Inndrivelse av administrative sanksjoner utstedt til nettjenester etablert i tredjeland etter personvernforordningen

Kandidatnummer:
132

Antall ord:
14343

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

[11.12.2017]

Innholdsfortegnelse

1 Innledning

1.1 Aktualitet

82 % av EUs befolkning brukte internett minst en gang hver tredje måned i 2016.[1] For Norges del er det tilsvarende tallet 96 %.[2] Internett blir et stadig viktigere verktøy for befolkning i dagliglivet, og utviklingen har vært enorm i nyere tid. Omfanget av innsamling og bruk av personopplysninger har økt kraftig, og stadig flere selskaper lever av å behandle personopplysninger.[3] Det er derfor nødvendig med effektive regler som sikrer brukernes grunnleggende rettigheter når de er tilkoblet internett.

Reddit.com er et av verdens største diskusjonsforum, hvor innholdet på nettsiden i all hovedsak er brukergenerert[4]. Diskusjonsforumet er USAs fjerde største nettside målt i unike brukere, og verdens åttende mest besøkte nettside.[5] Reddit.com har i snitt hatt 1.5 milliarder besøkende hver måned, hittil i 2017. Amerikanske borgere står for 41 % av disse besøkene, men også brukere i en rekke europeiske land bruker nettsiden jevnlig. Land som Storbritannia og Tyskland, dvs. land som per i dag er medlem av EU, er blant de fem nasjonene som besøker nettsiden oftest, med ca. 10 % av besøkene.[6]

Ved å besøke reddit.com gir brukerne automatisk fra seg informasjon til selskapet bak nettsiden. Informasjon om hvor brukeren befinner seg, om brukeren besøker nettsiden med telefon eller PC, og informasjon om nettsider brukeren tidligere har besøkt eller søkt på, er bare noen av opplysningene som brukerne gir fra seg ved å besøke nettsiden.[7] Slike opplysninger anses som personopplysninger, og behandlingen av slike opplysninger er nøye regulert i Europa for å forhindre misbruk og ulovlig overvåkning av internettbrukerne. Forutsatt at nettsider som reddit.com ulovlig behandler personopplysninger om brukere i EU,

[1] http://ec.europa.eu/eurostat/statistics-explained/index.php/Internet_access_and_use_statistics_-_households_and_individuals besøkt 04.12.2017
[2] https://www.ssb.no/ikthus besøkt 04.12.2017
[3] GDPR fortale punkt 6, Esteve (2017) s. 36
[4] Det vil si at det er brukerne av nettsiden som skaper innholdet ved å linke til nyhetsartikler, starte diskusjoner, kommentere på bilder, spørsmål osv. Brukerne oppretter også underforum med forskjellige temaer, som f.eks. underforum om TV-serier, nyheter, økonomi etc.
[5] https://www.alexa.com/siteinfo/reddit.com besøkt 20.10.2017
[6] https://www.statista.com/statistics/325144/reddit-global-active-user-distribution/ besøkt 04.12.2017
[7] https://www.reddit.com/help/privacypolicy/#section_information_we_collect_automatically besøkt 04.12.2017

oppstår spørsmålene; Kommer det europeiske regelverket til anvendelse? Og vil det i så fall være mulig å inndrive en administrativ sanksjon utstedt til virksomheter etablert utenfor EU?

Den 14. April 2017 ble forordning (EU) 2016/679 General Data Protection Regulation (GDPR) endelig vedtatt. Forordningen trer i kraft 25. mai 2018, og erstatter EUs gjeldende personverndirektiv 95/46/EC, som er gjennomført i norsk rett i personopplysningsloven[8].[9] Forordningen ventes å bli innlemmet i EØS-avtalen og skal gjennomføres i norsk rett.[10]

Forordningen vil ha rettsvirkning også utenfor EUs territorium ved at virksomheter etablert i tredjeland også omfattes av forordningens virkeområde, dersom nærmere bestemte kriterier er oppfylt. Etter forordningen kan tilsynsorganene ilegge administrative sanksjoner hvis det foreligger brudd på forordningen. Det vil si at administrative sanksjoner også kan utstedes til virksomheter etablert i tredjeland som omfattes av forordningen. Til tross for at det foreligger en adgang til å ilegge administrative sanksjoner mot virksomheter i tredjeland, mangler forordningen mekanismer og forslag til hvordan de administrative sanksjonene skal inndrives. Denne masteroppgaven vil derfor drøfte adgangen til å ilegge administrative sanksjoner mot virksomheter i tredjeland, og se på hvilke muligheter tilsynsorganene har for å inndrive disse sanksjonene.

1.2 Struktur og avgrensning

Masteroppgaven er delt i to hoveddeler. I oppgavens første hoveddel, punkt 2, vil personvernforordningen og personverndirektivets virkeområde bli redegjort for og nærmere drøftet. I oppgavens andre hoveddel vil det først i punkt 3 redegjøres for hvilke muligheter som eksisterer for inndrivelse av administrative sanksjoner utstedt til virksomheter i tredjeland. Deretter vil det i punkt 4 bli redegjort for personvernforordningens ekstraterritorialitet, før det drøftes hvorfor begrepet er viktig for muligheten til inndrivelse av administrative sanksjoner utstedt til virksomheter i tredjeland.

En forutsetning for å utstede og inndrive administrative sanksjoner er at en virksomhet har brutt en av forordningens mange bestemmelser om personvern. Oppgaven vil ikke redegjøre

[8] Lov 14. April 2000 nr. 31 om behandling av personopplysninger
[9] Justisdepartementets høringsnotat av 6. Juli 2017 snr. 17/4200 s. 3
[10] *ibid.*

for hva som er et personvernbrudd etter forordningen. Det vil si at det forutsettes å foreligge brudd på personvernforordningen i masteroppgavens andre hoveddel. For at virksomheter lovlig kan overføre personopplysninger til tredjeland må det foreligge et særskilt rettslig grunnlag. Hva dette rettslige grunnlaget kan være fremgår av forordningen, men det vil ikke redegjøres nærmere for dette i oppgaven.

1.3 Metode

Oppgaven bygger på tolkning av EU-lovgivning, avgjørelser fra EU-domstolen og internasjonale traktater. Derfor kan ikke alminnelig norsk juridisk metode anvendes for tolkningen av rettsgrunnlagene. Ved tolkning av EU-lovgivningen er det først og fremst lovbestemmelsene, dvs. artiklene, som skal ordlydstolkes. Det vil, som i alminnelig norsk juridisk metode, si at en naturlig språklig forståelse må utledes. Det fremgår av rettspraksis fra EU-domstolen at i tilfeller hvor ordlydstolkningen ikke er klar, skal bestemmelsen leses i lys av fortalen.[11] Fortalen er ikke et selvstendig rettsgrunnlag, og utgjør derfor kun et støttemoment i tolkningen av artiklene.[12] Således kan fortalen til en viss grad sammenlignes med rettskildevekten til forarbeidene i norsk rett. I tillegg vil formålet med rettsakten være av betydning, og artiklene i rettsakten må derfor tolkes i lys av dette.[13]

Oppgaven beror seg på tolkning av en forordning. En forordning er en bindende rettsakt hvor alle detaljer i regelverket skal følges i hele EU, jf. Treaty of the Functioning of the European Union (TFEU) artikkel 288 (1). Det følger av EØS-loven[14] artikkel 7 (1) bokstav a at "en rettsakt som tilsvarer en EØF-forordning skal som sådan gjøres til del av avtalepartenes interne rettsorden". Dette innebærer at når forordningen blir en del av EØS-avtalen, må Norge adoptere forordningen i sin helhet, eller vedta en lov som henviser direkte til forordningen.

[11] *Joined Cases C-404/*15 and C-659/15 PPU avsnitt 75
[12] Fredriksen og Mathisen (2014) s. 228
[13] *C-101/01* avsnitt 61 flg.
[14] Lov 27. November 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde.

Det er EU-domstolen som dømmer i siste instans for spørsmål om tolkningen av EU-rettsaktene.[15] Avgjørelsene til domstolen er bindende for alle medlemsland. Derfor er rettspraksis fra EU-domstolen en viktig kilde for forståelsen av EU-lovgivningen.

Norge er ikke en del av EU. Dette innebærer at det ikke er utarbeidet en offisiell norsk oversettelse av personvernforordningen i forbindelse med at forordningen ble vedtatt. Det utarbeides en norsk oversettelse i forbindelse med at forordningen skal bli en del av norsk rett. Foreløpig foreligger det kun en uoffisiell oversettelse av forordningsteksten.[16] Oppgaven vil likevel bruke den norske uoffisielle oversettelsen av pedagogiske hensyn. Der det er aktuelt med en ordlydstolkning, vil tolkningen imidlertid ta utgangspunkt i den engelske forordningsteksten.

1.4 Begrepsavklaring

1.4.1 Innledning

Det er en rekke definisjoner og begreper som er nødvendige for å forstå innholdet til personvernforordningen, og hvilke praktiske, rettslige og politiske problemer som forordningen kan skape. I det følgende vil sentrale definisjoner og begreper bli presentert. Det vil i punkt 1.4.2 bli presentert legaldefinisjoner av begreper som er sentrale for oppgaven. Deretter vil det i punkt 1.4.3 bli redegjort for hva som menes med ”overføring av personopplysninger”. Dette er et av vilkårene for at forordningen kommer til anvendelse for virksomheter etablert i tredjeland. Begrepet er ikke nærmere definert i forordningen, men er forsøkt tydeliggjort i rettspraksis fra EU-domstolen. Til slutt vil det i punkt 1.4.4 kort bli redegjort for begrepet ”ekstraterritorialitet”. Dette er et begrep som i seg selv ikke har rettsvirkning, men som det fremgår av drøftelsene punkt 3 og 4, kan det påvirke inndrivelsesmulighetene til tilsynsorganene.

[15] Treaty of the European Union artikkel 19 (3)
[16] https://www.regjeringen.no/contentassets/c907cd2776264a6486b8dd3ee00a4e3d/uoffisiell-norsk-oversettelse-av-personvernforordningen.pdf

1.4.2 Legaldefinisjoner

Personvernforordningen artikkel 4 oppstiller en rekke legaldefinisjoner, herunder personopplysninger, behandling, databehandler og behandlingsansvarlig. Dette er begreper som alle må foreligge for at forordningen i det hele tatt kan komme til anvendelse.

Det første begrepet som må klarlegges er ”personal data”, jf. artikkel 4 (1). En naturlig språklig forståelse av ”personal data” er informasjon som inneholder opplysninger om en person. ”Personal data”, eller ”personopplysning” som er Justisdepartementets oversettelse, er definert i forordningens artikkel 4 (1) som ”any information relating to an identified or identifiable natural person”. Begrepet er ikke tilsiktet å være en endring fra det gjeldende personverndirektivet og vil følgelig ikke medføre endringer i norsk rett. I personopplysningsloven er begrepet definert som ”opplysninger og vurderinger som kan knyttes til en enkelt person”, jf. § 2 (1). Opplysningene må altså ikke være tilknyttet en spesifikk person eller profil, men må være egnet til å identifisere en person.

Bestemmelsen må leses i lys av forordningens fortale. Det fremgår av punkt 23 at personlige opplysninger ikke skal anses som ”personal data” etter forordningen hvis opplysningene har blitt anonymisert i så sterk grad at det ikke er mulig ved bruk av alle rimelige tekniske hjelpemidler, å knytte opplysningene til en konkret person. Dette innebærer at definisjonen av ”personal data” vil kunne variere etterhvert som teknikker for å anonymisere og ”de-anonymisere” informasjon utvikles. Det gjør også at metoden som brukes for å samle inn og behandle opplysninger kan ha innvirkning på om det foreligger ”personal data” eller ikke.

Det er en rekke opplysninger som regnes som personopplysninger etter forordningsteksten som er naturlig å tenke at enten er harmløst at behandles, eller at det ikke er personopplysninger i det hele tatt. Eksempler på dette er bilder, hodeform, e-postadresse eller hvilke filmer en ser på tjenester som Netflix eller YouTube.[17]

Definisjonen av ”processing” fremgår av artikkel 4 (2): ”any operation or set of operations which is performed on personal data”. Justisdepartementet har oversatt begrepet til ”behandling” i sitt lovforslag. En naturlig språklig forståelse av ”processing” er bearbeidelse eller bruk av informasjon. Bearbeidelsen kan være både automatisk eller manuell, og den er

[17] Eksempler hentet fra https://www.datatilsynet.no/om-personvern/personopplysninger/, besøkt 16.10.17

teknologinøytral.[18] Artikkel 4 (2) har en rekke eksempler på hva som er ”processing”. Det er klart ut fra den lange ikke-uttømmende listen at det er lagt til grunn en lav terskel for når det er tale om ”processing”. Det fremgår at bl.a. ”collection”, ”use” eller ”destruction” er eksempler på ”processing”. Det kan også leses ut fra *Schrems*-dommen (C-362/14) at overføring fra EU til USA er tilstrekkelig til at det foreligger en behandling av personopplysninger.[19] Dette innebærer at vilkåret setter svært få begrensinger for når forordningen kommer til anvendelse.

Videre må det avklares hva en ”controller”, jf. artikkel 4 (7), og en ”processor”, jf. artikkel 4 (8), er. En naturlig språklig forståelse av ”controller”, eller ”behandlingsansvarlig” på norsk, er den som er ansvarlig for hvordan opplysninger behandles, enten i form av hvilke tekniske løsninger som skal anvendes eller ved finansiering av behandlingen av opplysninger. En ”processor”, på norsk ”databehandler”, er den som på vegne av en ”controller” bearbeider opplysninger. Definisjonene har samme ordlyd som i personverndirektivet. Det er ikke noe i veien for at en behandlingsansvarlig bearbeider sine egne innsamlede opplysninger. Således kan en virksomhet være både ”controller” og ”processor” etter forordningen. Dette påvirker ikke ansvarsgrunnlaget virksomheten har etter forordningen, da både ”controller” og ”processor” er pliktig til at behandlingen ikke bryter med forpliktelsene etter forordningen, jf. artikkel 24, jf. artikkel 28.

