og ytringernes indvirkning på andre rettigheder.[25]

Begrænsninger i ytringsfriheden

I visse tilfælde kan beskyttelsen i artikel 8 og artikel 10 føre til modsatrettede

resultater. Dette gælder for eksempel, når der skal ske en afvejning mellem de to rettigheder i forhold til billedmateriale, udtalelser eller oplysninger om private forhold. Domstolen har i den forbindelse fastslået, at der gælder en bred skønsmargin for staterne ved håndhævelsen af de to rettigheder over for hinanden.[26] I visse tilfælde kan beskyttelsen af privatlivet efter artikel 8 derfor føre til begrænsninger i retten til ytringsfrihed efter artikel 10.

I forhold til artikel 8 har Domstolen for eksempel påpeget, at statens positive forpligtelse indebærer, at staten iværksætter efterforskning ved rimeligt begrundede påstande om krænkelser.[27] Denne pligt indebærer blandt andet, at staten sikrer effektive retsmidler, så det er muligt at identificere og strafforfølge personer, der krænker andre på internettet.[28]

Staten har ligeledes en positiv forpligtelse efter artikel 8 til at beskytte den enkelte mod nedværdigende og forhånende udtalelser om en gruppe personer, for eksempel på grund af race, religion eller seksualitet.[29]

Grove ytringer, der har til hensigt at undergrave konventionens formål, vil ikke være beskyttet af konventionen i medfør af artikel 17 om rettighedsmisbrug. Artikel 17 anvendes for eksempel ved ytringer, der opildner eller opfordrer til terrorisme, had, drab eller forbrydelser mod statens selvstændighed og sikkerhed.[30]

4.2.1.2 Privatliv og personoplysninger

Retten til respekt for privatliv fastslår, at ingen må gøres til genstand for vilkårlig indblanding i deres private forhold, familie, hjem eller korrespondance. Denne ret til privatliv omfatter også visse oplysninger (personoplysninger) om den enkelte.[31] Enhver har ret til lovens beskyttelse mod sådan indblanding.

Den Europæiske Menneskerettighedsdomstol har fastslået, at beskyttelsen af personoplysninger også indebærer en selvbestemmelsesret med hensyn til egne personoplysninger:

> "The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life […]. Article 8 of the Convention thus provides for the right to a form of informational self

> determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged."[32]

Herudover har Domstolen også anført, at brug af oplysninger til andre formål end dem, som oplysningerne oprindeligt blev indhentet til, begrænses af beskyttelsen i artikel 8.[33]

Domstolen har endvidere anført, at det forhold, at den efterfølgende brug af oplysningerne kan være lovlig, ikke fritager fra kravet om lovhjemmel for overhovedet at indsamle oplysningerne. Domstolen udtalte sig om dette i en sag om videooptagelser foretaget af politiet uden lovhjemmel. Optagelserne blev efterfølgende brugt under en retssag. Domstolen anførte i den forbindelse, at:

> "Issues relating to the fairness of the use of the evidence in the trial must […] be distinguished from the question of lawfulness of the interference with private life and are relevant rather to Article 6 than to Article 8."[34]

Spørgsmålet om myndighedernes adgang til oplysninger på internettet, herunder ved masseovervågning, behandles på nuværende tidspunkt i to verserende sager ved Domstolens storkammer.[35]

Ved siden af artikel 8 i Den Europæiske Menneskerettighedskonvention gælder også Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (1981) og ændringsprotokollen (2018), der sikrer retten til privatliv forbindelse med behandling af personoplysninger.[36]

4.2.2 RETNINGSLINJER OG ANBEFALINGER

Europarådet har vedtaget en række **erklæringer og anbefalinger** om forholdet mellem teknologi og menneskerettigheder, herunder i forhold til sociale medier, søgemaskiner, kunstig intelligens, algoritmer, Big Data, overvågning og internetbrugeres rettigheder. Disse standarder er retningsgivende, men ikke retligt bindende.

Blandt andet har Europarådets ministerkomité i sin anbefaling vedrørende ytringsfrihed og internetfiltre anført, at medlemsstaterne har en forpligtelse til at sikre ytringsfriheden i sin regulering af brugen af internetfiltre.[37] Ligeledes vedtog ministerkomiteen i 2016 den første anbefaling vedrørende menneskerettigheder og erhverv, der følger op på FN's retningslinjer og opfordrer Europarådets medlemsstater til at styrke den nationale implementering af disse.[38]

Europarådets parlamentariske forsamling har også vedtaget en række standarder, der vedrører teknologi og menneskerettigheder, herunder resolution 1843(2011) om beskyttelse af privatliv og personoplysninger på internettet[39] og resolution 2311 om menneskerettigheder og erhverv.[40]

Instituttet har udarbejdet er faktaark over Europarådets standarder inden for menneskerettigheder og teknologi, der er tilgængeligt her.[41]

4.3 EU

4.3.1 BINDENDE REGLER

EU's **Charter for Grundlæggende Rettigheder** beskytter **ytrings- og informationsfriheden** (artikel 11), **retten til respekt for privatliv** (artikel 7) samt **behandlingen af personoplysninger** (artikel 8).[42]

Af Chartrets artikel 47 følger, at enhver, hvis rettigheder og friheder er blevet krænket, skal have adgang til effektive retsmidler for en domstol.

4.3.1.1 Ytrings- og informationsfrihed

Chartrets artikel 11 om ytringsfrihed binder i lighed med FN's Konvention om Borgerlige og Politiske Rettigheder og Den Europæiske Menneskerettighedskonvention alene staterne, hvilket fremgår udtrykkeligt af ordlyden af bestemmelsen.

Til gengæld findes der **bindende regler i EU, som forpligter private aktører til at fjerne ulovligt indhold fra deres platforme, og som derfor kan udgøre et indgreb i ytrings- og informationsfriheden**. Dette er tilfældet, fordi virksomhederne i disse tilfælde handler ud fra en forpligtelse fastsat af

medlemsstaterne eller EU.

Det følger af **e-handelsdirektivets**,[43] at udbydere af digitale tjenester som udgangspunkt er ansvarsfri for det indhold, de formidler, men at de har pligt til at fjerne ulovligt indhold, når de får kendskab til det (artikel 14). Hvis virksomheden undlader dette, kan den ifalde ansvar for medvirken til den ulovlige handling. Denne særlige form for "handlepligt" kaldes *for* ***notice and takedown*-princippet**.[44]

Af direktivets artikel 15 følger desuden, at staterne **ikke må pålægge virksomhederne en generel forpligtelse til at overvåge** indhold på deres tjenester og platforme. **Forholdet mellem begrænsning af ytringsfriheden og overvågning fremgår dermed udtrykkeligt af e-handelsdirektivet**.

Virksomhedernes filtrering og gennemgang af indhold på nettet i relation til privatlivet er behandlet i afsnit 5.2.

For en nærmere beskrivelse af e-handelsdirektivets indvirkning på sociale mediers praksis henvises til instituttets rapport om demokratisk deltagelse på Facebook. Rapporten konkluderer blandt andet, at der er behov for præcisering af sociale mediers "handlepligt" efter e-handelsdirektivet samt en effektiv retshåndhævelse af deres medvirkensansvar, såfremt de udlader at fjerne ulovligt indhold rettidigt. Rapporten er tilgængelig her.

E-handelsdirektivet er på nuværende tidspunkt ved at blive revideret i EU, hvor der er lagt op til en omfattende reform af platformenes ansvar.[45]

Forpligtelser rettet mod platforme og andre private aktører på nettet til at fjerne indhold følger også af andre EU-retlige regler, herunder blandt andet: direktiv om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og børnepornografi [46], direktiv om ophavsret på det digitale indre marked[47] samt ændringsdirektivet om audiovisuelle medietjenester.[48] Se instituttets høringssvar om ændringsdirektivet og dets danske implementering her.

Senest forhandler EU om en forordning om forebyggelse af udbredelsen af **terrorrelateret onlineindhold**, der indeholder en række forpligtelser for virksomheder til at fjerne ulovligt indhold. Instituttet har forholdt sig til tidligere

versioner af udkastet til forordningen her og her.

EU-Domstolen har set nærmere på forpligtelser rettet mod digitale platforme og tjenester i en række domme.

I **SABAM mod Scarlet Extended**[49] tog domstolen stilling til spørgsmålet om brug af indholdsfiltrering for at forebygge krænkelse af immaterielle rettigheder.[50] Domstolen fandt, at virksomheder ikke må pålægges at bruge et indholdsfilter, idet dette svarer til en tidsubegrænset overvågning af samtlige oplysninger om brugerne. En sådan generel overvågning strider mod e-handelsdirektivets artikel 15. Domstolen understregede, at brugen af filtre kan krænke beskyttelsen af personoplysninger i **Chartrets artikel 8** og friheden til at modtage eller videregive oplysninger i **Chartrets artikel 11**.[51]

Senest har EU-Domstolen i **Glawischnig-Piesczek mod Facebook Ireland Limited**[52] afgjort, at e-handelsdirektivets artikel 15 *ikke* forhindrer en medlemsstat i at påbyde Facebook at fjerne ulovligt indhold. Dette omfatter også indhold, der er identisk med indhold, der tidligere er erklæret ulovligt eller *"har samme betydning"* som indhold, der tidligere er erklæret ulovligt. Domstolen fremhævede imidlertid, at påbuddet *ikke* må indebære en forpligtelse for Facebook til at foretage "en selvstændig vurdering" af indholdet.[53] Domstolen præciserede ikke, hvad der ligger i "selvstændig vurdering", men anførte, at platformen skal anvende "automatiserede teknikker og søgemetoder".[54] Dommen giver ikke noget svar på, hvor hurtigt og effektivt Facebook eller andre platforme skal fjerne ulovligt brugergenereret indhold.

Brugen af automatiserede metoder (indholdsfiltre mv.) rejser nogle væsentlige menneskeretlige spørgsmål, som behandles nærmere nedenfor i afsnit 5.1.2, og som Domstolen ikke tog stilling til i dommen.

4.3.1.2 Privatliv og personoplysninger

Retten til respekt for privatlivet er beskyttet i artikel 7 i Chartret. I Chartret er der også en udtrykkelig beskyttelse af personoplysninger i artikel 8.

Inden for EU-retten har visse menneskerettigheder **direkte virkning mellem private.** Dette gælder blandt andet retten til databeskyttelse, der er udmøntet i

databeskyttelsesforordningen.[55]

Databeskyttelsesforordningens artikel 6 og 9 regulerer både offentlige og privates behandling af personoplysninger. Når det gælder platformenes indsamling af oplysninger om borgere, er det klare udgangspunkt, at der skal gives **samtykke** til virksomheder, før de må indsamle og bruge personoplysninger. Personoplysninger skal forstås bredt som enhver form for oplysninger, der kan relateres til en person, jf. artikel 4.[56]

Forordningen baserer sig på en række centrale principper om beskyttelse af personoplysninger, herunder navnlig: **princippet om lovlighed, rimelighed og gennemsigtighed** i forbindelse med behandling af personoplysninger, jf. forordningens artikel 5, stk. 1, litra a, krav om **formålsbestemthed** (artikel 5, stk. 1, litra b), hvorefter personoplysninger ikke må bruges til formål, der er uforenelige med det formål, hvortil de er indsamlet, samt princippet om **dataminimering** (artikel 5, stk. 1, litra c), hvorefter der ikke må indsamles flere personoplysninger, end hvad der er strengt nødvendigt.

Forordningen giver også borgerne et sæt af rettigheder i forhold til virksomheden, herunder navnlig: **indsigts- og indsigelsesret** i forbindelse med indsamlede personoplysninger, blandt andet indsigelse mod videregivelse af oplysninger med henblik på **markedsføring** (artikel 21, stk. 2), ret til **berigtigelse af data** (artikel 16), ret til sletning af data, også kaldet **retten til at blive glemt** (artikel 17) samt ret til **dataportabilitet** (artikel 20).

Databeskyttelsesforordningen trådte i kraft i maj 2018 og dens nærmere fortolkning, herunder i forhold til virksomheders indsamling og brug af personoplysninger, vil i den kommende tid blive fastlagt af EU-domstolen i takt med, at der afgøres sager på området. I Danmark er forordningen suppleret af databeskyttelsesloven.[57]

Ved siden af databeskyttelsesforordningen gælder også direktivet om databeskyttelse inden for elektronisk kommunikation (**e-databeskyttelsesdirektivet, også kaldet *e-privacy*-direktivet**)[58], som blandt andet regulerer lagring af trafikdata til elektronisk kommunikation. E-databeskyttelsesdirektivet er på nuværende tidspunkt ved at blive revideret og forventes erstattet af en forordning, hvis formål er at modernisere reglerne og

tilpasse og tilføje dem til databeskyttelsesforordningen og den digitale virkelighed, herunder ved i øget grad at regulere tech-giganternes kommunikationstjenester.[59]

Det nuværende e-databeskyttelsesdirektiv er centralt i den retspraksis om logning, som EU-Domstolen har udviklet.[60]

Direktivet er også blevet anvendt af EU-Domstolen i **Planet49**[61] i forhold til virksomheders pligt til at indhente aktivt samtykke til lagring af cookies.