1.4.3 ”Overføring av personopplysninger”

Til tross for at forordningen har en egen bestemmelse med legaldefinisjoner, er det særlig en definisjon som mangler, definisjonen av ”overføring av personopplysninger”. Dette er et viktig, men komplisert inngangsvilkår for forordningens territorielle virkeområde. Dette fordi det må skje en overføring av personopplysninger, for at opplysningene kan behandles i et annet land enn der opplysningene er samlet inn, som for eksempel i et tredjeland. Det kan rimelig nok heller ikke foretas en ulovlig overføring av personopplysninger til tredjeland uten at det kan fastslås at det har skjedd en overføring av opplysninger. ”Overføring” er et vanskelig begrep så lenge det er tale om informasjon som er elektronisk lagret, ettersom det da er et abstrakt objekt og ikke noe en person har fysisk. Begrepet fordrer også at en har en

[18] jf. artikkel 4 (2) første setning.
[19] Padova (2016) s. 145

god teknisk forståelse. En vil mest sannsynlig få en betydelig annerledes definisjon av ”overføring av personopplysninger”, avhengig om en spør en jurist eller en som jobber innenfor IT-fagområdet.

Hva som regnes som overføring av data, herunder personopplysninger, til tredjeland etter personverndirektivet, er behandlet av EU-domstolen i *Lundqvist*-dommen (C-101/01) Domstolens forsøk på å avgjøre hva overføring av data er, har blitt kritisert, da definisjonen kan fremstå som utdatert, ut fra dagens teknologiske løsninger.[20] Det er likevel den eneste tunge rettskilden innenfor EU-retten som har behandlet spørsmålet, og dommen er dermed svært viktig for å kunne utlede en legaldefinisjon.

Et av spørsmålene i Lundqvist-dommen var om opplastning av materiale til en hjemmeside representerer en overføring av personopplysninger til tredjeland. Dommen omhandlet Lundqvist som jobbet frivillig for den svenske kirken. Hun opprettet en hjemmeside hvor hun publiserte nyheter som var av interesse for den gruppen hun jobbet med. En av nyhetene hun publiserte omhandlet en vaktmester som hadde falt på isen og brukket beinet, og derfor var blitt sykemeldt. Dette var regnet som sensitive personopplysninger da det var helseopplysninger.

Domstolen klargjør først at spørsmålet om opplastning av materiale til en hjemmeside utgjør overføring av personopplysninger ikke er definert i personverndirektivet. Videre klargjør domstolen at de bare vurderer om Lundqvist har overført data til utlandet, ikke om operatøren av vertstjenesten[21] hun har lastet opp hjemmesiden til har gjort det. Domstolen understreker at de må se hen til lovgivers hensikt, og påpeker at kontrollen med overføring av personopplysninger til tredjeland kommer i tillegg til den øvrige reguleringen, og må forstås i denne sammenheng. Direktivet mangler referanser til internett, og det blir påpekt at direktivet ikke har klargjort om en operatør av en vertstjeneste skal anses å foreta behandlingen i det landet operatøren er etablert, ved forretningsadressen eller i de landene hvor operatørens servere er plassert. Domstolen uttaler at om en skal tolke direktivet slik at opplastning representere overføring til tredjeland, ville det i praksis bety at direktivet regulerte bruk av internett helt generelt. Dette anså domstolen at ikke var hensikten til lovgiver.

[20] Bing (2014) s.141-142
[21] Vertstjeneste er en tjeneste som drifter servere som en nettside ligger lagret på

Domstolen kommer frem til en todelt definisjon av overføring gjennom bruk av formålsbetraktninger. Første delen går på skillet mellom push- og pullteknologi. Domstolen skiller mellom det at noen må besøke en nettside (pull) og f.eks. å sende informasjonen i et nyhetsbrev (push).[22] Domstolen la til grunn at det er en lavere terskel for når det foregår overføring av personopplysninger når det anvendes push-teknologi. Definisjonen kan argumenteres for å ha noe for seg da hendelsen i dommen er fra samme år som Google Inc. ble opprettet. Det var derfor lite til ingen indeksering[23] av nettsider.[24] På den andre siden kan definisjonen sies å være et blindspor da publisering, og da behandling, av personopplysninger vil kunne være både push- og pullteknologi avhengig av hvordan den individuelle bruker oppsøker informasjonen.[25] Illustrerende for hvordan en publikasjon kan være både push- og pullteknologi er nettavisers nyhetsartikler. Hvis en person går inn på en nettavis og leser en artikkel, er dette ifølge domstolen pullteknologi, siden brukeren selv oppsøker informasjonen. Hvis den samme personen får en notifikasjon på telefonen sin om samme artikkel vil det derimot være pushteknologi.

Den andre delen av definisjonen som domstolen anvender baserer seg på tankegangen om at overføring av personopplysninger er noe konkret og holdbart som fysisk overføres fra punkt a til punkt b.[26] Denne tankegangen har til dels også vært brukt i *Amazon* og *Weltimmo*-dommene, jf. punkt 2.4.3. Det er imidlertid litt unaturlig å tenke på personopplysninger som noe fysisk som flytter seg fra et punkt til et annet, da det til tross for at det er lagret et eller flere steder, vil kunne være tilgjengelig fra flere forskjellige steder på samme tid. Personopplysninger kan også kopieres uten at det forringer verdien eller egenskapene til opplysningene.

Siden forordningen ikke definerer hva "overføring av personopplysninger" er, og forordningen er tilsiktet å, i det store og hele, videreføre personverndirektivet, må domstolens tidligere tolkning av "overføring av personopplysninger" legges til grunn for forståelsen av begrepet, også etter innføringen av GDPR. Det vil si at det fremdeles ikke er helt klart hva som vil være "overføring av personopplysninger", men vilkåret vil være situasjonsbetinget. Som et minimum må personopplysningene være tilgjengelig for behandling. Hvis en

[22] Bing (2014) s. 141-142
[23] Indeksering er en organisering av informasjon som gjør det søkbart for en søkemotor, Jf. https://support.google.com/customsearch/answer/4513925?hl=en besøkt 07.12.2017
[24] Bing (2014) s. 141
[25] *op.cit. s*. 141-142
[26] *ibid.*

virksomhet lagrer sine personopplysninger på en server i et tredjeland, er det vanskelig å tale om noe annet enn en "overføring av personopplysninger" til tredjeland, da opplysningene har blitt "flyttet" ut av EUs territorium.

1.4.4 Ekstraterritorialitet

Ekstraterritorialitet er et begrep som brukes gjennomgående i denne oppgaven. Begrepet er en klassifisering av effekten nasjonal lovgivning kan ha utenfor sin territorielle jurisdiksjon. I punkt 4 vil begrepet drøftes nærmere. Det vil blant annet bli belyst hvilken effekt ekstraterritorialitet har på forståelsen av personvernforordningen, og hvordan klassifiseringen kan ha innvirkning på gjennomføringsevnen av forordningen. I det følgende vil begrepet kort defineres.

Begrepet "ekstraterritorialitet" kan forstås på mange måter. *International Law Commission*, definerer "ekstraterritorial jurisdiksjon" som

> "an attempt to regulate by means of national legislation, adjudication or enforcement the conduct of persons, property or acts beyond its borders which affect the interests of the State in the absence of such regulation under international law."[27]

Begrepet innebærer følgelig en beskrivelse av når nasjonal rett får innflytelse utenfor sin territorielle jurisdiksjon. Det kan også skilles mellom ekstraterritoriell innflytelse ("impact") og omfang ("scope").[28] Distinksjonen mellom disse, er hovedsakelig formålet med rekkevidden av den nasjonale lovgivningen.

Begrepet er kontroversielt da det vært anerkjent en god stund at linjen mellom territoriell og ekstraterritoriell jurisdiksjon blir vanskeligere å trekke etterhvert som overføring av data på tvers av landegrenser finner sted.[29] Det er også kontroversielt fordi den ekstraterritorielle effekten av lovgivning er av mange ansett som et inngrep i staters suverenitet.[30] Et alternativ til begrepet ekstraterritorialitet er *Brussels-effekten,* som først ble brukt som et eget begrep av Anu Bradford i 2012.[31]

[27] Kuner (2015a) s. 238.
[28] Kuner (2015a) s. 235
[29] Gömann (2017) s. 568, Scott (2014) 1345
[30] Gömann (2017) s. 568, Kuner (2015a) s. 238
[31] Bradford (2012)

2 Virkeområde

2.1 Innledning

Virkeområdet til personvernforordningen er et av kjerneområdene til oppgavens problemstilling. Det er nødvendig å avklare virkeområdet til personvernforordningen for å kunne fastslå hvordan forordningen vil gjøre seg gjeldende overfor virksomheter etablert i tredjeland, som igjen nødvendiggjør behovet for effektive inndrivelsesmuligheter av administrative sanksjoner. Det fremgår av personvernforordningens fortale punkt 9 at forordningen langt på vei er ment å være en videreføring av personverndirektivet. Det er derfor naturlig å se hen til virkeområdet til personverndirektivet, både for å redegjøre for forskjellene og fordi store deler av rettspraksisen etter personverndirektivet er overførbar til personvernforordningen. Det vil derfor i punkt 2.2 redegjøres for virkeområdet til personverndirektivet. Videre i punkt 2.3 vil det bli redegjort for virkeområdet til personvernforordningen. I punkt 2.4 vil det bli redegjort for de mest sentrale dommene om virkeområdet til personverndirektivet, for å belyse forordningens virkeområde nærmere. Avslutningsvis i punkt 2.5 vil personvernforordningens virkeområde vurderes opp mot et konkret tilfelle, Reddit.com

2.2 Personverndirektivet

Personverndirektivet trådte i kraft 13.12.1995, og etablerte et felles vernenivå for behandling av personopplysninger innad i EU. Direktivet har blitt kritisert for å ha gitt medlemsland for stor fleksibilitet ved nasjonal implementering,[32] og at gjennomføringen av direktivet har vært for fragmentert.[33] Virkeområdet til direktivet er regulert i artikkel 4, og vil i det følgende bli redegjort for.

Det fremgår av artikkel 4 at hver medlemsstat skal anvende de nasjonale bestemmelser som er vedtatt i henhold til direktivet for behandling av personopplysninger som ”utføres i forbindelse med virksomheten i et foretak eid av den behandlingsansvarlige på

[32] Bing (2014) s. 129
[33] GDPR fortale punkt 9

medlemsstatens territorium.", jf. personverndirektivets artikkel 4 (1) bokstav a. Ordlyden tilsier derfor at det må være en virksomhet som er etablert i et av medlemslandene i Unionen, og at behandlingen av personopplysningene må ha sammenheng med hva virksomheten driver med i Unionen for at direktivet skal komme til anvendelse.

Videre fremgår det av artikkel 4 (1) bokstav c at direktivet også gjelder ved behandling av personopplysninger

> "som utføres av en behandlingsansvarlig som ikke er etablert på Fellesskapets territorium, og som med henblikk på behandling av personopplysninger benytter elektroniske eller andre hjelpemidler som befinner seg på nevnte medlemsstats territorium, med mindre disse hjelpemidlene benyttes bare med henblikk på transitt gjennom Fellesskapets territorium."

En naturlig språklig forståelse av bestemmelsen tilsier at direktivet gjelder når en virksomhet behandler personopplysninger innenfor EUs territorium uavhengig av hvor virksomheten er etablert. Dette gjelder imidlertid kun så lenge det ikke er tale om kun overføring av informasjon gjennom EU. For eksempel når informasjonen ikke har blitt brukt på en annen måte enn at den overføres gjennom nettverkskabler som befinner seg i EU.

Ordlyden i bestemmelsen kan tolkes dithen at så lenge det foregår innsamling av personopplysninger fra brukere i EU, så regulerer direktivet tilfellene. Det vil si at direktivet har et omfattende virkeområde. Det er derfor naturlig at EU har blitt kritisert for at de prøver å strekke seg utenfor EUs territorium ved lovgivningen.[34] Samtidig, så tyder ordlyden av "henblikk på behandling som befinner seg på nevnte medlemsstats territorium" på at enten all behandling må foregå innenfor EUs territorium, eller at alle "hjelpemidlene" som brukes i behandlingen må befinne seg i EU. Hvis man legger sistnevnte tolkning til grunn har direktivet begrenset med ekstraterritoriell rekkevidde, ettersom man da i prinsippet må anses som etablert i Unionen.

Virkeområdet som følger av artikkel 4 (1) bokstav c kan skape rettssikkerhetsproblemer for borgere i EU/EØS-området.[35] Dette fordi det er en veldig hårfin grense mellom virksomheter som faller innenfor og utenfor virkeområdet, slik direktivet er formulert.[36] Det vil si at to tilfeller som fremstår som nærmest identiske for brukerne, kan ha ulike krav til behandling av personopplysninger. En kan ikke forvente at den gjennomsnittlige bruker har kapasitet eller

[34] Kuner (2015a) s. 235
[35] Gömann (2017) s. 580
[36] *ibid.*

kunnskap om å undersøke dette for enhver behandlingsansvarlig som behandler deres personopplysninger. Dette innebærer at det tilfeldig hvorvidt personvernet for brukerne er tilstrekkelig ivaretatt eller ikke.[37]

2.3 Personvernforordningen

2.3.1 Artikkel 3 (1) Virksomheter etablert i Unionen

Virkeområdet til GDPR fremgår av forordningens artikkel 3. Artikkelens første ledd er tilnærmet ord for ord lik personverndirektivets artikkel 4 (1) bokstav a. Den eneste forskjellen er at forordningen taler om "the Union" istedenfor "national law", Dette skyldes at forordningen er totalharmonisert, mens det var mulig for medlemsland å ikke ratifisere direktivet fult ut. Ordlyden er også valgt for å unngå eventuelle konflikter med nasjonal lovgivning.[38]

Det fremgår her at forordningen gjelder ved behandlingen av personopplysninger "in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not." En naturlig språklig forståelse av bestemmelsen tilsier at forordningen gjelder når en databehandler eller behandlingsansvarlig er etablert i Unionen, og at denne virksomhetens virkeområde er tilknyttet behandlingen av personopplysningene. Det er også uten betydning hvor behandlingen foretas for at forordningen regulerer forholdet. Det skal altså ikke være mulig for en databehandler eller behandlingsansvarlig å overføre dataene for behandling til et tredjeland for å omgå regelverket.

Vilkåret "established"[39] er et godt innarbeidet kriterium som brukes i en rekke direktiv. Vilkåret er oversatt til "etablert" i både personverndirektivet og i den uoffisielle oversettelsen av personvernforordningen. En naturlig språklig forståelse av "established" er der en databehandler eller behandlingsansvarlig utøver hele eller deler av dets virke. Hva som skal til for at en virksomhet skal anses som etablert i EU/EØS er først og fremst utviklet gjennom domstolspraksis i EU-domstolen. Domstolpraksisen er blitt kodifisert gjennom en rekke EU-

[37] Gömann (2017) s. 580
[38] *op.cit.* s. 574
[39] Etableringsfriheten er en av de fire friheter i EU, jf. TFEU artikkel 50.

akter, og er godt oppsummert i fortalen til direktivet om elektronisk handel (2000/31/EC). Der fremgår det i fortalens punkt 19 at

> ”begrepet etablert innebærer faktisk utøvelse av økonomisk virksomhet gjennom et fast forretningssted på ubestemt tid. Dette kravet er også oppfylt når et selskap er stiftet for et gitt tidsrom. Etableringsstedet for et selskap som yter tjenester via et nettsted i Internett er verken det stedet der de tekniske midler som tjener som støtte for nettstedet befinner seg, eller det stedet der det er tilgang til nettstedet, men det stedet der selskapet utøver sin økonomiske virksomhet.”

Tilsvarende definisjon fremgår også av nyere lovgivning i EU som Tjenestedirektivets (2006/123/EF) artikkel 4 (5) og fortale punkt 37. Det er altså klart ut fra dette at det avgjørende vil være hvor selskapet utøver sin økonomiske virksomhet. Det kan sies at lovgivers vilje har vært å effektivt kunne regulere tilfeller som påvirker mange EU-borgere. Ordlyden stenger ikke for at en virksomhet kan anses som etablert i flere stater, f.eks. i tilfeller hvor selskaper er organisert som mor- og datterselskaper. Det er verdt å merke seg at etableringsvilkåret ikke forutsetter at virksomheten som regnes som etablert i unionen må være behandlingsansvarlig for at EUs personvernregler kommer til anvendelse.[40] I nyere rettspraksis fra EU-domstolen, *Weltimmo*- og *Amazon*-dommen, se punkt 2.4.3, er det lagt til grunn at det må foreligge en stabil territoriell tilknytning til EU, for at en virksomhet skal anses ”etablert i Unionen”. Dette innebærer at bruk av f.eks. serverparker i EU som eneste fysiske tilknytning kan være tilstrekkelig for at den territorielle tilknytningen i artikkel 3 (1) er oppfylt.[41]

2.3.2 Artikkel 3 (2) Virksomheter som ikke er etablert i Unionen

Det fremgår av GDPR artikkel 3 (2) at forordningen gjelder for behandling av personopplysninger til personer som befinner seg innenfor Unionen, når behandlingen er foretatt av databehandlere eller behandlingsansvarlig som ikke er etablert innenfor Unionen, når denne behandlingen er i tilknytning til enten ”the offering of goods or services (...) to such data subjects in the Union”, jf. bokstav a, eller når behandlingen gjelder ”the monitoring of their behaviour as far as their behaviour takes place within the Union”, jf. bokstav b. Det er altså to alternative vilkår for når forordningen regulerer databehandlere og behandlingsansvarlige som ikke er etablert i Unionen. Til tross for at vilkårene er alternative,

[40] van Alsenoy og Koekkoek (2015) s. 107
[41] de Hert og Czerniawski (2016) s. 233-236

vil de i mange tilfeller kunne anvendes for en og samme behandlingsansvarlig, som f.eks. ved sosiale medier.

Artikkel 3 (2) bokstav a "the offering of goods or services"

Ordlyden av "the offering of goods or services" er vid, og kan hvis man tolker bestemmelsen bokstavelig gjelde enhver nettside som er tilgjengelig for brukere som befinner seg innenfor Unionen. Bestemmelsen må derfor leses i lys av både fortalen, og da særlig punkt 23, og tidligere rettspraksis.

Det fremgår av fortalens punkt 23 at ved vurderingen av om en databehandler eller behandlingsansvarlig tilbyr varer eller tjenester til Unionen, må det vurderes om den behandlingsansvarlige eller databehandleren har til hensikt å tilby varer eller tjenester til et eller flere medlemsland innenfor Unionen. Det fremgår videre av fortalen at det i vurderingen må ses hen til hva slags kontaktinformasjon som foreligger, hvilket språk som benyttes på siden og, hvor varer eller tjenester må betales, hva slags valuta sluttbrukeren kan betale i. Listen som fremgår av fortalen er ikke uttømmende, og andre momenter kan derfor tillegges vekt i vurderingen, men dette vil være situasjonsbetinget.

Hvorvidt en virksomhet har til hensikt å tilby varer eller tjenester til registrerte i unionen som vurderingsmomentet, har fått en del kritikk da det fokuserer på databehandlers subjektive intensjon, og ikke på etterprøvbare kriterier som forretningsvirksomhet utført eller rettet mot EU-området. [42]

Ettersom det er vanskelig å bevise intensjonene til behandlere,[43] vil språk og valuta være viktige holdepunkter i vurderingen.[44]

Språk kan være en dårlig indikator for om en nettjeneste retter seg mot EU. Dette er særlig klart ved nettjenester som er på engelsk. Dette er fordi engelsk er et internasjonalt språk som brukes i en rekke land, både i og utenfor EU. Dette gjør at det er vanskelig å avklare om en nettside retter seg mot EU basert på engelsk som språk. Det er også andre problemer med bruk av språk som vurderingsmoment. For eksempel kan en nettside automatisk oversettes

[42] Gömann (2017) s. 585, Svantesson (2015) s. 232
[43] Gömann (2017) s. 585-586.
[44] Fortale punkt 23

gjennom tjenester som Google Translate basert på IP-adresse, eller at nettleseren automatisk oversetter alle språk som ikke er standardspråket på operativsystemet. Da er det ikke klart om nettsiden retter seg mot EU basert på språket. Hvis en nettside bruker et språk som utelukkende er brukt i Unionen, som f.eks. finsk, vil det imidlertid kunne være en god indikator på om nettjenesten retter seg mot Unionen.

Valuta kan være både et klart og et uklart vurderingsmoment, avhengig av hvilken valuta som brukes som betalingsmiddel. Det kan være et klart moment når det er brukt Euro eller en annen valuta som er brukt i EU/EØS-området. Det er imidlertid problemer hvis betalingen foretas med kryptovaluta som f.eks. Bitcoin, eller gjennom reklame, vervekampanjer eller andre ikke-monetære betalingsmåter. I slike tilfeller fremstår det som tilfeldig om EU-domstolen, eller et tilsynsorgan kommer frem til om behandlingen er regulert av forordningen eller ikke.[45]

Artikkel 3 (2) bokstav b "Monitoring of their behaviour"

Vilkåret "the monitoring of their behaviour as far as their behaviour takes place within the Union", jf. Artikkel 3 (2) bokstav b, kan være et betydelig mer uklart vilkår for når forordningen kommer til anvendelse. En naturlig språklig forståelse av bestemmelsen tilsier at forordningen kommer til anvendelse når en databehandler eller behandlingsansvarlig overvåker oppførselen til en bruker, så lenge denne oppførselen finner seg innenfor Unionen.

Det fremgår av fortalens punkt 24 at ved vurderingen om en databehandler eller behandlingsansvarlig overvåker oppførselen til personer i Unionen, må det avklares om personer er

> "tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."

Fortalen legger altså til grunn at det er den etterfølgende behandlingen av personopplysninger som er avgjørende for om bestemmelsen kommer til anvendelse. Det fortalen ikke har adressert, som fremstår som et problem ut fra en ordlydstolkning er vilkåret "as far as their behaviour takes place within the Union." I tilfeller som geo-tracking gjennom

[45] Gömann (2017) s. 586

GPS/GLOSNASS er det klart nok når en persons oppførsel kan sies å foretas "within the Union." Vilkåret er imidlertid betydelig mer uklart når det gjelder normalt bruk av internett.[46] Det er klart at, med mindre man bruker tjenester som stopper eller begrenser sporing på internett, så vil tilnærmet enhver nettside som en bruker går inn på skape metadata som selskaper som f.eks. Google Ads bruker for å skape en profil. Profilen vil være medvirkende for hvilke reklamer som kommer opp på nettsider, og hvilke søketreff som kommer på spesifikke søkeord, og kan dermed påvirke brukere.[47]

Det er på ingen måte åpenbart om det er tale om oppførsel som tar plass innenfor Unionen når en bruker en maskin plassert i et medlemsland og besøker en nettside, som ikke er etablert innenfor Unionen. Fysisk vil brukeren være innenfor EUs territorium, men innholdet på nettsiden, og da oppførselen til brukeren, kan utelukkende omhandle forhold som ikke har en tilknytning til EU.

Ordlyden åpner også for muligheten at en virksomhet kan samle inn informasjon om brukere i EU/EØS-området uten at forordningen kommer til anvendelse, hvis de bare samler inn informasjonen, men ikke bearbeider informasjonen, og bare selger dataene videre vil virksomhetene ikke reguleres av forordningen. Dette kan åpne for et gråmarked hvor virksomheter kjøper opplysningene fra virksomheter som har samlet inn opplysningene, men ikke behandlet opplysningene, kun for å unngå jurisdiksjonen til forordningen.[48]

Artikkel 3 (2) er en nyskapende bestemmelse, og er regnet som en av de viktigste endringene fra personverndirektivet.[49] Det er imidlertid uklart hvorvidt bestemmelsen lar seg håndheve i praksis.[50] En utfordring med artikkel 3 (2) bokstav a er som nevnt at det må avklares hvilket formål databehandleren eller behandlingsansvarlig har med behandlingen av personopplysningene. Denne subjektiviteten gjør det vanskelig både for domstoler, tilsynsorganer og virksomheter å vurdere om en handling faller innenfor virkeområdet til forordningen. Utfordringen knyttet til artikkel 3 (2) bokstav b er som nevnt spørsmålet om når oppførselen kan anses å foregå i unionen. Det territorielle omfanget av forordningen kan

[46] Gömann (2017) s. 587
[47] Datatilsynet (2015) s. 24
[48] Gömann (2017) s. 584-588
[49] de Hert og Czerniawski (2016) s. 238
[50] Gömann (2017) s. 587

dermed tilsynelatende være avhengig av om en behandler planlegger en videre behandling av personopplysninger.[51]

2.4 Rettspraksis

2.4.1 Innledning

Det foreligger flere dommer fra EU-domstolen om rekkevidden av personverndirektivet artikkel 4 (1), som også vil gjelde for den territorielle rekkevidden av GDPR. Dette fordi forordningens artikkel 3 (1) er tilnærmet identisk med formuleringen i personverndirektivet artikkel 4 (1) bokstav a, jf. ovenfor. De viktigste dommene for oppgavens problemstilling er *Google*-, *Amazon*- og *Weltimmo*-dommen.

2.4.2 *Google*-dommen

Google-dommen (c-131/12) omtales ofte som dommen om retten til å bli glemt.[52] Dommen omhandler Gonzales som sendte en klage til det spanske datatilsynet. Klagen gjaldt søkeresultater i Google som kom opp når man søkte på navnet hans. Gonzales ønsket at noen av søkeresultatene ble slettet fra Google, fordi det ikke lenger var relevant informasjon om hans personlige økonomi. Retten til å bli glemt er et viktig personvernprinsipp, og er lovfestet i GDPR artikkel 17. Det sentrale for oppgavens problemstilling er domstolens tolkning av direktivets artikkel 4 (1) bokstav a, da dette har overføringsverdi for forståelsen av personvernforordningens artikkel 3 (1), jf. over.

Som en del av avgjørelsen måtte domstolen vurdere om behandlingen av Gonzales personopplysninger var "[utført] i forbindelse med virksomheten i et foretak eid av den behandlingsansvarlige på medlemsstatens territorium.", jf. personverndirektivet artikkel 4 (1) bokstav a. I sakens faktum fremgår det at Google Spain var et datterselskap av Google Inc. Datterselskapet var, ifølge Google, etablert pga. salg av annonser. Google anførte også at selskapet i Spania ikke hadde noe med behandlingen av personopplysninger som søkemotoren bedrev. I følge Google kunne derfor ikke det spanske selskapet være ansvarlig etter

[51] Gömann (2017) s. 587, de Hert og Czerniawski (2016), s. 238
[52] Jones (2014) s. 599, Kropf (2014) s. 508

personverndirektivet.[53] Denne synet var den gjeldende praksisen blant internasjonale virksomheter.[54]

Domstolen uttalte i forbindelse med rekkevidden av direktivet at bare det at Google hadde etablert datterselskapet innenfor EUs territorium talte for at direktivet regulerte forholdet. Det mest avgjørende var imidlertid at søkemotoren helt klart rettet sine tjenester mot EU, og at salg av annonser, som var hovedgeskjeften til datterselskapet, ikke kunne skilles ut fra behandlingen foretatt av morselskapet, da annonsene var direkte tilknyttet søkeresultater i søkemotoren til morselskapet. Det at datterselskapet ikke kunne anses som en databehandler etter direktivet, stengte ikke for at direktivet regulerte forholdet. Siden datterselskapet var avhengig av morselskapet for å kunne selge annonser, var morselskapets behandling av personopplysninger "utført i forbindelse med" en etablert virksomhet i Unionen. Domstolen valgte å tolke vilkåret "utført i forbindelse med" utvidende ut fra hensynet til direktivet.[55]

Til tross for at domstolen utvidet virkeområdet til personverndirektivet, var det fortsatt en mulighet for selskaper å omgå direktivet gjennom geo-filtrering av tjenester.[56] Denne muligheten til å omgå reglementet er forsøkt rettet med personvernforordningen artikkel 3 (2).

2.4.3 *Weltimmo*- og *Amazon*-dommen

Weltimmo-dommen (C-230/14) og *Amazon*-dommen (C-191/15) omhandler begge overføring av personopplysninger for behandling innad i EU etter personverndirektivet. Dommene er likevel relevante for forståelsen av den territorielle rekkevidden av personverndirektivet, og da også personvernforordningen, da begge dommene bygger videre på tolkningen i *Google*-dommen vedrørende artikkel 4 (1) bokstav a i personverndirektivet. I *Weltimmo* uttaler domstolen at det er nødvendig å tolke artikkel 4 i personverndirektivet utvidende for å sikre en effektiv og fullstendig beskyttelse av grunnleggende rettigheter og særlig retten til personvern.[57] Dette utsagnet er overraskende da en slik utvidende tolkning av artikkel 4 i utgangspunktet kun er nødvendig når det er snakk om overføring av data til tredjeland, da nasjonale personvernregler i medlemsstatene er antatt å ha tilstrekkelig vern for personvernet

[53] C-131/12 avsnitt 22.
[54] Spiecker (2015) s. 1042
[55] Gömann (2017) s. 571, Spiecker (2015) s. 1042.
[56] Spiecker (2015) s. 1043
[57] C-230/14 avsnitt 25.

innad i Unionen.[58] Domstolen trengte derfor egentlig ikke å uttale seg om rekkevidden av personverndirektivet artikkel 4 (1) bokstav a.