En række af de bærende principper og regler i databeskyttelsesforordningen og e-databeskyttelsesdirektivet har længe været gældende ret i EU, og Domstolen har haft anledning til at udvikle dem og forholde sig til dem.

EU-Domstolen har i sin retspraksis blandt andet set på **retten til at blive glemt** (ved at få fjernet links til hjemmesider med personoplysninger fra Googles søgeindeks) **i forhold til hensynet til beskyttelse af ytringsfriheden**.

I **Google Spain**[62] fandt Domstolen, at en EU-borger under visse betingelser har ret til at få fjernet links til hjemmesider, der indeholder oplysninger om den pågældende, der **ikke længere er relevante** (retten til at blive glemt). Domstolen lagde bl.a. vægt på, at søgemaskiner muliggør sammenkædning af information, hvorved man kan fastlægge en mere eller mindre detaljeret profil af den enkelte.[63] Domstolen fastslog, at en søgemaskine kan være forpligtet til at fjerne links fra sit søgeindeks, selv når disse links henviser til hjemmesider, hvor den pågældende information er lovlig.[64]

Senest har EU-Domstolen i **CNIL v. Google**[65] anført, at den tidligere dom ikke indebærer en forpligtelse for Google til at fjerne links for borgere uden for EU. Domstolen fremhæver, at retten til beskyttelse af **personoplysninger ikke er absolut, men** skal afvejes konkret i forhold til andre grundlæggende rettigheder. Afvejningen mellem retten til respekt for privatlivet og beskyttelsen af personoplysninger og informationsfriheden **vil i praksis variere betydeligt rundt om i verden**.[66] Også inden for EU vil der skulle foretages en konkret afvejning af de to rettigheder, som kan føre til varierende udfald fra land til land.[67]

EU-Domstolen har i andre sager forholdt sig til spørgsmålet om jurisdiktion, som kan skabe særlige vanskeligheder i forhold til tech-giganterne, der ofte er etablerede uden for EU.

I **Wirtschaftsakademie**[68] fandt Domstolen, at Facebooks kontor i Tyskland var omfattet af det tyske datatilsyns jurisdiktion, selvom kontoret kun stod for salg af annonceplads. Domstolen vurderede i den konkrete sag, at Facebooks tyske kontor var dataansvarlig i fællesskab med en tysk virksomhed, der havde oprettet en fanside på Facebook. Når Facebook indsamlede oplysninger fra fansiden til brug for målrettet reklame rettet mod tyske borgere, kunne det tyske datatilsyn derfor stille krav til behandlingen af personoplysninger.[69]

EU-Domstolen har også set på **deling af personoplysninger til udenlandske myndigheder via Facebook.**

En af de væsentligste domme på området er **Maximillian Schrems**,[70] der handler om den såkaldte ***"safe harbor"*-aftale**[71] mellem Kommissionen og USA. Ifølge aftalen kunne personoplysninger om EU-borgere videregives til andre lande, der havde et "tilstrækkelig beskyttelseniveau" for oplysningerne. Sagen vedrørte Facebooks overførsel af oplysninger om EU-borgere til USA og endte med, at "*safe-harbor*"-aftalen blev underkendt. Domstolen lagde vægt på, at Kommissionen havde en **begrænset skønsbeføjelse** til at vurdere, om USA's beskyttelsesniveau var tilstrækkeligt, og at de skulle foretage en **streng efterprøvelse** af de krav, der fulgte af EU-retten, om personoplysninger og privatliv, før videregivelse til USA kunne tillades.[72] Domstolen fandt *ikke*, at "*safe harbor*"-aftalen opfyldte disse krav og lagde blandt andet vægt på, at ordningen veg for amerikanske sikkerhedskrav, og at EU-borgeres personoplysninger derfor ikke var beskyttet mod indgreb fra amerikanske myndigheder. Der var heller ikke nogen effektiv domstolsbeskyttelse mod disse indgreb.

"*Safe harbor*"-ordningen er efterfølgende blevet erstattet af "***privacy shield***"-aftalen, hvis lovlighed p.t. efterprøves ved EU-Domstolen.[73]

Domstolen har også forholdt sig til, hvem der kan anses for dataansvarlige, når oplysninger indsamles og deles mellem flere virksomheder til kommercielle formål.

Sagen **Fashion ID**[74] vedrørte en virksomheds brug af "synes godt om"-knappen fra Facebook på sin hjemmeside. Brugen af knappen indebar, at oplysninger om brugere af Fashion ID's hjemmeside blev delt med Facebook. Domstolen konkluderede, at Fashion ID og Facebook **delte ansvaret** for personoplysningerne.[75] I forhold til krav om **samtykke** og **oplysningspligt** over for brugeren var det Fashion ID og ikke Facebook, der skulle sikre overholdelse af reglerne, idet krav til samtykke og oplysning skal være opfyldt *inden* indsamling af personoplysningerne.[76] EU-Domstolen fandt her, at et forhåndsafkrydset felt *ikke* udgør et gyldigt samtykke, da dette kræver en aktiv handling fra brugeren.

4.3.2 RETNINGSLINJER OG ANBEFALINGER

Også inden for EU er der vedtaget en række retningslinjer og anbefalinger, der vedrører tech-giganter.

Som de væsentligste eksempler kan nævnes en samarbejdsaftale ***(Code of Conduct)*** mellem Kommissionen og Facebook, Microsoft, Twitter og YouTube vedrørende bekæmpelse af hadefulde ytringer[77] samt igangværende arbejder vedrørende ansvar og pligter for digitale platforme.[78]

I den forbindelse er Kommissionens henstilling om foranstaltninger til effektiv bekæmpelse af ulovligt indhold på nettet central, da den udpensler nogle af de tiltag, som Kommissionen opfordrer virksomhederne til at iværksætte for at bekæmpe ulovligt indhold.[79]

For en nærmere gennemgang af de EU-retlige problematikker, der knytter sig til indholdsregulering og ytringsfrihed, henvises til instituttets EU-studie (FRAME) om ICT og menneskerettigheder, der er tilgængeligt her.

Der henvises endvidere til instituttets fakta-ark om indholdsfiltre og platformenes regulering af ytringsfriheden her.

Inden for beskyttelse af privatliv og personoplysninger bidrager en række udtalelser fra den tidligere Artikel 29-arbejdsgruppe og det nuværende Europæiske Databeskyttelsesråd med fortolkning af beskyttelsens omfang.

4.4 DANSK RET

Beskyttelsen af ytringsfriheden følger af **grundlovens § 77** og retter sig mod staten.

Spørgsmålet om sociale medier og ytringsfrihed er også behandlet af Ytringsfrihedskommissionen, som er nedsat af Justitsministeriet, og hvis rapport blev offentliggjort i april 2020.[80] Regeringen har udtalt, at man afventer Kommissionens analyse, før eventuel ny dansk regulering på området introduceres.[81]

Danske regler om strafferetligt eller erstatningsretligt medvirkensansvar kan efter omstændighederne føre til, at udbydere af digitale platforme og tjenester ifalder ansvar for ulovligt indhold på internettet.

Inden for strafferetten kan det for eksempel være medvirkensansvar for digitale, seksuelle krænkelser,[82] ærekrænkelser efter straffelovens regler eller overtrædelser af racismeparagraffen.

Instituttet har tidligere fremhævet, at der er behov for at få tydeliggjort rammerne for medvirkensansvar, for eksempel hvor hurtigt en platform forventes at reagere.

I forhold til **beskyttelsen af personoplysninger** suppleres databeskyttelsesforordningen i Danmark af databeskyttelsesloven, og Datatilsynet fører tilsyn med begge regelsæt, ligesom tilsynet udsteder vejledninger mv. på området.

KAPITEL 5

TECH-GIGANTERNE OG DE MENNESKERETLIGE UDFORDRINGER

5.1 YTRINGS- OG INFORMATIONSFRIHED

5.1.1 LOVLIGT INDHOLD, ULOVLIGT INDHOLD OG GRÅZONERNE

For at forstå virksomhedernes påvirkning af borgernes ytrings- og informationsfrihed er det væsentligt at **sondre mellem lovligt og ulovligt indhold**.

Ytringsfriheden er ikke absolut, men dens grænser er defineret ved lovgivning for at sikre mod vilkårlig indgriben. Det betyder kort sagt, at ytringer, der ikke er forbudt ved lov, er tilladte. Ligeledes er det retlige udgangspunkt, at det er den, der ytrer sig, der står til ansvar.

Samtidig er det staten, som skal sikre overholdelse af **øvrige menneskeretlige forpligtelser**, som for eksempel artikel 8 i Den Europæiske Menneskerettighedskonvention, artikel 20, stk. 2, i Konventionen om Borgerlige og Politiske Rettigheder og artikel 4 i Racediskriminationskonventionen. Heri ligger et behov for hurtige reaktioner, når ulovligt indhold bliver identificeret, så indhold ikke er tilgængeligt og videredeles.

Når virksomheder fjerner **ulovligt indhold** efter **et konkret påbud fra staten, er det staten**, der skal sikre, at ytringsfriheden ikke krænkes. I disse situationer **håndhæver** virksomheden statens påbud, og det menneskeretlige ansvar er klart.

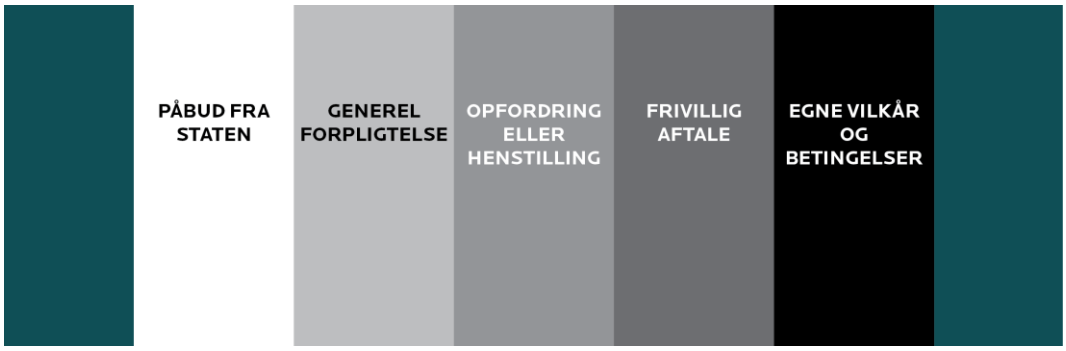
Hvis der ikke er tale om et konkret påbud, men derimod en **generel forpligtelse i henhold til loven**, bevæger man sig imidlertid ind i en **gråzone** i forhold til statens ansvar.

Eksempelvis er virksomhederne underlagt en *notice and takedown*-forpligtelse efter e-handelsdirektivet. Dette kan man kalde en generel forpligtelse i henhold til loven.

Hvis der ikke er tale om generelle forpligtelser i loven til at fjerne indhold, men derimod **opfordringer eller henstillinger** fra staten til virksomhederne, bliver spørgsmålet om det menneskeretlige ansvar endnu mere uklart: er det i disse tilfælde fortsat statens ansvar at sikre, at ytringsfriheden ikke krænkes i de situationer, hvor virksomheden fjerner indhold?

Det samme er tilfældet, når staten indgår **frivillige aftaler** med platformene eller udsteder ikke-bindende retningslinjer om reguleringen af indhold.

Hertil kommer virksomhedernes egne **vilkår og betingelser**, som i praksis fører til, at store mængder **lovligt indhold** bliver fjernet. Alle de store platforme har deres egne vilkår og betingelser for, hvilke emner der må debatteres, uagtet om indlæggene er lovlige. Desuden foregår der en udvælgelse af, hvilket indhold den enkelte præsenteres for eller har mulighed for at tilgå. Platformenes regulering af lovligt indhold hviler på de normer for acceptable ytringer og god adfærd, som den enkelte platform har defineret. Disse er **kommercielt definerede grænser** til forskel fra grænser, der er fastsat med udgangspunkt i menneskerettens standarder for ytringsfrihed.



De mange gråzoner gør, at tech-giganterne opererer uden klare juridiske regler, hvilket er særlig problematisk, når man ser på deres store indflydelse på samfund og demokrati. Fordi gråzonerne er juridisk uafklarede, er der en risiko for, at virksomhederne fjerner lovligt indhold for at være "på den sikre side". Risikoen for overregulering har ført til anbefalinger om, at **staten altid skal forpligte virksomhederne i lovform**.[83]

5.1.1.1 Hjemmelskravet

Menneskeretten stiller krav til staterne om, at indgreb i ytringsfriheden skal have **hjemmel**. Dette krav sætter visse betingelser for hjemlen, idet en hjemmel skal være formuleret med tilstrækkelig klarhed, præcision og være tilgængelig for borgeren. Formålet er, at borgeren kan indrette sin adfærd og har mulighed for at forudsige konsekvenserne af en eventuel handling eller ytring.[84]

Det menneskeretlige hjemmelskrav bliver udfordret af ovennævnte gråzoner (afsnit 5.1.1). Hjemmelskravet vil eksempelvis næppe kunne opfyldes af frivillige aftaler mellem staten og platformene.[85] Hjemmelskravet vil desuden rejse spørgsmål om, hvor præcis en generel forpligtelse om *notice and takedown* skal være for at opfylde kravet.