Weltimmo-dommen omhandlet det slovakiske selskapet Weltimmo som driftet en nettside med ungarske boligannonser. Det var gratis å reklamere på nettsiden de første 30 dagene, deretter løp det en månedlig kostnad. En gruppe annonsører kontaktet nettsiden for å få sine annonser og personopplysninger slettet etter de første 30 dagene. Selskapet gjorde ikke dette, og brukte informasjonene til å kreve inn penger gjennom inkassoselskap. Weltimmos bruk av personopplysninger ble klagd inn til det ungarske tilsynsorganet som bøtela selskapet. Weltimmo påklaget vedtaket, og spørsmål rundt vedtaket endte i EU-domstolen. Dommen har blitt omtalt som "the missing half" av *Google*-dommen.[59] Dette fordi domstolen i *Weltimmo*-dommen forsøkte å klargjøre rekkevidden av artikkel 4 (1) bokstav a i personverndirektivet, nærmere bestemt hva som skal til for at et selskap er etablert i Unionen. Domstolen uttaler at det må kreves en "real and effective activity" for at et selskap skal anses som etablert i EU/EØS.[60] Det å gi informasjon på brukernes nasjonalspråk var tilstrekkelig for å anses som "etablert". Det vil for eksempel si at en nettside som benytter svensk språk må anses for å være etablert i EU. Dermed utvider domstolen hva som skal anses som "etablert" sammenlignet med en naturlig språklig forståelse av ordlyden. Det å kun ha en representant som et kontaktpunkt for brukere, var også tilstrekkelig for at selskapet skulle anses etablert i unionen, uavhengig av hvor denne representanten befant seg.[61]

Amazon-dommen omhandlet Amazon EU som er et registrert selskap i Luxembourg. Selskapet driver en tysk nettside, amazon.de, som solgte varer til bl.a. østeriske kunder. Når en handlet i nettbutikken, måtte brukerne akseptere en standardavtale som inkluderte adgangen til bruk av personopplysninger. Det fremgikk av standardavtalen at forholdet var regulert av luxembourgsk lovgivning. Et av spørsmålene som kom for EU-domstolen var hvilket medlemslands regelverk som regulerte behandlingen av personopplysninger på amazon.de. Var det hvor virksomheten rettet sine tjenester, i dette tilfellet Østerrike? Eller var det landet hvor virksomheten var etablert, altså Luxembourg? For at østerisk rett kunne legges til grunn, måtte virksomheten kunne anses som etablert i Østerrike.

[58] Gömann (2017) s. 572-573
[59] *op.cit.* s. 572
[60] C-230/14 avsnitt 32
[61] C-230/14 avsnitt 30 og 33

Domstolen uttalte, med henvisning til *Weltimmo*-dommen, at "an establishment cannot exist merely because of the undertakings' is accessible [from a Member state]."[62] Domstolen krevde dermed en begrenset, men stabil fysisk tilstedeværelse for at et selskap skulle være etablert i et medlemsland.[63]

Hva gjelder behandling av personopplysninger som "utføres i forbindelse med virksomheten i et foretak", jf. artikkel 4 (1) bokstav a, la domstolen i både *Amazon* og *Weltimmo* seg på en betydelig lavere terskel enn *Google*-dommen. I *Weltimmo*-dommen mente domstolen at ettersom den behandlingsansvarlige publiserte personopplysninger på nettsiden sin og tidvis brukte denne informasjonen til å sende regninger, var det ingen tvil om at behandlingen av personopplysninger utføres i forbindelse med virksomheten til foretaket.[64]

Mens *Google*-dommen utvidet den territorielle rekkevidden i personverndirektivet, har *Weltimmo*- og *Amazon*-dommen tilnærmet uthulet vilkåret om at databehandling må skje i tilknytning til den territorielle aktiviteten til virksomheten.[65] Det kan således sies at artikkel 4 (1) bokstav a i personverndirektivet, etter avgjørelsene, har et så vidt virkeområde at det kun er tilfeller hvor databehandlere i tredjeland ikke har noen som helst territoriell tilknytning til EU, som faller utenfor.[66] Dette vil også ha betydning for rekkevidden av personvernforordningen artikkel 3 (1).

2.5 Reddit.com og territoriell tilknytning

2.5.1 Innledning

Slik forordningens virkeområde er formulert, vil det være virksomheter etablert utenfor EU som klart faller innenfor virkeområdet til personvernforordningen, og virksomheter som klart faller utenfor virkeområdet. Enkelte virksomheter etablert i tredjeland vil imidlertid ikke like tydelig kunne plasseres innenfor eller utenfor forordningens virkeområde. I disse tilfellene må det foretas en mer grundig avveining av om forordningen kommer til anvendelse. Internasjonale nettsider hvor innholdet ikke har en logisk geografisk avgrensning kan særlig

[62] C-191/15 avsnitt 76
[63] Gömann (2017) s. 572-573
[64] C-230/14 avsnitt 38
[65] Gömann (2017) s. 574
[66] *ibid.*

være vanskelig å plassere. Dette vil i det følgende bli illustrert med et konkret eksempel, nettsiden reddit.com.

2.5.2 Reddit.com og artikkel 3 (1)

Reddit.com en amerikansk nettside som eies av et amerikansk holdingselskap.[67] Driften av nettsiden skjer på et selvstendig grunnlag gjennom det amerikanskregistrerte datterselskapet Reddit inc. Det er derfor klart at virksomheten Reddit Inc må anses som etablert i USA, altså utenfor EU. Spørsmålet er om virksomheten også kan anses som "etablert i Unionen", jf. artikkel 3 (1) .

For at reddit.com skal anses som "etablert i Unionen" kreves det, som redegjort for over, at reddit.com har en stabil territoriell tilknytning til Unionen. Reddit.com lagrer sine data på Amazon sine servere gjennom en skylagringstjeneste.[68] Amazon er et amerikansk selskap, men anses som etablert i Unionen, blant annet på grunn av nettbutikker i en rekke europeiske land som er driftet av datterselskapet Amazon EU, jf. *Amazon*-dommen. Amazon sine servere befinner seg i en rekke forskjellige land, både innenfor og utenfor Europa.[69] Spørsmålet er om reddit.com skal anses å ha en stabil territoriell tilknytning til Unionen gjennom Amazon sin skylagringstjeneste, som blant annet har servere i Europa.

Bruken av skylagringstjenesten medfører at reddit.com sine data sjeldent vil være på den samme serveren hele tiden. Dataene blir i utgangspunktet lagret på den eller de serverne som har ledig kapasitet og som har minst forsinkelse til brukernes forespørsler. Således kan det være tilfeldig om data, herunder personopplysninger, er lagret i Europa eller ikke. Dette taler i retning av at reddit.com ikke har en stabil territoriell tilknytning til Unionen.

En skylagringstjeneste påvirker ikke bare hvor dataene er lagret, men også hvilken "vei" dataene tar til en bruker.[70] Når en bruker i f.eks. Oslo åpner en nettside, kan dataene komme fra en node[71] i USA, Russland, Nederland etc., alt etter hvor det er kapasitet i nettverket til

[67] http://www.advance.net besøkt 20.10.2017
[68] https://web.archive.org/web/20160410193437/http://www.redditblog.com/2009/11/moving-to-cloud.html besøkt 10.09.2017
[69] https://aws.amazon.com/?nc2=h_lg besøkt 10.09.2017
[70] Bing (2014) s.142-144
[71] En node er et punkt i et nettverk som f.eks. en server, switch eller router. For utfyllende definisjon se f.eks. https://www.computerhope.com/jargon/n/node.htm besøkt 02.09.2017

raskest å overføre dataene til brukeren i Oslo. Dataene vil altså alltid ta raskeste vei, og dette vil variere ut fra trafikken i nettverket og således gjøre det tilfeldig hvilke land dataene går igjennom eller hentes fra.

EU-domstolen har, gjennom *Amazon*- og *Weltimmo*-dommen, vist at den territorielle tilknytningen til EU ikke trenger å være spesielt stor for at direktivet skal gjelde.[72] Da forordningen strekker seg lenger enn direktivet, kan det tilsi at forordningen gjelder for reddit.com. Til tross for at nettsiden bruker Amazon sin tjeneste, så er det imidlertid ikke gitt at reddit.com lagrer informasjonen på serverne i Europa. Videre er ikke reddit.com og Amazon i samme type virksomhetsforhold som Google Spain og Google Inc. i *Google*-dommen, ettersom Amazon og Reddit Inc kun er kontraktspartnere, og ikke mor- og datterselskap. Dette gjør det vanskelig å avgjøre om den territorielle tilknytningen er tilstede.

Bruk av skylagringstjenester har skapt juridiske problemer når domstoler må ta stilling til om et selskap må overlevere personopplysninger til myndigheter. Dette er godt illustrert i en dom[73] avsagt mot Google i District of Columbia Federal Court. I dommen ble Google pålagt å utlevere informasjon som var lagret i deres skytjeneste. Google anførte i dommen at hvis amerikanske myndigheter skulle få overlevert personopplysningene måtte de kontakte myndighetene i de landene hvor opplysningene var lagret, hvilket var gjeldende praksis på daværende tidspunkt.[74] Domstolen mente at dette ikke var praktisk gjennomførbart siden Google lagret opplysningene i sin skylagringstjeneste. Informasjonen myndighetene krevde utlevert kunne dermed ikke spores tilbake til en konkret server, og informasjonen kunne forflytte seg til enhver tid. Således mente domstolen at amerikanske myndigheter ikke måtte be myndighetene i de landene hvor serverne var lokalisert om innsyn, men at Google, som et amerikansk selskap, måtte forholde seg til amerikansk lovgivning, også for informasjon lagret utenfor USA.[75] Til tross for at dommen omhandler amerikanske forhold og ikke konkret omhandlet spørsmålet om etablering, illustrerer den godt problemet med å bruke plasseringen til servere hvor informasjonen er lagret som et avgjørende moment i vurderingen av hvor en virksomhet skal anses etablert.

[72] Gömann (2017) s. 571-572
[73] Case No.1 16-mj-00757 (BAH)
[74] https://arstechnica.com/tech-policy/2017/09/feds-google-stops-challenging-most-us-warrants-for-data-on-overseas-servers/ besøkt 15.09.2017
[75] Case No.1 16-mj-00757 (BAH)

Da det ikke er klart om reddit.com i det hele tatt lagrer informasjon i EU, til tross for at de bruker Amazon sin skytjeneste, kan nettsiden ikke anses å ha en stabil territoriell tilknytning til EU. Virksomheten Reddit Inc kan følgelig ikke regnes som "etablert i Unionen", jf. forordningen artikkel 3 (1). For å avgjøre om forordningen kommer til anvendelse må det således vurderes om nettsiden oppfyller vilkårene i artikkel 3 (2).

2.5.3 Reddit.com og artikkel 3 (2)

Som redegjort for over, fremgår det av artikkel 3 (2) bokstav a at forordningen også gjelder for virksomheter som ikke er etablert i EU, når behandlingen av personopplysninger har sammenheng med "the offering of goods or services" til brukere i Unionen. Det avgjørende vil være om nettsiden har til hensikt å tilby varer og tjenester til brukere i Europa. Spørsmålet er om reddit.com oppfyller dette vilkåret.

Reddit.com har et stort antall underforum som retter seg mot lokale og nasjonale forhold i ulike europeiske land. Dette er et klart moment som tilsier at nettsiden retter seg mot brukere i EU.

Nettsiden har blant annet et underforum for norske forhold med over 80 000 registrerte brukere.[76] Det er i tillegg egne underforum om forskjellige byer rundt omkring i Norge. Samtidig er det viktig å huske på at alle underfora som blir opprettet på nettsiden opprettes av brukerne selv. Det er ingenting i veien for at en tilfeldig bruker oppretter underforumet "r/norge2". Videre er det brukere på fritiden, og ikke selskapet som moderer innholdet på nettsiden. Dette vanskeliggjør vurderingen av om nettsiden retter seg mot EU.

Et moment som taler for at nettsiden retter seg mot EU, er at det i nyere tid er innført et datascript som påvirkes av IP-adressen til brukerne ved opprettelse av en konto. Hvis en person med norsk IP-adresse oppretter en brukerprofil, blir vedkommende automatisk en del av det norske underforumet "r/Norge". Det må imidlertid nevnes at IP-adresse er noe mange brukere manipulerer, enten fordi de ønsker å kryptere dataene sine, eller f.eks. ved at de kobler seg til jobbservere via en VPN-klient.

[76] https://reddit.com/r/norge besøkt 06.12.2017

Det at Reddit er på et .com domene taler for at nettsiden ikke retter seg mot europeiske brukere, da det er et amerikansk domene. Reddit.com eier imidlertid en rekke andre domener tilknyttet navnet. Hvis en går inn på nettadressen reddit.de eller reddit.fr blir man automatisk videresendt til reddit.com. Dette kan være en taktikk for å sikre at andre ikke kan misbruke merkenavnet deres, ved å starte opp en konkurrerende nettside eller en phishing-nettside. Hva slags domene nettsiden bruker, bør etter dette ikke tillegges avgjørende vekt i vurderingen av om reddit.com har til hensikt å tilby varer og tjenester til europeiske brukere.

Ved første øyekast så kan reklame tilsynelatende være et viktig vurderingsmoment for å avgjøre om en nettside retter seg mot europeiske brukere. Dette vil imidlertid i stor grad avhenge av hvordan reklameplassene er tilbudt annonsørene. Det er hovedsakelig to forskjellige metoder som anvendes på nett. Den ene er den mer klassiske tilnærmingen til annonsesalg, som er tilsvarende den en finner i trykte aviser og på TV. I disse tilfellene har annonsøren kjøpt en spesifikk plass og redaktøren har gitt retningslinjer på størrelse, innhold osv. som de aksepterer. Ved bruk av denne måten å selge annonseplass på, vil reklamen på en nettside kunne være et viktig moment i retning av at en nettside retter seg mot europeiske brukere, når reklamen gjelder produkter eller tjenester som er tilgjengelige i Europa.