5.1.1.2 GNI

Tech-giganterne har i mange år haft fokus på anmodninger fra stater om at fjerne indhold og/eller udlevere oplysninger om deres brugere. I 2008 oprettede de deres eget branchenetværk, **Global Network Initiative (GNI)**, der har udarbejdet retningslinjer for, hvordan virksomhederne kan respektere borgernes ytringsfrihed og ret til privatliv i deres håndtering af anmodninger fra stater. Som led i dette arbejde offentliggør mange af virksomhederne årlige transparensrapporter, hvor de dokumenterer, hvor mange statslige henvendelser de har modtaget og imødekommet. Der er dog ingen lovgivningsmæssige krav til disse transparensrapporter, og koordineringen af virksomhedernes fjernelse af indhold via GNI er blevet kritiseret for at være en uigennemsigtig proces.[86]

Tech-giganternes praksis i dag er overvejende således, at staters henvendelser (vedrørende ulovligt indhold) behandles med udgangspunkt i menneskerettens standarder om lovhjemmel, legitimt formål og nødvendighed (herunder proportionalitet), mens virksomhedernes egne processer (vedrørende lovligt indhold) – for eksempel deres håndhævelse af såkaldte fællesskabsregler – ikke betragtes som et menneskeretligt anliggende.[87]

Alt dette fører til **tre uafklarede forhold** for beskyttelsen af ytringsfriheden:

1. Hvor vidtrækkende skal **statens ansvar** for at sikre ytringsfriheden være i **gråzonerne** mellem konkrete påbud om at fjerne **ulovligt indhold** og virksomhedernes fjernelse af **lovligt indhold** i medfør af egne vilkår og betingelser?

2. Bør tech-giganterne pålægges at **beskytte ytringsfriheden i deres vilkår og betingelser, når de fjerner lovligt indhold**, og hvor langt bør deres ansvar i givet fald strække sig?

3. Skal staten som led i sin positive forpligtelse til at sikre ytringsfriheden **regulere tech-giganternes praksis vedrørende lovligt indhold**?

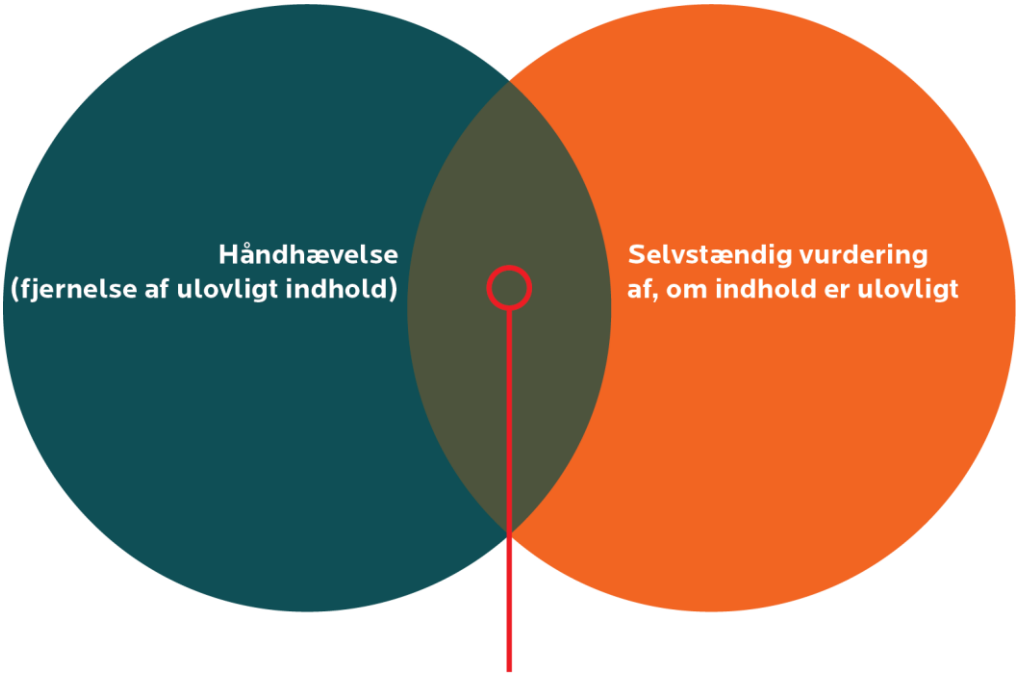
Spørgsmål 1 handler om statens ansvar i forhold til samtlige digitale platforme og tjenester mv., og ikke kun til tech-giganterne. Dog vil virksomhedens størrelse, markedsdominans og dens betydning for samfund og demokrati indvirke på konsekvenserne af indgrebet.

Vurderingen af, om indhold er ulovligt, vil ofte være en kompleks juridisk vurdering, hvor der kan indgå mange modsatrettede hensyn. Vurderingen kan også være kontekstafhængig: indhold kan for eksempel i én sammenhæng opfattes som opfordringer til ulovligheder og i en anden sammenhæng tjene et journalistisk formål.

FN's specialrapportør for ytringsfrihed har fremhævet, at den komplekse juridiske vurdering af ulovligt indhold *ikke* bør uddelegeres til virksomheder og anfører i den forbindelse:

> "Complex questions of fact and law should generally be adjudicated by public institutions, not private actors whose current processes may be inconsistent with due process standards and whose motives are principally economic."[88]

Det er her centralt at sondre mellem på den ene side **den selvstændige vurdering** af, om indhold er ulovligt, og på den anden side fjernelse af indhold (**håndhævelse**).



Indhold, der er "identisk" eller har "samme betydning" som ulovligt indhold

Den blotte **håndhævelse** svarer til, at virksomhederne fjerner indhold efter et påbud (eller efter omstændighederne i medfør af en generel forpligtelse). Håndhævelsestilfældet illustreres bedst ved EU-Domstolens afgørelse i **Glawischnig-Piesczek mod Facebook Ireland Limited,**[89] hvor Domstolen fandt, at staten kan kræve, at Facebook fjerner indhold, der tidligere er erklæret ulovligt, eller når indholdet "*har samme betydning*" som indhold, der tidligere er erklæret ulovligt. Domstolen fremhævede imidlertid, at dette ikke må indebære en forpligtelse for Facebook til at foretage "*en selvstændig vurdering*" af indholdet.[90]

Statens konkrete anmodninger eller generelle forpligtelser for virksomheder til at fjerne ulovligt indhold er ikke i sig selv uforeneligt med menneskeretten. Der kan imidlertid stilles krav til, hvordan håndhævelsen kan ske, eksempelvis hvor

hurtigt virksomhederne skal reagere, når de bliver bekendt med ulovligt indhold.[91]

Det er mere uklart, hvilke betingelser der skal være opfyldt, når virksomhederne skal foretage en **selvstændig vurdering** af, om indhold er ulovligt – idet denne vurdering indvirker på ytringsfriheden. Som nævnt ovenfor anbefaler FN's specialrapportør for ytringsfrihed, at sådanne afgørelser ikke uddelegeres til private virksomheder.

Når tech-giganterne i praksis forventes at **vurdere** store mængder indhold for at fjerne ulovligt indhold (enten ud fra en generel forpligtelse, en opfordring eller en henstilling eller med afsæt i en frivillig aftale), er der risiko for overregulering[92], idet virksomhederne hellere fjerner for meget end for lidt for ikke at ifalde ansvar og sjældent er underlagt krav om at begrunde deres beslutninger over for borgerne. En sådan **overregulering kan i praksis føre til begrænsninger i ytringsfriheden, hvor lovligt indhold bliver fjernet**.[93]

At uddelegere vurderingen til virksomheder bør derfor som minimum kræve, at staten fører tilsyn med, at vurderingen sker i overensstemmelse med menneskerettens krav.

Både overreguleringen af indhold og den massive dataindsamling (se afsnit 5.2) kan medføre en *chilling effect* på ytrings- og informationsfriheden. Den Europæiske Menneskerettighedsdomstol lægger i sin praksis om ytringsfrihed vægt på, at statens indgreb i ytringsfriheden ikke får en *chilling effect* på lovlige ytringer.[94]

Samlet set opstår der en risiko for, at staten fralægger sig ansvaret for overholdelsen af ytringsfriheden (og de øvrige menneskerettigheder) ved uddelegeringen til private virksomheder.[95]

Advarslen mod at lade private aktører forestå vurderingen af ulovligt indhold intensiveres, når vurderingen foretages via automatiserede indholdsfiltre og uden efterfølgende menneskelig kontrol, se afsnit 5.2.1 om indholdsfiltre.

Spørgsmål 2 og 3 handler om henholdsvis virksomheders og statens ansvar, når der er tale om virksomheder, som udøver en betydelig indflydelse på samfundet (**tech-giganter**). Modsat spørgsmål 1 er fokus her virksomhedernes praksis i forhold til **lovligt indhold**.

I lyset af den væsentlige rolle, som tech-giganterne spiller for ytringsfriheden, har flere eksperter anbefalet, at den **menneskeretlige beskyttelse tilpasses den digitale tidsalder ved at forpligte tech-giganterne til at overholde menneskerettighederne.** Virksomhederne er for eksempel ikke i dag forpligtet til at beskytte ytringsfriheden, men kan – med udgangspunkt i deres egne vilkår og betingelser – frit fjerne lovligt indhold.

Et problem ved at lade fjernelse af **lovligt indhold** på internettet stå ureguleret er, at virksomhederne i praksis spiller en central rolle for borgernes mulighed for at nyde deres ytrings- og informationsfrihed. Tech-giganterne råder over de platforme, hvor den offentlige debat udspilles, og de har samtidig – med udgangspunkt i deres vilkår og betingelser – frit råderum til at fjerne brugere af platformen og konkret indhold.

Europarådet har i den forbindelse anført:

> "(…) private entities can impose (and be 'encouraged' to impose) restrictions on access to information without being subject to the constitutional or international law constraints that apply to state limitations of the right to freedom of expression."[96]

Specialrapportøren for ytringsfrihed har anført, at platformenes regulering af indhold bør tage udgangspunkt i menneskerettens standarder (A/74/486, punkt 42):

> "When company rules differ from international standards, the companies should give a reasoned explanation of the policy difference in advance, in a way that articulates the variation. For example, were a company to decide to prohibit the use of a derogatory term to refer to a national, racial or religious group – which, on its own, would not be subject to restriction under human rights law – it should clarify its decision in accordance with human rights law."

I dele af litteraturen er der blevet argumenteret for, at tech-giganterne – på grund af deres betydningsfulde samfundsmæssige rolle – skal være ju**ridisk forpligtede** til at sikre ytringsfriheden på deres platforme.[97]

Andre – som FN's specialrapportør for ytringsfrihed – har anført, at platformene bør anerkende, at menneskerettighederne er den globale rettesnor, som de skal indrette deres virksomheder efter. Konkret har specialrapportøren anbefalet, at der tages afsæt i **FN's retningslinjer for menneskerettigheder og erhverv**, hvorefter virksomhederne bør sikre, at alle dele af deres forretning respekterer menneskerettigheder. De skal i den forbindelse gennemføre regelmæssige, menneskeretlige konsekvensanalyser og imødegå de menneskeretlige risici, som disse måtte pege på. Herudover har han anbefalet, at virksomhederne opererer ud fra princippet om transparens og ansvarlighed.[98]

I forhold til **statens mulige positive forpligtelser** med hensyn til tech-giganternes indholdsregulering af lovligt indhold (spørgsmål 3) har det været anført, at staterne som udgangspunkt bør indrette reguleringen af tech-giganterne således, at beskyttelsen af **ytringsfrihedens sikres bedst muligt**, for eksempel ved at stille krav til øget **transparens** i virksomhedernes indholdsregulering.[99]

5.1.2 UDFORDRINGER VED ADGANGEN TIL EFFEKTIVE RETSMIDLER

Udover gråzonerne for selve den materielle beskyttelse af ytringsfriheden er det også svært for borgeren at få adgang til den **processuelle beskyttelse**. En sådan beskyttelse følger af artikel 13 i Den Europæiske Menneskerettighedskonvention og artikel 47 i EU Chartret for Grundlæggende Rettigheder om adgang til **effektive retsmidler** for den, hvis rettigheder er krænket.

Statens pligt til at sikre effektive retsmidler er også et væsentligt element i FN's retningslinjer for menneskerettigheder og erhverv, hvor det tillige understreges, at virksomhederne også bærer et (ikke-juridisk) ansvar for at sikre effektive klagemekanismer i tilknytning til de produkter og tjenester, de tilbyder.

Den enkelte borger vil ofte ikke få kendskab til, om indhold er fjernet, fordi det blev anset for ulovligt, eller fordi det stred mod platformens vilkår og betingelser (eller befandt sig et sted i gråzonerne imellem de to).

I de situationer, hvor virksomheder vurderer og fjerner indhold, har den enkelte borger ikke samme processuelle adgang til at få prøvet, om indholdet er beskyttet af ytringsfriheden, som hvis staten selv fjernede indholdet.[100] Hvis indholdet er blevet fjernet via indholdsfiltre uden menneskelig kontrol, kan det tillige være uklart for virksomhederne selv, hvorfor indholdet er blevet fjernet (se nærmere om indholdsfiltre nedenfor i afsnit 5.1.2.).

Hertil kommer de situationer, hvor virksomhederne uddelegerer dele af processen til såkaldte "*trusted notifiers*" (troværdige meddelere).[101] "Troværdige meddelere" er i EU blevet defineret som personer eller organisationer, som virksomheden anser for at have en særlig ekspertise i forhold til at vurdere potentielt ulovligt indhold.[102]

Institut for Menneskerettigheder har tidligere anbefalet, at der bør sikres et effektivt klagesystem, der som minimum indebærer, at borgere bliver informeret, når de har fået indhold fjernet eller blokeret, bliver oplyst om grundlaget for beslutningen og får mulighed for at gøre indsigelser inden for en rimelig tidsfrist.

FACEBOOK-TILSYN

Facebook er i gang med at etablere et uafhængigt tilsyn med 40 medlemmer, der skal fungere som en "appelinstans" i sager om fjernelse af indhold, herunder være med til at sikre transparens i sagerne. Tilsynet er etableret som led i Facebooks selvregulering og skal afgøre principielle sager med udgangspunkt i platformens vilkår og betingelser, herunder afvejningen mellem ytringsfriheden og andre hensyn og rettigheder.[103]

Tilsynet vil alene forholde sig til indhold, der *er* blevet fjernet, og ikke vurdere om indhold, der fortsat er tilgængeligt på platformen, burde fjernes.

Det er blevet påpeget, at Facebooks tilsynsmyndighed potentielt kan blive en af de mest magtfulde instanser for håndhævelsen af ytringsfriheden – med jurisdiktion på tværs af et stort antal lande. Tilsynet er blevet kritiseret for at

minde om en privat domstol, der ikke er tilknyttet staten og derfor ikke er forpligtet af grundlæggende processuelle regler i lighed med øvrige domstolslignende myndigheder.[104]

5.1.3 RISICI VED BRUGEN AF AUTOMATISEREDE INDHOLDSFILTRE

Tech-giganterne gør i større eller mindre grad brug af automatiserede indholdsfiltre til deres indholdsregulering. Dette gælder både i forhold til ulovligt og lovligt indhold.[105]

5.1.3.1 Automatiserede indholdsfiltre

Automatiserede indholdsfiltre er algoritmer, som **automatisk identificerer og fjerner** – eller hindrer *upload* af – **indhold på nettet**. Indholdsfiltrene er baseret på **maskinlæring**, hvor en læringsalgoritme analyserer store mængder data om indhold for at finde sammenhænge og mønstre i dataene. Disse sammenhænge og mønstre kan bruges af indholdsfiltret til at klassificere nye eksempler, der enten skal fjernes eller tillades.

I visse tilfælde vil filtrets resultater efterfølgende blive **gennemgået af en person**, der skal afklare, om indholdet reelt skal fjernes. I andre tilfælde er der **ingen menneskelig kontrol** med indholdsfiltret.

Algoritmer kan **ikke forstå konkrete omstændigheder** eller andre sammenhænge, heller ikke når disse vil være indlysende for et menneske. Selv algoritmisk sofistikerede indholdsfiltre udviklet på store datasæt af høj kvalitet vil derfor i praksis altid have en **begrænset præcision i sorteringen.** Det vil sige, at de kommer til at fjerne både for lidt og for meget.[106]

Det er desuden et problem, at det oftest er **umuligt at få indblik i, hvorfor og hvordan filtret har truffet en "beslutning"** om at fjerne indhold.

FN's specialrapportør for ytringsfrihed har anført, at indholdsfiltre rejser særlige menneskeretlige risici, og at platformene skal være opmærksomme på begrænsningerne ved de automatiserede løsninger.[107]

5.1.3.2 *Upload*-filtre

En særlig problemstilling opstår, når der er tale om automatiserede filtre til forudgående blokering af indhold (**såkaldte *upload*-filtre**) eller lignende redskaber, der indebærer, at indhold end ikke kan uploades på platformen.

FN's specialrapportør for ytringsfrihed har fremhævet de udfordringer, som en sådan forudgående "censur" vil føre til, og anført, at sådanne filtre næppe vil være forenelig med ytringsfriheden – heller ikke, hvis de underlægges menneskeligt tilsyn, da indgrebet er for intensivt til, at efterfølgende menneskelig kontrol kan opveje det.[108]

I lyset af dette har instituttet tidligere anbefalet, at *upload*-filtre ikke bruges til indhold, der ikke tidligere er blevet vurderet ulovligt, når virksomhederne skal opfylde krav om for eksempel "passende foranstaltninger" for at hindre ulovligt indhold. Instituttet har i øvrigt anbefalet, at vurderingen af, om indhold er ulovligt, underlægges myndighedstilsyn.

Er der derimod tale om indhold, som allerede er blevet vurderet ulovligt, kan *upload*-filtre anvendes til at forhindre (gen)upload af indholdet på platformen – noget, som platformene efter omstændighederne kan være forpligtet til.

CHRISTCHURCH

I 2019 skete der et terrorangreb mod Al Noor moskéen i den New Zealandske by Christchurch. Gerningsmanden livestreamede angrebet på sin Facebookprofil, og videoen gik hurtigt viralt på blandt andet Facebook, YouTube, Twitter og Reddit. Det viste sig at være en vanskelig opgave for de involverede sociale medier at fjerne videoen, da den hurtigt blev delt, downloaded og lagt ud i forskellige udgaver og størrelser. De involverede tech-giganter er siden blevet kritiseret for ikke at være effektive nok til at finde og fjerne videoen, men også for at videoen overhovedet kunne finde vej til deres platforme.[109] I den forbindelse kan automatiserede teknikker og søgemetoder være nødvendige.[110]

5.1.3.3 Automatisk udvælgelse af indhold

Tech-giganterne bruger også algoritmer til at udvælge, hvilket indhold der gøres tilgængelig for den enkelte borger. Specialrapportøren for ytringsfrihed har fremhævet, at brugen af kunstig intelligens styrer adgangen til information på måder, der er uigennemsigtige for den enkelte borger og sommetider endog for platformen selv. Dette kan medføre, at borgeren tilbydes begrænset eller slet ingen eksponering for bestemte typer af vigtige sociale eller politiske historier.[111]

Denne problemstilling omtales ofte som **filterbobler** eller **ekkokamre** med henvisning til, at overbevisninger forstærkes ved gentagelse, hvilket i yderste tilfælde kan have betydning for **informationsfriheden**.[112]

FILTERBOBLER OG EKKOKAMRE

Filterbobler og ekkokamre henviser til, at en algoritme sorterer i de informationer, som borgeren præsenteres for, på baggrund af de informationer, som tjenesten har om borgeren (for eksempel placering, tidligere søgehistorik, tidligere opslag mm.). Borgeren skubbes herved ubemærket i retning af nyheder og debatter, der bestyrker vedkommendes egne holdninger.[113]

FN's specialrapportør for ytringsfrihed har fremhævet følgende:

> "The intersection of technology and content curation raises novel questions about the types of coercion or inducement that may be considered an interference with the right to form an opinion."[114]

Europarådets ministerkomité har ligeledes advaret mod den mulige manipulation i algoritmiske processer, herunder deres indvirkning på menneskerettighederne.[115]

Der kan næppe stilles krav om, at tech-giganterne helt skal afstå fra brugen af indholdsfiltre, automatiseret udvælgelse af indhold mv., men der kan og bør sættes minimumskrav til brugen.

I den forbindelse kan det overvejes, om tech-giganternes brug af indholdsfiltre, automatiseret udvælgelse af indhold mv. kan reguleres ved en reel og kontinuerlig menneskelig kontrol med de automatiserede systemer og deres udvikling: et effektivt klagesystem (se ovenfor) samt udførlige transparensrapporter med formkrav til, hvilke oplysninger platformene skal afgive.[116]

5.2 RETTEN TIL RESPEKT FOR PRIVATLIV OG BESKYTTELSEN AF PERSONOPLYSNINGER

5.2.1 OVERVÅGNINGSKAPITALISME

Forretningsmodellen for tech-giganterne er i vid udstrækning baseret på indsamling og brug af så mange oplysninger som muligt om borgerne. Dette sker på baggrund af:

1. oplysninger, borgerne bevidst afgiver, og
2. oplysninger, borgerne ubevidst afgiver, fordi de kan udledes af adfærd, søgemønstre, præferencer, sociale netværk osv.[117]

Forretningsmodellen er særlig karakteristisk for tech-giganter som Google og Facebook, idet borgernes oplysninger indgår som (den eneste) betaling for at bruge deres tjenester og platforme. Forretningsmodellen udgør imidlertid en **markedslogik**, der rækker langt ud over tech-giganterne.[118]

Markedet for handel med oplysninger omfatter også kommercielle aktører som for eksempel datamæglere (”***data brokers***”), der samler og sælger oplysninger fra diverse kilder,[119] og ”***ad tech***”-virksomheder, som tilbyder specialdesignede analyser og værktøjer til brug for digital markedsføring.[120]

De oplysninger, der indsamles af virksomhederne, bruges til at udvikle profiler af borgerne, til at forudsige adfærd, til målrettet markedsføring og til at påvirke borgernes køb og holdninger.[121]

Den omfattende indsamling og brug af personoplysninger er blevet beskrevet som **overvågningskapitalisme**.

Overvågningskapitalismen er kendetegnet ved, at virksomhederne opsamler og genererer oplysninger om alle aspekter af borgernes liv, herunder deres erfaringer, præferencer, sociale liv, kommunikation, forbrugsmønster, kulturelle og politiske aktiviteter mv. og omsætter disse data til produkter, der kan sælges. Som led i denne praksis er der **skabt nye produkter og markeder**, der er baseret på evnen til at kunne forudsige og påvirke borgeres adfærd.[122]

Man taler om, at overvågningen er til stede over alt (”***ubiquitous surveillance***”)[123], idet den enkelte overvåges i det digitale rum og i det fysisk rum – og både i det offentlige og i privatsfæren – via smartphones og ”***internet of things devices***”.[124]

INTERNET OF THINGS (IOT)

IoT er en teknologi, der forbinder genstande til internettet, så de løbende kan sende relevant information. Der kommer hele tiden nye ”intelligente ting” på markedet, der kan overvåge og kommunikere med borgernes hjem og bil eller monitorere fysisk aktivitet og søvnmønstre. Da teknologien bygger på en omfattende indsamling og behandling af personlige oplysninger, afføder dens udvikling nye databeskyttelsesudfordringer

Virksomhedernes omfattende dataindsamling påvirker borgernes ret til respekt for privatliv og personoplysninger.

Retten til respekt for privatliv og beskyttelse af personoplysninger giver en bred beskyttelse af borgernes digitale aktiviteter. Beskyttelsen gælder ikke blot selve indholdet af for eksempel en e-mail, men også metadata, der kan analyseres, aggregeres og sammenstilles med andre data, for derved at afsløre oplysninger om den enkeltes adfærd, sociale forhold, private præferencer og identitet.[125]

Udarbejdelsen af detaljerede profiler kan bruges til såkaldt "***micro-targeting***".[126] Et af de mest omtalte eksempler på dette er Cambridge Analytica-sagen, hvor data indsamlet via en app på Facebook blev brugt til målrettet påvirkning i forbindelse med det amerikanske præsidentvalg. I oktober 2019 blev Facebook idømt en bøde på £500.000 for brud på den britiske databeskyttelseslov i forbindelse med Cambridge Analytica-sagen.[127]

CAMBRIDGE ANALYTICA

Cambridge Analytica var et britisk konsulentfirma, der tilbød virksomheder og politiske aktører analyse og rådgivning med henblik på målrettet annoncering. I 2018 blev det afsløret, at Cambridge Analytica havde indsamlet personlige oplysninger fra 87 millioner Facebookbrugere i forbindelse med det amerikanske præsidentvalg i 2016. Oplysningerne blev brugt til at påvirke uafklarede vælgere i de amerikanske svingstater til at stemme på Donald Trump.[128]

Det er blevet anført, at tech-giganternes forretningsmodel grundlæggende strider mod den menneskeretlige beskyttelse af privatliv.[129]

FN's specialrapportør for privatliv har anført:

> "The tendency of Big Data to intrude into the lives of people by making their informational selves known in granular detail to those who collect and analyse their data trails is fundamentally at odds with the right to privacy and the principles endorsed to protect that right.
> Much of the economy of the modern Internet depends on harvesting complex data about potential customers in order to sell them things, a practice known as "Surveillance Capitalism". However, surveillance does not seem any more justifiable to data-driven efficiency than child-labour is to an industrial economy. It is only the most convenient and easiest way to exploit the information. It is not a fundamental right as is the right to privacy. Indeed, the data-driven economy would survive and prosper if minimal standards and improved technologies

> forced corporations and governments into a world in which ordinary people had much greater control over their own data." [130] (Noter udeladt)