Den andre måten å selge annonseplass på er en automatisert prosess, hvor selskaper som Google Ads har laget profiler basert på metadata, og selger annonseplassen til høystbydende annonsør, i det en bruker laster inn nettsiden.[77] Denne prosessen foregår automatisk og utføres av boter[78]. På nettsider som anvender denne prosessen, vil reklamen som en bruker ser være basert på hva brukeren tidligere har brukt internett til. Altså baserer reklamen seg på brukerens tidligere søkehistorikk, og reklamen plasseres på nettsiden ved hjelp av informasjonskapsler[79]. Nettsiden vil på denne måten inneholde reklame for lokale selskaper og produkter. For brukerne, vil nettsiden derfor anses som rettet mot europeiske brukere. Ettersom markedsføringen vil variere fra bruker til bruker, og ikke er et aktivt valg fra nettsidens side, vil imidlertid bruk av slik markedsføring ikke kunne tillegges stor vekt i vurderingen av om nettsiden omfattes av forordningens virkeområde, ved å rette seg mot europeiske borgere.

[77] Datatilsynet (2015) s.18-26
[78] En bot er en programvare som kjører automatiske oppgaver over internett.
[79] Informasjonskapsel eller cookie, er ”en liten tekstfil som lastes ned og lagres på brukers datamaskin når brukeren åpner en nettside. Informasjonskapselen brukes for eksempel til å lagre innloggingsdetaljer, huske handlekurv i nettbutikken eller registrere hvor brukeren beveger seg rundt på nettstedet.” jf. https://www.nkom.no/teknisk/internett/cookies/informasjonskapsler-cookies besøkt 12.10.2017

Hva gjelder markedsføringen på reddit.com er det den mer tradisjonelle måten å selge annonseplass på som anvendes. Majoriteten av annonsene som vises har enten et fokus på det amerikanske markedet eller på nettjenester som er tilgjengelig for alle.[80] Dette taler i retning av at nettsiden ikke retter seg mot europeiske brukere. Det er imidlertid mulig for en annonsør å kjøpe annonseplass enten i konkrete underforum som f.eks. r/Norge, eller annonseplass basert på lokasjon, hvor man har mulighet til å velge f.eks. brukere med norsk eller svensk IP-adresse.[81] Dette taler klart for at nettsiden retter seg mot europeiske brukere.

Ordlyden i artikkel 3 (2) bokstav a sier klart nok at betaling ikke er nødvendig for at en tjeneste er rettet mot EU. Det fremgår imidlertid av fortalen at der hvor betaling finner sted, så vil bruken av valuta være et viktig moment i vurderingen om en tjeneste retter seg mot EU. Reddit.com er gratis å bruke, men det er mulig for brukere av nettsiden å betale for og hjelpe med driften av nettsiden, enten i form av et abonnement eller en engangssum. Reddit.com oppgir summen i amerikanske dollar. Dette tilsier at siden ikke retter seg mot EU.

På den andre siden så er det mulig å gjennomføre betalingen med Bitcoin eller via PayPal. Ved bruk av PayPal får brukere automatisk opp summen i lokal valuta og med informasjon om hva valutakursen er. Dette kan tilsi at nettsiden retter seg mot europeiske brukere, både på grunn av at de oppgir prisen i lokal valuta og fordi Paypal er en tjeneste som er tilgjengelig og i bruk i Europa.

Til tross for at det er mange momenter som tilsier at forordningen ikke regulerer reddit.com, er det flere sterke momenter som tilsier at tjenesten faller innunder forordningens virkeområde, blant annet det automatiske scriptet basert på IP-adresse, muligheten til å annonsere bare mot europeiske brukere, og alt innholdet som er eurosentrisk. Dette må tillegges avgjørende vekt i vurderingen.

Konklusjonen må etter dette være at reddit.com omfattes av forordningens virkeområde, jf. artikkel 3 (2) bokstav a, fordi nettsiden har til hensikt å tilby en tjeneste rettet mot europeiske brukere.

[80] Stikkprøver ved bruk av forskjellige nettlesere i tilfeldige underforum. Tatt stikkprøver en gang i måneden i perioden august 2017-november 2017.
[81] ads.reddit.com besøkt 10.10.2017

3 Håndheving og administrative sanksjoner

3.1 Personvernforordningen

Personvernforordningen gir nasjonale tilsynsorganer adgang til å ilegge administrative sanksjoner ved brudd på personvernforordningen. Hvilken myndighet det nasjonale tilsynsorganet skal ha etter forordningen fremgår av artikkel 58. Artikkel 58 (1) regulerer tilsynsorganenes myndighet til å etterforske mulig personvernbrudd. I artikkel 58 (2) fremgår de korrigerende tiltakene tilsynsorganene kan ilegge, hvis de etter undersøkelser har kommet frem til at det foreligger brudd på personvernforordningen. Det foreligger flere tilgjengelige administrative sanksjoner som tilsynsorganene kan ilegge, herunder stopp eller begrensing av adgang til å behandle personopplysninger, jf. bokstav f, stopp i overføring av personopplysninger til en mottaker i tredjeland, jf. bokstav j, og adgang til å ilegge administrative bøter, heretter bøter, i henhold til artikkel 83, jf. bokstav i. Det er sistnevnte tiltak som er kjernen for oppgaven. De øvrige sanksjonene vil det ikke redegjøres for nærmere.

De generelle vilkårene for ileggelse av bøter fremgår av artikkel 83. Det fremgår at bøter kan ilegges i tillegg eller istedenfor for de korrigerende tiltakene som fremgår av artikkel 58 (2) bokstav a til h og bokstav j. Vilkårene for når bøter kan ilegges fremgår av artikkel 83 (2) bokstav a til k. Vurderingene for når det kan ilegges bøtes er underordnet for oppgaven, og vil ikke gås nærmere inn på.

Nektelse av å innrette seg etter tiltak pålagt av tilsynsorganet etter artikkel 58 (2), jf. artikkel 83 (2), kan medføre bøter opptil 20 000 000 euro, eller opp til 4 % av det samlede globale årsomsetning til selskapet i det foregående regnskapsåret dersom dette beløpet er høyere, jf. artikkel 83 (6).

Bøter er ansett som straff etter den europeiske menneskerettskonvensjon (EMK). Dette medfører at klarhetskravet for ileggelsen av bøter er betydelig strengere enn ved ileggelse av tvangsmulkt som det er adgang til etter personverndirektivet. Det at ileggelsen av bøter etter forordningen er ansett som straff, medfører at det ikke uten videre kan ilegges flere bøter for

samme forhold, da dette kan stride mot forbudet mot dobbeltforfølgning etter EMK tilleggsprotokoll 4 artikkel 7. Det medfører også at adgangen til å påklage vedtaket inn til domstolene må være ivaretatt for ikke å krenke retten til en rettferdig rettergang etter EMK artikkel 6.[82]

Forordningen oppstiller dermed en rekke administrative sanksjoner som kan ilegges databehandlere og behandlingsansvarlige i tredjeland, men mangler mekanismer for hvordan sanksjonene kan inndrives. Det må derfor vurderes hvilke muligheter for inndrivelse som eksisterer uavhengig av forordningen.

3.2 Hvordan kan man inndrive bøter utstedt til tredjeland?

3.2.1 Innledning

Når inndrivelse av bøter ikke springer direkte ut av forordningen, må alternative muligheter for inndrivelse vurderes. Mulighetene for inndrivelse vil i stor grad variere og i mange tilfeller være avhengig av ulike faktorer. Hvilke muligheter som er tilgjengelig og ønskelig å anvende vil i stor grad avhenge av hvem databehandler og behandlingsansvarlig er, ettersom noen virksomheter vil være villig til å betale for å fremstå som et firma som ønsker å rette opp i personvernbrudd. I hvilket land databehandler og behandlingsansvarlig befinner seg vil også være relevant. Dette fordi det kan variere hvor tett kontakt det er mellom et medlemsland og et tredjeland. Dersom medlemslandet og tredjelandet har tette bånd vil tilsynsorganet kunne lettere få hjelp til å inndrive bøtene.

I det følgende vil det bli presentert potensielle løsninger på problemstillingen knyttet til inndrivelse av bøter i tredjeland.

[82] Prop 62 L (2015-2016) s. 24, s. 28 flg.

3.2.2 Pålagt samarbeid mellom tilsynsorganer i EU

Innledning

Selv om personvernforordningen ikke løser spørsmålet om hvordan bøter skal inndrives overfor selskaper i tredjeland, oppstiller forordningen likevel enkelte mekanismer for samarbeid som potensielt kan bidra til å forenkle inndrivelsen, også i tredjeland. Det er et uttalt mål at personvernforordningen skal bli et "one-stop shop"[83], gjennom totalharmoniseringen. Det vil si at virksomheter ikke skal behøve å sette seg inn i de forskjellige medlemslandenes lovgivning, men har et felles europeisk regelverk å forholde seg til. For å oppnå målsetningen om et "one-stop shop", pålegger forordningen medlemslandenes tilsynsorganer å samarbeide. Dette samarbeidet er regulert i forordningens artikkel 60 til 62. Det fremgår av artikkel 61 (1) at tilsynsorganene skal utveksle relevant informasjon og yte gjensidig bistand for å sikre en ensartet gjennomføring og anvendelse av personvernforordningen. Det fremgår også av samme bestemmelse at tilsynsorganene skal iverksette tiltak for å sikre et effektivt samarbeid. Hvilke krav forordningen i detalj stiller til det administrative samarbeidet vil det ikke bli redegjort for da dette faller utenfor oppgavens problemstilling.

Bilaterale avtaler om inndrivelse av bøter

Den mest åpenbare fordelen med det administrative samarbeidet mellom medlemslandene er at medlemslandene kan nyte godt av øvrige medlemslands bilaterale avtaler med tredjeland. Det fremgår av forordningen artikkel 50 at det er en delt kompetanse mellom medlemslandene og Kommisjonen hva gjelder å inngå avtaler for inndrivelse av bøter i tredjeland. Det er naturlig å legge til grunn at en virksomhet som behandler personopplysninger om brukere i et medlemsland, også behandler personopplysninger om brukere i en rekke andre medlemsland. Kommisjonen ønsker naturlig nok at alle medlemslandene har like avtaler som omhandler personvernforordningen. Det er imidlertid naturlig at et medlemslands avtaleinngåelse med et tredjeland kan være avhengig av tidligere samarbeidsavtaler, diplomatiske forhold, felles historie o.l. Dette kan medføre ujevn

[83] https://www.eugdpr.org/eugdpr.org.html besøkt 15.11.2017

maktbalanse mellom medlemslandene. Det pålagte samarbeidet mellom tilsynsorganene kan avhjelpe dette, ettersom tilsynsorganet i det medlemslandet som har fremforhandlet en avtale med tredjelandet, kan utstede boten på vegne av eller sammen med, de øvrige tilsynsorganene som har undersøkt personvernbruddet.

Det å bruke et medlemslands bilaterale avtale med et tredjeland som inndrivelsesgrunnlag for andre medlemsland, kan skape flere problemer. For det første vil muligheten til å inndrive bøter for personvernbrudd overfor andre medlemslands brukere, være avhengig av den konkrete avtalen med tredjelandet. Dersom avtalen stenger for inndrivelse av bøter for personvernbrudd overfor andre medlemslands brukere kan man risikere at norske brukere, for eksempel dersom Norge inngår en avtale om inndrivelse av bøter med India, stilles bedre enn brukere i øvrige europeiske land. Dette vil kunne skape problemer med målsetningen om et totalharmonisert personvernregelverk i EU, som kan medføre at Kommisjonen vil prøve å stoppe den bilaterale avtalen.

Et annet problem er tredjelandets intensjon med avtalen. Om et tredjeland kun ønsker å samarbeide med et konkret medlemsland, vil en avtale som åpner for at alle medlemsland i EU kan inndrive bøter fort resultere i at tredjelandet trekker seg fra avtalen. Et tredje problem som kan oppstå er at tilsynsorganet i det aktuelle medlemslandet, for eksempel Datatilsynet, ikke vil bruke den bilaterale avtalen til å inndrive bøter for personvernbrudd i andre europeiske land, når det ikke foreligger brudd med norske brukeres personvern. Det kan også tenkes at Datatilsynet er tilbakeholdne med å utnytte den bilaterale avtalen til å inndrive bøter for personvernbrudd i andre medlemsland, fordi de ikke ønsker at tredjelandet skal trekke seg fra avtalen. I så tilfelle vil Datatilsynet miste sin mulighet til å inndrive bøter i fremtiden, hvor det potensielt er klare personvernbrudd ovenfor norske brukere.

Samarbeid med tredjeland om inndrivelse av bøter

Et godt samarbeid med det aktuelle tredjelandet vil kunne danne et solid fundament, som kan bidra til at myndighetene i det aktuelle tredjelandet vil hjelpe til med inndrivelse av bøter. Dette kan skje dersom myndighetene i tredjelandet anser samarbeidet med medlemslandet som viktigere enn at virksomheten skal unnslippe boten. Som det fremgår av fremstillingen om ekstraterritorialitet i punkt 4, skal det imidlertid ikke mye til før tredjeland føler at EU overskrider sin jurisdiksjon og territorium når det vedtas regler som får effekt utenfor EU. Det

vil derfor være en hårfin balansegang mellom utnyttelse av godt samarbeid og å overskride sitt handlingsrom.

En styrke ved det administrative samarbeidet er at det vil bidra til at de forskjellige tilsynsorganene tolker regelverket likt i hele EU, og at de legger seg på samme bøtenivå. Hvis personvernreglene blir harmonisert i hele EU, og ikke bare på papiret, vil dette kunne medføre at virksomheter utenfor EU respekterer at det blir ilagt bøter. Dette kan forenkle inndrivelsen av bøtene i tredjeland. Dette har en todelt forklaring.

Uten et harmonisert regelverk og bøtenivå vil virksomheten, for det første, kunne få et inntrykk av at det er vilkårlig hvilke land som prøver å bøtelegge virksomheten, eller at det er vilkårlig hvor høy boten kommer til å være. Hvis håndhevingen ikke oppleves som vilkårlig for virksomheten, vil det kunne bidra til en enklere inndrivelse. Dette fordi virksomheten ikke får inntrykket av at de blir bøtelagt fordi de er etablert i et tredjeland.

For det andre, vil et totalharmonisert regelverk i hele EU-området gjøre det enklere for virksomheter utenfor EU å gå inn i det europeiske markedet, fordi de kun må forholde seg til ett regelsett om personvern. Dette vil være fristende for virksomheter, da den potensielle økonomiske fordelen av tilgang til EU, for mange virksomheter vil være betydelig større enn størrelsen på bøtene som kan bli utstedt. Det er imidlertid stilt spørsmål hvor effektivt medlemslandenes tilsynsorgan kan totalharmonisere den praktiske anvendelsen av forordningen.[84] Til tross for at forordningen skal være totalharmoniserende må medlemslandenes tilsynsorganer likevel tolke og anvende regelverket likt, og dette er ikke nødvendigvis gitt ettersom medlemslandene har ulike rettstradisjoner. [85] Et land som tradisjonelt har satt personvernet høyt, vil i mange tilfeller tolke reglementet annerledes enn medlemsland hvor personvernet ikke har fått en like fremtredende plass i rettshistorien. Det vil si at virksomhetene likevel må sette seg inn i personvernreglene i de landende de ønsker å operere i.[86]

[84] Blume (2015) s. 237
[85] *op.cit.* s. 237-238
[86] *Ibid.*

Erfaringer fra andre rettsområder

Det tvungne samarbeidet mellom medlemsstatene som forordningen legger opp til er ingen nyskapning i EU-lovgivningen. Tilsvarende samarbeidsordninger finnes også på andre rettsområder i EU. For eksempel finnes det regler for administrativt samarbeid i EUs forbrukerlovgivning, nærmere bestemt i Consumer Protection Cooperation (2006/2004/EC), heretter CPC-forordningen. CPC-forordningen har tilsvarende obligatorisk samarbeid mellom tilsynsorganene i medlemslandene som den som legges til grunn i forordningen. CPC-forordningen har bidratt til et større samarbeid mellom forbrukertilsynsorganene på tvers av landegrensene, og har, ifølge tilsynsorganene selv, vært en viktig del i opprettelsen og driften av ICPEN. ICPEN er en internasjonal forbrukerrettighetsorganisasjon, med medlemmer fra en rekke forskjellige land, herunder USA, Norge og Tyrkia, og med bl.a. UNCTAD og Kommisjonen som observatører. Effekten av organisasjonens arbeid kan selvfølgelig diskuteres, men de har ifølge seg selv, vært en viktig pådriver for at en rekke land har bedret forbrukerrettighetene.[87] Organisasjonen har ingen formell makt, men et slikt samarbeid er klart nok med på å sette fokus på de problemene organisasjonen arbeider med. Dette vil kunne ha overføringsverdi til personvernområdet. Med flere land enn bare de europeiske som jobber for et harmonisert regelverk, øker sannsynligheten betraktelig for at en kan vedta like, eller i det minste tilnærmet like regler om personvern, gjennom handelsavtaler som WHO, OECD eller lignende samarbeidsorganer. Dette vil igjen forenkle inndrivelsen av bøter ettersom virksomheter antas å lettere ville innrette seg etter europeisk regelverk som også samsvarer med tredjelandets nasjonale regelverk. Dette går ikke direkte på inndrivelse av bøter, men vil kunne bidra til et felles regelverk som åpner for at tilsynsorgan har en effektiv inndrivelsesmulighet.

3.2.3 Internasjonal handel

Det er klart at overføring og behandling av personopplysninger har blitt en stor del av økonomien til virksomheter som tilbyr nettbaserte tjenester. Det er videre klart at mye av inntektene kommer via bl.a. annonsesalg basert på personopplysninger.[88] Da dette i mange tilfeller er annonsesalg, dvs. handel, på tvers av landegrenser, er det naturlig å se hen til om

[87] https://www.icpen.org/initiatives besøkt 19.10.2017, https://www.icpen.org/who-we-are besøkt 19.10.2017
[88] Datatsilsynet (2015) s.11, 27 med videre henvisninger

General Agreement of Tariffs and Trade, heretter GATT, kan bidra til at tilsynsorganer kan inndrive bøter via hjelpemidler som følger av handelsavtalen. GATT er en global handelsavtale og omhandler ikke direkte inndrivelse av bøter. GATT stiller generelle krav til handel mellom landene, men stenger imidlertid ikke for at hvert medlemsland kan fremforhandle avtaler som stiller landet i en gunstigere posisjon enn det som følger **av** GATT. Det vil si at GATT kan åpne for å skape fremtidige rettsgrunnlag om inndrivelse av bøter.

Det fremgår av GATT artikkel I et generelt prinsipp om "most favoured nation-treatment." Dette prinsippet innebærer at et land må ilegge samme tollsats på varer fra alle land som eksporterer til dette landet, med mindre det foreligger en konkret handelsavtale.[89] Videre hjemler GATT artikkel VI adgangen til å ilegge "anti-dumping", eller "countervailing measures" mot land som ikke følger prinsippene om frihandel som følger av GATT-avtalen. Denne bestemmelsen gir adgang til å ilegge straffetoll til et eksporterende land hvis man finner det bevist at landet gir ulovlige subsidier til eksportøren. Det er ifølge GATT bare lov å ilegge straffetoll mot et land, hvis det bryter med frihandelsavtalen.[90] Det er altså en snever tilgang til å ilegge en høyere tollsats etter GATT-avtalen. Dette gjør det ulovlig å ilegge straffetoll på varer som stammer fra et tredjeland som bryter personvernreglene uten at det foreligger en handelsavtale som regulerer dette. Det kan således ikke ilegges straffetoll mot et tredjeland som et pressmiddel for at myndighetene i landet skal oppfordre virksomheter til å betale bøtene**.** Det må imidlertid påpekes, at hvis det hadde vært adgang til å ilegge straffetoll, ville myndighetene i mange tilfeller ikke vært villige til å ilegge straffetollen pga. diplomatiske og økonomiske konsekvenser dette kan få for landet.

Til tross for at GATT ikke åpner for en straffetoll pga. personvernbrudd, stenger avtalen ikke for at land ved inngåelse av handelsavtaler inkluderer adgangen til utstedelse og inndrivelse av bøter ved personvernbrudd. En handelsavtale som inkluderer adgangen til å inndrive bøter, vil i seg selv, ikke føre til at en virksomhet etablert i tredjeland vil respektere en bot utstedt av et europeisk tilsynsorgan. Det vil imidlertid føre til at det foreligger et gyldig rettsgrunnlag i tredjelandet for inndrivelse, og således åpne opp for at myndigheter, tilsvarende namsfogden, i tredjelandet vil begjære utlegg og bidra til inndrivelsen av boten. For tredjeland vil en handelsavtale som inkluderer adgangen til å inndrive bøter ved personvernbrudd, være mer

[89] https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm besøkt 25.08.2017, Harrison (2005) s. 1663-1689

[90] Dette er en forenklet fremstilling av adgangen til ileggelse av straffetoll, for mer utfyllende: https://www.wto.org/english/tratop_e/adp_e/adp_info_e.htm besøkt 25.08.2017

aktuelt å inngå med EU enn med EØS-landene. Dette er fordi den potensielle økonomiske fordelen av å få tilgang til EUs indre marked er betydelige større enn adgangen til markedet i Norge, Island og Liechtenstein.

Det er Kommisjonens prerogativ å forhandle handelsavtaler med tredjeland.[91] Det vil derfor bare være en institusjon innenfor EU som kan forhandle frem handelsavtaler som inkluderer beskyttelse av personvern. Det at det bare er en institusjon som forhandler om slike avtaler, kan begrense antall avtaler som inkluderer etterlevelse av forordningen utenfor EUs territorium.

Det er flere problemer med denne tilnærmingen for å sikre personvernet. Det første problemet med denne tilnærmingen går på den ekstraterritorielle effekten av å inngå avtaler som får rettsvirkning i tredjeland. Det vil i mange tilfeller være tvilsomt om et tredjeland er villig til å adoptere EUs personvernregler slik at personvernreglene får rettsvirkning for virksomheter som er etablert i tredjelandet. Dette hovedsakelig fordi det begrenser statens egen suverenitet. Det kan også være fordi virksomhetene som potensielt bryter personvernreglene generer større inntekter for tredjelandet, enn hva tilgangen til det indre markedet sannsynlig vil generere av inntekter for landet. Dette vil i stor grad avhenge av industrien til tredjelandet.

Det andre problemet med handelsavtaler som inkluderer beskyttelse av personvernet til europeiske brukere omhandler innenrikspolitikk. Når EU, eller Norge, inngår en handelsavtale med et tredjeland, vil landet verne om sine egne viktige industrier. Det vil derfor ikke være ønskelig for hverken Kommisjonen eller medlemslandene å inngå avtaler som kan skade en viktig industri i Unionen på bekostning av et potensielt bedre personvern. Det vil i slike tilfeller være en avveining mellom hvor viktig industrien er, og i hvor stor grad virksomheter i tredjelandet bryter personvernet til europeiske brukere. Et tredje problem med dette er at til tross for at personvern er høyt på EUs politiske agenda, er det ikke gitt at personvern får en viktig rolle når det inngås forhandlinger med tredjeland om avtaler som i utgangspunktet omhandler andre rettsområder.

Et siste problem med å inngå handelsavtaler som åpner for inndrivelse av bøter ved personvernbrudd, er at det i stor grad vil være avhengig av det politiske klimaet i tredjelandet. Hvis det er en økende trend i tredjelandet om å drive med proteksjonisme av nasjonal industri,

[91] Følger av TFEU artikkel 207. Council of Europe skal assistere Kommisjonen i forhandlingene, men det er Kommisjonen som skal forhandle med tredjeland, jf. artikkel 207 (3). Følger også av ERTA-doktrinen, nå kodifisert i TFEU artikkel 3 (2). Se også Bourgous (1998) s. 156-159.

og ikke drive med internasjonalisering av handel og annet samarbeid, vil det være svært vanskelig å inngå avtaler om nettopp dette.

3.2.4 Andre virkemidler i forordningen

Ettersom det er tvilsomt om tilsynsorganer i det hele tatt kan inndrive bøter utstedt i tredjeland for brudd på personvernet åpner for spørsmålet om en i det hele tatt skal utstede bøter til behandlingsansvarlige og databehandlere etablert i tredjeland, eller om tilsynsorganene bør velge alternative sanksjoner for å sikre personvernet. Det er selvfølgelig ingenting som hindrer et tilsynsorgan å utstede en bot når vilkårene er oppfylt, men hvis bøtene ikke kan inndrives, mister de fort sin pønale og avskrekkende karakter.

Det foreligger en adgang for tilsynsorganet til å stoppe overføring av personopplysninger til tredjeland, jf. artikkel 58 (2) bokstav f. Som det fremgår av Kongresshøringen fremstilt i punkt 4, er det en stor bekymring blant bedrifter at overføring av data mellom EU og USA skal stoppe, da overføringen utgjør en signifikant økonomisk verdi for selskapene. Det er klart at virksomheter ikke behandler personopplysninger uten at det har en verdi for virksomheten. En stopp i overføringen av data til tredjelandet vanskeliggjør muligheten for virksomheten til å tjene penger på denne behandlingen. Dette innebærer at en stopp i overføring fremstår som mer pønalt for en virksomhet i et tredjeland, enn en bot som uten inndrivelse ikke medfører et økonomisk tap. Hvis det ilegges bøter, bør det altså ilegges sammen med et opphold i overføring av data som ikke opphører før boten er blitt betalt. Hvis dette gjøres er det to utfall som er sannsynlige. Det ene er at overføringen er såpass viktig for virksomheten at de velger å etterkomme kravene fra tilsynsorganet, det vil si at boten betales. Det andre utfallet er at personopplysningene om europeiske brukere er av mindre betydning for virksomheten, så de velger å ignorere pålegget. I det siste tilfellet vil da beslutningen om en stopp i overføring forhåpentligvis hindre, men i det minste vanskeliggjøre, fremtidige personvernbrudd ettersom virksomheten ikke lenger har tilgang til nye personopplysninger. Hvor effektiv en slik løsning er, vil i stor grad avhenge av hvilken teknisk løsning som blir valgt. Det vil ikke redegjøres for hvilke alternativer som finnes, men det er klart at en teknisk løsning som enkelt kan omgås av virksomheten, mister hele sin verdi.

Som det fremgår av *Schrems*-dommen er i utgangspunktet alle avgjørelser om at et tredjeland ivaretar en adekvat beskyttelse av personopplysninger bindende for medlemslandene, jf.

TFEU artikkel 288. Denne vurderingen er da også bindende for tilsynsorganene. Det fremgår videre av dommen at det er en delt kompetanse mellom Kommisjonen og medlemslandene å forsikre at personvernet er tilstrekkelig vernet. I tilfeller hvor det ikke er tilstrekkelig vern, og da også ved brudd, er det adgang for tilsynsorganene å "suspend the transfer of data in question, irrespective of the general assessment made by the Commission in its decision"[92] i følge Advocate General Bot.[93] Dette vil også være tilfellet etter at GDPR trer i kraft. Det vil tilsynelatende være adgang til å pålegge en stopp i overføring av personopplysninger til tredjeland uavhengig av på hvilket rettslig grunnlag personopplysningen er lovlig overført.

En annen løsning som ikke følger direkte av forordningen, men som kan være aktuell i fremtiden, er å blokkere nettsider som konsekvent bryter personvernet. Av tekniske grunner vil ikke denne løsningen være aktuell for alle typer virksomheter. Det vil kunne være aktuelt for tjenester som Google, Facebook, Reddit o.l. nettsider, men for virksomheter som bruker web beacons, informasjonskapsler, trackere osv.[94] for å samle inn informasjon på andre nettsider enn sine egne, vil dette være et mindre aktuelt sanksjonsmiddel. Det foreligger ikke en generell adgang til å stenge ute nettsider etter GDPR, og det kan potensielt stride mot et nettnøytralitetsprinsipp[95], men det er foreslått i den reviderte CPC-forordningen at forbrukertilsynsorganer har myndighet til å stenge svindelnettsider.[96] EU har altså vært inne på tanken om muligheten til å blokkere nettsider som er tilgjengelige innenfor Unionen i nyere lovgivning enn GDPR. CPC-forordningen er ikke endelig vedtatt, så dette punktet kan forsvinne. Det åpner imidlertid spørsmålet om dette er en fruktbar vei å gå for å hindre personvernbrudd. I tillegg til spørsmålet om det strider mot et nettnøytralitetsprinsipp, er det et spørsmål om hvordan en nettside effektivt kan stenges for europeiske brukere.

Piratnettsteder som The Pirate Bay er gode eksempler på problemene med å stenge en nettside som løsning for å hindre personvernbrudd. Det foreligger en rekke eksempler på at piratnettsteder har blitt stengt og beslaglagt av nasjonale myndigheter. I flere av disse tilfellene har det ikke tatt lang tid før alternative nettsider har overtatt for den stengte nettsiden. Et annet problem er måten nettsider kan bli blokkert eller stengt på. I tingrettsdommen, TOSLO-2015-67093, var det reist spørsmål om norske internettleverandører måtte stenge adgangen til å besøke kjente piratnettsteder for sine

[92] Advocate General Bot Opinion Case C-362/14 avsnitt 81.
[93] Dette kan også leses ut av domsavsigelsen i C-362/14.
[94] Fremstilling av hvordan dette foregår kan leses i Datatilsynet (2015)
[95] Se Direktiv 2002/22/EC om nettnøytralitet
[96] http://ec.europa.eu/consumers/consumer_rights/unfair-trade/docs/cpc-revision-proposal_en.pdf avsnitt 12

brukere. Internettleverandørene ble dømt til å stenge adgangen til nettsiden via DNS-blokkering[97], en løsning som er svært enkel for brukere å omgå.[98]

Det å stenge en nettside kan bidra til inndrivelse av bøter ved at det blir formidlet at blokkeringen oppheves hvis boten blir betalt. Det er imidlertid ikke i veien for at nettsiden oppretter alternative domener for å omgå blokkeringen, og således vil være tilgjengelig i EU uten at boten er betalt.

Det er altså flere svakheter ved å stenge en nettside for å hindre fremtidig personvernbrudd og for å få inndrevet boten som er utstedt. Dette er således ikke en løsning som bør anvendes, med mindre en velger en teknisk løsning som er vanskelig å omgå for virksomheter som bryter med personvernreglene.

[97] DNS-blokkering er en måte å sperre datatrafikk, for nærmere beskrivelse se f.eks. https://www.tek.no/artikler/guide-har-du-fatt-opp-denne-meldingen/276676 besøkt 05.09.2017
[98] Se f.eks. https://www.tek.no/artikler/piratpartiet-har-satt-opp-apen-dns-server/192514 besøkt 05.09.2017

4 Ekstraterritorialitet og personvernforordningen

4.1 Praktisk betydning av "Ekstraterritorialitet"

Det har i lengre tid vært diskusjoner knyttet til om EU, gjennom sin lovgivning og handlemåte går utover sitt mandat og prøver å regulere andre land.[99] Denne diskusjonen ble for alvor aktualisert innen personvern etter Google-dommen[100], og særlig etter vedtakelsen av den kommende forordningen.[101] Forordningens artikkel 3 oppstiller en lav terskelen for når forordningen kan få virkning utenfor EUs territorium.[102] Videre har Kommisjonen uttalt at "EU data protection standards have to apply regardless of the geographical location of a company or its processing facility."[103] Derfor er det ikke rart at diskusjonen har igjen blitt aktuell når forordningen skal gjennomføres. I det følgende vil begrepet ekstraterritorialitet bli drøftet inngående. Det vil også bli vurdert hvilken betydning ekstraterritorilitet har for gjennomføringsevnen av personvernforordningen.

Som nevnt i punkt 1.4.4 har det vært anerkjent en god stund at linjen mellom territoriell og ekstraterritoriell jurisdiksjon blir vanskeligere å trekke etterhvert som overføring av data på tvers av landegrenser finner sted[104] og den ekstraterritorielle effekten av lovgivning er av mange ansett som et inngrep i staters suverenitet.[105]

Begrepet ekstraterritorialitet har vært kritisert for å være tvetydig, da det kan brukes i tilfeller der EU-lovgivning blir aktivert hos rettssubjekter som befinner seg helt eller delvis utenfor EUs territorium.[106] Scott skriver "where a measure is defined as extraterritorial, it will be unlawful unless an alternative, recognized jurisdictional base can be found."[107] Videre viser hun til viktigheten av den territorielle virkningen av EU-lovgivningen ved henvisning til *Air Transport Association of America*-dommen (C-366/10), heretter *ATAA*-dommen. I dommen

[99] Bradford (2012)
[100] van Alsenoy og Koekkoek (2015). Spiecker (2015) s. 1041-1043
[101] Svantesson (2015), Colonna (2014)
[102] Se punkt 2
[103] COM(2012)09 final 25.01.2012 s. 10
[104] Gömann (2017) s. 568, Scott (2014) s. 1345
[105] Gömann (2017) s. 568, Kuner et.al (2013) s. 147
[106] Scott (2014) s. 1344
[107] *op.cit.* s. 1345

kom EU-domstolen frem til at det var grunnlag for å ilegge amerikanske, og andre nasjonaliteters flyselskaper en miljøavgift, da avgiften ble ilagt alle flyruter som lettet eller landet i EU. Domstolen konkluderte med at klimakvotedirektivet (2003/87/EF) ikke kunne tolkes utvidende til å hjemle miljøavgiften for flyselskaper utenfor EU. For å sikre formålet med klimakvotedirektivet, hjemlet EU-domstolen midlertid miljøavgiften i internasjonal sedvane. Det kan derfor argumenteres for at direktivet fikk ekstraterritoriell omfang. Samtidig så var ikke domstolen villig til å bygge beslutningen sin kun på direktivet. Hadde domstolen ikke funnet et alternativt rettsgrunnlag, hadde domstolen, etter alt å dømme, kommet til at ileggelsen av miljøavgiften var ulovlig. Dette skiller seg fra *Google*-dommen, hvor domstolen valgte å tolke EU-reglene om territoriell tilknytning utvidende slik at de kunne anvendes og få konsekvenser utenfor EUs territorium.[108]

Eksperter på EU-lov har argumentert for, at personverndirektivet ikke har "ekstraterritorielt omfang", men kan ha "ekstraterritoriell innflytelse".[109] På samme tid har eksperter utenfor EU uttalt at EUs personverndirektiv, og nå personvernforordning, er ekstraterritoriell av natur, og dermed har et ekstraterritorielt omfang.[110] Dette er godt illustrert i en Kongresshøring i USA om EUs personverndirektiv og hvilken betydning direktivet ville ha for USA. I høringen var det særlig fokus på personverndebatten i USA og hvilken påvirkning personverndirektivet hadde på amerikanske selskaper. I høringen var det flere ekspertuttalelser fra bl.a. forretningsledere av IT-selskaper, jussprofessorer, advokater og representanter fra EU. [111] Det er klart ut fra uttalelsene fra de amerikanske og canadiske representantene at direktivet har en ekstraterritoriell natur, da det regulerer tilnærmet all data som overføres fra og til EU. Flere av høringsuttalelsene uttrykker bekymring for påvirkningskraften det vil ha på selskaper i USA. Det ble uttalt at amerikanske selskaper kan havne i store økonomiske vanskeligheter dersom EU velger å stoppe overføringen av personopplysninger fra sine medlemsland, hvilket i praksis vil tvinge amerikanske selskaper til å måtte følge europeisk lovgivning. [112]

Om personvernforordningen anses å være ekstraterritoriell i omfang eller har ekstraterritoriell innflytelse, kan sies å bare være en klassifisering uten rettsvirkning. Skillet er imidlertid viktig av særlig to grunner. For det første vil skillet ha betydning for EU-domstolens tolkning

[108] Se punkt 2.4
[109] Kuner (2015a) s. 235
[110] *op.cit.* s.235
[111] https://www.gpo.gov/fdsys/pkg/CHRG-107hhrg71497/html/CHRG-107hhrg71497.htm Transkripsjon, besøkt 20.10.17
[112] *ibid.*

av virkeområdet til forordningen. Hvis forordningen anses å ha et ekstraterritorielt omfang, vil det være mindre sannsynlig at EU-domstolen anvender andre rettsgrunnlag, som internasjonal sedvane, for å avsi en avgjørelse mot for eksempel virksomheter som ikke er etablert i EU. Det vil si motsatt av hva domstolen gjorde i *ATAA*-dommen, jf. over.

For det andre vil distinksjonen være viktig for tredjelands inntrykk av forordningen. Hvis forordningen fremstår som kun å ha ekstraterritoriell innflytelse, kan det argumenteres for at tredjeland ikke like lett vil få inntrykk av at personvernforordningen griper inn i deres suverenitet. Dette er fordi at forordningen da ikke fremstår som at EU prøver å regulere forhold utenfor sitt territorium. Dersom tredjeland tolker forordningen slik at de ikke er tvunget til å følge forordningen, kan det tenkes at tredjeland velger å innrette seg etter forordningens regler frivillig, fordi reglene objektivt sett fremstår som gode. Distinksjonen kan således ha betydning for hvor stor gjennomslagskraft forordningen får i praksis hva gjelder virksomheter etablert i tredjeland.

Den ekstraterritorielle rekkevidden til forordningen kan på mange måter sies og ikke være ulik det en finner i andre land og andre rettsområder. Forordningens artikkel 3 (2) gjelder, som redegjort for over, når det er virksomheter som retter seg mot EU, eller når overvåkningen gjelder oppførsel innenfor EU. Den er altså begrenset til å gjelde forhold som skjer innenfor EU og i tilknytning til EU-borgere. Dette har flere likhetstrekk med f.eks. skattereglene til USA som krever at amerikanske borgere bosatt utenfor USA fortsatt må betale skatt til USA[113], eller nasjoner som har f.eks. straffelover som åpner for å straffe handlinger som har skjedd utenfor landets grenser.[114]

Det er verdt å merke seg at EU ikke er alene om vedtak innenfor personvern som har ekstraterritoriell effekt. Den 28.06.2017 avsa canadisk Høyesterett en dom mot Google Inc. Domstolen var enige med saksøker at retten til å bli glemt på internett innebærer at søkeresultatene som må fjernes, ikke bare må fjernes fra den lokale søkemotoren, men også den internasjonale. I sin redegjørelse om hvorfor Google må fjerne søkeresultatene globalt, uttaler domstolen:

[113] https://www.irs.gov/individuals/international-taxpayers/us-citizens-and-resident-aliens-abroad besøkt 27.10.2017

[114] Eksempel på dette er f.eks. Lov 20. Mai 2005 nr. 28 om straff, §§ 101-109 som gir Norge adgang til å straffe krigsforbrytelser i andre land.

> "Where it is necessary to ensure the injunction's effectiveness, a court can grant an injunction enjoining conduct anywhere in the world. The problem in this case is occurring online and globally. The Internet has no borders — its natural habitat is global. The only way to ensure that the interlocutory injunction attained its objective was to have it apply where Google operates — globally."[115]

Franske tilsynsmyndigheter har ilagt tilsvarende sanksjoner mot Google etter personverndirektivet. Google har motsatt seg vedtakene, og spørsmålet om retten til å bli glemt på internett gjelder globalt skal snart avgjøres av EU-domstolen.[116]

Det territorielle aspektet ved EUs personvernforordning har blitt kritisert for å være enten eller, og mangler sikkerhetsmekanismer som skal hindre at jurisdiksjonen går for langt og fører til konflikter mellom EU og tredjeland. I praksis må derfor virkeområdet til forordningen tolkes i lys av hva som er praktisk gjennomførbart ovenfor virksomheter i tredjeland [117]

4.2 Er forordningen ekstraterritoriell i omfang eller innflytelse?

Hvilken merkelapp en bør sette på personvernforordningen er uklart. Som det er redegjort for over, er den potensielle rekkevidden til artikkel 3 (2) veldig vid. Hvis EU-domstolen og tilsynsorganene velger å tolke forordningen utvidende, taler dette klart fort at forordningen har et ekstraterritorielt omfang. Videre har Kommisjonen eksplisitt uttalt at lokasjonen til virksomheten ikke kan være av betydning for om personvernet skal anses å ha tilstrekkelig beskyttelse. Det er klart at Kommisjonens uttalelse i seg selv ikke har rettsvirkning, men vil være en relevant rettskilde hvis domstolen skal avsi en avgjørelse om virkeområdet til forordningen.

At forordningen bare kommer til anvendelse når virksomheter retter sine varer eller tjenester mot EU eller når overvåkningen gjelder oppførsel i EU, trekker i retning av at forordningen bare har ekstraterritoriell innflytelse, siden det som et minimum kreves en form for tilknytning til EU.

[115] Google Inc. v. Equustek Solutions Inc., 2017 SCC 34
[116] https://www.theguardian.com/technology/2017/jul/20/ecj-ruling-google-right-to-be-forgotten-beyond-eu-france-data-removed besøkt 01.12.2017
[117] Kuner (2015a) s. 241-242

Det finnes konkrete eksempler på at EUs personvernregler har fått virkning utenfor EUs territorium. Det mest klare eksempelet på dette finner en innenfor Cloud-computing, hvor en rekke av de største virksomhetene prøver å opprettholde kravene etter personverndirektivet også for de deler av virksomheten som faller utenfor direktivets jurisdiksjon.[118] Det har dermed blitt en bransjenorm innenfor det aktuelle IT-området. Dette kan skyldes at de økonomiske konsekvensene av å miste tilgangen til det europeiske markedet er så store, at det lønner seg å følge regelverket uavhengig om regelverket direkte regulere deres virksomhet eller ikke. Det er også tredjeland som velger å se til EU fremfor USA når personvernregler skal oppdateres. Dette kan tale for både at den kommende forordningen har ekstraterritorielt omfang og at den har ekstraterritoriell innflytelse.

Det er for tidlig å si om personvernforordningen er ekstraterritoriell i omfang eller innflytelse. Det må avgjørelser fra EU-domstolen til, før en kan si noe autorativt om hvilken linje regelverket vil legge seg på. Som det fremgår av redegjørelsen her og i punkt 3.2 er en ekstraterritoriell innflytelse linjen EU og tilsynsorganene bør legge seg på for å best kunne inndrive bøter for brudd på personvernforordningen.

[118] Spiecker (2015) s. 1052, Kuner (2015b) s. 61

5 Avslutning

> ”Der er en klar risiko for, at persondataretten som følge af den udbredte digitalisering vil drukne, og at det på et tidspunkt må erkendes, at den var en smuk vision, men i realiteten var den en illusion.”[119]

Dette uttalte Professor Blume i sin fremstilling om personvern i et stadig mer digitalisert samfunn. Uttalelsen er noe pessimistisk, men illustrerer godt viktigheten og problemer med den kommende personvernforordningen. Internett er et globalt fenomen uten felles kjøreregler. EUs virkeområde er i utgangspunktet avgrenset til Europa, men gjennom forordningen forsøker EU likevel å gi regler utenfor sin jurisdiksjon. På papiret fremstår dette som en god idé, men, som drøftelsene over viser, er det vanskelig gjennomførbart i praksis.

At regelverket mangler gjennomføringsevne, vil kunne være avgjørende for om tredjeland henter inspirasjon fra EUs personvernregler. Et godt fungerende regelverk vil lettere kopieres av tredjeland, enn et regelverk som på papiret virker godt, men som ikke fungerer like bra i praksis. Uten gjennomføringsevne vil altså den gode intensjonen bak den utvidede territorielle rekkevidden kunne slå ben under seg selv.

I fremstillingen om ekstraterritorialitet fremgår det at personverndirektivet har hatt påvirkningskraft utenfor EUs territorium på IT-området, ved at reglene fremstår som en global bransjestandard på noen områder. Det spørs om en slik effekt er det beste EU kan håpe på, også vedrørende forordningen, for å sikre at personvernet er ivaretatt utenfor EUs territorium. Dette vil likevel kunne være godt nok, så lenge de største aktørene innenfor IT-området velger å følge personvernforordningen, ettersom dette kan sette i gang en kjedereaksjon som gjør at mindre selskaper også velger å følge regelverket.

Det er ingen klar og åpenbar løsning på hvordan tilsynsorganene kan få inndrevet bøter som er utstedt til en virksomhet etablert i et tredjeland for brudd på personvernreglene.

Medlemslandene bør i størst mulig grad forsøke å inngå avtaler med tredjeland om inndrivelse av bøter, hvis denne delen av forordningen skal bli effektiv. På en side er det en fordel at dette er en delt kompetanse mellom medlemslandene og Kommisjonen, da det er flere som arbeider med å inngå avtaler om inndrivelse. På den andre siden så kan forskjellige

[119] Blume (2015) s. 245

samarbeidsavtaler skape problemer for harmoniseringen av personvernreglene i Europa. Dette fordi muligheten til inndrivelse av bøter i tredjeland vil være avhengig av hvilket lands tilsynsorgan som utsteder boten til virksomheten. Samarbeidet mellom tilsynsorganene kan redusere sannsynligheten for at dette blir et problem i praksis.

Det pålagte samarbeidet mellom tilsynsorganene kan være nøkkelen til å lykkes med en effektiv inndrivelse av bøter. Hvis det pålagte samarbeidet mellom tilsynsorganene ikke fungerer som tiltenkt, kan det bli vanskelig å oppnå målsetningen om at håndhevingen skal være et ”one-stop shop”. Som redegjort for over kan et ”one-stop shop” være avgjørende for om virksomheter i tredjeland er villige til å betale bøter, fordi det er sentralt at håndhevingen av regelverket ikke må fremstå som vilkårlig for å kunne inndrive bøtene.

Hva gjelder andre virkemidler, bør tilsynsorganene vurdere om stopp av overføring av personopplysninger til tredjeland bør anvendes istedenfor, eller i tillegg til, ileggelse av bøter. Det kan argumenteres for at begge sanksjonene bør ilegges ved alvorlige personvernbrudd. Dette fordi det viser både virksomheten og brukere at tilsynsorganet anser bruddet som så alvorlig at en enkelt sanksjon ikke er tilstrekkelig for å rette opp i personvernbruddet. Problemet med å kun ilegge bøter for virksomheter i tredjeland når det mangler en effektiv måte å inndrive bøtene på, er at bøtene kan miste sin pønale karakter, hvilket er uheldig.

Det er nok flere som vil argumentere for at det bare er de selskapene som ivaretar personvernet på en tilstrekkelig måte som vil overleve i det lange løp. Dette vil kunne begrunnes med at brukere vil velge å bruke de selskapene som ivaretar personvernet fremfor de som bryter personvernet. Dette forutsetter imidlertid at brukere har god kjennskap til personvernreglene, og en økt bevissthet rundt konsekvensene av personvernbrudd. Her vil tilsynsorganene spille en sentral rolle.

Litteraturliste

Artikler og bøker

van Alsenoy og Koekkoek (2015) van Alsenoy, Brendan og Koekkoek, Marieke ”Internet and jurisdiction after Google Spain: the extraterritorial reach of the ‘right to be delisted’“ *International Data Privacy Law*, 2015, Vol. 5, No. 2 105-120

Blume (2015) Blume, Peter “Persondatabeskyttelse i stormfyldt hav”, *Tidsskrift for Rettsvitenskap,* 2015, vol. 128 s. 226-246

Bing (2014) Bing, Jon ”Overføring av personopplysninger til utlandet – noen grunnleggende problemstillinger” *Lov og Rett* 2014 vol. 53 (3) s. 127-146

Bourgous (1998) Bourgous, Jacques ”External Realtions Powers of the European Community” *Fordham International Law Journal* 1998, vol. 22 (6) 156-159

Bradford (2012) Bradford, Anu ”The Brussels-effect” *Northwestern University Law Review* 2012 vol. 107 (1) s. 1-68

Colonna (2015) Colonna, Liane “Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?” *International Data Privacy Law* 2014 Volume 4 (3) s. 203–221

Datatilsynet (2015) “Det store datakappløpet” tilgjengelig fra https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/kommersialisering-norsk-endelig.pdf

Esteve (2015) Esteve, Asunción “The business of personal data: Google, Facebook, and privacy issues in the EU and the USA” *Internatinal Data Privacy Law* 2017, Vol. 7 (1) s. 36-47

Gömann (2017) Gömann, Merlin ”The New territorial scope of EU data protection law: deconstructing a revolutionary achievement” *Common Market Law Review* 2017, vol. 54 s. 567-590

Harrison (2005) Harrison, James. “Incentives for Development: The EC’s Generalized System of Preferences, India’s WTO Challenges and Reform” *Common Market Law Review*, 2005 vol. 42 (6) s. 1663-1689

Haukeland og Mathisen (2014)	Fredriksen, Halvard Haukeland og Mathisen, Gjermund, *EØS-rett*, 2. Utgave, Bergen, 2014 s. 228
De Hert og Czerniawski (2016)	de Hert, Paul og Czerniawski, Michal ”Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context”, *International Data Privacy Law*, 2016, Vol 6(3) s. 230-242
Jones (2014)	Jones, Jospeh “Control-alter-delete: The right to be forgotten” *European Intellectual Property Review* 2014 vol. 36(9) s. 595-60
Kopf (2014)	Kropf, John W. “Google Spain SL v. Agencia Española de Protección de Datos. Case –C-131/12” *The American Journal of International Law*, 2014 Vol. 108 (3) s. 502-509
Kuner (2015a)	Kuner, Christopher ”Extraterritoriality and regulation of international data transfer in EU data protection law, *International Data Privacy Law* 2015 vol. 5(4) s. 235-245
Kuner (2015b)	Kuner, Christopher “The European Union and the search for an international data protection framework”, *Groningen Journal of International Law*, 2015 s. 55-71
Kuner et.al (2013)	Kuner, Christopher, Cate, Fred H., Millard, Christopher og Svantesson, Dan Jerker B. “The extraterritoriality of data privacy laws—an explosive issue yet to detonate” *International Data Privacy Law* 2013, vol. 3 (3) s. 147-148
Padova (2016)	Padova, Yann ”The Safe harbour is invalid: what tools remain for data tranfers and what comes next?”, *International Data Privacy Law*, 2016, vol. 6(2) s. 139-161
Scott (2014)	Scott, Joanne, “The new EU “extraterritoriality”” *Common Market Law Review* 2014 Vol. 51 s. 1343-1380
Spiecker (2015)	Spiecker, Indra, ”A new framework for information markets: Google Spain”, *Common Market law Review*, 2015 Vol 52, s. 1033-1058
Svantesson (2015)	Svantesson, Dan Jerker B. ”Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation” *International Data Privacy Law*, 2015 Vol 5. (4), s. 226–234

Internettkilder og linker

http://ec.europa.eu/eurostat/statistics-explained/index.php/Internet_access_and_use_statistics_-_households_and_individuals besøkt 04.12.2017
https://www.ssb.no/ikthus besøkt 04.12.2017
https://www.alexa.com/siteinfo/reddit.com besøkt 20.10.2017
https://www.statista.com/statistics/325144/reddit-global-active-user-distribution/ besøkt 04.12.2017
https://www.reddit.com/help/privacypolicy/#section_information_we_collect_automatically besøkt 04.12.2017
https://www.regjeringen.no/contentassets/c907cd2776264a6486b8dd3ee00a4e3d/uoffisiell-norsk-oversettelse-av-personvernforordningen.pdf
https://support.google.com/customsearch/answer/4513925?hl=en besøkt 07.12.2017
https://www.datatilsynet.no/om-personvern/personopplysninger/, besøkt 16.10.17
http://www.advance.net besøkt 20.10.2017[1]
https://web.archive.org/web/20160410193437/http://www.redditblog.com/2009/11/moving-to-cloud.html besøkt 10.09.2017
https://aws.amazon.com/?nc2=h_lg besøkt 10.09.2017
https://www.computerhope.com/jargon/n/node.htm besøkt 30.10.2017
https://arstechnica.com/tech-policy/2017/09/feds-google-stops-challenging-most-us-warrants-for-data-on-overseas-servers/ besøkt 15.09.2017
https://reddit.com/r/norge besøkt 06.12.2017
https://www.nkom.no/teknisk/internett/cookies/informasjonskapsler-cookies besøkt 02.09.2017
ads.reddit.com besøkt 03.09.2017
https://www.eugdpr.org/eugdpr.org.html besøkt 15.11.2017
https://www.icpen.org/initiatives besøkt 19.10.2017,
https://www.icpen.org/who-we-are besøkt 19.10.2017
https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm besøkt 25.08.2017
https://www.wto.org/english/tratop_e/adp_e/adp_info_e.htm besøkt 25.08.2017
http://ec.europa.eu/consumers/consumer_rights/unfair-trade/docs/cpc-revision-proposal_en.pdf besøkt 24.10.2017
https://www.tek.no/artikler/guide-har-du-fatt-opp-denne-meldingen/276676 besøkt 05.09.2017
https://www.tek.no/artikler/piratpartiet-har-satt-opp-apen-dns-server/192514 besøkt 05.09.2017
https://www.gpo.gov/fdsys/pkg/CHRG-107hhrg71497/html/CHRG-107hhrg71497.htm Transkripsjon, besøkt 20.10.17
https://www.irs.gov/individuals/international-taxpayers/us-citizens-and-resident-aliens-abroad besøkt 27.10.2017
https://www.theguardian.com/technology/2017/jul/20/ecj-ruling-google-right-to-be-forgotten-beyond-eu-france-data-removed besøkt 01.12.2017

Kommisjonsuttalelser

COM(2012)09 final 25.01.2012 tilgjengelig fra: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0009&from=HR

Domsregister

EU-domstolen

C-101/01 *Bodil Lundqvist*

C- 366/10 *Air Transport Association of America & Others v. Secretary of State for Energy and Climate Change*

C-131/12 *Google Spain Sl., Google Inc v Agencia Española Protectión de Datos, Mario Soteja Gonzáles.*

C-230/14 *Weltimmo v Nemzeti*

C-362/14 *Maximillian Schrems v Data Protection Commissioner*

C-191/15 *Verein für Konsementeninformation v Amazon*

Joined Cases C-404/15 and C-659/15 PPU *Pál Aranyosi and Robert Căldăraru v Generalstaatsanwaltschaft Bremen*

Norske domstoler

TOSLO-2015-67093 *Warner Bros. Entertainment Norge AS mfl. og partshjelpere Norsk Videogramforening mfl. mot Telenor Norge AS*

Amerikanske domstoler

Case No.1 16-mj-00757 (BAH) *In the matter search of information associated with [redacted]@gmail.com that is stored at premises controlled by Google, inc.* Chief Judge Beryl A. Howell

Canadiske domstoler

Google Inc. v. Equustek Solutions Inc., 2017 SCC 34

Lovregister

EU lov:
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Personvernforordningen)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Personverndirektivet

C 326/47 Consolidated Version of Treaty of the Functioning of the European Union

C 326/13 Consolidated Version of Treaty of the European Union

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-handelsdirektivet)

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Direktiv om nettnøytralitet)

Directive 2003/87/EC of the European Parliament and of the Council of 13 October 2003 establishing a scheme for greenhouse gas emission allowance trading within the Community and amending Council Directive 96/61/EC (Klimakvotedirektivet)

Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Consumer Protection Cooperation-forordningen)

Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (2006/123/EF Tjenestedirektivet)

Lovforslag, ny Consumer Proteciton Cooperation Regulation, tilgjengelig fra http://ec.europa.eu/consumers/consumer_rights/unfair-trade/docs/cpc-revision-proposal_en.pdf

Norsk lov:
Lov 27. November 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde.
Lov 20. Mai 2005 nr. 28 om straff
Lov 14. April 2000 nr. 31 om behandling av personopplysninger

Forarbeider:
Prop 62 L (2015-2016) Endringer i forvaltningsloven mv. (administrative sanksjoner mv.)

Øvrige norske kilder:
Uoffisiell oversettelse av personvernforordningen:
https://www.regjeringen.no/contentassets/c907cd2776264a6486b8dd3ee00a4e3d/uoffisiell-norsk-oversettelse-av-personvernforordningen.pdf
Justis og Beredskapsdepartementet, Høringsnotat om "Ny personopplysningslov – gjennomføring av personvernforordningen i norsk rett" 6. juli 2017 Snr. 17/4200, tilgjengelig fra
https://www.regjeringen.no/contentassets/c907cd2776264a6486b8dd3ee00a4e3d/horingsnotat--ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett.pdf

Traktater
The General Agreement on Tariffs and Trade (GATT) 1994