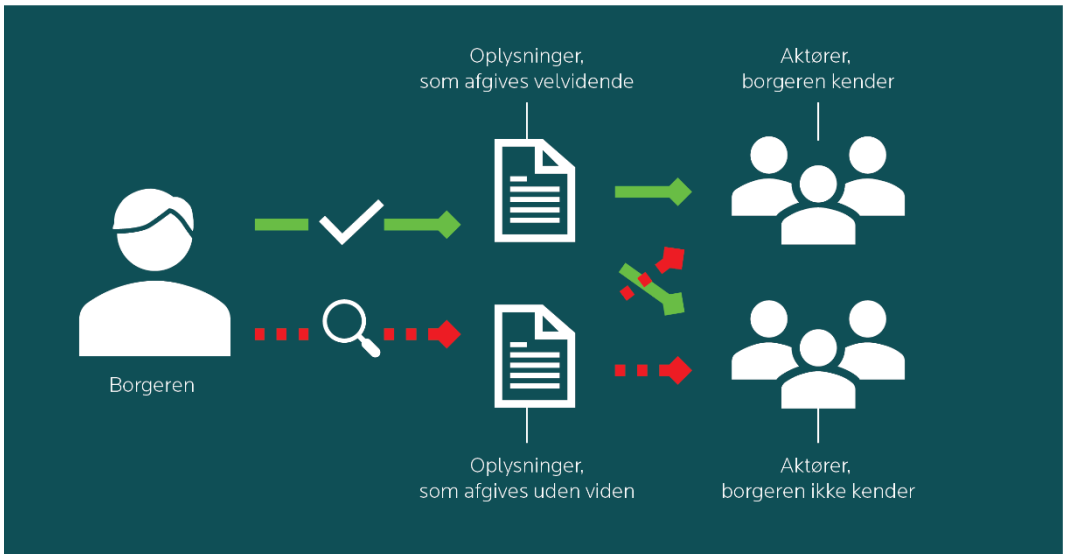
5.2.1.1 Manglende gennemsigtighed

Tech-giganternes omfattende indsamling og brug af oplysninger om borgerne udgør et uigennemsigtigt system, der udfordrer retten til privatliv. FN's specialrapportør for privatliv har fremhævet, at der sker en massiv deling af oplysninger mellem virksomheder (og stater), som den enkelte borger ikke kan få et indblik i.[131]

Det uigennemsigtige samspil mellem de mange aktører på markedet fører til **et rettighedstab**, der er blevet beskrevet således:

> "When using available software and services online, users are defaulted into bundles of relationships with first- and third-party service providers, which are collecting their information in ways that leave little room for real choice or escape."[132]

Markedets nuværende struktur indebærer således, at oplysninger om den enkelte borger deles og bruges af en lang række aktører, som borgeren ikke kender til. De uigennemsigtige relationer aktørerne imellem medfører blandt andet, at borgeren ikke ved, hvem en klage skal rettes imod.



5.2.1.2 Konkurrenceret som menneskeretligt værn

Da der er tale om et relativt nyt marked, er **tech-giganternes magt tillige blevet undersøgt i lyset af konkurrence- og forbrugerretten**[133] og gennem regulering af standarder ("*protocols*").[134] Tiltag inden for disse områder kan få en positiv effekt på de menneskeretlige udfordringer.

For eksempel har de tyske konkurrencemyndigheder i en sag om Facebooks konkurrenceretlige styrke på markedet fremhævet, at når adgangen til personoplysninger er afgørende for en virksomheds markedsstyrke (som tilfældet er for Facebook), er spørgsmålet om indsamling og behandling af personoplysninger ikke kun et persondataretligt spørgsmål, men også et konkurrenceretligt spørgsmål.[135] Manglende **gennemsigtighed** om virksomhedernes brug af personoplysninger kan føre til uberettigede konkurrencefordele.[136] Dette har ført til forslag om, at lovgivere skal arbejde for at samtænke konkurrenceretten og retten til privatliv og persondata, blandt andet ved at konkurrencemyndighederne vurderer **privatliv og personoplysninger som et konkurrenceparameter**.[137]

5.2.1.3 Forøgede risici på grund af automatisering

Udfordringerne for menneskeretten forstærkes af den øgede brug og genbrug af data, som værktøjer baseret på kunstig intelligens ofte vil indebære. Dette er blevet fremhævet af FN's specialrapportør for ytringsfrihed i en nylig rapport om kunstig intelligens:

> "AI challenges traditional notions of consent, purpose and use limitation, transparency and accountability — the pillars upon which international data protection standards rest. Because AI systems work by exploiting existing datasets and creating new ones, the ability of individuals to know, understand and exercise control over how their data are used is deprived of practical meaning in the context of AI. Once data are repurposed in an AI system, they lose their original context, increasing the risk that data about individuals will become inaccurate or out of date and depriving individuals of the ability to rectify or delete the data."[138]

Databeskyttelsesforordningen indeholder **i artikel 22 et forbud** mod automatiserede afgørelser, der *betydeligt påvirker* borgeren. Forbuddet gælder både for offentlige og private, men det er ikke klart, hvordan "afgørelser", der

”betydeligt påvirker” borgeren, skal forstås i forhold til tech-giganternes indsamling og automatiserede behandling af personoplysninger.

Artikel 29-arbejdsgruppen (nu erstattet af det Europæiske Databeskyttelsesråd) har udtalt, at tech-giganternes markedsføring, der ofte baserer sig på automatiseret behandling, *ikke* anses for at påvirke individet betydeligt og **derfor ikke er forbudt efter artikel 22.** I visse tilfælde kan markedsføringen **dog påvirke borgeren betydeligt**. Dette afhænger blandt andet af, 1. hvor ”dybdegående” profileringen er, herunder om den indebærer sporing på tværs af forskellige websteder, enheder og tjenester, 2. borgernes egne forventninger og ønsker til tjenesten, 3. annonceringsmåden og 4. om markedsføringen gør brug af viden om borgerens eventuelle sårbarheder.[139]

Der findes hverken dansk eller EU-praksis om bestemmelsens rækkevidde og fortolkning i forhold til tech-giganternes indsamling og behandling af personoplysninger.

5.2.2 PERSONDATARETLIGE UDFORDRINGER VED TECH-GIGANTERNES PRAKSIS

Tech-giganternes forretningsmodel udfordrer flere af de centrale persondataretlige principper, som gennemgås i det følgende.

Tech-giganternes brug af personoplysninger kan generelt opdeles i to:

1. **Kommercielle formål**, der kan være alt fra udvikling af egne tjenester og produkter til videresalg til øvrige private aktører.

2. **Bidrag til myndighedsopgaver**, som navnlig politiets efterforskning, samt til kriminalitetsbekæmpelse eller efterretningsvirksomhed.

Sidstnævnte falder uden for emnet for denne rapport, men det kan kort bemærkes, at for så vidt angår statslig overvågning, herunder virksomhedernes videregivelse af oplysninger til myndighederne, er staten bundet af sine **menneskeretlige forpligtelser**.[140]

GLOBAL NETWORK INITIATIVE (GNI)

Når tech-giganterne anmodes om at udlevere oplysninger om den enkelte bruger til staterne, sker der en vis selvregulering gennem **Global Network Initiative (GNI)**. I regi af GNI har de deltagende virksomheder forpligtet hinanden til at overholde menneskeretlige standarder ved anmodninger fra stater, der vedrører retten til privatliv. Initiativet har den begrænsning, at det kun vedrører tilfælde, hvor stater retter henvendelse til virksomhederne, og *ikke* de tilfælde, hvor virksomheden handler på eget initiativ. Det betyder, at virksomhedens praksis, for eksempel i forhold til indsamling af oplysninger om sine brugere til kommercielle formål, ikke er omfattet af initiativet

For så vidt angår **de kommercielle formål** reguleres brugen af personoplysninger – inklusive indsamling og videregivelse af data – af de regler om respekt for privatliv og databeskyttelse, som binder private aktører.

Det mest relevante regelsæt er **databeskyttelsesforordningen**. Tech-giganternes adgang til oplysninger udfordrer her særligt kravene til **dataminimering, formålsbestemthed, (oplyst) samtykke og indsigt.**[141]

5.2.2.1 Dataminimering

Kravet om **dataminimering**[142] betyder, at både typen og mængden af personoplysninger skal være relevant og tilstrækkelig i forhold til det formål, hvortil oplysningerne er indsamlet. Konsekvensen af dette krav er, at virksomheder **ikke må indsamle flere personoplysninger end højst nødvendigt**, og at de ikke må indsamle oplysningerne uden formål (se afsnit 5.2.2.2).

Dataminimeringskravet udfordres af den gængse forretningsmodel, der er baseret på at indsamle og generere så meget viden om den enkelte som muligt.[143]

Herudover er præcisionen og effektiviteten i algoritmisk baserede værktøjer typisk afhængig af store mængder af oplysninger, hvilket ligeledes udfordrer kravet om at indsamle og behandle så få oplysninger som muligt.[144]

5.2.2.2 Formålsbestemthed

I forlængelse af dette gælder kravet om **formålsbestemthed**[145], der begrænser virksomheders adgang til at indsamle og behandle oplysninger. I kravet ligger, at personoplysninger kun må indsamles til udtrykkelige, bestemte og lovlige formål, samt at oplysninger ikke må viderebehandles på en måde, der er *uforenelig* med det oprindelige formål. Formålsbestemtheden skal blandt andet sikre, at borgeren med rimelighed kan forudsige databehandlingens omfang og konsekvenser.

I en forretningsmodel, hvor tech-giganter indsamler og udleder personoplysninger fra en lang række datapunkter, vil kravet om formålsbestemthed typisk blive håndteret ved beskrivelser af meget brede formål med dataindsamlingen i de respektive forretningsbetingelser. Sådanne brede og upræcise formål med dataindsamlingen risikerer at udvande princippet om formålsbestemmelse.

5.2.2.3 Indsigtsretten

Efter databeskyttelsesreglerne har den enkelte borger ret til indsigt i egne data, herunder hvilke personoplysninger der behandles, og hvem oplysningerne deles med. **Indsigtsretten**[146] skal blandt andet sikre, at databehandlingen er gennemsigtig for den enkelte borger, og at denne kan vurdere, om databehandlingen er rimelig og lovlig.

I praksis er der imidlertid en stadig stigende **informationsasymmetri** mellem den enkelte borger og tech-giganterne. Borgeren har meget begrænset indsigt i, hvilke personoplysninger platformene behandler, særligt de data og den profil, der genereres på baggrund af den enkeltes forskellige digitale aktiviteter. Man kan sige, at tech-giganterne ved stadigt mere om de enkelte borgere, mens de enkelte har begrænset indsigt i den databehandling, der vedrører dem selv.

5.2.2.4 Samtykke

Den enkelte persons mulighed for kontrol med egne data er et centralt element i beskyttelsen af personoplysninger, og her spiller **samtykket**[147] en vigtig rolle som en ud af flere ”hjemler” til at behandle oplysninger. Samtykket er den enkeltes mulighed for at give tilladelse til en given databehandling, og denne viljestilkendegivelse skal ske frivilligt, specifikt og informeret.

Kravet om et frivilligt, specifikt og informeret samtykke udfordres af digitale tjenester, idet borgeren ofte samtykker til tjenestens vilkår uden indsigt i de betingelser, der samtykkes til. Fordi tech-giganternes platforme og tjenester er så udbredte og dermed for mange spiller en helt central rolle, oplever den enkelte borger ikke samtykket som et reelt (frivilligt og oplyst) valg, men derimod som en forudsætning for at kunne deltage i relevante netværk, debatter, informationssøgning, mv.[148]

Hertil kommer, at borgeren ikke nødvendigvis vil have kendskab til de ofte vidtrækkende konsekvenser af et samtykke, herunder videresalg og brug af personoplysninger til målrettet markedsføring eller profilering, fordi samtykket ikke bliver beskrevet lettilgængeligt og letforståeligt af platformen. Den retsgaranti, som et samtykke indebærer, kan risikere at blive udhulet både af længden og kompleksiteten på samtykkeerklæringen og af det antal af gange, borgeren bliver anmodet om at samtykke (*consent fatigue*).[149] Det er desuden usikkert, hvorledes borgerens ret til at trække samtykket tilbage kan håndhæves effektivt i de tilfælde, hvor oplysninger om borgeren (herunder profiler om borgeren udarbejdet af algoritmiske værktøjer) er videregivet til andre kommercielle aktører.[150]

Kravene til samtykke er blandt andet adresseret af det franske datatilsyn, **CNIL**, der i 2019 gav Google en bøde på EUR 50 millioner. Dette er CNIL's første bøde, efter databeskyttelsesforordningen blev vedtaget, og bødens størrelse er ifølge CNIL begrundet i alvoren af de konstaterede brud på de grundlæggende principper i forordningen om gennemsigtighed, information og samtykke.[151]

Kravene til samtykke spillede også en central rolle, da datatilsynet i februar 2020 udtalte alvorlig kritik af DMI's brug af personoplysninger via bannerannoncer fra Google.[152] I afgørelsen fastslog Datatilsynet, at både DMI og Google har en økonomisk interesse i databehandlingen, og at samtykkemodellen på dmi.dk ikke lever op til lovgivningens krav om gennemsigtighed, blandt andet fordi det kræver et ekstra skridt for borgeren at afslå at give samtykke. Muligheden for at afslå samtykke skal således fremgå ligeså enkelt og tydeligt som muligheden for at give samtykke.

5.2.2.5 Manglende prøvelse ved de europæiske domstole

Spørgsmålet om tech-giganternes brug af personoplysninger til kommercielt brug er hverken blevet vurderet af Den Europæiske Menneskerettighedsdomstol (i forhold til et potentielt statsansvar) eller af EU-Domstolen (i forhold til de EU-retlige forpligtelser, som påhviler virksomhederne), men rundt om i medlemsstaterne bliver tech-giganternes forpligtelser i henhold til EU-rettens beskyttelse af privatliv og personoplysninger prøvet på nationalt plan.

Da de europæiske domstole endnu ikke har undersøgt tech-giganternes adfærd i lyset af retten til privatliv og beskyttelsen af personoplysninger, varierer beskyttelsen i de enkelte medlemslande, ligesom der mangler en fælles europæisk forståelse af persondatarettens rækkevidde.

En beslægtet problemstilling består i, at det kan være svært for den enkelte borger at gennemskue, hvor og hvordan sager mod tech-giganterne skal indbringes. Denne problemstilling er afspejlet i EU-Domstolens domme som for eksempel **Google Spain, CNIL mod Google** og **Wirtschaftsakademie.** I EU-retsligt regi er det tanken, at Det Europæiske Databeskyttelsesråd skal medvirke til en ensretning af reglerne.[153]

KAPITEL 6

UDVALGTE PUBLIKATIONER FRA INSTITUT FOR MENNESKERETTIGHEDER

6.1 FAKTA-ARK

Fakta-ark om automatiserede indholdsfiltre på digitale platforme (2019):
https://menneskeret.dk/sites/menneskeret.dk/files/media/dokumenter/udgivelser/policy_briefs/faktaark_om_automatiske_indholdsfiltre_paa_digitale_platforme.pdf

Fakta-ark over Europarådets standarder på teknologi og menneskerettigheder (2019):
https://menneskeret.dk/sites/menneskeret.dk/files/media/dokumenter/faktaark_om_europaraadet_menneskerettigheder_og_teknologi.pdf

Fakta-ark over FN's standarder på teknologi og menneskerettigheder (2019):
https://menneskeret.dk/sites/menneskeret.dk/files/media/dokumenter/udgivelser/faktaark_qa/faktaark_om_fn_menneskerettigheder_og_teknologi_-_dansk_version.pdf

Fakta-ark om privatliv og databeskyttelse (2018):
https://menneskeret.dk/sites/menneskeret.dk/files/media/dokumenter/udgivelser/faktaark_qa/faktaark_om_databeskyttelse_og_retten_til_privatliv.pdf

6.2 RAPPORTER

Institut for Menneskerettigheder (2019). Rapport om demokratisk deltagelse på Facebook:
https://menneskeret.dk/sites/menneskeret.dk/files/04_april_19/Rapport%20om%20demokratisk%20deltagelse.pdf

Institut for Menneskerettigheder (2017). Rapport om hadefulde ytringer i den offentlige online debat:
https://menneskeret.dk/sites/menneskeret.dk/files/media/dokumenter/udgivelser/ligebehandling_2017/rapport_om_hadefulde_ytringer_2._oplag_2017.pdf

6.3 HØRINGSSVAR

Institut for Menneskerettigheder, Høringssvar vedrørende gennemførelse af AVMS-direktivet (2019): https://menneskeret.dk/hoeringssvar/gennemfoerelse-avms-direktivet

Institut for Menneskerettigheder, Høringssvar vedrørende forebyggelse af udbredelsen af terrorrelateret online-indhold (2018): https://menneskeret.dk/hoeringssvar/hoering-forslag-forordning-forebyggelse-udbredelsen-terrorrelateret-online-indhold

6.4 UDGIVELSER

Jørgensen, Rikke Frank red. (2019) *Human Rights in The Age of Platforms,* MIT Press: https://menneskeret.dk/udgivelser/human-rights-in-the-age-of-platforms

Jørgensen, Rikke Frank (2017). Framing human rights: exploring storytelling within internet companies, *Information, Communication & Society*, 21:3, p. 340-355: https://www.tandfonline.com/doi/full/10.1080/1369118X.2017.1289233

Jørgensen, Rikke Frank (2017). What Platforms Mean When They Talk About Human Rights, *Policy and Internet, 9:3*, p. 280-296: https://onlinelibrary.wiley.com/doi/abs/10.1002/poi3.152

Jørgensen, Rikke Frank m.fl. (2017). EU-studie om ICT og menneskerettigheder (FRAME): https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/udgivelser/research/frame/frame_-_ict_and_human_rights.pdf

Jørgensen, Rikke Frank og Olsen, Birgitte Kofod red. (2018). *Eksponeret - Grænser for privatliv i en digital tid*, Gads Forlag: https://menneskeret.dk/udgivelser/eksponeret-graenser-privatliv-digital-tid

Jørgensen, Rikke Frank og Pedersen, Anja Møller (2017). Online service providers as human rights arbiters in Taddeo & Floridi, *The Responsibilities of Online Service Providers*, Springer, p. 179-199: https://link.springer.com/chapter/10.1007/978-3-319-47852-4_10

Jørgensen, Rikke Frank og Zuleta, Lumi (2020). Private Governance of Freedom of Expression on Social Media Platforms. Nordicom 41(1): https://content.sciendo.com/view/journals/nor/41/1/article-p51.xml

O´Brien, Claire Methven (2018), Business and Human Rights – A Handbook for legal practitioners, udgivet for Europarådet: https://rm.coe.int/business-and-human-rights-a-handbook-of-legal-practitioners/168092323f

[1] Se Rikke Frank Jørgensen og Birgitte Kofod Olsen reds., *Eksponeret – grænser for privatliv i en digital tid*, Gads Forlag 2019.
[2] Se FN's rapport om forenings- og forsamlingsfrihed i den digitale æra A/41/41, 17. maj 2019, tilgængelig her: https://undocs.org/A/HRC/41/41
[3] Se for eksempel FN's rapport om menings- og ytringsfrihed A/73/348, punkt 17f., 28. august 2018, tilgængelig her: https://undocs.org/A/73/348
[4] Se for eksempel EU's handlingsplan for bekæmpelse af desinformation (JOIN (2018) 36 final), tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52018JC0036&from=GA. Se også: https://menneskeret.dk/udgivelser/demokratisk-deltagelse-paa-facebook
[5] Se for eksempel: Kommissionens meddelelse om onlineplatforme og det digitale indre marked – Muligheder og udfordringer for Europa COM(2016) 288 final, tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:52016DC0288&from=EN
[6] Se Joris van Hoboken: "The Privacy Disconnect" i Rikke Frank Jørgensen red., *Human Rights in the Age of Platforms*, MIT Press 2019, s. 255-284.
[7] Jack M Balkin, "Old-School/New-School Speech Regulation" (2014), *Harvard Law Review* 127 (8):2296-234, tilgængelig her: https://harvardlawreview.org/2014/06/old-schoolnew-school-speech-regulation/ Se også: Rikke Frank Jørgensen red., *Human Rights in the Age of Platforms*, MIT Press, 2019, s. xvii-xlv.
[8] Paul Nemitz, "Constitutional democracy and technology in the age of artificial intelligence" (2018) Vol. 376, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, tilgængelig her: http://doi.org/10.1098/rsta.2018.0089
[9] Se Emily Laidlaw, *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility*, Cambridge University Press, 2015, s. 44-57.
[10] Rikke Frank Jørgensen, *Framing the Net: The Internet and Human Rights*, Edward Elgar 2013, s. 93-95.
[11] Se Martin Moore, *Tech Giants and Civic Power*, Kings College London, april 2016, tilgængelig her: https://www.kcl.ac.uk/policy-institute/assets/cmcp/tech-giants-and-civic-power.pdf

[12] Amnesty International, *Surveillance Giants*, 2019, tilgængelig her: https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF s. 11f.
[13] Se for eksempel FN's rapporter A/HRC/29/31 og A/HRC/27/37, tilgængelige her: https://www.undocs.org/A/HRC/29/31 og her: https://undocs.org/A/HRC/27/37
[14] Se rapport fra FN's specialrapportør for ytringsfrihed A/74/486, tilgængelig her: https://undocs.org/en/A/74/486. Se også: Menneskerettighedskomiteens General Comment No. 34 (2011) om de to typer af rettigheder, tilgængelig her: https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf
[15] Se Racediskriminationskomiteens General Comment No. 35 (2013), punkt 12, tilgængelig her: https://www.refworld.org/type,GENERAL,CERD,,53f457db4,0.html
[16] Se rapport fra FN's specialrepræsentant for generalsekretæren, A/HRC/17/31, tilgængelig her: https://www.ohchr.org/Documents/Issues/Business/A-HRC-17-31_AEV.pdf. Se også: Stéphanie Lagoutte: *The State Duty to Protect Against Business-related human rights abuses,* DIHR Research Papers 2014/1, tilgængelig her: https://www.humanrights.dk/publications/state-duty-protect-against-business-related-human-rights-abuses
[17] Se Nora Götzman red., *Handbook on Human Rights Impact Assessment*, Edward Elgar, 2019.
[18] Se Alex Warofka, "An Independent Assessment of the Human Rights Impact of Facebook in Myanmar" *(Facebook, 2018),* tilgængelig her: https://about.fb.com/news/2018/11/myanmar-hria/
[19] Se Anne Mette Lauritzen og Frederik Stjernfelt, *Dit opslag er blevet fjernet,* Gyldendal, 2019, s. 171.
[20] Se rapport fra FN's fact-finding mission i Myanmar, s. 14 nederst: A/HRC/39/64, tilgængelig her: https://undocs.org/en/A/HRC/39/64
[21] Se rapport fra FN's specialrapportør for ytringsfrihed, A/HRC/38/35, tilgængelig her: https://undocs.org/en/A/HRC/38/35
[22] Se rapport fra FN's højkommissær for menneskerettigheder A/HRC/39/29, tilgængelig her: https://undocs.org/A/HRC/39/29. Se endvidere: Jørgensen, Rikke Frank og Lumi Zuleta (2020). Private Governance of Freedom of Expression on Social Media Platforms. Nordicom 41(1):

https://content.sciendo.com/view/journals/nor/41/1/article-p51.xml?language=en

[23] Se EMD-sag: Times Newspapers Ltd mod Storbritannien, præmis 27, tilgængelig her: https://hudoc.echr.coe.int/eng#{"dmdocnumber":["848220"],"itemid":["001-91706"]}. For et samlet overblik over Den Europæiske Menneskerettighedsdomstols praksis om ytringsfrihed på nettet henvises i øvrigt til Dirk Voorhoof, "Same standards, different tools? The ECtHR and the protection and limitations of freedom of expression in the digital environment" i *Human Rights Challenges in the Digital Age: Judicial Perspectives*, januar 2020.

[24] Se EMD-sag Delfi A/S mod Estland, præmis 115 og 116, tilgængelig her: https://hudoc.echr.coe.int/eng#{"itemid":["001-155105"]}. Se også: EMD-sag Magyar Helsinki Bizottság mod Ungarn, tilgængelig her: https://hudoc.echr.coe.int/eng#{"itemid":["001-167828"]} og EMD-sag Høiness mod Norge, tilgængelig her: https://hudoc.echr.coe.int/eng#{"itemid":["001-191740"]}

[25] Se EMD-sag Appleby m.fl. v. Storbritannien, præmis 47-49, tilgængelig her: https://hudoc.echr.coe.int/eng#{"itemid":["001-61080"]}. Se også: Europarådets forskningsrapport 2011, "Positive obligations on member States under Article 10 to protect journalists and prevent impunity", p. 4-5, tilgængelig her: https://www.echr.coe.int/Documents/Research_report_article_10_ENG.pdf

[26] Se EMD-sag Von Hannover mod Tyskland, tilgængelig her: https://hudoc.echr.coe.int/eng#{"itemid":["001-61853"]}, EMD-sag Couderc mod Frankrig, tilgængelig her: https://hudoc.echr.coe.int/eng#{"itemid":["001-158861"]} og EMD-sag Delfi mod Estland, tilgængelig her: https://hudoc.echr.coe.int/eng#{"itemid":["001-155105"]}.

[27] Jon Kjølbro, *Den Europæiske Menneskerettighedskonventionen – for praktikere* (4. udgave). Djøf Forlag, 2017, s. 798.

[28] Jon Kjølbro, *Den Europæiske Menneskerettighedskonventionen – for praktikere* (4. udgave). Djøf Forlag, 2017, s. 800 med henvisning til EMD-sag K.U. mod Finland, præmis 40-51, tilgængelig her: https://hudoc.echr.coe.int/eng#{"itemid":["001-89964"]}

[29] Jon Kjølbro, *Den Europæiske Menneskerettighedskonventionen – for praktikere* (4. udgave). Djøf Forlag, 2017, s. 802.

[30] Se EMD-sag Paksas mod Litauen, præmis 88, tilgængelig her: https://hudoc.echr.coe.int/eng#{"itemid":["001-102617"]}. Se også: Jon Kjølbro, *Den Europæiske Menneskerettighedskonvention – for praktikere* (4. udgave). Djøf Forlag, 2017, s. 1073.

[31] Se navnlig EMD-sag S & Marper mod Storbritannien, tilgængelig her: https://hudoc.echr.coe.int/eng#{"itemid":["001-90051"]} . Se også et overblik over Domstolens praksis om persondatabeskyttelse i Domstolens fakta-ark af oktober 2019, tilgængeligt her: https://www.echr.coe.int/Documents/FS_Data_ENG.pdf

[32] Se EMD-sag Satakunnan mod Finland, præmis 137, tilgængelig her: https://hudoc.echr.coe.int/eng#{"itemid":["001-175121"]}

[33] Se EMD-sag M.S. mod Sverige, præmis 35, tilgængelig her: https://hudoc.echr.coe.int/eng#{"itemid":["001-58177"]} og EMD-sag Perry mod Storbritannien, præmis 39ff, tilgængelig her: https://hudoc.echr.coe.int/fre#{"itemid":["001-61228"]}

[34] Se EMD-sag Perry mod Storbritannien, præmis 48, tilgængelig her: https://hudoc.echr.coe.int/fre#{"itemid":["001-61228"]}

[35] Se EMD-sag Centrum För Rättvisa mod Sverige, tilgængelig her: https://hudoc.echr.coe.int/eng#{"itemid":["001-183863"]} og Big Brother Watch m.fl. mod Storbritannien, tilgængelig her: https://hudoc.echr.coe.int/eng#{"itemid":["001-186048"]}

[36] Se Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (1981), tilgængelig her: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

[37] Anbefaling fra Europarådets ministerkomité CM/Rec(2008)6, tilgængelig her: https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2008-6-of-the-committee-of-ministers-to-member-states-on-measures-to-promote-the-respect-for-freedom-of-expression-and-informati?inheritRedirect=false

[38] Anbefaling fra Europarådets ministerkomité CM/Rec(2016)3, tilgængelig her: https://edoc.coe.int/en/fundamental-freedoms/7302-human-rights-and-business-recommendation-cmrec20163-of-the-committee-of-ministers-to-member-states.html. Se også: Claire Methven O´Brien, *Business and Human Rights, a handbook for legal practitioners*, (CoE, 2018), tilgængelig her: https://rm.coe.int/business-and-human-rights-a-handbook-of-legal-practitioners/168092323f

[39] Se Europarådets resolution 1843(2011) om beskyttelsen af privatliv og personoplysninger på internettet, tilgængelig her:

http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=18039&lang=en

[40] Se Europarådets resolution 2311 "Human rights and business – what follow-up to Committee of Ministers Recommendation CM/Rec(2016)3?", tilgængelig her: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=28296&lang=en

[41] En samlet oversigt over standarder relateret til artikel 8 er tilgængelig her: https://www.coe.int/en/web/portal/personal-data-protection-and-privacy, og i relation til artikel 10 her: https://www.coe.int/en/web/portal/protecting-freedom-of-expression-and-information

[42] Se Den Europæiske Unions Grundlæggende Charter (2010/C 83/02), tilgængeligt her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:12010P&from=EN

[43] Se e-handelsdirektivet 2000/31/EC, tilgængeligt her: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031

[44] Se også: Thomas Riis m.fl., "Leaving the European Safe Harbor, Sailing Towards Algorithmic Content Regulation", Journal of Internet Law, Vol. 22, No. 7, 2019, tilgængelig her: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3300159

[45] Se Europaparlamentets baggrundspapir af 20. maj 2020, tilgængeligt her: https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA(2020)649404_EN.pdf

[46] Se Europaparlamentets og Rådets direktiv 2011/93/EU af 13. december 2011 om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og børnepornografi, tilgængeligt her: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:32011L0093

[47] Se Europaparlamentets og Rådets direktiv 2019/790 af 17. april 2019 om ophavsret og beslægtede rettigheder på det digitale indre marked, tilgængeligt her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32019L0790&from=EN

[48] Se Europaparlamentets og Rådets direktiv 2018/1808 af 14. november 2018 om ændring af direktiv 2010/13/EU om audiovisuelle medietjenester, tilgængeligt her: https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:32018L1808&from=DA

[49] Se EU-Domstolens afgørelse i C-70/10 (SABAM mod Scarlet Extended), tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:62010CJ0070&from=DA, se også: C-360/10, hvor samme problemstilling behandles: http://curia.europa.eu/juris/document/document.jsf?text=&do

cid=119512&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=1499753. Rækkevidden af artikel 15 er også behandlet i C-484/14 og C-324/09.

[50] Se EU-Domstolens afgørelse i C-70/10 (SABAM mod Scarlet Extended), præmis 40, tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:62010CJ0070&from=DA

[51] Se EU-Domstolens afgørelse C 70/10 (SABAM mod Scarlet Extended), præmis 50, tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:62010CJ0070&from=DA

[52] Se EU-Domstolens afgørelse C 18/18 (Glawischnig-Piesczek mod Facebook Ireland Limited), tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=1501064

[53] Se EU-Domstolens afgørelse C 18/18 (Glawischnig-Piesczek mod Facebook Ireland Limited), præmis 45, tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=1501064

[54] Se EU-Domstolens afgørelse C 18/18 (Glawischnig-Piesczek mod Facebook Ireland Limited), præmis 46, tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=1501064

[55]Se Databeskyttelsesforordningen (Generel Data Protection Regulation, EU) 2016/679, tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[56] Se også: Artikel 29-arbejdsgruppens udtalelse nr. 4/2007 om begrebet personoplysninger, tilgængelig her: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_da.pdf

[57] 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), tilgængelig her: https://www.retsinformation.dk/Forms/r0710.aspx?id=201319

[58] Se Europaparlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om databeskyttelse inden for elektroniske kommunikation, tilgængeligt: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32002L0058&from=DA

[59] Se herom Erklæring fra Det Europæiske Databeskyttelsesråd om revisionen af e-databeskyttelsesforordningen og om dennes indvirkning på beskyttelse af enkeltpersoner med hensyn til den

private og fortrolige karakter af deres kommunikation, tilgængelig her: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_da.pdf

[60] Se EU-Domstolens afgørelse i de forenede sager C-203/15 (Tele2 Sverige AB mod Post- och telestyrelsen) og C-698/1 (Secretary of State for the Home Department mod Tom Watson m.fl.), tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:62015CJ0203&from=EN

[61] Se EU-Domstolens afgørelse i C-673/17 (Planet49), tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=7376436

[62] Se EU-Domstolens afgørelse i C-131/12 (Google Spain), tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=7376861

[63] Se EU-Domstolens afgørelse i C-131/12 (Google Spain), præmis 80f., tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=7376861

[64] Se EU-Domstolens afgørelse i C-131/12 (Google Spain), præmis 88, tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=7376861

[65] Se EU-Domstolens afgørelse i C-507/17 (CNIL mod Google), tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=DA&mode=req&dir=&occ=first&part=1&cid=7377476

[66] Se EU-Domstolens afgørelse i C-507/17 (CNIL mod Google), præmis 60, tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=DA&mode=req&dir=&occ=first&part=1&cid=7377476

[67] Se EU-Domstolens afgørelse i C-507/17 (CNIL mod Google), præmis 67, tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=DA&mode=req&dir=&occ=first&part=1&cid=7377476. Se også: Christopher Docksey, "The EU approach to the protection of rights in the digital environment: today and tomorrow – State obligations and

responsibilities of private parties – GDPR rules on data protection, and what to expect from the upcoming ePrivacy regulation" i *Human Rights Challenges in the Digital Age: Judicial Perepctives* (CoE 2020).

[68] Se EU-Domstolens afgørelse C-210/16 (Wirtschaftsakademie), tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=7019567

[69] For yderligere om jurisdiktionsspørgsmål og håndhævelsen af menneskerettigheder i det digitale rum henvises til Human Rights Challenges in the Digital Age: Judicial Perspectives (CoE & ECoHR 2020)

[70] Se EU-Domstolens afgørelse C-362/14 (Maximillian Schrems), tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=7378769

[71] Kommissionens beslutning af 26. juli 2000 (om Safe Harbor-principperne) er tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:32000D0520&from=en

[72] Se EU-Domstolens afgørelse C-362/14 (Maximillian Schrems), præmis 78, tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=7378769

[73] Se generaladvokatens forslag til afgørelse i sag C-311/18, tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=471129

[74] Se EU-Domstolens afgørelse C-40/17 (Fashion ID), tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=7380173

[75] Se EU-Domstolens afgørelse C-40/17 (Fashion ID), præmis 101, tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=7380173

[76] Se EU-Domstolens afgørelse C-40/17 (Fashion ID), præmis 102 ff., tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&do

cid=216555&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=7380173

[77] Se samarbejdsaftalen angående bekæmpelse af hadefulde ytringer online her: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/countering-illegal-hate-speech-online_en

[78] Se Kommissionens arbejde vedrørende ansvar og pligter for digitale platforme her: https://ec.europa.eu/digital-single-market/en/online-platforms-digital-single-market

[79] Kommissionens henstilling 2018/334 af 1. marts 2018 (om foranstaltninger til effektiv bekæmpelse af ulovligt indhold på nettet) er tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32018H0334&from=en

[80] Se Ytringsfrihedskommissionens betænkning her: https://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2020/betaenkning_nr._1573_2020_del_1.pdf

[81] Se justitsministerens svar til Retsudvalget på REU (Alm. del), spørgsmål nr. 355 af 15. oktober 2019, tilgængeligt her: https://www.ft.dk/samling/20182/almdel/reu/spm/355/index.htm

[82] Se herom også justitsministerens svar af 24. oktober 2019 på spørgsmål nr. 363 (Alm. del), tilgængeligt her: https://www.ft.dk/samling/20182/almdel/reu/spm/363/svar/1600521/2094110.pdf

[83] Se rapport fra FN's specialrapportør for ytringsfrihed A/HRC/38/35, tilgængelig her: https://undocs.org/en/A/HRC/38/35

[84] Se blandt andet EMD-sag The Sunday Times mod Storbritannien, præmis 47-49, tilgængelig her: https://hudoc.echr.coe.int/rus#{"itemid":["001-57584"]}

[85] Se EU-studie om ICT og menneskerettigheder (FRAME) 2017, s. 27, tilgængelig her: https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/udgivelser/research/frame/frame_-_ict_and_human_rights.pdf samt bilaget til Europarådets anbefaling – Recommendation CM/Rec(2018)2 of the Committee of Ministers to member states on the roles and responsibilities of internet intermediaries, punkt 1.1.1.

[86] Se navnlig The Rise of Content Cartels, Evelyn Douek, tilgængelig her: https://knightcolumbia.org/content/the-rise-of-content-cartels

[87] Se Rikke Frank Jørgensen, Rights Talk: In the Kingdom of Online Giants, i *Human Rights in the Age of Platforms*, MIT Press, 2019, s. 163-187. Se også: Rikke Frank Jørgensen, "What

platforms mean when they talk about human rights", *Internet Policy*, Vol. 9, issue 3, 2017, s. 280-296.

[88] Se rapport fra FN's specialrapportør for ytringsfrihed A/HRC/38/35, s. 7, tilgængelig her: https://undocs.org/en/A/HRC/38/35

[89] Se EU-Domstolens afgørelse C 18/18 (Glawischnig-Piesczek mod Facebook Ireland Limited), tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=1501064

[90] Se EU-Domstolens afgørelse C 18/18 (Glawischnig-Piesczek mod Facebook Ireland Limited), præmis 45, tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=1501064

[91] Jacob Mchangama, "Nu skal danske politikere holde tungen lige i munden – ellers kan det gå hårdt ud over din ytringsfrihed", Berlingske, 18. februar 2020. Artiklen er tilgængelig her: https://www.berlingske.dk/kommentatorer/nu-skal-danske-politikere-holde-tungen-lige-i-munden-ellers-kan-det

[92] Se for eksempel Daphne Keller, "Empirical evidence of 'over-removal' by Internet Companies under Intermediary Liability Laws" (The Center for Internet and Society), tilgængelig her: http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws

[93] Ekspertrapport til Europarådet, MSI-NET (2016) 06 re 3 Final, Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications, s. 20, tilgængelig her: https://rm.coe.int/study-hr-dimension-of-automated-data-processing-incl-algorithms/168075b94a

[94] Se bl.a. EMD-sag Pedersen og Baadsgaard mod Danmark, præmis 93, tilgængelig her: https://menneskeret.dk/sites/menneskeret.dk/files/afgoerelsesdatabase/2004-12-17_49017.99_pedersen_and_baadsgaard_v._denmark.pdf

[95] Se Daphne Keller, "Who do You Sue? State and Platform Hybrid Power Over Online Speech" (2019, Hoover Institution), tilgængelig her: https://www.hoover.org/research/who-do-you-sue

[96] Se Europarådet, Menneskerettighedskommissionen, "The rule of law on the Internet and in the wider digital world" (CoE, 2014), tilgængelig her: https://www.statewatch.org/news/2014/dec/coe-hr-comm-

rule-of-law-on-the%20internet-summary.pdf. Se også: Felix Schwemer, "Trusted notifiers and the privatization of online enforcement", Computer Law & Security Review, Vol. 35, Issue 6 (2019), tilgængelig her: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3287754

[97] Balkin, Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation 2018, s. 1194, samt Molly K. Land i Regulating Private Harms Online: Content Regulation under Human Rights Law i *Human Rights in the Age of Platforms*, red. Rikke Frank Jørgensen, 2019, og Emily Laidlaw, Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility, Cambridge University Press 2015. Se også: Angelopoulos m.fl. i "Study of fundamental rights framework for self-regulation and privatized enforcement online", 2017, samt Laidlaw: "Online Platform Responsibility and Human Rights" i Platform Regulations:
How Platforms are Regulated and How They Regulate Us. Official Outcome of the UN IGF Dynamic Coalition on Platform Responsibility, 2017.

[98] Se rapport fra FN's specialrapportør for ytringsfrihed A/HRC/38/35, tilgængelig her: https://undocs.org/en/A/HRC/38/35. Se også: A/HRC/32/38, tilgængelig her: https://undocs.org/en/A/HRC/32/38, samt A/73/348, tilgængelig her: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/270/42/PDF/N1827042.pdf?OpenElement

[99] Se igen rapport fra FN's specialrapportør for ytringsfrihed A/HRC/38/35, A/HRC/32/38 samt A/73/348. Se også: Wagner m.fl., "Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act", ACM Conference on Fairness, Accountability, and Transparency (2020), tilgængelig her: https://www.researchgate.net/publication/338802975_Regulating_Transparency_Facebook_Twitter_and_the_German_Network_Enforcement_Act

[100] Balkin, Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation 2018, s. 1177.

[101] Schwemer, Trusted notifiers and the privatization of online enforcement, november 2019, i : Computer Law & Security Review.

[102] Se Kommissionens henstilling 2018/334 om foranstaltninger til effektiv bekæmpelse af ulovligt indhold på nettet, punkt 4, litra g, tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A32018H0334

[103] Se Facebooks nyhed https://about.fb.com/news/2019/09/oversight-board-structure/, samt Mark Zuckerbergs brev https://about.fb.com/wp-content/uploads/2019/09/letter-from-mark-zuckerberg-on-oversight-board-charter.pdf

[104] Se "Some questions regarding Facebook's oversight board and remediation of human rights impacts", del I og II, tilgængelig her: http://opiniojuris.org/2020/03/03/some-questions-regarding-facebooks-oversight-board-and-remediation-of-human-rights-impacts-part-i/ og http://opiniojuris.org/2020/03/04/some-questions-regarding-facebooks-oversight-board-and-remediation-of-human-rights-impacts-part-ii/

[105] Ekspertrapport til Europarådet, MSI-NET (2016) 06 re 3 Final, Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications, s. 18, tilgængelig her: https://rm.coe.int/study-hr-dimension-of-automated-data-processing-incl-algorithms/168075b94a

[106] Se herom Europarådet, "Study on the Human Rights Dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications" (CoE, 2016), tilgængelig her: https://rm.coe.int/draft-study-on-the-human-rights-dimensions-of-automated-data-processin/168075c4da

[107] Se rapport fra FN's specialrapportør for ytringsfrihed A/73/348, tilgængelig her: https://undocs.org/pdf?symbol=en/A/73/348

[108] Se specialrapportørens brev af 13. juni 2018, tilgængeligt her: https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-OTH-41-2018.pdf . Se endvidere note fra FN's specialrapportør for ytringsfrihed A/73/348 punk 16 og 40, tilgængelig her: https://undocs.org/A/73/348

[109] Se Thomas Aagaard, tilgængelig her: "Terror i Christchurch: Derfor er det så svært at fjerne massakrevideoen fra nettet", *Berlingske*, 19. marts 2019, tilgængelig her: (https://www.berlingske.dk/internationalt/terror-i-christchurch-derfor-er-det-saa-svaert-at-fjerne)

[110] Se EU-Domstolens afgørelse C 18/18 (Glawischnig-Piesczek mod Facebook Ireland Limited), præmis 46, tilgængelig her: http://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=1501064

[111] Se rapport fra FN's specialrapportør for ytringsfrihed A/73/348, tilgængelig her: https://undocs.org/pdf?symbol=en/A/73/348
[112] Se Europarådet, "Study on the Human Rights Dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications" (CoE, 2016), tilgængelig her: https://rm.coe.int/draft-study-on-the-human-rights-dimensions-of-automated-data-processin/168075c4da, se også: Anne Mette Lauritzen og Frederik Stjernfelt, *Dit opslag er blevet fjernet,* Gyldendal, 2019, s. 45ff.
[113] Se Nationalt Center for Forebyggelse af Ekstremisme, *Ekkokamre*, 7. august 2019: https://stopekstremisme.dk/ekstremisme/opslagsvaerk/ekkokamre
[114] Se rapport fra FN's specialrapportør for ytringsfrihed A/73/348 paragraf 24, tilgængelig her: https://undocs.org/pdf?symbol=en/A/73/348
[115] Se Europarådets deklaration om algoritmers manipulative evner, februar 2019, tilgængelig her: https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b. Se også: Amnesty International, *Surveillance Giants*, 2019, tilgængelig her: https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF s. 35f.
[116] Se rapport fra FN's specialrapportør for ytringsfrihed A/73/348, tilgængelig her: https://undocs.org/pdf?symbol=en/A/73/348
[117] Se Shoshana Zuboff, *The Age of Surveillance Capitalism*, PublicAffairs, 2019.
[118] Se Shoshana Zuboff, *The Age of Surveillance Capitalism*, PublicAffairs, 2019.
[119] Se Bilag 4 til FN-rapport A/HRC/62, tilgængeligt her: https://undocs.org/A/HRC/37/62
[120] "How do data companies get out data?" (*Privacy International* 2018), tilgængelig her: https://privacyinternational.org/long-read/2048/how-do-data-companies-get-our-data
[121] Se Artikel 29-gruppens udtalelse nr. 2/2010 om adfærdsbaseret annoncering på internettet, tilgængelig her: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_da.pdf
[122] Shoshana Zuboff, *The Age of Surveillance Capitalism*, PublicAffairs, 2019.
[123] Se Amnesty International, *Surveillance Giants*, 2019, tilgængelig her:

https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF

[124] Se Artikel 29-arbejdsgruppens udtalelse 8/2014 om den seneste udvikling inden for tingenes internet, tilgængelig her: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_da.pdf

[125] Se EU-Domstolens afgørelse i de forenede sager C-203/15 (Tele2 Sverige AB mod Post- och telestyrelsen), C-698/1 (Secretary of State for the Home Department mod Tom Watson m.fl.), tilgængelig her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:62015CJ0203&from=EN, FN-rapport A/HRC/39/29, tilgængelig her: https://undocs.org/A/HRC/39/29 og A/HRC/27/37 paragraf 19, tilgængelig her: https://undocs.org/A/HRC/27/37

[126] Se Amnesty International, *Surveillance Giants*, 2019, tilgængelig her: https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF s. 29-33.

[127] Se for eksempel Thomas Breinstrup, "Facebook betaler millionbøde for datamisbrug", (*Berlingske,* 2019), tilgængelig her: https://www.berlingske.dk/virksomheder/facebook-betaler-millionboede-for-datamisbrug

[128] Se Anne Mette Lauritzen og Frederik Stjernfelt, *Dit opslag er blevet fjernet,* Gyldendal, 2019, s. 16f.

[129] Se for eksempel Amnesty International, *Surveillance Giants*, 2019, tilgængelig her: https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF, s. 25f, og FN-rapport A/HRC/27/37 paragraf 2, tilgængelig her: https://undocs.org/A/HRC/27/37

[130] Se rapport fra FN's specialrapportør for privatliv A/HRC/37/62, bilag 2, tilgængeligt her: https://undocs.org/A/HRC/37/62

[131] Se FN-rapport A/HRC/39/29, tilgængelig her: https://undocs.org/A/HRC/39/29

[132] Se Joris van Hoboken, "The Privacy Disconnect", i *Human Rights in the Age of Platforms*, red. Rikke Frank Jørgensen, MIT Press 2019, s. 255-285. Se også: Bennett Cyphers m.fl. "Behind the One-Way Mirror, a deep dive into the technology of corporate surveillance", *Electronic Frontier Foundation*, 2019. Rapporten er tilgængelig her: https://www.eff.org/document/behind-one-way-mirror-deep-dive-technology-corporate-surveillance

[133] Se European Data Protection Supervisors udtalelse 8/2016, tilgængelig her: https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf, European Data Protection Boards

erklæring, tilgængelig her: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_en.pdf og Europakommissionens rapport, "Shaping Europe's Digital Future" 2019, tilgængelig her: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

[134] Mike Masnick, "Protocols, Not Platforms: A Technological Approach to Free Speech", 21. august 2019, tilgængelig her: https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech

[135] Det tyske datatilsyns afgørelse er tilgængelig her: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html. Sagen er blandt andet beskrevet her: https://www.slaughterandmay.com/media/2536711/facebook-germany-a-new-frontier-for-privacy-and-competition.pdf

[136] Se European Data Protection Supervisors udtalelse 8/2016, tilgængelig her: https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf og "Competition and data" (*Privacy International*), tilgængelig her: https://www.privacyinternational.org/explainer/2293/competition-and-data

[137] "Tech companies are trying to redefine privacy – what's missing is real competition on privacy" (*Privacy International, 2019*), tilgængelig her: https://privacyinternational.org/long-read/2939/tech-companies-are-trying-redefine-privacy-whats-missing-real-competition-privacy. Se også Pernille Tranberg & Gry Hasselbalch, Data ethics - the new competitive advantage, Publishare 2016, kapitel 10.

[138] Se rapport fra FN's specialrapportør for ytringsfrihed A/73/348, paragraf 35, tilgængelig her: https://undocs.org/pdf?symbol=en/A/73/348

[139] Se Artikel 29-gruppens retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, s. 23, tilgængelige her: https://www.datatilsynet.dk/media/6914/wp251rev01_da-profilering.pdf).

[140] For en gennemgang af myndigheders adgang til overvågning af borgernes internetadfærd, se rapport af Henrik Udsen, *Danske myndigheders registrering af borgernes adfærd på internettet – regelgrundlaget og de tilhørende kontrolmekanismer,* juni 2017, tilgængelig her: http://justitia-int.org/wp-content/uploads/2017/06/Rapport_Danske-

myndigheders-registrering-af-borgernes-adfærd-på-internettet_14-06-17.pdf

[141] For en gennemgang af databeskyttelsesreglerne efter forordningen, se Birgitte Kofod Olsen, *Håndbog i Data Ansvarlighed*, Djøfs Forlag, 2019.

[142] Databeskyttelsesforordningens artikel 5, stk. 1, litra c.

[143] Se Rikke Frank Jørgensen og Tariq Desai, "Right to Privacy Meets Online Platforms: Exploring Privacy Complaints against Facebook and Google", *Nordic Journal of Human Rights*, Vol. 35, No. 2., 2017, s. 106-126.

[144] Se det norske datatilsyns rapport om persondataretlige udfordringer ved Big Data, september 2013, tilgængelig her: https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/big-data/

[145] Databeskyttelsesforordningens artikel 5, stk. 1, litra b.

[146] Databeskyttelsesforordningens artikel 15.

[147] Databeskyttelsesforordningens artikel 6, stk. 1, litra a, og artikel 9, stk. 1, litra a. Se endvidere artikel 7.

[148] Se "Competition and data" (*Privacy International*), tilgængelig her: https://www.privacyinternational.org/explainer/2293/competition-and-data. Databeskyttelsesforordningen krav om samtykke er blandt andet omdrejningspunktet i en aktuel sag rejst af organisationen noyb.eu mod Google, Instagram, WhatsApp og Facebook, omtalt her: https://noyb.eu/en/gdpr-noybeu-filed-four-complaints-over-forced-consent-against-google-instagram-whatsapp-and

[149] Se Lilian Edwards, Privacy, Law, Code and Social Networking Sites, i Research handbook on governance of the internet (Ian Brown red., Edward Elgar, 2013), Rikke Frank Joergensen, The Unbearable Lightness of User Consent, i 3 Internet policy review 4 (2014); Brendan Van Alsenoy et al., Privacy notices versus informational self-determination: Minding the gap, i 28 International Review of Law, Computers & Technology 2, 185–203 (2014).

[150] The role of the courts in addressing the human rights implications of new and emerging technologies i Human Rights Challenges in the Digital Age: Judicial Perspectives (CoE & ECoHR 2020).

[151] Se "The CNIL's restricted committee imposes a financial penalty of 50 million euros against GOOGLE LLC" (*CNIL*, 2019), tilgængelig her: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc. For en gennemgang af 13 sager vedrørende databeskyttelse rejst mod Google og Facebook i årene 2011-2016, se Rikke Frank Jørgensen og Tariq Desai, "Right to Privacy

Meets Online Platforms: Exploring Privacy Complaints against Facebook and Google", *Nordic Journal of Human Rights*, Vol. 35, No. 2., 2017, s. 106-126, tilgængelig her: https://www.tandfonline.com/doi/full/10.1080/18918131.2017.1314110

[152] Datatilsynets afgørelse af 11. februar 2020 om DMI's behandling af personoplysninger om hjemmesidebesøgende, tilgængelig her: https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/feb/dmis-behandling-af-personoplysninger-om-hjemmesidebesoegende/

[153] Se Justitsministerens svar på spørgsmål 711 fra Retsudvalget om et fælles europæisk system: https://www.ft.dk/samling/20191/almdel/reu/spm/711/svar/1632156/2146952/index.htm. Se også: Kommissionens strategipapir, "A European Strategy for Data", tilgængelig her: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf