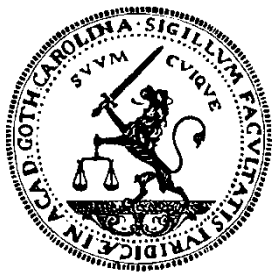


JURIDISKA FAKULTETEN
vid Lunds universitet

Jeanette Jönsson

När molnen hopar sig vid horisonten

En analys avseende EU:s regler om överföring av personuppgifter till tredjeländer och deras förenlighet med rätten till personlig integritet

JURM02 Examensarbete

Examensarbete på juristprogrammet
30 högskolepoäng

Handledare: Peter Gottschalk

Termin för examen: HT2014

”*You have zero privacy anyway. Get over it.”*

Scott McNealy, 1999

Innehåll

Summary

Today, people all around the world, consciously or unconsciously, use services provided by cloud computing where large amounts of personal data is placed and stored. Personal data is one of the most valuable assets a company can hold, and therefore companies utilise such data for commercial purposes. At the same time, the surveillance powers and the collection of personal data have increased among enforcement and security agencies controlled by governments. Certain countries, for example the U.S., have laws authorising enforcement and security agencies to access personal data of U.S. citizens and non-U.S. citizens in order to ensure, *inter alia*, national security. The development of information and communication technology in the last three decades has resulted in a paradigm shift regarding the processing of personal data and today, vast amounts of personal data is being transferred and exchanged between companies and governments across the globe every second.

This thesis examines the current and the proposed future EU data protection rules regarding transfer of personal data from the EU to third countries in relation to EU citizens´ right to privacy. Due to the significance of the current development in cloud computing and its effect on the international exchange of personal data, the EU data protection framework are examined in a cloud context. The existing EU Data Protection Directive regulates the processing of personal data wholly or partially by automatic means. The Data Protection Directive shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy. It shall also ensure the free flow of personal data within the Union. As a general rule, the Directive prohibits the transfer of personal data to third countries unless that country ensures an adequate level of protection. A transfer of personal data from the Union to a third country, which cannot provide an adequate level of protection, may take place where one of the derogations from the adequacy principle applies. This means that such a transfer may be lawful if the data subject has consented to the transfer or if the transfer is made on terms ensuring adequate safeguards. Such terms may be provided by BCRs, standard contractual clauses or Safe Harbor principles.

The majority of the personal data uploaded to the cloud, when using for example social media, is considered to be information that is included in the meaning of private life. Article 8 of the ECHR and Article 7 and 8 of the EU Charter of Fundamental Rights protect such personal data against unlawful interference. It is argued that the ECHR and the EU Charter of Fundamental Rights imply a negative obligation on the EU not to adopt laws that facilitate the transfer of EU citizens´ personal data to third countries where they are put at risk from actions taken by that third country that would

constitute an unlawful interference, that would violate the above-mentioned human rights.

Further, this thesis analyses whether the purposed rules regarding transfer of personal data to third countries in the draft of the EU General Data Protection Regulation are likely to increase the protection of EU citizens' right to privacy. The Data Protection Directive´s derogations, which permit transfer of personal data to a third country where an adequate level of protection is not provided, are retained in the proposal for a General Data Protection Regulation. Although the rules can be considered to have been developed to facilitate its interpretation and application, it is argued in the thesis that the rules expand the ability of cloud customers and cloud providers to transfer personal data to a third country which does not provide an adequate level of protection. Such expanded opportunities to transfer personal data outside the EU are questionable from a human right perspective.

The borderless character of cloud computing leads to problems regarding which country´s law applies on the processing of personal data in the cloud. The human right to privacy is valued and regulated differently around the world, where Europe can be regarded as the part of the world where the right to privacy is protected the most. Therefore, a transfer of personal data from the EU to a third country may pose a risk of weakened protection for EU citizens. Such risk arises due to a gap in the laws of human right protection that must be addressed either at a national, regional or international level. This thesis explores opportunities of the EU to influence a solution to this global problem. In conclusion, three alternatives are demonstrated to be possible solutions of the aforementioned problem; (1) a unilateral solution which expands the territorial scope of the EU data protection regulation, resulting in an extraterritorial application of the regulation, (2) a bilateral or multilateral solution, meaning the development of an international data protection agreement, or (3) a multilateral solution, meaning the EU acting as a leader and EU norm diffusion. Solving the aforementioned problem in an effective way might require a combination of these three options.

Sammanfattning

Nu för tiden använder människor världen över, medvetet eller omedvetet, molntjänster, där stora mängder personlig information placeras och lagras. Personuppgifter är en av de mest värdefulla tillgångar ett företag kan inneha, och således utnyttjar företag runt om i världen sådan personlig information för kommersiella syften. Samtidigt har statliga myndigheters övervakning av personer och insamling av personlig information ökat. Det finns länder som exempelvis USA, vilka har lagar som ger olika myndigheter befogenheter att övervaka både inhemska och utländska medborgare för att bl.a. upprätthålla nationell säkerhet. Utvecklingen av informations- och kommunikationsteknologi under de senaste tre decennierna har inneburit ett paradigmskifte vad gäller hantering av personuppgifter och numera överförs stora mängder personuppgifter varje sekund mellan företag och myndigheter världen över.

I denna uppsats studeras EU-rättens nuvarande och, eventuellt, framtida regler avseende överföring av personuppgifter till tredjeländer i förhållande till EU-medborgares rätt till personlig integritet. Reglerna analyseras ur ett molntjänstsammanhang, eftersom utvecklingen av molntjänster har bidragit till ett ökat internationellt utbyte av personuppgifter. EU:s nuvarande dataskyddsdirektiv reglerar automatisk behandling av personuppgifter och har till syfte att skydda fysiska personers rätt till personlig integritet, men även att säkerställa det fria flödet av personuppgifter inom unionen. I dataskyddsdirektivet anges att det som huvudregel är förbjudet att överföra personuppgifter till tredjeland. Det är däremot tillåtet att överföra uppgifter till tredjeland om en adekvat skyddsnivå kan garanteras i detta tredjeland. Från detta krav på adekvat skyddsnivå, föreskrivs det undantag vilka möjliggör en överföring till ett tredjeland som inte kan säkerställa en adekvat skyddsnivå. Ett sådant undantag föreligger om det istället finns ett samtycke från den registrerade, eller om registerföraren tillämpar BCR:s, modellklausuler eller principerna som är fastställda i *Safe Harbor*-ramverket.

Merparten av den typ av personlig information som laddas upp i molnet, vid användning av exempelvis sociala medier, utgör uppgifter om privatlivet och är skyddade mot otillåtna ingrepp enligt Europakonventionen artikel 8 och EU-stadgan artikel 7 och 8. I uppsatsen argumenteras för att den i Europakonventionen och EU-stadgan föreskrivna rätten till personlig integritet innebär en negativ skyldighet för EU att inte föreskriva regler vilka tillåter en överföring av personuppgifter till tredjeländer där de riskerar att behandlas på ett sätt som innebär en otillåten inskränkning i de ovan nämnda mänskliga rättigheterna.

I uppsatsen undersöks det även om de föreslagna reglerna om överföring av personuppgifter till tredjeländer i förslaget till allmän dataskyddsförordning medför ett förstärkt skydd av EU-medborgarnas rätt till personlig integritet. De undantag som återfinns i dataskyddsdirektivet behålls även i förslaget till allmän dataskyddsförordning. Även om reglerna har utvecklats och specificerats för att underlätta både tolkning och tillämpning, argumenteras det i denna uppsats för att reglerna innebär en ökad möjlighet för bl.a. EU-baserade molntjänstkunder och molntjänstleverantörer att överföra person-uppgifter till ett tredjeland som inte kan säkerställa en adekvat skyddsnivå. En sådan ökad möjlighet till överföring kan ifrågasättas ur ett människorättsperspektiv.

Hantering av personuppgifter i molnet problematiseras av dess gränslösa karaktär. Rätten till personlig integritet värderas och regleras olika runt om i världen, där Europa kan anses utgöra den världsdel där rättigheten skyddas allra högst. Vid en överföring av personuppgifter från EU till ett tredjeland kan det således uppkomma en risk för ett försvagat integritetsskydd för den EU-medborgare vars uppgifter överförs till ett tredjeland. Det uppstår därför en lucka i skyddet som måste lösas på nationell, regional eller internationell nivå. I denna uppsats undersöks vilka möjligheter EU har att påverka lösningen av denna gränsöverskridande problematik. Sammanfattningsvis påvisas det att EU har tre alternativa möjligheter, vilka är följande; (1) en unilateral lösning genom att utvidga EU:s dataskyddslagstiftning till att ha en extraterritoriell effekt, (2) en bilateral eller multilateral lösning genom att förhandla fram avtal med andra länder eller arbeta fram ett internationellt avtal, eller (3) en multilateral lösning genom EU-ledarskap och normspridning. Eventuellt krävs det en kombination av de tre nämnda alternativen för att åstadkomma en effektiv lösning på detta globala problem.

Förord

Lund, du fick mig på fall från första stund. Mina fem år som student har gjort mig många erfarenheter rikare och tiden har på många sätt varit helt fantastisk. Jag ska dock inte sticka under stol med att dessa fem år på juristprogrammet stundtals varit krävande. Jag har många nära och kära att tacka för att jag nu lyckats segla skutan i hamn.

Tack, mina älskade vänner. Tack för vilda fester, pampiga baler, nödvändiga kaffepauser och härliga skratt. Tack för att ni förgyllt min tid i Lund och delat oförglömliga minnen.

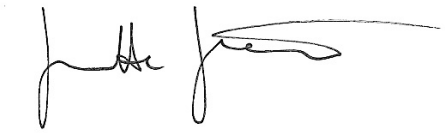
Tack, till mina fina kollegor på Kontoret. Tack för alla skratt, spännande pingismatcher, djupa diskussioner och fantastiskt pluggsällskap. Särskilt tack för all uppmuntran under höstens långa dagar. Ni har satt guldkant på en ibland ganska grå vardag.

Det största tacket av alla riktar jag till min fantastiska familj. Ni är min stora trygghet. Till min älskade mamma och pappa, jag kan inte med ord beskriva min enorma kärlek och tacksamhet till er. Er ständiga uppmuntran har under dessa fem år varit ovärderlig. Tack för att ni stöttar mig i allt jag tar mig för i livet och för att ni tror på mig, i vått och torrt, när jag själv tvivlar.

Tack kära pappa, för all din tid du spenderat med att korrekturläsa inte bara denna uppsats, utan allt jag skrivit under mina år på juristprogrammet.

Avslutningsvis vill jag rikta ett stort tack till min handledare, Peter Gottschalk. Tack för ditt stora intresse och engagemang för mitt uppsatsämne, samt för värdefulla kommentarer och givande diskussioner under arbetets gång.

Lund, januari 2015



Förkortningar

Artikel 29-gruppen	Article 29 Data Protection Working Party
ATAA	U.S. Air Transport Association
BCR	Binding Corporate Rules
Dataskyddsdirektivet	Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av person-uppgifter och det fria flödet av sådana uppgifter
Ds	Departementsserien
ECHR	The Convention for the Protection of Human Rights and Fundamental Freedoms
EU	Europeiska unionen
EU-domstolen	Europeiska unionens domstol
EU-kommissionen, kommissionen	Europeiska kommissionen
Europadomstolen	Europeiska domstolen för de mänskliga rättigheterna
Europakonventionen, konventionen	Europeiska konventionen av den 4 november 1950 om skydd för de mänskliga rättigheterna
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
FEU	Fördraget om europeiska unionen
FEUF	Fördraget om europeiska unionens funktionssätt
FISA	Foreign Intelligence Surveillance Act
FTC	U.S. Federal Trade Commission
LIBE-utskottet	Utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor
Lissabonfördraget	Lissabonfördraget om ändring av fördraget om Europeiska unionen och fördraget om upprättandet av Europeiska gemenskapen, undertecknat i Lissabon den 13 december 2007
NIST	National Institute of Standards and Technology
NSA	National Security Agency
Rådet	Europeiska rådet
SOU	Statens offentliga utredningar

1 Inledning

1.1 Bakgrund

Människor lämnar dagligen digitala fotspår efter sig. Användandet av informations- och kommunikationsteknologi i den digitala tidsåldern, framförallt i form av molntjänster, har resulterat i ett paradigmskifte vad gäller hantering av personlig information. Användandet av sociala nätverk, e-mail och sökmotorer innebär att vi dagligen placerar stora mängder personlig information, som rör exempelvis enskilda personers aktiviteter, åsikter och vanor, i det s.k. molnet där de behandlas och lagras av dem som tillhandahåller dessa onlinetjänster. Molntjänster är till sin karaktär globala och följaktligen överförs personuppgifter mellan företag, organisationer och myndigheter över hela världen. Detta ger upphov till komplexa gränsöverskridande situationer vilket aktualiserar flera jurisdiktioner.

Företag runt om i världen är idag angelägna om att utnyttja insamlad information för kommersiella syften. För stora IT-företag som exempelvis Google, Facebook och Apple, är insamlandet av användares personuppgifter en stor del av deras affärsidé. Idag är personuppgifter en av de mest värdefulla tillgångar ett företag kan inneha. Anonymitet är inte längre lönsamt. Samtidigt har insamlandet av personlig information ökat markant hos statliga myndigheter, vilka genom övervakning av sitt lands befolkning har för avsikt att bl.a. garantera nationell säkerhet.[1] Enskildas identiteter har således blivit en handelsvara i dagens samhälle, där enskilda genom att dela med sig av sina personuppgifter på nätet kan byta till sig sociala relationer eller en känsla av trygghet. Att dela med sig av sina personuppgifter på detta sätt innebär dock en stor risk för att företag och myndigheter behandlar personuppgifterna på ett sätt som kan kränka den enskilde individens personliga integritet. Detta är en risk som blir särskilt påtaglig när personuppgifter överförs från EU till tredjeländer, vilka eventuellt inte har regler som skyddar EU-medborgarnas personliga integritet. Användandet av molntjänster har lett till en inte tidigare skådad behandling av EU-medborgares personuppgifter utanför EU.

Att EU-medborgare utsätts för övervakning av tredjeländers underrättelse-tjänster fick sin bekräftelse i juni 2013, när visselblåsaren Edward Snowden avslöjade att den amerikanska underrättelsetjänsten NSA, genom ett datorprogram vid namn PRISM, hade direkt tillgång till lagrade

[1] Inspiration hämtad från: Brandel, Svenska Dagbladet: *Vem ska äga makten över dig på nätet?* och Rauhofer (2008), s. 185 f.
[2] Se Kopstein & Sottek (2013) och Greenwald, *The Guardian*, 6 juni 2013.
[3] Koops (2012), s. 354 och 365 f.
[4] Jfr Reichel (2013), s. 109 f och Hettne & Otken Eriksson (2011), s. 39 ff.
[5] Jareborg (2004), s. 4 f.
[6] Agell (2002), s. 246 och Jareborg (2004), s. 4 och Sandgren (2005), s. 655 f.

personuppgifter hos bl.a. de amerikanska företagen Facebook, Amazon och Apple.[2] Dessa IT-företag lagrar och behandlar EU-medborgares personliga information i form av exempelvis privata textmeddelanden, bilder, kontaktuppgifter och sociala relationer.

Denna form av behandling av EU-medborgares personuppgifter utanför EU leder självklart till en viss oro gällande skyddet av EU-medborgarnas personliga integritet. Rätten till personlig integritet skyddas i Europa som en mänsklig rättighet genom både Europakonventionen och EU-stadgan. Rättigheten ska genomsyra all lagstiftning och för närvarande utgör EU:s dataskyddsdirektiv det yttersta ramverket för EU:s medlemsstaters nationella dataskyddslagstiftning. Dataskyddsdirektivet syftar dels till att skydda fysiska personers grundläggande fri- och rättigheter, särskilt rätten till privatliv, vid behandling av personuppgifter, dels till att säkerställa det fria flödet av sådana uppgifter mellan medlemsstaterna. Direktivet innehåller även regler för att garantera EU-medborgares skydd av personuppgifter när dessa överförs till tredjeländer. Det har dock ansetts att dataskyddsdirektivet passerat sitt bäst-före-datum, varför ett förslag till ny dataskyddsförordning har presenterats av EU-kommissionen. Frågan är om de nuvarande reglerna samt det nya förslagets regler om överföring av personuppgifter till tredjeländer, innebär ett tillräcklig skydd för EU-medborgarnas rätt till respekt för privatlivet och skydd av personuppgifter.

Det kan konstateras att den situation vi för närvarande befinner oss i, när personuppgifter behandlas i molnet, berör personlig integritet i ett gränsöverskridande sammanhang. Således uppstår en problematik gällande hur överföringar av personuppgifter till tredjeländer bör regleras. Teknologin utvecklas i allt snabbare takt och vi blir mer beroende av att ständigt vara uppkopplade mot Internet. Vi lockas att dela med oss av vårt privatliv och riskerar därför att förlora kontrollen av det vi väljer att dela med oss av. Det är ett politiskt känsligt och kontroversiellt ämne som diskuteras flitigt i media. Det är därmed av stort intresse att undersöka EU-rättens regler om överföring av personuppgifter till tredjeländer i förhållande till rätten till respekt för privatlivet och skydd av personuppgifter.

1.2 Syfte och frågeställning

Utifrån den ovan presenterade bakgrunden kan konstateras att nya gränsöverskridande rättsliga problem uppkommer i takt med en ökad globalisering och teknisk utveckling. Syftet med denna framställning är att i ett molntjänstsammanhang undersöka EU-rättens nuvarande samt, förväntade, framtida regler avseende överföring av personuppgifter till tredjeländer i förhållande till EU-medborgares rätt till personlig integritet. Således är avsikten att analysera vilket ansvar EU har för att skydda EU-medborgarnas fundamentala rättigheter. Vidare är avsikten med uppsatsen att undersöka potentiella möjligheter för EU att påverka skyddet av EU-medborgares rätt till personlig integritet i tredjeländer.

[2] Se Kopstein & Sottek (2013) och Greenwald, *The Guardian*, 6 juni 2013.

Inom ramen för det ovan presenterade syftet, avses följande huvudfrågeställningar behandlas:

- Kan reglerna om överföring av personuppgifter till tredjeländer i EU:s dataskyddsdirektiv, beaktat ur ett molntjänstsammanhang, anses vara förenliga med EU-medborgarnas rätt till respekt för privatlivet och skydd av personuppgifter, såsom de skyddas i Europakonventionen artikel 8 och EU-stadgan artikel 7 och 8?
- Kommer de nya reglerna om överföring av personuppgifter till tredjeländer, såsom de föreslagits i kommissionens förslag till allmän dataskyddsförordning, att innebära ett ökat eller minskat skydd för EU-medborgarnas personliga integritet?
- Vilka möjligheter har EU att åstadkomma ett likvärdigt skydd för EU-medborgares rätt till personlig integritet utanför EU:s territorium?

För att besvara de tre huvudfrågeställningarna kommer även följande delfrågor att utredas:

- Vad är molntjänster och vilka risker finns det med ett användande av molntjänster?
- Under vilka omständigheter får personuppgifter överföras till tredjeländer enligt dataskyddsdirektivet?
- Vilka förändringar kommer förslaget till allmän dataskydds-förordning att medföra vad gäller regler om överföring av personuppgifter till tredjeländer?
- Vilket skydd uppställer Europakonventionen artikel 8 och EU-stadgan artikel 7 och 8 gällande behandling av personuppgifter?
- Vilken extraterritoriell effekt har rättigheterna i Europakonventionen och EU-stadgan?

1.3 Metod och material

Denna uppsats berör juridik i ett tekniskt sammanhang och de frågeställningar jag avser att besvara i uppsatsen är delvis utformade på ett sätt lämpade för en juridisk utredning. Jag har dock även valt att formulera icke-traditionella frågor, vilket kommer att innebära en viss utmaning vad gäller tillämpning av metod och material. En klassisk rättsdogmatisk metod adresserar ofta juridiska problem på ett endimensionellt sätt. Enligt detta synsätt tas lagen för given, för att sedan tillämpas på en samhällsfråga eller på en social utveckling. En sådan metod tar följaktligen inte i beaktande att samhället idag formas av den tekniska utvecklingen. Detta kräver en mer vidsträckt metod, där juridiska, sociala och tekniska insikter tillämpas för att åstadkomma lösningar på juridiska problem vilka inte bara ser bra ut i teorin, utan även fungerar i praktiken.[3] Avsikten är att i denna uppsats, genom tillämpning av olika metoder och med beaktade av flera relevanta dimensioner, försöka skapa en helhetsbild kring den komplexa problematiken som uppstår avseende rätten till personlig integritet vid ett användande av molntjänster.

[3] Koops (2012), s. 354 och 365 f.

En dimension som ska beaktas i uppsatsen är den tekniska. Avsikten med uppsatsen är att belysa det juridiska problemet gällande behandling av personuppgifter ur ett molntjänstsammanhang. Det är därmed av vikt att inledningsvis i denna uppsats presentera molntjänster ur en teknisk kontext, samt att även försöka placera och klargöra molntjänsters roll i det digitaliserade samhället. En sådan redogörelse avser att ge läsaren en insikt i den problematik som uppkommer vid tillämpandet av ny teknologi. Avsikten är således att redogöra för den tekniska infrastrukturen, på vilken sedan lagstiftningen ska appliceras.

Vid redogörelsen för de EU-rättsliga regelverken inom området för dataskydd kommer en traditionell EU-rättslig metod att tillämpas. Således kommer primärrätt, sekundärrätt i form av bindande och icke-bindande rättsakter, EU-domstolens rättspraxis, samt förarbeten att studeras och analyseras.[4] Den EU-rättsliga metoden utgör vidare en variant på en klassisk rättsdogmatisk metod, där syftet är att beskriva, systematisera och tolka innehållet i gällande rätt.[5] Att strikt hålla sig till denna metod kan dock medföra en risk för att framställningen blir alltför deskriptiv. Avsikten är därmed att i denna uppsats tillämpa en rättsanalytisk metod. En sådan metod har utvecklats inom doktrinen då det anses att rättsvetenskapen även ska verka för att kritiskt granska lagstiftning och rättstillämpning, samt föreslå förbättringar.[6]

I denna uppsats kommer amerikansk rätt att presenteras i exemplifierande syfte. Avsikten är att lyfta fram amerikansk reglering inom området för att underbygga argumentation, vilken kommer att föras i uppsatsens analys. Tanken är att utifrån ett begränsat underlag redogöra för den amerikanska rätten. Denna metod kan därmed beskrivas som en utländsk utblick, vars syfte är att fungera som en form av ”argumentationsbank”.[7]

I denna framställning kommer problemformuleringar, vilka kan definieras som tvärvetenskapliga, att behandlas. I dessa delar av uppsatsen argumenterar jag för EU som en global och folkrättslig aktör, och avser därmed att studera EU:s externa relationer gentemot omvärlden. Inom den klassiska EU-rättsliga metoden argumenteras det för att rättsordningen kan behandlas utifrån två olika nivåer, dels den gemensamma europeiska nivån, dels den nationella nivån. När EU-rätten däremot ska behandlas i ett externt sammanhang uppkommer det ett behov av att tillämpa en utvidgad EU-rättslig metod. Det är därför lämpligt att i detta fall argumentera för en tredje nivå, vilken behandlar EU:s påverkan och ageranden som en del i ett globalt sammanhang. Detta innebär att EU:s regelverks extraterritoriella effekt i tredjeländer kommer att studeras och analyseras.

I det ovanstående stycket nämnda del av uppsatsen kommer dessutom en form av tvärvetenskapligt angreppssätt tillämpas. EU:s externa relationer kommer i denna del att studeras utifrån statsvetenskapliga teorier om *multi-level governance*.[8] En användning av tvärvetenskaplig forskning görs i syfte

[4] Jfr Reichel (2013), s. 109 f och Hettne & Otken Eriksson (2011), s. 39 ff.
[5] Jareborg (2004), s. 4 f.
[6] Agell (2002), s. 246 och Jareborg (2004), s. 4 och Sandgren (2005), s. 655 f.
[7] Sandgren (2007), s. 75.
[8] Jfr Eckes (2013), s. 187 f.

att kunna redogöra för förslag på hur gällande rättsregler kan utvecklas och förändras samt hur det bör ske.[9] I framställningen lyfts två författare och teoribildare fram, Ian Manners och Anu Bradford. Manners är den person som presenterade konceptet om EU som en normativ makt och utgör således en viktig källa vid argumentationen kring EU:s möjligheter att sprida normer internationellt.[10] Bradford har utvecklat teorin om EU som en normativ makt och presenterar teorin om *Brysseleffekten*,[11] enligt vilken EU har lyckats höja standarden inom ett antal rättsområden globalt genom att verka som en internationell aktör.[12] I doktrin kan det återfinnas stöd för en sådan utvidgad juridisk metod p.g.a. den ökade globaliseringen i världen.[13]

Vad gäller val av material i de delar av uppsatsen som redogör för gällande rätt samt förslag till ny lagstiftning inom EU, tas utgångspunkt i lagstiftning, rättspraxis, förarbeten och kommenterande doktrin. I EU-rättsliga sammanhang är det av intresse att påpeka att primärrätten är bindande rättskällor, vilka beaktas vid tolkningen av sekundärrätten.[14] EU-domstolens rättspraxis är relevant för tolkningen och tillämpningen av sekundärrätten och utgör ett komplement till den skrivna rätten.[15] Även ett förtydligande av förarbeten är på sin plats i förhållande till EU-rätten. I uppsatsen tillämpas förarbeten till EU-rättslig lagstiftning bestående av Europaparlamentets och rådets ändringsförslag samt LIBE-utskottets publicerade yttranden. Förarbetenas betydelse vid EU-rättslig tolkning har ökat, men det ska understrykas att de inte tillmäts samma betydelse som förarbeten har inom den svenska rättskälleläran.[16]

Avsikten är vidare att underbygga uppsatsens deskriptiva avsnitt och analys med brett och nyanserat material. Rätten till personlig integritet vid överföring av personuppgifter till tredjeländer är ett ämne som inom svensk doktrin är relativt outvecklat, varför utländskt material till stor del kommer att användas. En stor inspirationskälla och språngbräda för denna framställning utgörs av en artikel publicerad 2013 av Judith Rauhofer och Casper Bowden.[17] I artikeln belyser författarna de EU-rättsliga dataskyddsreglerna om överföring av personuppgifter till tredjeländer ur ett mänskorättsperspektiv. I övrigt har urvalet av material baserats på de främsta författarna inom rättsområdet. Mer okonventionellt material kommer även till viss del använts, t.ex. i form av blogginlägg. Materialet är hämtat från bloggar drivna av, eller blogginlägg publicerade av, välkända författare inom respektive rättsområde. Det ska poängteras att ett kritiskt förhållningssätt tillämpas gentemot de olika källorna.

Vid framställningen av det EU-rättsliga dataskyddet har bl.a. Artikel 29-gruppens uttalanden används som källa. Artikel 29-gruppen är en oberoende

[9] Gräns (2013), s. 429 f.
[10] Se Manners (2002), s. 238 f.
[11] Svensk översättning av ”*the Brussels effect*”.
[12] Se Bradford (2012).
[13] Se van Gestel, Micklitz & Poiares Maduro (2012/13), s. 8. För vidare resonemang kring en förnyad syn på tillämpning av juridisk metod i en globaliserad värld hänvisas till resonemang förda i van Gestel, Micklitz & Poiares Maduro (2012/13).
[14] Jfr Hettne & Otken Eriksson (2011), s. 41 ff.
[15] Jfr Hettne & Otken Eriksson (2011), s. 49.
[16] Jfr Hettne & Otken Eriksson (2011), s. 114.
[17] Rauhofer & Bowden (2013).

rådgivande grupp från EU-kommissionen. Deras uppgift är att dels se till att dataskyddsdirektivet tillämpas på ett entydigt sätt, dels att lämna yttranden kring dess tolkning och tillämplighet.[18]

I den del av uppsatsen som kommer behandla rätten till respekt för privatlivet och skydd av personuppgifter såsom de garanteras i Europakonventionen och EU-stadgan, kommer material i form av praxis från Europadomstolen och EU-domstolen att presenteras. Syftet med att redogöra för praxis är att identifiera de principer och resonemang domstolarna tillämpar som grund för sina avgöranden. Utvald praxis anses vara grundläggande för tolkningen av rätten till respekt för privatlivet och skydd av personuppgifter. Det ska påpekas att viss försiktighet påkallas vid generaliseringen av de principer som framkommer *in casu* av avgörandena från Europadomstolen och EU-domstolen.[19] Vad gäller EU-domstolens praxis beaktas även generaladvokatens förslag till avgörande, då detta är vägledande för EU-domstolens avgörande.[20] Vidare tillämpas svensk och internationell doktrin för att tolka praxis.

I uppsatsen behandlas material publicerat t.o.m. november 2014.

1.4 Avgränsning

Skydd för den personliga integriteten vid överföring av personuppgifter till tredjeländer är ett komplext och gränsöverskridande problem som väcker frågor inom flera rättsområden. Det är således inledningsvis nödvändigt att tydliggöra de avgränsningar som görs mot andra relevanta rättsområden och rättsfrågor.

Ämnet avser att avhandlas utifrån ett molntjänstsammanhang och därmed kommer tekniska begrepp att presenteras inledningsvis. I uppsatsen kommer det dock inte ske någon grundlig redovisning för molntjänsterna och deras funktion och tillämpning. Endast det som är relevant för läsarens förståelse gällande tillämpningen och betydelsen av molntjänster i dagens informations- och kommunikationssamhälle kommer att presenteras.

Utgångspunkten är att redogöra för EU:s regler gällande överföring av personuppgifter till tredjeland. En avgränsning sker således gentemot nationell rätt och hur dataskyddsdirektivet implementerats i medlemsstaterna. Det ska även tydliggöras att uppsatsen avser att främst redogöra för de regler i dataskyddsdirektivet och förslaget till allmän dataskyddsförordning som berör överföring av personuppgifter till tredjeländer. Övriga materiella regler gällande skydd för och behandling av personuppgifter kommer endast att kort beröras. Överföring av personuppgifter internt inom EU kommer inte att beröras.

Frågan om överföring av personuppgifter till tredjeländer väcker även frågor om jurisdiktion, lagval samt internationellt erkännande och verkställighet. I uppsatsen kommer det inte att redogöras för regler inom den internationella

[18] Se EU-kommissionen, *Information om Artikel 29-gruppen*.
[19] *In casu*-avgörande innebär avgöranden vilka utgår från omständigheter i det enskilda fallet. Se Nowak (2003), s. 105.
[20] Jfr Hettne & Otken Eriksson (2011), s. 116 ff.

privat- och processrätten, utan endast konstateras att ytterligare problematik med hänsyn till detta rättsområde kan uppstå. Det ska påpekas att frågan om internationell verkställighet är särskilt intressant i förhållande till de rättsregler och internationella avtal som kommer redogöras för i uppsatsen, eftersom dessa avser att reglera gränsöverskridande rättsförhållanden. Även om dessa rättsfrågor är intressanta, faller det utanför uppsatsen huvudfokus.

Avgränsningar är även nödvändiga i förhållande till internationella regelverk gällande gränsöverskridande personuppgiftsöverföringar. I framställningen kommer de mänskliga rättigheterna, rätten till respekt för privatlivet, samt rätt till skydd av personuppgifter såsom de garanteras i Europakonventionen och EU-stadgan, att utgöra utgångspunkten vid redogörelsen för vilket skydd EU-medborgare besitter vid behandling av deras personuppgifter. Regelverk som ”OECD:s riktlinjer för integritets-skydd och gränsöverskridande flöden av personuppgifter” från 1980 och ”Europarådets konvention 108”[21], vilka även de behandlar skydd av personuppgifter vid gränsöverskridande överföringar, kommer inte att behandlas i denna uppsats. En sådan avgränsning motiveras av att OECD:s riktlinjer utgör en samling icke-bindande principer som medlemsstater kan välja att ansluta sig till. En anslutning till Europarådets konvention 108 kan i sin tur inte verkställas direkt i Europadomstolen, efterlevnaden av konventionen kan därmed inte prövas i domstol.[22] Vidare kommer en avgränsning ske mot FN:s konvention om medborgerliga och politiska rättigheter, där en enskild skyddas mot godtyckliga eller olagliga ingrepp i privatlivet enligt artikel 17. EU är inte ansluten till dessa regelverk och fokus kommer således placeras på de europarättsliga regleringarna gällande rätten till respekt för privatlivet och skydd av personuppgifter. EU är i sitt arbete bundna att efterleva och respektera EU-stadgans föreskrivna fri- och rättigheter. Vidare ska det noteras att EU inte är bunden av Europa-konventionen, men det pågår förhandlingar avseende en sådan anslutning och enligt FEU artikel 6(2) är avsikten att en sådan anslutning ska ske.

Ytterligare avgränsningar är nödvändiga i förhållande till redogörelsen för de aktuella rättigheterna i Europakonventionen och EU-stadgan. EU:s förhållande till Europakonventionen kommer endast att kort beröras för att uppmärksamma problematiken. Vidare ska det noteras att EU-stadgans artiklar 7 och 8 om respekt för privatlivet och skydd av personuppgifter är närbesläktade, men ändock separata grundläggande rättigheter. Skillnaden mellan dessa två rättigheter i EU-stadgan kommer endast att belysas i korthet.

Det kommer i uppsatsen att redogöras för Europakonventionens och EU-stadgans extraterritorialitet. Frågan om mänskliga rättigheter och extra-territorialitet är komplicerad och under utveckling inom både praxis och doktrin. En begränsning görs således i denna framställning innebärande att endast relevant praxis för den situation som uppstår när personuppgifter överförs från EU till tredjeländer, kommer att presenteras. Inom området för extraterritorialitet av mänskliga rättigheter återfinns ett flertal tillvägagångs-sätt vilka har utvecklats inom praxis och doktrin. I denna framställning är

[21] Europarådets konvention om skydd för personuppgifter vid automatisk databehandling av personuppgifter, 28 januari 1981, ETS 108 (1981).
[22] Jfr Kuner (2013), s. 37.

det inte möjligt att uttömmande redogöra för denna utveckling av utrymmesskäl.

Avslutningsvis ska avgränsningar gällande EU:s agerande som en global och folkrättslig aktör göras. I den aktuella delen av uppsatsen är syftet att redogöra för utvalda modeller och teorier gällande extraterritorialitet och normativ makt. Dessa modeller och teorier avser främst att utgöra argumentationsgrundande material. EU:s ageranden globalt är ett rättsområde där mycket fortfarande är oklart. Avsikten är att i denna uppsats endast presentera exemplifierande lösningar på det gränsöverskridande problemet gällande överföringar av personuppgifter och således är intentionen inte att göra en djupare analys av statsvetenskapliga teorier om EU:s roll som global aktör.

1.5 Forskningsläge

Frågan om skydd för personuppgifter vid överföring till tredjeländer är en specifik forskningsfråga och har framförallt belysts av författare som Judith Rauhofer och Christopher Kuner. Vid Queen Mary University i London pågår för närvarande ett forskningsprojekt vilket syftar till att hantera olika rättsliga aspekter i förhållande till utvecklingen av molntjänster.[23] Inom detta projekt finns det en inriktning för dataskyddsreglering i molnet, där framförallt författarna Christopher Millard och Kuan Hon har publicerat material där de bl.a. studerar dataskyddsdirektivet och förslaget till allmän dataskyddsförordning ur ett molntjänstsammanhang.

I Sverige bedrivs forskning vid Institutet för rättsinformatik vid Stockholm universitet om bl.a. dataskyddsregleringars territoriella räckvidd och extraterritoriella effekt. Författare som forskat och publicerat material inom detta område är Dan J. Svantesson och Lianne Colonna.

När det gäller forskning om mänskliga rättigheter och dess extraterritoriella verkan är Marko Milanovic en av de främsta forskarna. Han har bl.a. utvecklat modeller för exempelvis Europakonventionens tillämplighet i tredjeländer i förhållande till rätten till personlig integritet i den digitala tidsåldern.

1.6 Terminologi

Denna uppsats innehåller ett flertal centrala begrepp, vilka är av stor betydelse för läsarens förståelse av det i framställningen behandlade ämnet. Många av de i uppsatsen återkommande begreppen har varit föremål för diskussion i doktrin och deras innebörd är således omtvistad. Det är därför av vikt att inledningsvis kommentera terminologin.

Ett centralt begrepp för uppsatsen är ***personuppgift***. Begreppets innebörd har diskuterats flitigt i doktrin och dess definition har under de senaste åren, i takt med den digitala utvecklingen, förändrats och utvecklats. Med

[23] Cloud Legal Research Project. Detta forskningsprojekt finansieras huvudsakligen genom forskningsanslag från Microsoft, samt med stöd från EU-kommissionen. Forskningen är dock akademisk fristående från Microsoft och EU-kommissionen.

personuppgift avses i denna uppsats all slags information som avser och som kan hänföras till en identifierad eller identifierbar fysisk person (*den registrerade*). En identifierbar person är en person som kan identifieras, direkt eller indirekt, framför allt genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för personens fysiska, psykiska, ekonomiska, kulturella eller sociala identitet.[24] Exempel på uppgifter som klassificeras som personuppgift är IP-adresser, fotografier, angivande av arbetsförhållande, hälsotillstånd och fritidsintressen.[25] I denna uppsats kommer även personlig data och personlig information användas som synonymer till begreppet personuppgift.

Vidare avser ***den registrerade*** den fysiska person som direkt eller indirekt är identifierad eller identifierbar genom en personuppgift.

En ***registeransvarig*** är den fysiska eller juridiska person, den myndighet, den institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen, villkoren och medlen för behandling av personuppgifter.[26] Vid hänvisning till den registeransvarige i molntjänstsammanhang avses ofta en molntjänstkund, d.v.s. den som köper en molntjänst.

Registerförare är den fysiska eller juridiska person, den myndighet, den institution eller annat organ som behandlar personuppgifter för den registeransvariges räkning.[27] Vid hänvisning till en registerförare i molnsammanhang avses ofta molntjänstleverantören, d.v.s. den som tillhandahåller en molntjänst.

En ***underleverantör*** är den fysiska eller juridiska person, den myndighet, den institution eller annat organ som behandlar personuppgifter för registerförarens räkning.[28]

Med ***behandling av personuppgifter*** avses i denna uppsats varje åtgärd eller serie av åtgärder som vidtas beträffande personuppgifter, vare sig det sker på automatisk väg eller inte. Exempel på behandling är insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, blockering, radering eller förstöring.

Begreppet ***överföring*** är av vikt att definiera, då uppsatsen särskilt belyser den gränsöverskridande problematik som uppstår vid användandet av molntjänster. Hur begreppet ska definieras är dock oklart och många regelverk innehåller olika definitioner. I denna uppsats kommer begreppet tilldelas en förhållandevis enkel definition. Med överföring avses således i denna uppsats en förflyttning av personuppgifter över nationsgränser.[29] Begreppet export används i uppsatsen som synonym till begreppet överföring.

[24] Jfr dataskyddsdirektivet artikel 2(a).
[25] Jfr C-101/01 *Lindqvist*, p. 24 – 27.
[26] Jfr dataskyddsdirektivet artikel 2(d).
[27] Jfr dataskyddsdirektivet artikel 2(e).
[28] Jfr Edvardsson & Frydlinger (2013), s. 117 f.
[29] För en redogörelse kring begreppet ”överföring”, se Kuner (2013), s. 11 ff.

När det i uppsatsen talas om ***tredjeland*** åsyftas ett land som inte är medlem i EU eller EES.

I uppsatsen kommer diskussioner att föras kring skillnader mellan ***det verkliga livet*** och ***den virtuella världen***. Med det verkliga livet avses händelser och ageranden vidtagna i en miljö där en enskild person inte är uppkopplad till ett nätverk, såsom Internet. Den virtuella världen avser istället händelser och ageranden vidtagna i en miljö där en enskild person är uppkopplad till ett nätverk.

Slutligen ska det nämnas att när begreppet ***personlig integritet*** nämns i framställningen, är avsikten att detta ska utgöra ett samlingsbegrepp för rätten till respekt för privatlivet och skydd av personuppgifter, såsom de regleras i Europakonventionen artikel 8 och EU-stadgan artikel 7 och 8.

1.7 Disposition

Uppsatsen består av, utöver detta inledande kapitel, sex kapitel som är disponerade enligt följande.

I uppsatsen ***andra kapitel*** presenteras översiktligt molntjänster och dess funktion. I detta kapitel presenteras även de risker ett användande av molntjänster kan medföra och hur detta kan påverka EU-medborgarnas rätt till personlig integritet.

I det ***tredje kapitlet*** behandlas EU:s dataskyddsdirektiv, som reglerar skydd av personuppgifter vid automatiserad behandling. I kapitlet kommer det kort redogöras för dataskyddsdirektivets syfte och dess materiella regler. Avsikten är främst att redogöra för reglerna om överföring av personuppgifter till tredjeländer, med särskilt fokus på dess tillämplighet ur ett molntjänstsammanhang.

Det ***fjärde kapitlet*** avser att presentera EU-kommissionens förslag till allmän dataskyddsförordning. Kapitlet inleds med en kort introduktion avseende de generella förändringar förslaget vid ett införande kommer innebära. Vidare kommer förslagets regler om överföring av personuppgifter till tredjeländer att redogöras för, samt vilka konsekvenser de nya reglerna kan förväntas medföra vad gäller transnationellt dataflöde.

I uppsatsens ***femte kapitel*** presenteras rätten till personlig integritet som en mänsklig rättighet. Således kommer Europakonventionens artikel 8 och EU-stadgans artikel 7 och 8 att redogöras för. Vidare presenteras relevant praxis från både Europadomstolen och EU-stadgan avseende skydd för personlig integritet vid behandling av personuppgifter.

I ***kapitel sex*** kommer läsaren att introduceras för EU:s externa skyldigheter och möjligheter. Teorier och modeller avseende Europakonventions och EU-stadgans extraterritoriella verkan kommer att presenteras. Vidare kommer en teori gällande EU:s dataskyddslagstiftnings extraterritorialitet att redogöras för. Slutligen kommer EU:s möjligheter att exportera normen om skydd för personlig integritet att redogöras för genom statsvetenskapliga teorier om EU som en global aktör.

Uppsatsen kommer sedan avslutas med en analys i ***kapitel sju***. I denna avslutande analys kommer frågeställningarna att diskuteras och försöka besvaras. Vidare avslutas kapitlet med en avslutande reflektion för att sammanfatta de slutsatser som presenteras i analysen.

2 Molnet – en introduktion om dess potential och risker

Molntjänster är en av de största teknologiska revolutionerna i modern tid. I sin enklaste form kan molntjänster beskrivas som ett sätt att leverera datorresurser via ett nätverk, vanligtvis Internet, anpassade till varje användares individuella behov.[30] Miljontals EU-medborgare är användare av onlinetjänster som Facebook, Google och Amazon och är således även användare – eventuellt omedvetet – av tjänster som tillhandahålls i det s.k. molnet. EU spår en ljus framtid för molntjänster, eftersom det gynnar sysselsättningen och den ekonomiska tillväxten inom unionen.[31] Användandet av molntjänster har skapat nya möjligheter för dataregister, informationsöverföring och social kommunikation, vilket värdesätts högt i dagens uppkopplade samhälle. Den tekniska utvecklingen har emellertid en baksida i form av påtagliga risker för intrång och kränkning av enskilda individers personliga integritet.

I följande kapitel kommer molntjänster och dess funktion att närmare beskrivas. Vidare kommer det ges en kort redogörelse för vilka risker ett användande av molntjänster medför och vilket hot tredjeländers lagstiftning kan utgöra mot EU-medborgares rätt till personlig integritet.

2.1 Vad består molnet av?

Det finns ett flertal definitioner av molntjänster, men den mest frekvent använda är NIST:s[32] definition, vilken anger att en molntjänst utgör:

> ”… a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”[33]

Att köpa datorkapacitet via ett nätverk, vanligtvis Internet, är således i stort sett vad molntjänster ytterst handlar om. Molntjänster kan beskrivas som lagring, hantering och användning av datorkapacitet på fjärrbaserade datorer som kan nås via Internet. Detta innebär att molntjänstkunder kan få tillgång till datakapacitet anpassad till sina behov utan att behöva investera i egen

[30] Edvardsson & Frydlinger (2013), s. 30 och Hon & Millard, *Cloud Technologies and Services* (2013), s. 3.
[31] COM(2012) 529 final, s. 2.
[32] NIST är en del av det amerikanska näringsdepartementet.
[33] Mell & Grance, *NIST:s definition av molntjänster* (2011), p. 2.

IT- och datorkapacitet.[34] NIST:s definition identifierar dessutom tre olika tjänstemodeller för molntjänster.[35]

Tjänstemodellerna benämns ofta med samlingsnamnet SPI-modellen. De tre olika tjänstemodellerna kan beskrivas som olika delar i en värdekedja.[36] Längst ner i denna värdekedja befinner sig tjänstemodellen IaaS (*Infrastructure as a Service*). IaaS innebär att en molntjänstleverantör tillhandahåller en basal infrastruktur, såsom serverar, lagringsutrymme och bandbredd.[37] IaaS-tjänster tillgängliga för enskilda personer via Internet är exempelvis lagringstjänsterna Dropbox[38] och Amazon S3.[39] Ytterligare exempel på nyttjande av IaaS-tjänster är TV-bolags distribution av on-demand filmer och TV-program till sina kunder.[40]

I mitten av värdekedjan återfinns tjänstemodellen PaaS (*Platform as a Serivce*).[41] PaaS innebär att molntjänstleverantören tillhandahåller en plattform där molnkunden kan utveckla, testa och köra egna datorprogram i en kontrollerad miljö.[42] Ofta kan kunderna genom tillgängliggörande av verktyg utveckla exempelvis egna webbsidor och appar. En stor PaaS-leverantör är exempelvis Google App Engine[43] som tillhandahåller en tjänst för sina kunder som gör det möjligt för dem att skapa och utforma egna webbsidor.[44]

Högst i värdekedjan finns modellen SaaS (*Software as a Service*). SaaS är den mest använda molntjänsten och innebär att molntjänstkunden nyttjar en mjukvara som tillhandahålls av molntjänstleverantören.[45] SaaS benämns även ofta som ”*IT-on demand*”.[46] Exempel på SaaS-tjänster är Google, Twitter och Facebook. Även programvaror som tillhandahålls av Microsoft, vilka erbjuder mjukvara för e-mail, ordbehandlingsprogram m.m., utgör SaaS-tjänster.[47]

Molntjänster har utvecklats till att ingå i stora delar av vissa företags verksamheter idag. Företag, organisationer, myndigheter och även enskilda personer kan därmed nå sitt innehåll och använda sin mjukvara i molnet när och var de vill, t.ex. på en stationär dator, en surfplatta eller en smart mobiltelefon. Genom att använda molntjänster kan företag minska sina investeringar i datorkapacitet genom att dela mjukvara, infrastruktur och plattformar, samtidigt som skalbarheten och molntjänsternas karaktär av att vara en ”*pay-as-you-go*”-tjänst, gör att företag kan anpassa sitt behov efter varierande efterfrågan. Därutöver – liksom vid traditionell outsourcing –

---

[34] COM(2012) 529 final, s. 2, Hon & Millard, *Cloud Technologies and Services* (2013), s. 3 och Edvardsson och Frydlinger (2013), s. 13.
[35] Mell & Grance, *NIST:s definition av molntjänster* (2011), p. 2.
[36] Evardsson & Frydlinger (2013), s. 25.
[37] Mell & Grance, *NIST:s definition av molntjänster* (2011), p. 2.
[38] Se https://www.dropbox.com/.
[39] Se http://aws.amazon.com/s3/.
[40] Edvardsson & Frydlinger (2013), s. 26.
[41] Mell & Grance, *NIST:s definition av molntjänster* (2011), p. 2.
[42] Hellström (2011), s. 38.
[43] Se https://cloud.google.com/appengine/docs.
[44] Edvardsson & Frydlinger (2913), s. 26.
[45] Mell & Grance, *NIST:s definition av molntjänster* (2011), p. 2.
[46] Ibid och Hellström (2011), s. 38.
[47] Se exempelvis https://office.com/start/default.aspx.

innebär användningen av molntjänster att företag kan fokusera på sin kärnverksamhet och således lämna underhåll och IT-säkerhet till experter inom området. Detta kan även leda till ytterligare besparingar samt förbättringar av infrastruktur och informationssäkerhet.[48] Undersökningar har visat att 80 procent av de företag och organisationer som använder molntjänster har minskat sina kostnader med 10 – 20 procent.[49] Framtiden för molntjänster ser ljus ut och användningen av tjänsterna förväntas växa snabbt runt om i världen.[50]

2.2 Risker vid en ökad molnighet

Molntjänster erbjuder många fördelar och kan underlätta både ekonomiskt och organisatoriskt för både privata och offentliga aktörer. Användande av molntjänster medför dock åtskilliga risker. Användning av molntjänster innebär till stor del en överföring av uppgifter mellan olika aktörer, framförallt mellan en registeransvarig, som i de flesta fall utgör en molntjänstkund, och en registerförare, som utgör molntjänstleverantören. När personlig data överförs mellan molntjänstkunder och molntjänst-leverantörer, överförs de aktuella uppgifterna över nationella gränser och därmed också mellan olika jurisdiktioner. Det är vanligt att personuppgifter dessutom överförs till tredjeländer.[51] Risker som uppstår vid ett sådant överförande av personuppgifter är att det kan uppkomma en brist i kontrollen och en oklarhet kring hur och vem som hanterar uppgifterna när de överförs till en molntjänstleverantör i tredjeland. Denna brist på transparens avseende hur och av vem uppgifterna hanteras innebär svårigheter för molntjänstkunder att ha vetskap om var geografiskt personuppgifterna lagras och hanteras.[52] Dessutom finns det en risk att tredjelandet har lagar vilka föreskriver en skyldighet för molntjänst-leverantören att utlämna personuppgifter till offentliga myndigheter i syfte att t.ex. bekämpa brottslighet eller tillvarata nationens säkerhet.[53] Det uppstår således ett gränsöverskridande problem där lagstiftningar utanför EU kan komma att bli tillämpliga vid hanteringen av en EU-medborgares personuppgifter. Inom EU finns det ett omfattande rättsligt skydd för personuppgifter medan möjligheten till liknande rättsligt skydd utanför unionen är betydligt mindre. Det kan krasst uttryckas med att det föreligger ett hot från tredjeländer gentemot EU-medborgares rätt till personlig integritet.[54]

Ett exempel på ett tredjeland vars lagar hanterar skydd av personuppgifter annorlunda om det rör utländska medborgare är USA. Vad gäller molntjänster är USA ett av de länder vars företag har utvecklat tjänsterna mest och därmed finns det många molntjänstleverantörer etablerade i landet. Exempel på stora IT-företag som är etablerade i USA är Facebook, Google och Amazon. När dessa företags molntjänster utnyttjas, finns det en

[48] Rauhofer & Bowden (2013), s. 1.
[49] COM(2012) 529 final, s. 3 f.
[50] Edvardsson & Frydlinger (2013), s. 39.
[51] Kuner (2013), s. 102.
[52] Ibid, s. 103 f.
[53] Rauhofer & Bowden (2013), s. 3.
[54] WP 179, s. 5 f.

överhängande risk att personuppgifter överförs till USA. Exempelvis är det inskrivit i Facebooks användarpolicy att personer som inte är bosatta inom USA har, genom att skapa ett konto hos Facebook, även samtyckt till att deras personuppgifter överförs till USA.[55] Intrång i EU-medborgares personliga integritet kan då lätt uppstå. Framförallt kan två möjliga risker för intrång identifieras.

För det första finns det en risk att IT-företag, trots deras eventuella anslutning till Safe Harbor,[56] behandlar EU-medborgarnas personuppgifter på ett sätt som enligt EU:s regelverk inte är tillåtet. USA har ingen federal lagstiftning som syftar till att skydda enskildas rätt till integritet. Amerikansk skyddslagstiftning för enskildas integritet återfinns istället inom sektorer, som exempelvis hälsovård, och i de olika delstaternas lagstiftningar. USA har således ett lapptäcke av lagstiftning vad gäller skydd för personlig integritet och det leder till en osäkerhet och förvirring bland medborgarna avseende vilka rättigheter de åtnjuter.[57] Ett exempel som visar att dataskyddet skiljer sig åt mellan EU och USA är rätten att bli bortglömd. Inom EU har en variant av en sådan rätt tolkats in i dataskyddsdirektivets artikel 12(b) och 14(a).[58] I förslaget till allmän dataskyddsförordning regleras en sådan rätt i artikel 17. I USA finns det för närvarande ingen erkänd rätt för enskilda att få data raderat som är lagrat hos IT-företag.[59] Studeras exempelvis Facebooks användarpolicys kan det utläsas att de föreskriver en rätt för användarna att radera sina data, men all personlig information kan endast raderas om användarna väljer att radera hela sitt konto på Facebook.[60] Användare av Facebook som är bosatta inom EU, har genom att skapa ett konto hos Facebook ingått avtal med Facebook Irland. Facebook Irland är således bundna att efterfölja EU:s regler om dataskydd. Det är känt att EU-medborgares personliga information överförs från Facebook Irland till dess moderbolag i USA. När vi således kräver att Facebook Irland ska radera personuppgifter, kan vi aldrig vara säkra på att en total radering sker, då uppgifterna kan ha exporterats till USA för vidare behandling, där någon lagstadgad rätt att bli bortglömd inte föreligger.[61]

För det andra kan amerikansk reglering gällande offentliga myndigheters åtkomst till utländska personers personuppgifter utgöra ett hot mot EU-medborgares rätt till personlig integritet. I USA regleras bl.a. elektronisk övervakning av främmande makter genom lagen FISA. Denna lag har utvecklats under 2000-talet mot bakgrund av bl.a. terroristattacken den 11

[55] Se Facebook Inc., Policy om rättigheter och skyldigheter, p. 17(1).
[56] Se avsnitt 3.2.2.4 för redogörelse av Safe Harbor, samt den bristande verkställigheten av ramverket.
[57] Solove (2004), s. 64.
[58] Se mål C-131/12 *Google Spain* mot *AEPD*, p. 87, där EU-domstolen ansåg att EU-medborgare har en rätt gentemot sökmotorer att kräva att information om dem raderas. Domstolen erkänner i detta avgörande inte en rätt att bli bortglömd, utan påpekar att detta är en rätt för den registrerade att begränsa åtkomsten till sin personliga information.
[59] Rubinstein m.fl. (2008), s. 273 f.
[60] Se Complaint against Facebook Ireland Ltd. (2011).
[61] Se exempelvis Complaint against Facebook Ireland Ltd. (2011), s. 2 och Facebook, *Privacy policy*, 1 januari 2015. Det ska påpekas att Facebook är bundna av Safe Harbor och således är bundna att efterleva Safe Harbor-principerna. Som kommer redogöras för i avsnitt 3.2.2.4 är det dock oklart hur seriöst företagen ser på dessa principer och hur principerna efterlevs i praktiken.

september 2001. Den senaste reformen av FISA gjordes 2008[62] och innebar en drastisk skillnad för utländska medborgare vars personuppgifter, d.v.s. privata kommunikationer och liknande, behandlas eller lagras av amerikanska leverantörer av elektroniska kommunikationstjänster. Ändringen innebar att § 1881a infördes i FISA. Denna paragraf gör det möjligt för högre tjänstemän inom den amerikanska regeringen och amerikanska underrättelsemyndigheter att besluta om övervakning av personer vilka misstänks befinna sig utanför USA, under en period upp till ett år, för att erhålla tillgång till utländsk underrättelseinformation.[63] Ett sådant beslut om övervakning av en utländsk medborgare ska inlämnas till den s.k. FISA-domstolen, tillsammans med en under ed lämnad utsaga från myndigheten. Ingen annan bevisning krävs vid handläggandet av ärendet. Detta beslut ska sedan godkännas av FISA-domstolen.[64] Reglerna innebär att den amerikanska regeringen kan erhålla tillstånd att övervaka utländska medborgares elektroniska kommunikation för att på så sätt få tillgång till utländsk underrättelseinformation.[65]

I juni 2013 publicerade den brittiska nyhetstidning *The Guardian* en artikel, som sedan kom att följas av många fler, gällande de s.k. Snowden-avslöjandena. Det var den amerikanske s.k. visselblåsaren Edward Snowden som avslöjade hur den amerikanska regeringen, genom olika underrättelsetjänster som exempelvis NSA, hade fått tillgång till stora mängder personuppgifter från stora amerikanska IT-företag. FISA-domstolen hade godkänt ett beslut om att förelägga ett amerikanskt IT-företag att lämna ut all kommunikation under en tremånaders period. IT-företaget var dessutom belagt med förbud att för allmänheten avslöja att personlig information utlämnats till amerikanska underrättelsetjänster eller att det förelåg ett domstolsbeslut om sådant föreläggande mot företaget.[66] Dagen därpå avslöjades att den amerikanska underrättelsemyndigheten använt sig av ett datorprogram vid namn PRISM, vilket gav dem en direkt tillgång till personuppgifter som lagrats hos de stora IT-företagen Apple, Facebook och Google. Enligt uppgifter ska NSA genom PRISM fått tillgång till exempelvis lagrad sökhistorik, innehåll i privata mail och livechat-meddelande.[67]

I det fjärde tillägget till Förenta Staternas konstitution stadgas ett skydd för enskilda mot oskäliga husrannsakningar utförda av staten. Detta skydd är inte ett specifikt skydd av personuppgifter, men det innebär vissa begränsningar mot offentliga myndigheter som söker tillgång till eller avser att övervaka bl.a. virtuella områden av en persons privata sfär.[68] Skyddet som föreskrivs i det fjärde tillägget är dock som huvudregel inte applicerbart på utländska medborgare, utan kan endast åtnjutas av amerikanska

[62] FISA Amendments Act of 2008 (FAA).
[63] 50 U.S.C. § 1881a(a).
[64] 50 U.S.C. § 1881a(g).
[65] Milanovic (2014), s. 9 f och van Hoboken & Rubinstein (2014), s. 503 f.
[66] Se exempelvis Greenwald, *The Guardian*, 6 juni 2013.
[67] van Hoboken & Rubinstein (2014), s. 504. Det ska poängteras att nämnda företag och den amerikanska regeringen har förnekat alla dessa anklagelser.
[68] Solove (2004), s. 189.

medborgare. Detta innebär således att en utländsk medborgare åtnjuter ett mycket svagare skydd i USA än vad dess egna medborgare åtnjuter.[69]

Snowden-avslöjandena och PRISM-skandalen bidrog till redan förekommande rykten om den amerikanska regeringens övervakning av både egna och utländska medborgare. Mycket kritik riktades både mot den amerikanska regeringen och de anklagade IT-företagen p.g.a. den avslöjade behandlingen av enskildas personliga information. Riskerna med att använda molntjänster och att överföra personuppgifter till tredjeländer uppmärksammades dessutom ytterligare inom EU. Molntjänstindustrin, framförallt leverantörer verksamma i USA, drabbades hårt av avslöjandena och människors tveksamhet till att använda sig av molntjänster växte. Det är dock troligt att molntjänstindustrin kommer att repa sig efter skandalen. Det kvarstår däremot många olösta problem vad gäller regleringen kring internationell överföring av personuppgifter och skyddet för den personliga integriteten.[70]

[69] Rauhofer & Bowden (2013), s. 22 f.
[70] van Hoboken & Rubinstein (2014), s. 491.

3 Skydd för personuppgifter vid överföring till tredjeländer

Molntjänster är till sin karaktär globala och många företag som tillhandahåller onlinetjänster som exempelvis sociala nätverk, mailklienter och e-handelssidor, använder sig idag av molntjänster. Data överförs mellan företag och organisationer varje sekund över hela världen och ger upphov till komplexa gränsöverskridande situationer som spänner över flera jurisdiktioner. Relevant för skyddet av EU-medborgarnas personliga integritet är således under vilka förutsättningar det är tillåtet, för exempelvis en molntjänstkund, att överföra personuppgifter till en molntjänstleverantör i ett tredjeland. Regler avseende automatisk behandling av personuppgifter har harmoniserats inom EU och EES[71] genom dataskyddsdirektivet, vilket sedan har implementerats i medlemsstaternas nationella lagstiftningar.

I följande kapitel redogörs det översiktligt för dataskyddsdirektivets syfte och materiella bestämmelser. Vidare presenteras bestämmelserna om överföring av personuppgifter till tredjeland, samt dess tillämplighet ur ett molntjänstsammanhang.

3.1 Dataskyddsdirektivet – en introduktion

Behandling av personuppgifter som företas på helt eller delvis automatiserad väg är reglerad genom EU:s dataskyddsdirektiv om skydd för enskilda personer med avseende på behandling av personuppgifter och det fria flödet av sådana uppgifter. Direktivet syftar till att skydda fysiska personers grundläggande fri- och rättigheter, särskilt rätten till privatliv, samt att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna.[72]

För att uppnå detta ändamål innehåller dataskyddsdirektivet en lång rad bestämmelser om när och hur personuppgifter får behandlas. I dessa bestämmelser anges vilka rättigheter som tillkommer personer vars uppgifter blir föremål för insamling och behandling. Detta gäller särskilt rätten att bli informerad om vilken behandling som sker, rätten till tillgång till uppgifterna, rätten att göra invändningar och rätten till rättslig prövning.[73]

[71] Härefter kommer det endast att hänvisas till EU vid redogörelse för dataskyddsdirektivet, denna hänvisning inbegriper dock även EES.
[72] Se dataskyddsdirektivet artikel 1.
[73] Jfr dataskyddsdirektivet artikel 6 – 12

Vad gäller krav på säkerhet vid behandling av personuppgifter anges det i dataskyddsdirektivet att varje behandling ska utföras på ett legitimt sätt för ett precist uttryckt ändamål, vilket är begränsat till en nödvändig tidsram.[74] Vidare ska den registeransvarige skydda uppgifterna från förlust och ändringar samt otillåten spridning eller tillgång till uppgifterna. Detta gäller särskilt vid överföring av personuppgifter mellan olika nätverk.[75] Det är normalt sett den registeransvarige som bestämmer för vilka ändamål som personuppgifterna ska behandlas. I de fall en registeransvarig anlitar en registerförare för att utföra behandlingen för den registeransvariges vägnar, förutsätts det att registerföraren ger tillräckliga garantier för att nödvändiga säkerhetsåtgärder tillämpas vid behandlingen av personuppgifterna.[76] Det finns ingen möjlighet för medlemsstaterna att i sina nationella genomförandebestämmelser göra undantag från dessa krav.[77]

3.2 Överföring av personuppgifter till tredjeländer

Som ovan nämnts är ett av dataskyddsdirektivets främsta syften att främja det fria flödet av personuppgifter inom unionen.[78] Flertalet molntjänster är dock etablerade utanför EU vilket medför att EU-baserade molntjänstkunder i sin affärsverksamhet kommer att överföra personuppgifter till tredjeland. Bestämmelserna om överföring av personuppgifter till tredjeländer är därmed centrala för att upprätthålla en hög skyddsnivå vid behandling av EU-medborgarnas personuppgifter. Att låta personuppgifter flöda fritt över internationella gränser är avgörande för yttrandefriheten, liksom för andra viktiga rättigheter och värderingar. Samtidigt är det viktigt att uppgifterna skyddas i en värld där dataflödet inom sociala och ekonomiska sammanhang ökar.[79]

Avsikten inom EU är att dataskyddsdirektivet ska åstadkomma en harmonisering av integritetsskyddet och således medföra ett starkt skydd för EU-medborgarnas rättigheter. Det integritetsskydd som en EU-medborgare erhåller vid behandling av sina personuppgifter utanför EU:s gränser kan i många fall framstå som svagt vid en jämförelse med det skydd som garanteras inom EU. Det är således av vikt att EU-medborgarna erhåller ett starkt skydd mot att personuppgifter exporteras till tredjeländer där deras rättigheter eventuellt kan utsättas för otillåtna ingrepp.[80]

3.2.1 En adekvat skyddsnivå

Huvudregeln gällande överföring av personuppgifter till tredjeländer återfinns i dataskyddsdirektivet artikel 25. Artikeln föreskriver att sådan överföring av personuppgifter som är under behandling eller som är avsedda att behandlas efter överföring till tredjeland endast får ske om ifrågavarande

[74] Se dataskyddsdirektivet artikel 6.
[75] Jfr dataskyddsdirektivet artikel 17(1) och Ds 2014:23, s. 19.
[76] Jfr dataskyddsdirektivet artikel 17(2).
[77] Ds 2014:23, s. 19.
[78] Jfr dataskyddsdirektivet artikel 1(1).
[79] Rauhofer & Bowden (2013), s. 3.
[80] Edvardsson & Frydlinger (2013), s. 127f.

tredjeland säkerställer en adekvat säkerhetsnivå.[81] Syftet med att införa denna bestämmelse var bl.a. att åstadkomma viss påtryckning mot tredjeländer att anta dataskyddsregleringar vilka upprätthåller en liknande standard och skyddsnivå som EU:s dataskyddsdirektiv.[82]

Bedömningen av om skyddsnivån i ett tredjeland är adekvat ska enligt artikel 25(2) ske på grundval av de förhållanden som har samband med den aktuella överföringen. Härvidlag ska särskilt beaktas uppgifternas art, den eller de avsedda behandlingarnas ändamål och varaktighet, ursprungslandet, det slutliga bestämmelselandet, de allmänna respektive särskilda rättsregler som gäller i ifrågavarande tredjeland liksom de regler för yrkesverksamhet och säkerhet som gäller där.[83] Denna bedömning kan utföras av dels kommissionen,[84] dels den aktör som avser att överföra uppgifterna till tredje land.[85] Det är endast ett fåtal länder som EU-kommissionen hittills har förklarat vara en garant för en adekvat skyddsnivå.[86]

Molntjänster är till sin natur gränsöverskridande och dataskyddsdirektivets restriktion mot överföringar av personuppgifter till tredjeländer har ansetts försvåra deras framväxt. Det finns dock undantag till när överföring kan ske trots att det inte föreligger en adekvat skyddsnivå i aktuellt tredjeland.[87] Nedan presenteras dessa undantag och tillämplighet på molntjänster.

3.2.2 Undantag för tillåtande av överföring

3.2.2.1 Samtycke

Artikel 26(1)(a) föreskriver att överföring av personuppgifter till ett tredjeland, som inte utgör en garant för en adekvat skyddsnivå, får ske i de fall den registrerade otvetydigt har samtyckt till överföringen. Samtycket måste vara av sådant slag att det har getts frivilligt och för ett särskilt ändamål, samt även vara en informerad viljeyttring genom vilken den registrerade godtar behandling av personuppgifter som rör vederbörande.[88] Bestämmelsen är utformad med avsikt att omfatta ett samtyckte till specifika engångsöverföringar och inte återkommande eller fortlöpande överföringar. Nämnda former av överföringar är dock vanliga vid användande av molntjänster. Det är svårt – om inte omöjligt – för den registeransvarige att erhålla den registrerades samtycke, med enligt lag

[81] Se dataskyddsdirektivet artikel 25(1).
[82] Jfr dataskyddsdirektivet artikel 25(5) och Hon & Millard (2013), s. 255.
[83] Se dataskyddsdirektivet artikel 25(2).
[84] Jfr dataskyddsdirektivet artikel 25(6).
[85] När bedömningen utförs av den aktör som avser exportera personuppgifter till tredje land ska den ske i enlighet med det som föreskrivs i dataskyddsdirektivet artikel 25(2). I praktiken anses det vara riskfullt för en aktör att utföra bedömningen av om det föreligger en adekvat skyddsnivå på egen hand. Endast i specifika situationer genomförs denna bedömning av enskilda aktörer. Jfr diskussion i Rauhofer & Bowden (2013), s. 4.
[86] Länder som EU-kommissionen har förklarat har en adekvat skyddsnivå per den 1 mars 2013 är Andorra, Argentina, Kanada, Färöarna, Guernsey, Isle of Man, Jersey, Nya Zeeland, Schweiz och Uruguay. Se *Commission decisions on the adequacy of the protection of personal data in third countries*, senast uppdaterad den 24 juni 2014. Vidare har även Artikel 29-gruppen förklarat att Monaco har en adekvat skyddsnivå vad gäller behandling av personuppgifter, se WP 198.
[87] Hon & Millard (2013), s. 254 f.
[88] Se dataskyddsdirektivet artikel 2(h).

nödvändig precision, inför varje överföring. Bestämmelsen om samtycke har därför ofta kritiserats då den inte garanterar en tillräcklig skyddsnivå vid behandling av personuppgifter i molnet.[89]

Ytterligare en fråga som uppkommer när undantaget om samtycke tillämpas för att rättfärdiga en överföring till tredjeland, är vem som är den registrerade som enligt lag ska lämna samtycket, och vem som faktiskt överför uppgifterna. Problemet kan exemplifieras enligt följande. En användare av en SaaS-tjänst, t.ex. ett socialt nätverk, kan samtidigt definieras som både den registrerade och den registeransvarige. Om vederbörande är medveten om att de personuppgifter han eller hon laddar upp på det sociala nätverket kommer att överföras, behandlas och lagras i ett tredjeland som inte erbjuder en adekvat skyddsnivå, kan det argumenteras för att han eller hon som användare av SaaS-tjänsten har givit sitt samtycke till överföringen. Detta eftersom användaren samtidigt agerar som både den registrerade och den registeransvarige.[90]

Om ovan nämnda situation problematiseras ytterligare, kan tveksamhet med det lämnade samtycket uppstå, t.ex. vid tillfällen då en användare av det sociala nätverket laddar upp personuppgifter vilka anknyter till andra personer än användaren själv, exempelvis ett fotografi vilket gestaltaltar användarens vänner. I dessa fall är det användaren i rollen som den registeransvarige som lämnar samtycket, inte de registrerade, som utgörs av personerna på fotografiet.[91] Är den registeransvarige en enskild person, ska det nämnas att nämnda situation kan omfattas av det så kallade hushållsundantaget.[92] Det kan däremot konstateras att ett införskaffande av samtycke från den registrerade till rättfärdigande av överföring av personuppgifter till tredjeland, är problematiskt och opraktiskt vad gäller behandling av uppgifter i molntjänster.[93]

3.2.2.2 Binding Corporate Rules

Ytterligare ett undantag från dataskyddsdirektivet artikel 25, om adekvat skyddsnivå, stadgas i artikel 26(2). Denna bestämmelse anger att överföring av personuppgifter till tredje land som inte utgör en garant för adekvat skyddsnivå får ske om den registeransvarige ställer tillräckliga garantier för att privatliv och enskilda personers grundläggande fri- och rättigheter skyddas samt för utövningen av motsvarande rättigheter.[94] Sådana garantier kan framgå av lämpliga avtalsklausuler som exempelvis stadgas genom BCR:s. BCR:s är bindande företags- och koncerninterna regler som avser att skapa en uppförandekod vad gäller hanteringen av internationella överföringar av personuppgifter som sker inom exempelvis en global koncern eller multinationellt företag.[95]

---

[89] WP 114, s. 10 – 12, Hon & Millard (2013), s. 261 f och Rauhofer & Bowden (2013), s. 5.
[90] Hon & Millard (2013), s. 261.
[91] Ibid.
[92] Se dataskyddsdirektivet artikel 3(2). Hushållsundantaget innebär att reglerna i dataskyddsdirektivet inte omfattar sådan behandling av personuppgifter som sker för privat bruk eller bruk inom hushållet.
[93] Rauhofer & Bowden, s. 5 och Hon & Millard (2013), s. 262.
[94] Se dataskyddsdirektivet artikel 26(2).
[95] Edvardsson & Frydlinger (2013), s. 132 och Hon & Millard (2013), s. 267.

BCR:s utformades först år 2003 av Artikel 29-gruppen som ett alternativ för multinationella företag att kunna överföra personuppgifter internt, trots EU:s exportrestriktioner. Enligt Artikel 29-gruppen kan en tillräcklig intern kontroll och säkerhet för enskildas rättigheter uppnås genom att BCR:s upprättas inom ett multinationellt företag.[96] Vid ett upprättande av BCR:s måste de anpassas till den specifika företagsgrupp som är aktuell och reglerna ska sedan godkännas av berörda nationella dataskydds-myndigheter.[97] BCR:s har dock inte utnyttjats i någon större utsträckning. Företag har funnit processen för att få reglerna godkända både besvärlig, kostsam och tidskrävande.[98] Användningen av BCR:s har dessutom varit föremål för kritik p.g.a. att de fram till 2012 endast kunde tillämpas av registeransvariga.[99] Som ett gensvar på kritiken utvecklade Artikel 29-gruppen en möjlighet även för registerförare att nyttja BCR:s i sin verksamhet.[100] Detta innebär att efter att en registerförare har säkrat ett godkännande av upprättade BCR:s av relevant nationell dataskydds-myndighet, kan en registeransvarig sluta ett så kallat serviceavtal med registerföraren, vilket måste innehålla vissa nödvändiga bestämmelser. Personuppgifter kan sedan överföras från den registeransvarige till medlemmar av registerförarens bolagskoncern, vilka är bundna att efterfölja koncernens BCR:s. Detta innebär att uppgifter kan överföras till bolag eller datacenter som är etablerade utanför EU. Även vidarebefordring av personuppgifter från registerföraren till en underleverantör är tillåtet under vissa särskilda förhållanden.[101]

Artikel 29-gruppen har yttrat sig angående registerförares BCR:s och har angett att även registerförare etablerade i tredjeland kan erhålla ett godkännande av BCR:s från någon av EU:s medlemsstaters nationella dataskyddsmyndigheter.[102] I praktiken innebär detta att registerförare i tredjeland kan behandla personuppgifter som exporterats från EU, utan att omfattas av någon av EU:s medlemsstaters nationella lagstiftning. I en situation där registerföraren bryter mot BCR:s kan det således uppstå problem med verkställighet. Exempelvis kan det uppstå svårigheter vid en situation då en medlemsstats domstol utdömer skadestånd mot en register-förare i tredjeland. Möjligheten en medlemsstat och dess verkställande myndigheter har att i en sådan situation verkställa domen, gentemot en registerförare som inte har några tillgångar i den aktuella medlemsstaten, kan framstå som begränsade.[103] Uppstår en sådan situation har Artikel 29-gruppen angett att en registerförares meddelade godkännande av BCR:s ska kunna upphävas.[104] Emellertid bekräftar detta uttalande även att ett sådant upphävande inte skulle ha en retroaktiv effekt. Ett upphävande kan därför uppfattas som en klen tröst för en registrerad vars dataskydd och rättigheter har kränkts av en registerförare i tredjeland efter en export av person-uppgifter från EU. Huruvida ett godkännande av registerförares BCR:s kan

[96] WP 74, s. 10 ff.
[97] Rauhofer & Bowden (2013), s. 5.
[98] Hon & Millard (2013), s. 273.
[99] Ibid, s. 267.
[100] WP 195, s. 2.
[101] Hon & Millard (2013), s. 268 och Edvardsson & Frydlinger (2013), s. 132 f.
[102] WP 195, s. 8 och 18.
[103] Rauhofer & Bowden (2013), s. 6.
[104] WP 195, s. 11.

komma att underlätta det gränsöverskridande flödet av personuppgifter kan sägas vila på de nationella medlemsstaternas dataskyddsmyndigheter och vilka befogenheter de besitter att godkänna BCR:s, vilket kan variera mellan de olika medlemsstaterna.[105]

3.2.2.3 Modellklausuler

Modellklausuler[106] är ytterligare en mekanism som EU-kommission har utvecklat för att möjliggöra export av personuppgifter till tredjeländer som saknar en adekvat skyddsnivå. Dataskyddsdirektivet artikel 26(4) stadgar en rätt för kommission att, i enlighet med ett visst förfarande, besluta att vissa modellklausuler kan tillämpas i avtal gällande överföring av personuppgifter till mottagare utanför unionen.[107] Klausulerna innehåller skyldigheter dels för de registeransvariga som vill exportera personuppgifter, dels för de registeransvariga eller registerförare som mottar personuppgifterna i ett tredjeland. Dessa modellklausuler ska innebära ett tillräckligt integritetsskydd för de registrerade när deras personuppgifter behandlas i ett tredjeland. Vidare regleras viktiga frågor rörande överföringen av uppgifter, som exempelvis de registrerades rättigheter och hur eventuella tvister som uppkommer med anledning av avtalet ska lösas.[108]

Kommission har genom beslut antagit tre olika alternativ av modellklausuler. Två alternativ avser att reglera förhållandet när en registeransvarig avser att överföra personuppgifter till annan registeransvarig i tredjeland.[109] Båda dessa alternativ kan tillämpas som underlag till avtal, dock föredrar registeransvariga att tillämpa den senast uppdaterade versionen av modellklausulerna.[110] Det tredje alternativet av modellklausuler är anpassade till förhållandet då en registeransvarig ska överföra personuppgifter till en registerförare i tredje land.[111] Denna version av modellklausuler innehåller särskilda bestämmelser om överföring av personuppgifter från registerföraren till andra underleverantörer. Förutsättningar för att sådan överföring ska vara tillåten är att underleverantören genom avtal är förpliktigad att behandla uppgifterna i enlighet med de krav EU ställer på dataskydd, genom dataskyddsdirektivet, samt att det föreligger lämpliga tekniska och säkerhetsmässiga åtgärder i det land som utgör slutdestinationen.[112]

De av kommissionen antagna modellklausulerna har kritiserats för att inte vara tillräckligt flexibla för att kunna tillämpas i molntjänstavtal. För att en användare av en molntjänst, exempelvis en registeransvarig, ska kunna utnyttja modellklausulerna måste de göra detta utan tillägg eller förändringar av klausulerna. Något annat vore självklart rättsosäkert. I dessa

[105] Rauhofer & Bowden (2013), s. 6 f.
[106] Även kallade standardavtalsklausuler.
[107] Jfr dataskyddsdirektivet artikel 26(4) och WP 196, s. 18 f.
[108] Edvardsson & Frydlinger (2013), s. 131.
[109] Se KOM (2001/479/EG) och KOM (2004/915/EG).
[110] Hon & Millard (2013), s. 267. Anledningen till att registeransvariga föredrar att tillämpa den senaste uppdaterade versionen är för att den versionen innehåller uppdateringar som grundar sig på förslag framställda av ICC (*International Chamber of Commerce*) och andra företagsgrupper.
[111] Se KOM (2010/87/EU).
[112] Rauhofer & Bowden (2013), s. 7.

sammanhang är situationen ofta sådan att molntjänstleverantören, ofta registerföraren, har en starkare förhandlingsposition än vad den registeransvarige har. I praktiken är det därför osannolikt att en registerförare skulle gå med på att åta sig betungande dataskyddsbestämmelser som kan påverka omfattningen av de tjänster de kan erbjuda samt vilka underleverantören de kan samarbeta med.[113]

Vidare saknas det modellklausuler som är anpassade till förhållandet när en registerförare vill överföra personuppgifter till annan registerförare i tredje land. I praktiken innebär detta att problem uppstår i en situation där det exempelvis finns ett molntjänstavtal mellan en EU-baserad registeransvarig och en EU-baserad registerförare, och den sistnämnde vill nyttja tjänster som en underleverantör i tredje land erbjuder. Det föreligger således en lucka i de rättsliga instrument som avser att underlätta gränsöverskridande dataflöde. Denna lucka kommer sannolikt att förbli till dess kommissionen antar modellklausuler anpassade till förhållandet mellan två registerförare.[114]

3.2.2.4 Safe Harbor

Många molntjänstleverantörer är etablerade i USA och ett transatlantiskt samarbete är viktigt för flertalet EU-baserade molntjänstkunder. Det föreligger dock en stor skillnad mellan EU och USA gällande inställningen till integritetsskydd och EU-kommissionen har förklarat att USA inte kan säkerställa en adekvat skyddsnivå. Således är export av personuppgifter till USA från EU förbjudet.[115] Till förmån för den ekonomiska utvecklingen har det dock varit av stort intresse att, trots de skilda inställningarna till integritetsskydd, försöka åstadkomma en överenskommelse vilken kunde möjliggöra transatlantiska överföringar av personuppgifter.[116] EU-kommissionen utvecklade därför tillsammans med det amerikanska näringsdepartementet[117] ett *Safe Harbor*-ramverk. Ramverket godkändes år 2000 av EU och stadgar ett antal riktlinjer som amerikanska organisationer måste efterleva för att tillförsäkra EU-medborgares personuppgifter en tillräckligt hög skyddsnivå.[118]

Amerikanska organisationer som har för avsikt att ansluta sig till Safe Harbor måste upprätta en policy genom vilken de åtar sig att uppfylla sju grundläggande principer. Syftet med de grundläggande principerna är att tillförsäkra ett starkt skydd för de personuppgifter som överförs från EU till USA. Dessa principer är liknande de regler om skydd för behandling av personuppgifter som återfinns i dataskyddsdirektivet.[119] En anslutning till

[113] Rauhofer & Bowden (2013), s. 7 f.
[114] Hon & Millard (2013), s. 272 f och Rauhofer & Bowden (2013), s. 8.
[115] Edvardsson & Frydlinger (2013), s. 129 och Rauhofer & Bowden (2013), s. 3.
[116] US-EU Safe Harbor, Overview.
[117] Svensk översättning av U.S. Department of Commerce.
[118] Rauhofer & Bowden (2013), s. 3 och Edwards (2009), s. 454. Se kommissionens beslut 2000/520/EG.
[119] Edvardsson & Frydlinger (2013), s. 130, Colonna (2014), s. 204 f och Edwards (2009), s. 454. De sju grundläggande principerna är: (1) de registrerade måste erhålla information om syftet med behandlingen av personuppgifter, (2) de registrerade ska ha möjlighet att välja om personuppgifter får utlämnas till tredje person, (3) vid utlämnande till tredje man måste principerna under (1) och (2) efterföljas, (4) de registrerade ska ha tillgång till den

Safe Harbor är helt frivillig. Amerikanska organisationer som beslutar sig för att delta i Safe Harbor måste offentligt deklarera att de följer de grundläggande principerna. Anslutning sker således genom självcertifiering, vilken årligen måste uppdateras skriftligen till det amerikanska närings-departementet. Därefter är organisationerna certifierade och tas då upp på den s.k. Safe Harbor-listan, där alla certifierade organisationer och företag anges.[120] Amerikanska organisationer kan således uppnå en adekvat skyddsnivå utan att vara bundna av EU-lagstiftning eller riskera att ställas inför rätta vid en medlemsstats nationella domstol.[121]

Verkställighet av Safe Harbor sker som huvudregel i USA och i enlighet med gällande självregleringar.[122] Självregleringarna understöds sedan vid behov av verkställighet enligt amerikansk lagstiftning. Den amerikanska myndigheten FTC genomför den statliga tillsynen av efterlevnaden av Safe Harbor. Om en organisation underlåter att följa de uppsatta principerna kan detta angripas genom nationell eller federal lagstiftning, vilka stadgar ett förbud mot illojal eller bedräglig handling. FTC har befogenhet att, vid bristande efterlevnad av principerna, civilrättsligt sanktionera organisationer genom att utdöma en form av företagsböter, samt även utesluta dem från Safe Harbor.[123]

Huruvida organisationerna agerar i förenlighet med principerna i praktiken samt hur effektiv verkställigheten är vid underlåtelse av principerna, har dock ifrågasatts under senare år. En undersökning som genomfördes 2008 visade att endast ca. 70 procent av de angivna organisationerna på Safe Harbor-listan hade förnyat sitt certifikat det aktuella året. Vidare efterlevde endast ca. 20 procent av de listade organisationerna de sju grundläggande principerna som anges i Safe Harbor.[124] Med dessa siffror till hands kan det därför ses som anmärkningsvärt att FTC gjorde sitt första ingripande mot en Safe Harbor-ansluten organisation först år 2011. Detta ingripande gjordes mot IT-företaget Google som hade underlåtit att följa två principer vid insamlande av information från deras mailklient Gmail.[125] Ingripandet ledde dock till en förlikning mellan FTC och Google, vilken i korthet innebar att Google hädanefter skulle agera i förenlighet med Safe Harbor-principerna.[126]

Artikel 29-gruppen har i ett yttrande riktat viss kritik mot Safe Harbor-ramverket och menar att EU-baserade företag som exporterar person-uppgifter till USA inte endast kan förlita sig på att organisationen som

---

information som registreras om dem, (5) det ska finnas en skälig säkerhet vilken syftar till att förhindra otillåten tillgång, spridning eller utlämning/förlust av uppgifterna, (6) personuppgifterna måste vara relevanta för behandlingen samt uppdaterade och korrekta, samt (7) för att tillse att principerna i Safe Harbor efterlevs ska det finnas effektiva rättsmedel för de registrerade så att de registrerade kan föra talan mot organisationen om denna inte agerar i förenlighet med de grundläggande principerna. Se US-EU Safe Harbor-principerna, tillgängliga via: http://www.export.gov/safeharbor/eu/eg_main_018475.asp.

[120] US-EU Safe Harbor, Overview och Colonna (2014), s. 205.

[121] Rauhofer & Bowden (2013), s. 8.

[122] US-EU Safe Harbor, Overview.

[123] US-EU Safe Harbor, Overviw och Colonna (2014), s. 206 f.

[124] Hon & Millard (2013), s. 262 f.

[125] FCT, FCT Charges Deceptive Privacy Practices in Google´s Rollout of Its Buzz Social Network, (FCT File No. 102 3136) (2011).

[126] Ibid och Colonna (2014), s. 207.

mottar uppgifterna är upptagna på Safe Harbor-listan. Ett företag som vill exportera data bör istället söka bevis på att den amerikanska organisationen innehar ett certifikat samt efterlever de grundläggande principerna.[127] Vidare anser Artikel 29-gruppen att de nu gällande Safe Harbor-principerna inte garanterar att tillräckliga skyddsåtgärder vidtas av den mottagande organisationen. Vid användandet av molntjänster uppkommer enligt Artikel 29-gruppen säkerhetsrisker gällande bl.a. förlust av information, osäker eller otillräcklig radering av uppgifter samt förlust av kontroll över uppgifter. Detta är risker som idag inte regleras på ett tillfredsställande sätt i Safe Harbor-ramverket.[128]

[127] WP 196, s. 17.
[128] Ibid, s. 18.

4 EU-kommissionens förslag till allmän dataskyddsförordning

När dataskyddsdirektivet trädde i kraft 1998 hade mobiltelefoner decimeterlånga antenner och mindre än en procent av EU:s medborgare hade tillgång till Internet. Numera överförs och utväxlas enorma mängder personuppgifter över kontinenten och runtom i världen på endast några bråkdelar av en sekund. Globalisering tillsammans med tekniska framsteg har förändrat det sätt på vilket personuppgifter insamlas, görs tillgängliga och används. Konsekvensen har delvis blivit så att vissa enskilda personer har tappat förtroendet för IT-företag och myndigheter som behandlar deras personuppgifter via exempelvis Internet.[129] Uppfattningen inom EU är att det nuvarande dataskyddsdirektivet är bristfälligt och inte tillgodoser EU:s medborgare ett tillräckligt skydd vid automatiserad behandling av personuppgifter.[130] Det har därför ansetts nödvändigt att inom EU upprätta ett kraftfullare och mer sammanhängande regelverk för skydd av personlig data, och som dessutom ska underlätta för företag som driver sin verksamhet med hjälp av exempelvis molntjänster.[131]

I följande kapitel presenteras EU-kommissionens förslag till en allmän dataskyddsförordning. Framförallt kommer de angivna reformerna vad gäller regler för överföring av personuppgifter till tredje land att redogöras för samt vilken förändring av det gällande rättsläget reformen förväntas medföra.

4.1 Allmänt om förslagets syfte och innehåll

Den 25 januari 2012 presenterade Europeiska kommissionen ett förslag till förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter. Denna förordning ska ersätta det gällande dataskyddsdirektivet och syftar till att modernisera, effektivisera samt ytterligare harmonisera reglerna om skydd för personuppgifter inom EU och EES.[132] Förordningen kommer, till skillnad mot dataskyddsdirektivet, att vara direkt tillämpligt i medlemsstaterna.[133]

[129] Pressmeddelande, EU-kommissionen: Förslag om genomgripande reform av reglerna om uppgiftsskydd, s. 1.
[130] Rauhofer & Bowden (2013), s. 9.
[131] Förslag till allmän dataskyddsförordning, s. 2 och Pressmeddelande, EU-kommissionen: Förslag om genomgripande reform av reglerna om uppgiftsskydd, s. 1.
[132] Kuner (2013), s. 46. Härefter kommer endast hänvisning ske till EU, men i de fall EU behandlas i förhållande till förslaget till allmän dataskyddsförordning, avses även EES.
[133] Se FEUF artikel 288.

Bakgrunden till förslaget om en allmän dataskyddsförordning är den snabba tekniska utvecklingen och de utmaningar som till följd av detta har uppstått vad gäller skydd av personuppgifter. Datadelning och insamling av uppgifter har ökat väsentligt i omfattning och ny teknik gör det möjligt för både privata företag och myndigheter att använda sig av personuppgifter när de bedriver sina verksamheter.[134] Vidare tillgängliggör enskilda personer allt oftare personlig information via Internet. Att bygga upp ett förtroende för onlinetjänster är i framtiden avgörande för den ekonomiska utvecklingen inom EU. Det är därför viktigt att inrätta en reglering som ger en mer sammanhängande ram för uppgiftsskydd inom EU, vilken också underbyggs av en strikt tillsyn. Detta kan innebära en möjlighet för den digitala ekonomin att utvecklas, stärka rättssäkerheten, samt även ge enskilda personer kontroll över sina egna uppgifter.[135]

Som ovan nämnts presenterades förslaget om allmän dataskyddsförordning av EU-kommissionen 2012. Därefter har förslaget behandlats av EU:s olika organ samt även reviderats ett flertal gånger.[136] För tillfället diskuteras förslaget återigen av de två lagstiftande institutionerna inom EU, Europaparlamentet och rådet. EU:s rättvisekommissionär har i ett pressmeddelande uttalat att reformen om dataskydd är en prioritering inom EU och målet är att förslaget ska antas av Europaparlamentet och rådet innan årsskiftet 2014-15. Om denna tidsplan följs, kan en allmän dataskyddsförordning träda ikraft redan 2016.[137] Lagstiftningsprocessen har således dragit ut på tiden och har även påverkats mycket av inträffade händelser såsom Snowden-skandalen. Processen har även varit föremål för stark lobbying av företrädare från näringslivet och regeringar från tredjeländer.[138] Lobbyverksamheten har beskrivits som en av de mest intensiva och mest välfinansierade som skett inom EU.[139]

Förslaget avser att stärka den registrerades rättigheter genom att föreskriva ytterligare principer om dataskydd, vilka inte tidigare reglerats i det nu gällande dataskyddsdirektivet.[140] Det kan bl.a. nämnas att reglerna gällande den registrerades rätt att informeras om hur och vilka personuppgifter som behandlas samt under hur lång tid dessa uppgifter avses att lagras av den registeransvarige, kommer att utvidgas.[141] Vidare införs det även rätt för den

[134] Förslag till allmän dataskyddsförordning, s. 1.
[135] Ibid, s. 1 f.
[136] Rådgivande utskott inom EU som behandlat förslaget är exempelvis LIBE. Förslag till förändringar i förslaget har bl.a. presenterats av arbetsgrupper inom rådet. Det senaste dokumentet presenterat av rådet med förslag på förändringar av EU-kommissionens förslag om dataskyddsförordning är tillgängligt via: http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2017831%202013%20INIT.
[137] Pressmeddelande, EU-kommissionen: Data Protection Day 2014: Full Speed on EU Data Protection Reform, s. 2 f.
[138] Rauhofer & Bowden (2013), s. 9 och Kuner m.fl. (2012), s. 116.
[139] Brandel, Svenska Dagbladet: *Vem ska äga makten över dig på nätet?*. Det amerikanska IT-bolaget Amazon är ett av företagen som genomfört en kraftig lobbyverksamhet. Företaget har lämnat in 95 lagförslag till syfte att förändra förslaget till allmän dataskyddsförordning.
[140] Hon m.fl. (2014), s. 14 f.
[141] Se förslag till allmän dataskyddsförordning artikel 14.

registrerade att bli bortglömd och få personuppgifter raderade för att förhindra ytterligare spridning av dem.[142]

Ett starkare rättighetsskydd för den registrerade innebär mer ansvar och striktare regler för registeransvarig och registerförare. Förslaget kommer att innebära att den registeransvarige exempelvis tillskrivs ett större ansvar där de åläggs att upprätta en intern policy samt genomföra åtgärder för att säkerställa och kunna visa att behandlingen av personuppgifter sker i enlighet med förordningen. Efterlevnaden av denna policy ska, om det är proportionerligt, kontrolleras av interna eller externa granskare.[143]

Kritiker menar dock att förslaget till en allmän dataskyddsförordning riskerar att leda till en avsevärd försvagning av det nuvarande dataskyddet.[144] Det anses även att förslaget har påverkats av pågående lobbying och således utformats på ett förmånligt sätt för företag, varpå konsekvensen blir en försvagning av EU-medborgarnas integritetsskydd.[145]

4.2 Överföring av personuppgifter till tredjeländer

Om förslaget till allmän dataskyddsförordning antas kommer det att medföra förändringar av EU:s befintliga bestämmelser för gränsöverskridande dataflöden.[146] Kapitel fem i förslaget innehåller bestämmelserna om överföring av personuppgifter till tredjeländer. Artikel 40 i förslaget stadgar den grundläggande principen för att överföring av personuppgifter till tredjeländer eller till en internationell organisation ska vara tillåten. Det anges att sådan överföring endast får ske under förutsättning att både den registeransvarige och registerföraren uppfyller de angivna villkoren i kapitel fem i förordningen samt även övriga bestämmelser i förordningen. Denna princip gäller även för vidare överföring av personuppgifter från tredjelandet eller den internationella organisationen, till ett annat tredjeland eller annan internationell organisation.[147] Sammanfattningsvis finns det tre olika möjligheter för att exportera personuppgifter till tredjeland, (1) om det föreligger ett beslut från EU-kommissionen om att ett tredjeland utgör en garant för en adekvat skyddsnivå[148], (2) om den registeransvarige har vidtagit lämpliga skyddsåtgärder genom ett juridiskt bindande instrument[149], eller (3) om ett av undantagen som anges i artikel 44 kan tillämpas.[150] Nedan kommer de nämnda möjligheterna att redogöras närmare för.

[142] Se förslag till allmän dataskyddsförordning artikel 17.
[143] Se förslag till allmän dataskyddsförordning artikel 22.
[144] Se bl.a. Rauhofer & Bowden (2013).
[145] Rauhofer & Bowden (2013), s. 9.
[146] Kuner (2013), s. 46 f.
[147] Se förslag till allmän dataskyddsförordning artikel 40.
[148] Förslag till allmän dataskyddsförordning artikel 41.
[149] Förslag till allmän dataskyddsförordning artikel 42.
[150] Förslag till allmän dataskyddsförordning artikel 44(1).

4.2.1 Artikel 41 – en adekvat skyddsnivå

Artikel 41 i förslaget föreskriver att överföring till tredjeland får ske efter beslut från EU-kommissionen om att tredjelandet eller den internationella organisationen ifråga utgör en garant för en adekvat skyddsnivå.[151] Denna bestämmelse motsvarar dataskyddsdirektivets artikel 25(6), men förslaget har även utvidgat EU-kommissionens befogenheter. Till skillnad mot dataskyddsdirektivets artikel 25(6), där EU-kommissionens befogenhet innebär att beslut om adekvat skyddsnivå fattas för ett tredjeland som helhet, innebär istället artikel 41 i förslaget att kommissionens befogenhet har vidgats till att även innefatta att beslut får fattas för ett territorium eller en behandlande sektor inom tredjelandet ifråga.[152] Vid sin bedömning av om ett tredjeland utgör en garant för en adekvat skyddsnivå, ska EU-kommissionen beakta och ta hänsyn till rättsstatsprincipen, om det finns möjlighet till effektiv rättsprövning i tredjelandet och om finns oberoende tillsynsmyndigheter.[153]

Rätten att kunna besluta om adekvat skyddsnivå för vissa sektorer inom ett tredjeland kommer vara av särskilt betydelse vad gäller molntjänster. EU-kommissionens vidgade befogenhet innebär att beslut kan fattas om att endast registeransvarigas och registerförares behandling av personuppgifter i tredjeland utgör en garant för adekvat skyddsnivå, detta trots att landet som helhet inte uppfyller de krav på dataskydd som EU uppställer. Ett sådant tillvägagångssätt kommer att gynna molntjänstindustrin, framförallt i länder som exempelvis USA där skydd för personlig integritet historiskt sett regleras inom specifika offentliga sektorer, som t.ex. inom hälsa och sjukvård.[154]

För att försäkra sig om att en adekvat skyddsnivå bibehålls samt att viss tillsyn utförs av EU, har LIBE-utskottet, i sitt yttrande över förslaget till allmän dataskyddsförordning,[155] föreslagit ett en *sunset*-bestämmelse ska införas gällande giltigheten av kommissionens beslut om adekvat skydds-nivå. Förslaget innebär att kommissionens beslut ska vara gällande i fem år efter förordningens ikraftträdande, såvida de inte ändrats, ersatts eller upphävts före utgången av denna period.[156] LIBE-utskottet har även föreslagit att EU-kommissionen ska inhämta ett yttrande från Europeiska dataskyddsstyrelsen[157] innan beslut om adekvat skyddsnivå fattas.[158] Dessutom anser LIBE-utskottet att kommissionen fortlöpande bör övervaka utvecklingen i tredjeländer och internationella organisationer, vilket kan påverka ett fattat beslut om adekvat skyddsnivå.[159] LIBE-utskottets förslag

[151] Jfr förslag till allmän dataskyddsförordning artikel 41(1).
[152] Kuner (2013), s. 47 och Rauhofer & Bowden (2013), s. 10.
[153] Jfr förslag till allmän dataskyddsförordning artikel 41(2).
[154] Rauhofer & Bowden (2013), s. 10 och Bradford (2012), s. 23.
[155] LIBE-utskottets förslag till ändringar i förslaget till allmän dataskyddsförordning antogs av Europaparlamentet den 12 mars 2014 utan några ändringar.
[156] Jfr Europaparlamentets betänkande, ändringsförslag 137, artikel 41(8).
[157] Genom förslag till allmän dataskyddsförordning artikel 64 fastslås att en europeisk dataskyddsstyrelse, bestående av representanter för de nationella dataskyddsmyndigheterna, ska inrättas. Europeiska dataskyddsstyrelsen ska ersätta Artikel 29-gruppen i deras arbete. Se förslag till allmän dataskyddsförordning, s. 14.
[158] Jfr Europaparlamentets betänkande, ändringsförslag 137, artikel 41(6a).
[159] Jfr Europaparlamentets betänkande, ändringsförslag 137, artikel 41(4a).

har ansetts bidra med viktiga förtydliganden och ändringar till förslaget om en allmän dataskyddsförordning. Det har dock ansetts att en sunset-bestämmelse inte får avse allt för kort period, eftersom det kan resultera i störningar i det internationella dataflödet och även komma att vara resurskrävande vad gäller att hantera förnyelse av beslut om adekvat skyddsnivå.[160]

4.2.2 Artikel 42 – lämpliga skyddsåtgärder

Internationell överföring av personuppgifter kommer även att vara tillåten om lämpliga skyddsåtgärder för personuppgifter vidtas genom juridisk bindande instrument.[161] Artikel 42 föreskriver således en möjlighet till tredjelandsöverföring när det inte föreligger något beslut om adekvat skyddsnivå.[162] Lämpliga skyddsåtgärder kan bl.a. ta formen av bindande företagsregler, standardiserade uppgiftsskyddsbestämmelser som antas av kommissionen, standardiserade uppgiftsskyddsbestämmelser som antagits av tillsynsmyndigheter, eller avtalsklausuler mellan den registeransvarige eller registerföraren och mottagaren av uppgifterna.[163]

Den föreslagna bestämmelsen motsvarar dataskyddsdirektivets artikel 26(4), vilken stadgar kommissionens rätt att anta modellklausuler.[164] Förslagets artikel 42(2)(c) innebär att denna möjlighet utvidgas ytterligare, eftersom även nationella tillsynsmyndigheter[165] kan anta modellklausuler som sedan kan tillämpas vid avtal om överföring av personuppgifter. Denna antagningsprocess ska följa en mekanism för enhetlighet och tillsynsmyndigheterna ska samarbeta inbördes samt med kommissionen. Processen innebär bl.a. att tillsynsmyndigheten ska inkomma med ett utkast av den planerade åtgärden till Europeiska dataskyddsstyrelsen och till kommissionen innan beslut fattas. Detta för att garantera en korrekt och enhetlig tillämpning av förordningen.[166] LIBE-utskottet har i sitt betänkande föreslagit att EU-kommissionens befogenhet att anta modellklausuler helt ska tas bort, och att denna befogenhet endast ska tilldelas de nationella tillsynsmyndigheterna.[167] Viss kritik har riktats mot denna utvidgning av de nationella tillsynsmyndigheternas beslutanderätt. Även om de nationella tillsynsmyndigheterna måste anta modellklausulerna i enlighet med den nya mekanismen för enlighet, finns det kritiker som menar att antagandet av modellklausuler på medlemsstatsnivå inte överensstämmer med

[160] Hon m.fl. (2014), s. 33 och 36.
[161] Se förslag till allmän dataskyddsförordning artikel 42(1).
[162] Förslag till allmän dataskyddsförordning, s. 12.
[163] Se förslag till allmän dataskyddsförordning artikel 42(2).
[164] Se ovan avsnitt 3.2.2.3. De krav som måste uppfyllas enligt förslag till allmän dataskyddsförordning artikel 43(2) är exempelvis att företagsbestämmelserna ska innehålla uppgifter om vilka överföringar som avser att omfattas av bestämmelserna vilken typ av behandling som avser utföras på uppgifterna, att den registeransvarige eller registerförare som är etablerad inom unionen ska ta på sig ansvaret om en enhet i företagsgruppen som inte är etablerad i unionen bryter mot de bindande företagsbestämmelserna etc.
[165] Med tillsynsmyndigheter avses en offentlig myndighet som är etablerad av en medlemsstat med ansvar för att övervaka tillämpningen av förordningen och medverka till dess enhetliga tillämpning i hela unionen. Se förslag till allmän dataskyddsförordning artikel 4(19) och 46.
[166] Se förslag till allmän dataskyddsförordning artikel 42(2)(c), 57 och 58.
[167] Jfr Europaparlamentets betänkande, ändringsförslag 138, artikel 42(2).

förordningens övergripande mål om att harmonisera reglerna inom unionen. Uppfattningen är att förslaget är ”företagsvänligt” och leder till en förstärkning av risken för ”*forum shopping*”[168] hos icke-EU baserade företag när dessa företag beslutar om etablering inom EU.[169]

Vidare lagstadgas rätten att tillämpa BCR:s genom förslagets artikel 42(2)(a), vilka måste godkännas av en tillsynsmyndighet i enlighet med förordningens artikel 43. Att tillämpningen av BCR:s lagstadgas är ett steg i riktning mot en harmoniserad union, eftersom BCR:s tidigare inte varit accepterade av vissa medlemsstater.[170] I artikel 43 beskrivs i detalj de villkor som måste uppfyllas för överföringar genom BCR:s. Utgångspunkt för dessa villkor är de nationella tillsynsmyndigheternas nuvarande praxis och krav, och är således i allmänhet liknande de krav som Artikel 29-gruppen angivit.[171] Tillämpningen av BCR:s begränsas i förslaget till förordningen, till en registeransvarig eller en registersförares företagsgrupp och dess anställda. Detta innebär således att förordningen öppnar upp för användning av BCR:s vad gäller avtal mellan registerförare, vilket tidigare även tillåtits av Artikel 29-gruppen.[172] EU-kommissionen bibehåller också viktiga befogenheter gällande antagande av delegerade akter samt precisering av vilket format och vilka rutiner som ska tillämpas vid utformandet av BCR:s.[173]

Det förekommer ett visst ifrågasättande angående hur tillämpligt och gynnande de nya reglerna om BCR:s kommer att vara beträffande molntjänster. De nya reglerna har även kritiserats för att endast gynna stora multinationella företag, och att det finns därför ett behov av att införa en möjlighet för överföring av personuppgifter som även kan tillämpas av mindre företag.[174] Liksom tidigare finns det inte någon bestämmelse i förslaget som möjliggör tillämpandet av BCR:s vid ett affärsförhållande mellan exempelvis en registerförare och en utomstående underleverantör, vilken inte ingår i den aktuella företagsgruppen.[175] LIBE-utskottet har dock föreslagit att BCR:s ska kunna tillämpas av registeransvariga och register-förare, men även av ”dess externa underleverantörer som omfattas av de bindande företagsreglerna”.[176] För att underlätta det transnationella dataflödet har detta ansetts som en viktig ändring att införa i förslaget till förordning.[177]

---

[168] ”Forum shopping” är ett begrepp inom den internationella privaträtten vilket åsyftar de situationer när en enskild person eller ett företag väljer att exempelvis etablera sig eller väcka talan i ett specifikt land p.g.a. att detta land erbjuder lagregler som anses mest förmånliga för den aktuella enskilda personen eller företaget.
[169] Rauhofer & Bowden (2013), s. 10.
[170] Hon m.fl. (2014), s. 33 och Gilbert (2012), s. 25.
[171] Förslag till allmän dataskyddsförordning, s. 12 och artikel 43(1) och (2). Jfr även avsnitt 3.2.2.2.
[172] Kuner (2013), s. 47.
[173] Se förslag till allmän dataskyddsförordning artikel 43(3) och (4).
[174] Kuner (2013), s. 49.
[175] Hon m.fl. (2014), s. 33.
[176] Jfr Europaparlamentets betänkande, ändringsförslag 139, artikel 43(1)(a) och 43(2)(a).
[177] Hon m.fl., s. 33 f och 36.

4.2.3 Artikel 44 – tillämpliga undantag

I artikel 44 i förslaget till allmän dataskyddsförordning redogörs och klargörs det för de undantag som tillåter en överföring av personuppgifter till tredjeland, trots att en adekvat skyddsnivå eller lämpliga skyddsåtgärder inte föreligger. Utgångspunkten för dessa undantag är de befintliga bestämmelserna om undantag i dataskyddsdirektivets artikel 26. Undantagen avser att främst vara tillämpliga på överföringar av personuppgifter till tredjeländer som är nödvändiga för att skydda viktiga samhälleliga intressen. Exempel på sådana intressen anges av kommissionen vara överföringar av uppgifter mellan konkurrensmyndigheter och social-försäkringsmyndigheter.[178]

I artikel 44(1)(a) anges att en överföring är tillåten när det föreligger ett samtycke från den registrerade. Detta undantag har dock begränsats mer än bestämmelsen om samtycke i det nu gällande dataskyddsdirektivet. Enligt det föreliggande förslaget är ett samtycke från den registrerade endast vara giltigt om vederbörande har blivit informerad om de risker en överföring kan medföra när det inte föreligger något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder.[179] Anledningen till denna skräpning av reglerna är troligtvis den förekommande ovetskapen bland enskilda personer angående vad de samtycker till när det gäller behandling av deras personuppgifter i olika sammanhang.[180]

Ytterligare en viktig förändring är införandet av artikel 44(1)(h), vilken föreskriver att överföring får ske om det är nödvändigt för att tillgodose den registeransvariges eller registerförarens berättigade intressen. Denna överföring får dock inte vara ofta förekommande eller omfattande och får endast förekomma sedan omständigheterna för den aktuella åtgärden har bedömts och dokumenterats.[181] En sådan överföring kräver att den nationella tillsynsmyndigheten underrättats.[182] Anmärkningsvärt är dock att det inte krävs något godkännande av den nationella tillsynsmyndigheten.[183] LIBE-utskottet har i sitt ändringsförslag tagit bort denna möjlighet till överföring.[184] Det faktum att överföringen inte får vara ofta förekommande eller omfattande, bör däremot utesluta ett missbruk av bestämmelsen från molntjänstindustrins sida, eftersom överföringar inom denna sektor är ofta förekommande och avser stora mängder personuppgifter.[185]

4.2.4 Den borttagna artikeln avseende utlämnande av personuppgifter

Värt att nämna vad gäller skyddet för personuppgifter vid överföring till tredjeländer är den borttagna artikeln ur utkastet till förordningen som

[178] Förslag till allmän dataskyddsförordning, s. 12.
[179] Se förslag till allmän dataskyddsförordning artikel 44(1)(a).
[180] Kuner (2013), s. 48.
[181] Jfr förslag till allmän dataskyddsförordning, s. 12 och artikel 44(1)(h).
[182] Se förslag till allmän dataskyddsförordning artikel 44(6).
[183] Kuner (2013), s. 48.
[184] Se Europaparlamentets betänkande, ändringsförslag 141, artikel 44(1).
[185] Hon m.fl. (2014), s. 34 och Kuner (2013), s. 48.

presenterades i november 2011.[186] Denna borttagna artikel reglerade överföringar och utlämningar av personuppgifter som inte var tillåtna enligt EU-rätten. Artikeln föreskrev att domar och beslut som meddelas av domstolar eller andra myndigheter i ett tredjeland, vilka ålägger en registeransvarig eller en registerförare att lämna ut personuppgifter får inte erkännas eller verkställas inom unionen. Sådana domar och beslut får endast erkännas och verkställas mot bakgrund av fördrag om ömsesidig rättslig hjälp eller ett gällande internationellt avtal mellan det tredjeland som framställer begäran och unionen eller en medlemsstat.[187] Mottas en begäran om utlämning av personuppgifter av en registeransvarig eller en registerförare, ska detta anmälas till den nationella tillsynsmyndigheten. Tillsynsmyndigheten har sedan befogenhet att pröva begäran och bedöma om den är förenlig med dataskyddsförordningen.[188] Artikeln är som ovan nämnt borttagen i kommissionens presenterade förslag från den 25 januari 2012.[189] LIBE-utskottet har dock föreslagit att en nästintill identisk bestämmelse införs i förordningen.[190]

Ett borttagande av denna bestämmelse har ansetts ge upphov till specifika risker relaterade till användningen av molntjänster i de fall när behandling sker av aktörer etablerade utanför EU. Ett återinförande av bestämmelsen skulle medföra större rättssäkerhet för den registrerade.[191] Sett ur ett företags- och molntjänstsammanhang kan bestämmelsen medföra problem när företaget enligt ett tredjelands lag är skyldiga att utlämna uppgifter. Det kan också medföra en stor belastning för de nationella tillsyns-myndigheterna, eftersom de enligt förslaget har en skyldighet att förhandspröva varje begäran om utlämning.[192]

[186] Utkast 56 om förslag till allmän dataskyddsförordning.
[187] Jfr utkast 56 om förslag till allmän dataskyddsförordning, artikel 42(1).
[188] Jfr utkast 56 om förslag till allmän dataskyddsförordning, artikel 42(2) – (4).
[189] I förslaget till allmän dataskyddsförordning uppmärksammas i ingresspunkt 90 problemet med tredjeländers lagar och andra författningar. Där anges att en extraterritoriell tillämpning av dess lagar kan strida mot internationell rätt och inverka menligt på det skydd av enskilda som garanteras inom unionen.
[190] Se Europaparlamentets betänkande, ändringsförslag 140, artikel 43a (ny).
[191] Rauhofer & Bowden (2013), s. 11 och Hon m.fl., s. 35.
[192] Hon m.fl., s. 35.

5 Rätt till personlig integritet – en mänsklig rättighet

Rätten till personlig integritet är i Europa sedan länge en erkänd mänsklig rättighet. Som det redogjorts för i framställningen ovan innebär tillkomsten av molntjänster och Internet många nya möjligheter för företag, myndigheter och enskilda personer, men samtidigt innebär det också nya utmaningar och risker bl.a. vad gäller intrång i enskilda personers rätt till personlig integritet.[193]

Följande kapitel redogör för vilken rätt till respekt för privatlivet samt skydd av personuppgifter som EU-medborgare har i dagens digitaliserade samhälle enligt de två regelverken Europakonventionen och EU-stadgan. Kapitlet kommer även att ge en bild av vilka åtgärder som har ansetts utgöra otillåtna inskränkningar i rätten till respekt för privatlivet och skydd av personuppgifter, vid behandling av dessa personuppgifter.

5.1 Rätt till personlig integritet enligt Europakonventionen

Europakonventionen utarbetades som en följd av de många övergrepp som skedde mot enskilda personer under andra världskriget och mellankrigstiden.[194] Europakonventionen avser att garantera ett skydd för enskildas friheter och rättigheter och består av själva Europakonventionen och ytterligare tolv tilläggsprotokoll.[195] Tolkning och verkställighet av Europakonventionen sker av Europadomstolen. En talan om kränkning av en rättighet skyddad i Europakonventionen kan väckas mot en konventionsstat av andra konventionsstater eller av enskilda sökanden, vilka är bosatta i en konventionsstat. Vidare krävs det att den sökande påverkas av den aktuella kränkningen av Europakonventionen.[196]

5.1.1 Kort om EU:s relation till Europakonventionen

Europarådet består för närvarande av 47 medlemsländer, vilka alla är anslutna och bundna att efterfölja Europakonventionen. Bland dessa konventionsstater återfinns även alla medlemsstater i EU.[197] I och med Lissabonfördragets ikraftträdande 2009 stadgades det i FEU artikel 6(2) att

[193] Rauhofer (2014), s. 1.
[194] Danelius (2012), s. 18 f och Rauhofer (2008), s. 192 f.
[195] Mowbray (2012), s 1.
[196] van Dijk, s. 32 f.
[197] Se Danelius (2012), s. 21.

EU har för avsikt att ansluta sig till Europakonventionen. Även i Europakonventionens fjortonde tilläggsprotokoll, som ännu inte trätt ikraft, anges det att EU kan bli part av konventionen.[198] Förhandlingar angående EU:s anslutning avslutades i april 2013 och EU-domstolen ska nu ges tillfälle att yttra sig angående anslutningsavtalet.[199] EU-domstolen har redan sedan tidigare uttalat sig i flertalet avgöranden att Europakonventionens principer och Europadomstolens praxis ska vara vägledande och respekteras av EU:s institutioner i deras arbete.[200]

Europadomstolen har även behandlat frågan gällande i vilken utsträckning konventionsstaterna kan bli föremål för tillsyn gällande kompabilitet med principerna om mänskliga rättigheter när de agerar inom unionsrättens område. Uttalat är att ett agerande från en konventionsstat, exempelvis implementering av ett EU-rättsligt direktiv som innebär en viss godtycklig bedömning från medlemsstaten vid tillämpningen, kan innebära en överträdelse av förpliktelserna i Europakonventionen och således leda till att konventionsstaten ställs till svars inför Europadomstolen.[201] Om en medlemsstat däremot tillämpar en EU-förordning, som inte lämnar utrymme för ett godtyckligt tillämpande av den enskilda nationella staten, kan ansvar för överträdelser av Europakonventionen inte uppkomma. Det kan således konstateras att det uppkommer en lucka i verkställigheten av Europakonventionen vid tillämpningen av viss EU-lagstiftning. Denna lucka kan endast upphöra genom EU:s anslutning till Europakonventionen.[202]

5.1.2 Artikel 8 – rätten till respekt för privatlivet

Europakonventionen artikel 8(1) stadgar att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Artikeln utgör både en positiv och en negativ rättighet för den enskilde. Den innebär dels en förpliktelse för konventionsstaten att inte vidta åtgärder som innebär ett ingrepp i den skyddade rättigheten, dels ålägger den konventionsstaten att vidta positiva åtgärder för att skydda den enskildes privatliv.[203] En konventionsstat kan således bli ansvarig för kränkning av en enskilds rättigheter om det visar sig att det rättsliga skyddet för den enskilde har varit otillräckligt. De krav på skyddsåtgärder som ska vidtas av staten måste dock vara rimliga. Det som kan förväntas av en konventionsstat är att staten utfärdar lagar som ger ett tillfredställande skydd åt medborgarnas privatliv.[204]

Rätten till respekt för privatlivet är en svårdefinierad rättighet med många aspekter. Europadomstolens praxis angående rättighetens innebörd är omfattande och utvecklas ständigt.[205] Praxis har framförallt berört vad som

[198] Se tilläggsprotokoll 14, artikel 17.
[199] Rainey m.fl. (2014), s. 18 f.
[200] Se mål C-238/99 P *Limburgse Vinyl Maatschappij m.fl.* mot *kommissionen*, C-244/99 P *DSM och DSM Kunststoffen* mot *kommissionen* och C-301/04 *Europeiska kommissionen* mot *SGL Carbon AG*. Jfr även FEU artikel 6(3).
[201] *Dangeville SA* mot *Frankrike*, p. 38 och Rainey m.fl. (2014), s. 17.
[202] Rainey m.fl. (2014), s. 17.
[203] Danelius (2012), s. 347.
[204] Ibid, s. 347.
[205] van Dijk (2006), s. 664 f.

omfattas av begreppet privatliv och Europadomstolen har uttalat att det varken är möjligt eller nödvändigt att ge begreppet en uttömmande definition.[206] Praxis anger att begreppet omfattar olika dimensioner av en enskilds fysiska och psykiska integritet. Privatlivet har av Europadomstolen ansetts omfatta bl.a. ett skydd för enskilda från att utsättas för åtgärder vilket rör behandling lagring och användning av information om den enskildes hälsa[207], sexuella läggning[208], biometriska information (exempelvis DNA-prov och fingeravtryck)[209] och foton föreställande den enskilde individen.[210] Vidare har det ansetts att en systematisk insamling och lagring av personuppgifter av statliga myndigheter kan utgöra en kränkning av rätten till privatliv.[211] Beroende på omständigheterna i varje enskilt fall kan artikel 8 anses ställa krav på behandling av personuppgifter i tre avseenden; dels i fråga om rätt för den enskilde att själv få del av uppgifterna, dels i fråga om skydd mot att tredje part får tillgång till uppgifterna.[212]

Det kan således konstateras rättigheten även inkluderar ett skydd av personuppgifter. Majoriteten av den personliga information som laddas upp i molnet av EU-medborgare eller EU-baserade företag och organisationer, kan följaktligen antas utgöra sådan personlig information som omfattas av Europakonventionens artikel 8(1).[213]

5.1.3 Inskränkningar i rätten till respekt för privatlivet

Rätten till skydd av privatlivet och den personliga integriteten i Europakonventionen artikel 8 är inte en absolut rättighet. I konventionens artikel 8(2) föreskrivs att ingrepp i rättigheten endast är tillåten om det är motiverat med hänsyn till bl.a. statens nationella säkerhet. För att en inskränkning ska vara tillåten krävs det att tre förutsättningar är uppfyllda. Dessa förutsättningar innebär att inskränkningen ska ha stöd i lag, vara nödvändig i ett demokratiskt samhälle, samt vara ägnad att tillgodose allmänna eller enskilda intressen. Nämnda förutsättningar redogörs för närmare i följande avsnitt.

5.1.3.1 Ingreppet ska ha stöd i lag

En förutsättning för att ingrepp i enskilds privatliv ska vara accepterat är att åtgärden har stöd i lag.[214] Den nationella bestämmelse som tillåter en åtgärd som innebär ett ingrepp i rättigheten, måste vara utformad på ett precist sätt samt vara tillgänglig för allmänheten. Vidare ska bestämmelsens

[206] Jfr *Niemietz* mot *Tyskland* [1992] och *Peck* mot *Förenade Konungariket* [2003].
[207] Se exempelvis *Z* mot *Finland* [1997].
[208] Se exempelvis *Bensaid* mot *Förenade Konungariket* [2001] och *Peck* mot *Förenade Konungariket* [2003].
[209] Se *S och Marper* mot *Förenade Konungariket* [2009].
[210] Se *Sciacca* mot *Italien* [2005].
[211] Se *Rotaru* mot *Rumänien* [2000], p. 43.
[212] SOU 2008:3, s. 78.
[213] Rauhofer & Bowden (2013), s. 18.
[214] Jfr Europakonventionen artikel 8(2).

konsekvenser vara förutsägbara för den enskilde.[215] Detta innebär således att i den rättsliga grunden för exempelvis insamling, lagring och utlämnande av personuppgifter måste det även finnas fastställda och tydliga gränser över ingreppets omfattning, karaktär och beskaffenhet. Framförallt måste det finnas skyddsåtgärder som avser att förhindra missbruk av personuppgifter och andra oproportionerliga åtgärder.[216]

5.1.3.2 *Ingreppet ska vara nödvändigt i ett demokratisk samhälle samt ägnat att tillgodose allmänna eller enskilda intressen*

Utöver att den ingripande åtgärden ska ha stöd i lag, krävs det att åtgärden är nödvändig i ett demokratiskt samhälle.[217] Europadomstolen har anfört att begreppet ”nödvändigt” i detta sammanhang inte är synonymt med ”oundgänglig”. Avsikten är istället att det ska föreligga ett angeläget samhälleligt behov vilket motiverar att ett ingrepp i rättigheten sker. Vid bedömning av om ett sådant samhälleligt behov föreligger, ska hänsyn tas till om ingreppet står i rimlig proportion till det syfte som avses uppnås genom åtgärden.[218] För att bedöma detta gör Europadomstolen en proportionalitetsbedömning, där den enskildes intresse för sin personliga integritet vägs mot det allmänna intresse åtgärden avser att uppfylla.[219] Konventionsstaterna har dock en viss frihet att avgöra huruvida ett ingrepp från staten ska vara tillåten. Denna frihet benämns som en konventionsstats skönsmarginal.[220] Detta innebär att om en konventionsstat har ansett att ett ingrepp uppfyller förutsättningarna samt är proportionerligt, godtar Europadomstolen som utgångspunkt denna bedömning. Omfattningen av skönsmarginalen varierar beroende på arten av det skyddade intresset. En stat har exempelvis en större frihet i sin bedömning när det gäller ett tillvaratagande intresse som rör den nationella säkerheten.[221]

5.1.4 Praxis från Europadomstolen

Europadomstolens rättspraxis gällande skydd av personuppgifter domineras av avgöranden som rör konventionsstaters övervakning av enskilda inom statens eget territorium.[222] Detta avsnitt avser att ge en förståelse för vilken typ av personlig information som ansetts ingå i begreppet privatliv, samt hur Europadomstolen har argumenterat kring huruvida ingreppen i rättigheten har ansetts uppfylla de förutsättningar som krävs för att vara en tillåten inskränkning i enlighet med artikel 8(2).

[215] Jfr exempelvis *Malone* mot *Förenade Konungariket* [1984], p. 66.
[216] Jfr Europadomstolen uttalande i *Segerstedt-Wiberg m.fl.* mot *Sverige* [2006], p. 76 och *M.M.* mot *Förenade Konungariket* [2012], p. 195 ff.
[217] Jfr EKMR artikel 8(2).
[218] Danelius (2012), s. 351 och van Dijk m.fl. (2006), s. 750.
[219] Rainey m.fl. (2014), s. 114 ff.
[220] Se exempelvis *Handyside* mot *Förenade Konungariket* [1976], p. 47. Skönsmarginal är den svenska översättningen av begreppet ”*margin of appreciation*”.
[221] Danelius (2012), s. 51 f och 351 f.
[222] Rauhofer & Bowden (2013), s. 19.

5.1.4.1 Amann mot Schweiz

Bakgrunden till detta mål är en man som 1981 blev registrerad av den schweiziska åklagarmyndigheten genom att en schweizisk myndighet hade avlyssnat ett telefonsamtal där han deltog. Informationen som registrerades skrevs på ett kort och nämnde bl.a. att mannen var en affärsman samt att mannen hade haft kontakt med den ryska ambassaden.[223] När mannen ca. 10 år senare fick kännedom om denna registrering begärde mannen ut informationen för att kontrollera det myndigheterna hade registrerat. Mannen fick ut informationen, men det fanns då två avsnitt i dokumentet som var överstrukit med blått. Mannen försöker förgäves att få ta del av den överstrukna delen men utan resultat. De schweiziska domstolarna ansåg att sökanden inte hade drabbats av en allvarlig överträdelse av hans personliga integritet.[224] Mannen hävdade därmed att hans rätt till respekt för privatlivet hade kränkts.[225]

Europadomstolen konstaterade att den information som hade registrerat på kortet onekligen innehöll uppgifter om mannens privatliv och att Europakonventionens artikel 8(1) således var tillämplig.[226] Ett kort som innehåller uppgifter om en persons privatliv utgör enligt domstolen ett ingrepp i privatlivet. Det spelar här ingen roll om uppgifterna som samlats in om mannen var känsliga eller inte, det är tillräckligt att uppgifter om privatlivet har lagrats av en myndighet för att ett ingrepp ska föreligga.[227]

Frågan som därefter skulle besvaras var huruvida åklagarmyndighetens lagring av detta kort utgjorde ett rättfärdigat ingrepp i privatlivet. Europadomstolen uttalar att både upprättandet av kortet samt lagringen av det samma, utgjorde ett ingrepp i mannens privatliv vilket inte hade stöd i den schweiziska lagstiftningen. Schweizisk lag ansågs inte kunna tillförsäkra den enskilde en tillräcklig tydlighet vad gällde villkoren för utnyttjandet av informationen av de offentliga myndigheterna. Med beaktande av den slutsatsen ansåg Europadomstolen det inte vara nödvändigt att undersöka huruvida de övriga kraven i artikel 8(2) var uppfyllda. Registreringen av kortet med information om mannens privatliv ansågs därför utgöra en otillåten kränkning av rätten till respekt för privatlivet.[228]

5.1.4.2 Rotaru mot Rumänien

Sökanden hade i detta fall dömts till ett års fängelse 1948 för att ha uttryckt kritik mot den dåvarande kommunistiska regimen i Rumänien. I början på 1990-talet väckte han talan mot staten för att beviljas vissa rättigheter som tidigare förföljd av kommunistregimen. I denna talan lades det fram bevisning från rumänska underrättelsetjänsten i form av ett brev innehållande uppgifter om mannens tidigare studier, politiska engagemang samt information om medlemskap i en högerextrem rörelse. Dessa uppgifter

[223] *Amann mot Schweiz* [2000], p. 10 – 15.
[224] Ibid, p. 20 – 30.
[225] Ibid, p. 42.
[226] Ibid, p. 65 – 67.
[227] Ibid, p. 70.
[228] Ibid, p. 80 – 81.

var enligt mannen felaktiga och han menade att lagring av dessa uppgifter utgjorde ett intrång i hans rätt till respekt för privatlivet.[229] Europadomstolen ansåg att både lagringen och användningen av dessa personuppgifter, i kombination med en vägran att låta den sökande korrigera uppgifterna, utgjorde ett ingrepp Europakonventionens artikel 8(1), rätten till respekt för privatlivet.[230]

Europadomstolen bedömde även huruvida ingreppet var en accepterad åtgärd i enlighet med artikel 8(2). Det konstaterades dock att innehavet och användningen av den personliga informationen inte hade stöd i rumänsk lag. Vidare konstaterade domstolen att ingen bestämmelse i den nationella rätten fastställde några gränser för utövandet av insamling och arkivering av information. Istället var begränsningarna av åtgärden beroende av en skönsmässig bedömning av offentliga myndigheter.[231] Sammanfattningsvis var förutsättningarna i artikel 8(2) inte uppfyllda och ingreppet utgjorde därmed en kränkning av mannens privatliv.

5.2 Rätt till personlig integritet enligt EU-stadgan

Inom EU stadgas EU-medborgarnas fundamentala rättigheter i EU-stadgan, som fick bindande juridisk rättsverkan först genom Lissabonfördragets ikraftträdande 2009.[232] Syftet med stadgan är att stärka skyddet av grundläggande rättigheter, mot bakgrund av samhällsutvecklingen, de sociala framstegen och den vetenskapliga och tekniska utvecklingen, genom att göra rättigheterna synliga för EU-medborgarna.[233]

Rättigheterna i EU-stadgan bygger till stor del på de garanterade rättigheterna i Europakonventionen med vissa skillnader vad gäller dess lydelser.[234] EU-stadgans artikel 52(3) föreskriver även att i den mån stadgans rättigheter motsvarar rättigheter garanterade i Europakonventionen, är avsikten och omfattningen av stadgans rättigheter densamma som i konventionen. Detta trots att EU-lagstiftningen i vissa fall kan ge ett mer omfattande skydd.

Kapitel två i EU-stadgan stadgar de grundläggande friheterna. EU-medborgarnas rätt till personlig integritet skyddas genom två rättigheter, artikel 7 som stadgar rätten till respekt för privatlivet och artikel 8 som stadgar en specifik rättighet för skydd av personuppgifter. Skydd av personlig information utgör dessutom en princip enligt FEUF artikel 16, där det anges att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

[229] *Rotaru* mot *Rumänien* [2000], p. 7 – 14.
[230] Ibid, p. 44.
[231] Ibid, se Europadomstolens argumentation under avsnitt 2.
[232] Rainey m.fl. (2014), s. 19.
[233] Se ingress till EU-stadgan.
[234] Rainey m.fl., (2014), s. 19.

5.2.1 Artikel 7 – rätt till respekt för privatlivet

I artikel 7 i EU-stadgan föreskrivs rätten till respekt för privatlivet. Rättigheten omfattar ett antal olika dimensioner av privatlivet och ska enligt EU-domstolen i sin praktiska tillämpning överensstämma med Europakonventionens artikel 8, så som den tolkats av Europadomstolen.[235] Kopplingen till Europakonventionen innebär således att artikel 7 i EU-stadgan främst ska tolkas i ljuset av Europakonventionen, och i andra hand i ljuset av EU-stadgans artikel 1.[236]

Artikel 7 skyddar bl.a. den enskildes kommunikationer, med vilket åsyftas alla former av utbyte av information som exempelvis telekommunikationer och data- eller internettrafik. Enligt praxis innebär detta i praktiken en rätt till skydd i samband med behandling, lagring och spridning av olika typer av personlig information.[237] Detta skydd överlappas till stor del av skyddet för den enskildes personuppgifter, vilket kommer att presenteras närmare nedan.[238]

5.2.2 Artikel 8 – rätt till skydd av personuppgifter

EU-stadgans artikel 8 stadgar rätten till skydd av personuppgifter som en rättighet skild från rätten till respekt för privatlivet. Införandet av en självständig rätt till uppgiftsskydd skiljer sig således från Europakonventionen, där personuppgiftsskyddet istället behandlas som en del av rätten till privatliv.[239] Artikel 8 har både i praxis och doktrin ansetts omfatta ett bredare spektrum av uppgifter och uppgiftsbehandlande åtgärder än rätten till privatliv. Med andra ord avser rätten till skydd av personuppgifter ge enskilda större kontroll över fler typer av personlig information. Personuppgiftsskyddet bör därför ses som en rättighet som i stor utsträckning överlappar rätten till privatliv, men som även garanterar enskilda ett större personuppgiftsskydd.[240]

Praxis från EU-domstolen gällande rätten till skydd för personuppgifter är fortfarande relativt begränsad. EU-domstolen har vid sin tolkning av EU-stadgans artikel 7 och 8 tagit hänsyn till Europadomstolens praxis och uttalat att dessa rättigheter avser att skydda all information som relaterar till en identifierad eller oidentifierad enskild person.[241] Det har i EU-rätten

[235] Jfr exempelvis de förenade målen C-92/09 och 93/09 *Volker und Markus Schecke GbR och Hartmut Eifert* mot *Land Hessen*, p 47 – 50 och de förenade målen C-293/12 och C-594/12 *Digital Rights Ireland Ltd* mot *Minister for Communications, Marine and Natural Resources m.fl. och Kärntner Landesregierung m.fl.*, p. 47.

[236] Lebeck (2013), s. 115. Artikel 1 i EU-stadgan föreskriver att den mänskliga värdigheten är okränkbar. Skyddet för den mänskliga värdigheten är en princip som ska ligga till grund för tolkningen av EU-stadgan i allmänhet.

[237] Se exempelvis de förenade målen C-92/09 och 93/09 *Volker und Markus Schecke GbR och Hartmut Eifert* mot *Land Hessen* och *Eifert*, p. 50.

[238] Lebeck (2013), s. 128.

[239] Jfr avsnitt 3.1.2 och Lynskey (2014), s. 570.

[240] Se bl.a. Lynskey (2014), s. 579 ff, Tzanou (2013), s. 90 f och Kokott & Sobotta (2013), s. 225 f.

[241] Se de förenade målen C-92/09 och 93/09 *Volker und Markus Schecke GbR och Hartmut Eifert* mot *Land Hessen*, p. 52. EU-domstolen hänvisade där till Europadomstolens uttalande i *Amann mot Schweiz* [2000] och *Rotaru mot Rumänien* [2000]. För redogörelse av de två sistnämnda målen, se avsnitt 5.1.4.

vidare gjorts en distinktion mellan olika typer av personuppgifter. Distinktionen baseras på hur betydelsefulla och integritetskänsliga uppgifterna har bedömts vara. Uppgifter som berör en enskilds hälsotillstånd, sexuella läggning och liknande har i praxis ansetts besitta ett starkare skydd än t.ex. uppgifter om kön, ålder eller yrke.[242] Det har även uttalats att skyddet för personuppgifter som uppstår i samband med kommersiella verksamheter har ett svagare skydd än det som uppstår vid icke-kommersiella sammanhang.[243]

Personuppgifter ska vidare, enligt EU-stadgan artikel 8(2), behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Enskilda personer ska ha rätt till tillgång till insamlade uppgifter som rör honom eller henne, samt att få rättelse av dem. Artikelns tredje punkt föreskriver vidare ett krav på att det såväl inom EU som i medlemsstaterna ska finnas oberoende institutioner som kontrollerar efterlevnaden av kravet på skydd av personuppgifter.[244] Skydd av personuppgifter regleras även i EU:s sekundärrätt, bl.a. i EU:s dataskyddsdirektiv.

Det argumenteras för att rätten till skydd av personuppgifter innebär ett informationellt självbestämmande för den enskilde. Ett informationellt självbestämmande innebär att EU-medborgare, i den mån de själva vill, kan sprida information om sig själva så länge denna spridning inte påverkar andra enskilda personer.[245]

5.2.3 Inskränkningar i EU-stadgans rättigheter

Liksom Europakonventionens artikel 8 är EU-stadgans artikel 7 och 8 inte absoluta rättigheter. EU-stadgans artikel 52(1) föreskriver att begränsningar av rättigheterna i vissa fall kan vara tillåtna. Begränsningar eller ingrepp i stadgans rättigheter måste vara föreskriven i lag och vara förenlig med det väsentliga innehållet i dessa rättigheter. Inskränkningar i rätten till privatliv och skydd av personuppgifter är med andra ord tillåtet om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors fri- och rättigheter. Det framgår också att det vid denna bedömning ska tas hänsyn till proportionalitetsprincipen.[246] EU-domstolens fasta praxis gällande proportionalitetsprincipen anger att för att en inskränkning i en rättighet ska vara godtagbar måste två förutsättningar vara uppfyllda. För det första måste den åtgärd som inskränkningen innebär vara ägnad att uppnå de legitima mål som eftersträvas. För det andra får åtgärderna inte gå utöver vad som är lämpligt och nödvändigt för att uppnå de eftersträvade målen. Bedömningen måste göras i varje enskilt fall utifrån de där givna förutsättningarna.[247]

---

[242] Lebeck (2013), s. 131.
[243] Se C-324/09 *L'Oréal SA m.fl.* mot *eBay International AG m.fl.*, p. 141 – 144.
[244] Ett motsvarade krav återfinns även i dataskyddsdirektivet.
[245] Lebeck (2014), s. 132 och Lynskey (2014), s. 589 ff.
[246] Jfr EU-stadgan artikel 52(1).
[247] Se exempelvis de förenade målen C-92/09 och 93/09 *Volker und Markus Schecke GbR och Hartmut Eifert* mot *Land Hessen*, p. 74, C-283/11 *Sky Österreich GmbH* mot *Österreichischer Rundfunk*, p. 50, och C-101/12 *Herbert Schaible* mot *Land Baden-Württemberg*, p. 29.

5.2.4 Praxis från EU-domstolen

Nedan presenteras relevant praxis från EU-domstolen samt en begäran om förhandsavgörande från EU-domstolen, avseende förhållandet mellan behandling av personuppgifter och rätten till respekt för privatlivet och skydd av personuppgifter.

5.2.4.1 Digital Rights Ireland

I de förenade målen C-293/12 och C-594/12 prövade EU-domstolen giltigheten av direktiv 2006/24/EG (datalagringsdirektivet).[248] Begäran om förhandsavgörande kom från nationella domstolar i Irland respektive Österrike. I Irland väckte ett bolag, vid namn Digital Rights, talan gällande lagligheten av nationella lagstiftnings- och myndighetsåtgärder avseende lagring av uppgifter om elektroniska kommunikationer. Digital Rights yrkade bl.a. att den nationella domstolen skulle ogiltigförklara datalagrings-direktivet och de nationella genomförandebestämmelserna. Detta p.g.a. att nationella genomförandebestämmelser bl.a. föreskrev att leverantörer av telefonitjänster var skyldiga att lagra uppgifter under en viss tid för att förebygga, avslöja och utreda brott, samt för att garantera statens säkerhet. Målet i Österrike hade sitt ursprung i flera mål där parter även där yrkat på ogiltigförklaring av nationell lagstiftning vilkas syfte har varit att införliva datalagringsdirektivet. De nationella domstolarna ställde mot denna bakgrund frågan till EU-domstolen huruvida lagring av personlig data i enlighet med datalagringsdirektivet var förenligt med artikel 7 och 8 i EU-stadgan.[249]

EU-domstolen inleder med att konstatera att datalagringsdirektivet innehöll bestämmelser vilket sammantaget gjorde det möjligt att dra mycket precisa slutsatser om enskilda personers privatliv vars uppgifter lagrades hos olika företag och myndigheter. De enskildas vanor i vardagslivet, deras stadig-varande och tillfälliga uppehållsorter, deras dagliga förflyttningar, de aktiviteter de utövar, deras sociala relationer och deras umgängeskretsar de rör sig i, utgjorde exempel på uppgifter som lagrats genom enskildas telefonabonnemang eller andra kommunikationsnät.[250] EU-domstolen konstaterar, i likhet med generaladvokatens uttalande i sitt förslag till avgörande,[251] att redan lagringsskyldigheten i fråga om de aktuella uppgifterna avseende personers privatliv utgör ett ingrepp i de rättigheter artikel 7 och 8 i EU-stadgan avser att skydda. Ett ingrepp i rättigheterna skedde även när nationella myndigheter medgavs tillgång till de lagrade uppgifterna vid t.ex. brottsbekämpning. Det rör sig således om två olika former av ingrepp i rätten till respekt för privatlivet och skydd av

[248] Europaparlamentets och rådets direktiv 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG.
[249] Se de förenade målen C-293/12 och C-594/12 *Digital Rights Ireland Ltd* mot *Minister for Communications, Marine and Natural Resources m.fl. och Kärntner Landesregierung m.fl.*, p. 17 – 21.
[250] Ibid, p. 25 – 29.
[251] Se Förslag till avgörande av generaladvokat Pedro Cruz Villalón i mål C-293/12 och 594/12, föredraget den 12 december 2012, p. 68 – 80.

personuppgifter. Den lagring som sker av enskildas uppgifter kan enligt domstolen ge enskilda en känsla av att deras privatliv ständigt bevakas.[252]

EU-domstolen går sedan vidare till att bedöma ingreppens proportionalitet och tar utgångspunkt i fast praxis gällande proportionalitetsprincipen. Inledningsvis konstateras det att den lagring som sker av uppgifter är ägnad att uppnå det eftersträvade målet enligt datalagringsdirektivet, vilket bl.a. är att ge nationella myndigheter möjlighet att exempelvis klara upp brott. EU-domstolen uttalar däremot att för att ingreppet ska vara proportionerligt måste åtgärden begränsas till vad som är strikt nödvändigt. Det krävs således att unionslagstiftningen föreskriver tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden. Vidare måste bestämmelsen även uppfylla vissa minimikrav för att möjliggöra ett effektivt skydd mot en föreliggande risk för missbruk, otillåten tillgång samt användning av enskildas personuppgifter.[253] EU-domstolen konstaterar att datalagringsdirektivet dels saknar generella begränsningar vad gäller den lagring av uppgifter som sker i syfte att bekämpa brott,[254] dels saknar direktivet något objektiv kriterium för att avgränsa behöriga nationella myndigheters tillgång till uppgifterna och deras senare användning av dessa. Datalagringsdirektivet angav endast att uppgifter fick lagras och användas för bekämpning av allvarliga brott. Denna formulering var enligt EU-domstolen en för allmänt hållen hänvisning och begränsning av ingreppet.[255] Vidare noteras det att tillgången till de lagrade uppgifterna och deras senare användning inte är underkastad någon förhandskontroll av domstol eller oberoende myndighet.[256] Slutligen konstaterar domstolen att datalagringsdirektivet dels saknar bestämmelser om skydd och säkerhet för lagrade personuppgifter, dels saknar bestämmelser som anpassar kraven till såväl mängden och arten av uppgifter samt även saknar bestämmelser som hanterar riskerna för otillåten tillgång till uppgifter. EU-domstolen menar också att kravet på oberoende tillsyn inte kan garanteras om uppgifterna lagras utanför EU.[257]

Vid en samlad bedömning fann EU-domstolen att datalagringsdirektivet inte levde upp till kravet på proportionalitet som uppställs enligt artikel 7, 8 och 52(1) i EU-stadgan. Datalagringsdirektivet ansågs inte vara förenligt med rätten till respekt för privatlivet och skyddet av personuppgifter och ogiltigförklarades därmed.[258]

5.2.4.2 Schrems v. Data Protection Commissioner – begäran om förhandsavgörande

Den 18 juni 2014 beslutade High Court i Irland att begära ett förhandsavgörande från EU-domstolen gällande bl.a. tolkningen av vissa bestämmelser i dataskyddsdirektivet i ljuset av artikel 8 i EU-stadgan.

[252] De förenade målen C-293/12 och C-594/12 *Digital Rights Ireland Ltd* mot *Minister for Communications, Marine and Natural Resources m.fl. och Kärntner Landesregierung m.fl.*, p. 34 – 36.
[253] Ibid, p. 49 – 55.
[254] Ibid, p. 57 – 59.
[255] Ibid, p. 60.
[256] Ibid, p. 61 – 62.
[257] Ibid, p. 66 – 68.
[258] Ibid, p. 69 – 70.

Bakgrunden till målet i den irländska domstolen var en talan väckt av Mr. Schrems, som hävdade att Facebook Irland, vid överföring av personlig information till moderbolaget Facebook Inc. vars huvudkontor finns USA, överförde personuppgifter till ett land där det inte erbjöds ett tillräckligt skydd av uppgifterna.[259] Mr. Shrems menade att amerikanska myndigheter kunde få tillgång till hans personuppgifter utan vare sig beslut från domstol eller annan myndighet.[260] Mr. Schrems menade att Snowden-skandalen, som ledde till ett avslöjande av det amerikanska PRISM-programmet, tydligt visade att USA inte har någon effektivt dataskydd för icke-medborgares personuppgifter. Överföringar av personuppgifter från Facebook Irland till Facebook Inc. I USA bör därför enligt Mr. Schrems upphöra omedelbart.[261]

Motparten i målet, den irländska dataskyddskommissionären[262], ansåg dock att Mr. Schrems talan var ohållbar. Detta p.g.a. av att Safe Harbor-regelverket, vilket har godkänts av EU-kommissionen, tillåter sådana dataöverföringar till amerikanska bolag och organisationer och att det således anses att USA genom regelverket kan garantera en adekvat skyddsnivå vad gäller behandling av personuppgifter.[263] Dataskyddskommissionären menade också att det inte fanns några bevis på att Facebook Inc., i Mr Schrems fall, hade brutit mot Safe Harbor-principerna.[264]

Den irländske domaren ansåg däremot inte att dataskyddskommissionärens argument var välgrundat. Domaren ansåg att Snowdens avslöjande visar att amerikanska myndigheter har tillgång till EU-medborgares personuppgifter vilka har överförts från EU till USA. Det kunde däremot inte anses bevisat att de amerikanska myndigheterna haft tillgång till Mr. Schrems personuppgifter.[265] Det konstateras att kärnan av rätten till respekt för privatlivet och skydd av personuppgifter är att den personliga integriteten ska förbli okränkt. Domaren hänvisar till EU-domstolens uttalande i de förenade målen C-293/12 och C-594/12 där det, som ovan nämnts, uttalades att, för att en inskränkning i EU-stadgans rättigheter ska vara godtagbar krävs det att det finns nödvändiga säkerhetsåtgärder i de fall nationella myndigheter ska tillåtas få tillgång till personuppgifter.[266] Den irländska domaren menar att det utifrån EU-domstolens uttalande inte är uppenbart om den förevarande användningen av Safe Harbor-regelverket uppfyller kraven på säkerhet i artikel 8 i EU-stadgan. Enligt Safe Harbor-systemet överförs personuppgifter till USA, där nationella myndigheter kan få tillgång till stora mängder data. Den irländske domaren anger att den amerikanska FISA-domstolen säkerligen gör ett bra och viktigt arbete, men att domstolens arbete, i bästa fall, kan beskrivas som en tillsyn av ansökningar

[259] Att det från Facebook Irland överförs personuppgifter till Facebook Inc. i USA kan utläsas av Facebooks användarvillkor, där det anges att Facebook strävar efter att efterfölja lokala lagar, men användare utanför USA ”*have consent to having their personal data transferred and processed in the United States*”. Se Facebook Inc., Policy om rättigheter och skyldigheter, p. 17(1).
[260] Se *Schrems* mot *Data Protection Commissioner* [2014] IEHC 310, p. 29.
[261] Ibid, p. 2.
[262] Svensk översättning av *Data Protection Commissioner*.
[263] *Schrems* mot *Data Protection Commissioner* [2014] IEHC 310, p. 3.
[264] Ibid, p. 30 – 33.
[265] Ibid, p. 42.
[266] Ibid, p. 44 – 45.

från amerikanska säkerhetsmyndigheter för övervakning av enskilda personer. Dessutom sker denna övervakning utanför EU:s territorium och under förhållanden där den registrerade inte har någon faktisk möjlighet att göra sig hörd eller ha synpunkter på den behandling av uppgifter som sker.[267]

Den kritiska fråga som således uppstår i detta fall är om tolkningen av dataskyddsdirektivet och Safe Harbor-regelverket, som tillåter överföring av personuppgifter till tredje land, som inte garanterar ett tillräckligt skydd för den registrerade, bör omvärderas i ljuset av artikel 7 och 8 i EU-stadgan. Frågan som således uppstod var huruvida den irländska data-kommissionären är bunden att följa kommissionens beslut om Safe Harbor, eller om dataskyddskommissionären får utföra en egen bedömning av huruvida tredjelandet kan garantera en adekvat skyddsnivå. Med tanke på den praktiska betydelse denna fråga har för alla medlemsstater i EU, ansåg domaren det vara av vikt att frågan avgörs av EU-domstolen och begärde därmed förhandsavgörande i enlighet med FEUF artikel 267.[268]

Huvudförfarandet vid EU-domstolen har inletts och den tolkningsfråga EU-domstolen har att pröva har utformats enligt följande.

> ”Ska det vid prövningen av ett klagomål som har ingetts till en oavhängig befattningshavare, vilken genom lag har fått i uppdrag att administrera och genomföra lagstiftningen om uppgiftsskydd, om att personuppgifter överförs till ett annat tredje land (i detta fall Amerikas förenta stater) *vars lagstiftning och praxis påstås inte innehålla ett adekvat skydd för den registrerade* [min kursivering], anses att denna befattningshavare är helt bunden av det motsatta gemenskaps-konstaterandet i kommissionens beslut (2000/520/EG) av den 26 juli 2000, med beaktande av artiklarna 7, 8 och 47 i Europeiska unionens stadga om de grundläggande rättigheterna, trots bestämmelserna i artikel 25(6) i direktiv 95/46/EG?”[269]

EU-domstolen avgörande i detta mål kommer innebära en viktig vägledning för framtida tillämpning av Safe Harbor och således även vara avgörande för ett fortsatt transatlantiskt dataflöde.[270]

[267] Ibid, p. 61 – 62.
[268] Ibid, p. 64 – 71 och 83 – 84. FEUF artikel 267 föreskrivs att EU-domstolen är behörig att meddela förhandsavgörande angående giltigheten och tolkningen av rättsakter som beslutas av bl.a. unionens institutioner.
[269] Se mål C-362/14 *Schrems* mot *Data Protection Commissioner*. EU-stadgan artikel 47 föreskriver var och en rätt till en rättvis och offentlig rättegång, samt att få sin sak prövad inför en oavhängig och opartisk domstol. Var och en ska vidare ha möjlighet att låta sig försvaras och företrädas.
[270] Padova (2014).

6 EU:s regler avseende dataskydd – *the long arm*?

I denna framställning har det flertalet gånger poängterats att användningen av molntjänster och dess globala karaktär bidrar till att öka komplexiteten av frågan hur EU-medborgare kan tillförsäkras ett tillräckligt omfattande skydd för sin personliga integritet. En överföring av personuppgifter från EU till ett tredjeland innebär en överföring till en geografisk plats, belägen utanför EU:s jurisdiktion.

I detta kapitel kommer EU:s eventuella skyldighet och möjlighet att upprätthålla ett skydd för EU-medborgares grundläggande fri- och rättigheter utanför EU:s jurisdiktion att i tur och ordning presenteras.

Det ska redan inledningsvis poängteras att det föreligger en rättslig oklarhet vad gäller den territoriella omfattningen av både Europakonventionen, EU-stadgan och EU:s dataskyddslagstiftningar. Det som presenteras är således diskussioner förda i doktrin beträffande bl.a. territoriella tillämpnings-bestämmelser. Området gällande EU:s normativa makt är även det ett outvecklat område och således kommer det endast att beröras kortfattat.

6.1 Mänskliga rättigheters territoriella räckvidd

I stater som betraktar skydd för personuppgifter som en grundläggande rättighet, ingår det i statens skyldighet att även reglera överföring av personuppgifter till tredjeländer. När stater väljer att reglera en sådan överföring innebär det att staten vidtagit en åtgärd för att säkerställa att uppgifterna inte ska berövas detta skydd efter att överföringen har genomförts. Frågan som däremot lämnas obesvarad är hur omfattande denna skyddande skyldighet för stater kan anses vara.[271]

6.1.1 Europakonventionen och dess eventuella extraterritorialitet

Som ovan har presenterats i avsnitt 5.1.2, innebär Europakonventionens artikel 8, om rätten till respekt för privatlivet, dels en negativ skyldighet för stater att inte agera på ett sätt som innebär en kränkning av rättigheten, dels en positiv skyldighet för en stat att vidta åtgärder för att skydda medborgarna från ingrepp i privatlivet.[272] En fråga som dock uppstår är

[271] Kuner (2013), s. 129.
[272] Se avsnitt 5.1.2 samt Danelius (2012), s. 347.

vilken skyldighet en konventionsstat har att skydda medborgarens rätt till personlig integritet utanför statens territorium. Rättsläget är idag oklart, men nedan kommer ett försök att göras att med hjälp av analogier utröna vilket extraterritoriellt ansvar en konventionsstat, samt även EU,[273] har gentemot sina medborgare.

Utgångspunkten för Europakonventionens territoriella tillämpningsområde stadgas i artikel 1. Artikeln anger att de anslutna staterna ska garanterna rättigheterna angivna i konventionen för var och en som befinner sig under statens jurisdiktion. Det kan då ifrågasättas om denna formulering innebär att en konventionsstat endast är ansvarig för skyddet av rättigheten inom statens geografiska territorium, eller om det innebär att staten är skyldig att sträva efter ett skydd för medborgare mot kränkningar av de garanterade rättigheterna oavsett var kränkningen sker geografiskt.[274] För att besvara denna fråga måste Europadomstolens praxis beaktas.

I målet *Assanidze* mot *Georgien*[275] valde Europadomstolen att begränsa konventionsstaternas ansvar territoriellt. Europadomstolen uttalade att konventionsstaterna är ansvariga för alla överträdelser av de i Europa-konventionen skyddade rättigheterna och friheterna, som sker inom konventionsstatens jurisdiktion – eller kompetens på annat sätt – vid tiden för överträdelsen. Domstolen förklarar vidare att detta innebär att en stat är ansvarig för de handlingar som offentliga myndigheter och andra företrädare för staten vidtar, i den mån de är verksamma inom ett territorium som kontrolleras av den aktuella konventionsstaten.[276] En konventionsstat är således enligt ovan nämnda praxis, inte skyldig att skydda sina medborgare från kränkningar av mänskliga rättigheter som sker utomlands av en tredje part.[277]

En sådan territoriell tillämpning av Europakonventionen kan dock uppfattas som problematisk vid användande av molntjänster, eftersom molntjänster till sin karaktär är globala. Det är däremot skäligt att Europakonventionen inte tillskriver konventionsstaterna ett ansvar att skydda en medborgare som väljer att bosätta sig i ett tredjeland. Ett sådant tankesätt baseras främst på den grundläggande folkrättsliga principen om icke-intervention och statssuveränitet.[278] En applicering av reglerna på situationer där molntjänster är involverade kan emellertid förändra synsättet. Molntjänster innebär en möjlighet för bl.a. företag att behandla och lagra personlig information på distans och på en plats utanför den registrerades jurisdiktion. Den registrerade kan således vara bosatt i en konventionsstat där den enskildes rättigheter och friheter skyddas. Samtidigt kan den enskildes personuppgifter befinna sig i ett tredjeland och således utanför konventions-statens jurisdiktion och territorium där konventionsstaten enligt Europa-

[273] EU har, som ovan nämnts, uttalat att de avser att följa Europakonventionen. Se bl.a. avsnitt 5.1.1.
[274] Rauhofer & Bowden (2013), s. 24.
[275] *Assanidze* mot *Georgien* [2004].
[276] Ibid, p. 137.
[277] Rauhofer & Bowden (2013), s. 25.
[278] Principen om icke-intervention har utvecklats inom folkrätten och stadgar en rätt till territoriell integritet och icke-intervention av det internationella samfundet i en stats inre angelägenheter.

domstolens uttalande, i det ovan angivna målet, inte har en skyldighet att agera för att skydda den enskildes rättigheter.[279]

I vissa fall har Europadomstolen däremot ansett att de garanterade rättigheterna i Europakonventionen har en extraterritoriell effekt. En sådan situation har ansetts vara när en konventionsstat avser att utlämna en person till ett tredje land där vederbörande riskerar att utsättas för tortyr. Denna situation ger upphov till en kränkning av artikel 3 i Europakonventionen vilken stadgar en absolut rättighet för en enskild att inte utsättas för tortyr, omänsklig eller förnedrande behandling eller bestraffning.[280] Målet *Soering* mot *Förenande Konungariket*[281] behandlade denna rättsfråga. I detta mål var den sökande en tysk medborgare, som satt fängslad i Storbritannien i avvaktan på utlämning till USA, där den sökande anklagades för att ha mördat sin flickväns föräldrar.[282] Den sökande klagade till Europadomstolen och menade att en utlämning till USA innebar en risk att dömas till dödsstraff. Att dömas till dödsstraff, i kombination med att den sökande då skulle behöva genomlida det s.k. *death row phenomenon* och således i flera år utsättas för extrem stress och psykiska trauman i väntan på att bli avrättad, utgjorde enligt Europadomstolen en omänsklig och förnedrande behandling och bestraffning, vilket strider mot artikel 3 i Europakonventionen.[283] Europadomstolen erinrade att konventionen inte omfattar åtgärder som företas av stater som inte är parter i konventionen. Däremot ansåg Europadomstolen att konventionsstaten har ett ansvar för att rättigheterna inte bortfaller endast p.g.a. att den aktuella behandlingen företas av ett tredjeland. Det bedömdes således som ett brott mot Europakonventionens artikel 3 att utlämna en enskild individ till ett tredjeland, där vederbörande riskerar utsättas för tortyr, omänsklig eller förnedrande behandling eller bestraffning.[284]

Under vissa omständigheter innefattar därmed Europakonventionens artikel 3 en extraterritoriell verkan och effekt. Europadomstolen tydliggjorde i *Soering* mot *Förenande Konungariket* att i en sådan situation är det den utlämnande konventionsstaten som gör sig skyldig till brott mot konventionen.[285] Domstolen försöker således inte överföra ansvar till ett tredjeland som inte är part i konventionen.[286]

När det gäller skydd för den personliga integriteten vid behandling av personuppgifter är det dock oklart hur långt en stats skyldighet att skydda

[279] Jfr diskussion i Rauhofer & Bowden (2013), s. 25.
[280] Ibid, s. 25. Att en rättighet i Europakonventionen är absolut innebär att det inte är tillåtet, under några omständigheter, att vidta åtgärder som innebär ett intrång i denna rättighet. Detta kan således jämföras med rätten till respekt för privatlivet vilken presenterade i avsnitt 5.1.2. Rätten till respekt för privatlivet utgör inte en absolut rättighet och det är således tillåtet för en stat att utifrån vissa förutsättningar vidta åtgärder som innebär intrång i denna rättighet.
[281] *Soering* mot *Förenande Konungariket* [1989].
[282] Ibid, p. 11 – 24.
[283] Ibid, p. 81. *The death row phenomenon* är ett begrepp som används för att beskriva den känslomässiga stress dödsdömda fångar upplever när de döms till döden, samt under tidsperioden fram tills deras avrättande.
[284] Ibid, p. 88 – 91.
[285] För liknande resonemang förda av Europadomstolen se *Chahal* mot *Förenande Konungariket* [1996] och *Jabari* mot *Turkiet* [2000].
[286] Rainey m.fl. (2014), s. 176.

sina medborgare sträcker sig.[287] De situationer där Europadomstolen har ansett att Europakonventionen har en extraterritoriell verkan, som exempelvis i *Soering* mot *Förenande Konungariket*, måste anses skilja sig fundamentalt från de rättigheter som avser att skydda medborgares personuppgifter vid behandling av dem. Samtidigt går det inte att bortse från att detta är ett högaktuellt ämne, med tanke på hur människor världen över idag använder Internet och sprider sina personuppgifter, kan det anses föreligga ett större ansvar hos både offentliga och privata aktörer att skydda mänskliga rättigheter.[288] Appliceras således ett liknande tankesätt om extraterritoriellt skydd av medborgares rätt till privatliv och skydd av personuppgifter, vilka behandlas i molntjänster och som överförs till tredjeland, kan det argumenteras för att det föreligger en skyldighet för konventionsstaterna att skydda sina medborgares personliga integritet även utanför statens territoriella gräns, åtminstone i de fall där kränkningen mot Europakonventionens artikel 8 sker utanför statens jurisdiktion och kränkningen är en konsekvens av en åtgärd vidtagen av konventionsstaten.[289]

Ett sådant tillvägagångssätt stöds av Milanovics teori om extraterritoriell tillämpning av bl.a. Europakonventionen artikel 8. Denna modell baserar sig på en distinktion mellan en stats positiva skyldighet att säkerställa eller garantera människors rättigheter, vilken sträcker till att vara en skyldighet att förebygga brott mot mänskliga rättigheter från tredje part, och staters negativa skyldighet att enbart respektera de mänskliga rättigheterna, vilken endast kräver att stater avstår från att inskränka individens rättigheter utan att det är motiverat.[290] Om den negativa skyldigheten att respektera rättigheten är territoriellt obegränsad, innebär det således att alla eventuella inskränkningar i denna rättighet, oavsett var i världen de sker, skulle aktualisera tillämpligheten av Europakonventionen. Det innebär dock inte att inskränkningen automatisk klassificeras som otillåten, utan inskränkningen ska bedömas mot de krav som finns enligt Europakonventionen för att utgöra en tillåten inskränkning i rättigheten.[291] Denna modell kommer dock enligt Milanovic eventuellt inte att tilltala aktörer som exempelvis regeringar, underrättelsetjänster och domstolar, vilka hade velat undvika svårigheterna med att uppfylla kraven för att utgöra en tillåten inskränkning, eller för den delen helt enkelt ser problem med att efterleva de restriktioner som Europakonventionen föreskriver.[292]

Att utröna den extraterritoriella omfattningen av skydd för personlig integritet i förhållande till övervakning av elektronisk kommunikation, är

[287] Kuner (2013), s. 129.
[288] Ibid, s. 130 f. Exempel på hur privata aktörer påverkas att ta ansvar för mänskliga rättigheter är den pågående utvecklingen av *corporate social responsibility* (CSR). CSR-regelverk har oftast ingen rättslig bindande verkan, utan utgör s.k. *soft law*. Det finns dock en möjlighet att CSR kommer utvecklas till att innebära en rättslig skyldighet för privata aktörer att skydda personuppgifter och rätten till privatlivet.
[289] Jfr diskussion i Rauhofer & Bowden (2013), s. 26.
[290] Milanovic (2014), s. 47.
[291] Ibid, s. 48.
[292] Ibid, s. 49 och se även Milanovics förda resonemang i Milanovic, *EJIL:Talk!* (2013).

och kommer att vara en av de mest utmanande frågorna kring tillämpningen av fundamentala rättigheterna i den digitala miljön.[293]

6.1.2 EU-stadgan och dess externa verkan

EU har som mål att arbeta för att bl.a. främja fred, mänskliga rättigheter och folkens välfärd.[294] Detta mål är även centralt vid EU:s arbete externt.[295] EU-stadgan utgör, vilket tidigare nämnts, ett rättsligt bindande dokument, vilket främst riktar sig till unionens institutioner, organ och byråer, men även till medlemsstaterna när dessa tillämpar unionsrätten. De nämnda aktörerna måste därför respektera rättigheterna, iaktta principerna och främja tillämpligheten av rättigheterna i enlighet med sina respektive befogenheter.[296] Tillämpning av EU-stadgan sker således primärt på medlemsstaternas territorier. Det territoriella tillämpningsområdet är dock inte begränsat till EU:s geografiska gränser, utan kan även aktualiseras i ett tredjeland. Detta kan ske genom EU:s externa relationer, t.ex. i samband med samarbeten mellan EU och ett tredjeland, eller medlemsstater och ett tredjeland. Eftersom EU-stadgan måste tillämpas överallt där EU-rätten på något sätt tillämpas, innebär det att EU-stadgan får en extraterritoriell effekt i de situationer EU-rätten tillämpas extraterritoriellt.[297] Därmed är EU-stadgan tillämplig på alla ageranden som de ovan nämnda aktörerna vidtar, oavsett var de utförs.[298]

EU-stadgans rättigheter ska dessutom tolkas i enlighet med likalydande rättigheter i Europakonventionen.[299] Detta innebär att vad gäller EU-stadgans extraterritorialitet kan vägledning hämtas från Europadomstolens praxis.[300] I vilken utsträckning en sådan vägledning kan tillämpas vid tolkningen av EU-stadgans extraterritorialitet är däremot oklar.[301]

6.2 Europarättsligt skydd för personlig integritet internationellt

De grundläggande intressena som skyddas av EU:s dataskyddsregler, vilka begränsar överföring av personuppgifter till tredjeländer, är skyddet av de grundläggande mänskliga rättigheterna, genom rätten till respekt för privatlivet och skydd av personuppgifter. I jämförelse med tredjeländer, prioriterar EU en hög skyddsnivå för personuppgifter. Det uppstår således en problematik kring hur EU-medborgares personuppgifter ska bibehålla

[293] Kuner, *EJIL:Talk*! (2013) och Milanovics förda argumentation i: Milanovic, Föreläsning om extraterritoriell effekt av människorättskonventioner (2014).
[294] Se FEU artikel 3(1).
[295] Lebeck (2013), s. 79.
[296] Jfr EU-stadgan artikel 51(1).
[297] Lebeck (2013), s. 59 f.
[298] *Implementation of the EU Charter of Fundamental Rights and its Impact on EU Home Affairs Agencies* (2011), s. 48.
[299] Jfr EU-stadgan artikel 52(3).
[300] *Implementation of the EU Charter of Fundamental Rights and its Impact on EU Home Affairs Agencies* (2011), s. 48.
[301] Det ska således påpekas att viss försiktighet vidtas vid antagande om huruvida EU-stadgan kan innebära ett likvärdigt ansvar för EU, som Europakonventionen argumenteras innebära.

denna relativt höga skyddsnivå när de överförts till ett tredjeland.[302] I det följande kommer olika teorier kring EU:s möjligheter att ”sprida” sitt skydd av personuppgifter till tredjeländer att presenteras.

6.2.1 Grundläggande utgångspunkter för EU:s externa relationer

Det är av vikt att redan inledningsvis i detta kapitel redogöra för utgångspunkter och mål vad gäller EU:s agerande i externa relationer. I Lissabonfördraget tydliggörs EU:s roll som en internationell aktör och definierar EU som en juridisk person, vilken kan ingå bindande rättsliga avtal med tredjeländer och internationella organisationer.[303] Utgångspunkten för EU:s externa ageranden föreskrivs närmare i FEU artikel 3(5). I artikeln anges det att EU i sina förbindelser med övriga världen ska bekräfta och främja sina värderingar och intressen samt bidra till skydd av sina medborgare. EU ska bl.a. bidra till skydd och respekt för de mänskliga rättigheterna.[304]

Det stadgas vidare i FEU artikel 21 att unionens åtgärder i internationella sammanhang ska utgå från de principer som har legat till grund för dess tillblivelse, utveckling och utvidgning och som EU strävar efter att föra fram i resten av världen, vilket är exempelvis principerna om demokrati, rättsstaten, de mänskliga fri- och rättigheternas universalitet och respekt för människors värde.[305] EU ska dessutom sträva efter att utveckla förbindelser och bygga partnerskap med tredjeländer samt främja multilaterala lösningar på gemensamma problem.[306] Dessa bestämmelser utgör således grunden för EU:s ageranden internationellt.[307]

6.2.2 Territoriell utvidgning av EU:s lagstiftning – en unilateral lösning?

För att EU ska kunna garantera ett skydd för EU-medborgares personliga integritet när personuppgifter överförts från EU till tredjeländer, finns möjligheten för EU att tillämpa bestämmelserna extraterritoriellt och på så sätt sprida värderingarna om dataskydd på ett unilateralt vis. I det gällande dataskyddsdirektivet[308] samt i förslaget till allmän dataskyddsförordning,[309] är bestämmelsen om regelverkens territoriella räckvidd författad på sådant sätt att dataskyddet i vissa situationer får en extraterritoriell verkan. Dessa bestämmelser anses i doktrin vara allt för vagt utformade och det uppstår en rättsosäkerhet avseende i vilka situationer en molntjänstaktör i ett tredjeland

[302] Kuner (2013), s. 160.
[303] FEUF artikel 216(1).
[304] Jfr FEU artikel 3(5). FEU artikel 2 anger att EU bland andra värden, bygger på respekt för mänskliga rättigheter.
[305] Jfr FEU artikel 21(1) första stycket.
[306] Jfr FEU artikel 21(1) andra stycket.
[307] van Vooren m.fl. (2013), se avsnitt 1.1.: *The EU´s Mission Statement in Global Governance*.
[308] Se dataskyddsdirektivet artikel 4.
[309] Se förslag till allmän dataskyddsförordning artikel 3.

blir bunden att efterleva de EU-rättsliga dataskyddsreglerna.[310] En teori om hur extraterritoriella tillämpningsbestämmelser kan utformas i dataskydds-lagstiftningar kommer i det följande att presenteras.

Dataskyddslagar antas och revideras för närvarande runt om i hela världen, alla med en ökad extraterritoriell räckvidd.[311] Anledning till detta är bl.a. den ökade användningen av molntjänster där den geografiska placeringen av uppgifter kan vara oklar, och den ökade uppmärksamheten på personlig integritet som en skyddsvärd mänsklig rättighet.[312] Det kan å ena sidan vara rimligt att föreskriva extraterritoriell tillämpning av dataskyddslagar för att stater ska kunna utvidga dataskyddet till att även innefatta ageranden vidtagna av utländska aktörer mot statens medborgare och invånare. Det kan å andra sidan anses att en extraterritoriell tillämpning av dataskydds-lagstiftningar är oskäligt, eftersom det är omöjligt för företag, organisationer m.m. på Internet att anpassa sina ageranden till samtliga dataskyddslagar som de kommer i kontakt med runtom i världen.[313]

Hur regleringen av den extraterritoriella tillämpningen av dataskydds-lagstiftning ska utformas har diskuterats i doktrin av bl.a. Dan Svantesson. Dataskyddslagar innehåller en mängd olika rättsregler och Svantessons uppfattning är därför att det är både felaktigt och naivt att tro att en och samma bestämmelse om territoriell tillämpning kan tillämpas på dessa olika materiella regler. Svantesson har därför presenterat en metod, ”*the layered approach*”, som kan tillämpas vid utformandet av territoriella tillämpningsbestämmelser. Metoden innebär att de olika materiella bestämmelserna i en dataskyddslagstiftning indelas i tre olika s.k. skikt, vilka är (1) bestämmelser om förebyggande av missbruk, (2) rättighets-bestämmelser, och (3) administrativa bestämmelser.[314] Till det första skiktet, bestämmelser om förebyggande av missbruk, sorteras regler som syftar till att motverka eller bestraffa otillåten behandling och insamling av personuppgifter. Bestämmelser som istället innebär exempelvis en rätt för den registrerade att få tillgång till sina uppgifter eller rätta felaktiga uppgifter, sorteras till det andra skiktet, där rättighetsbestämmelser redovisas. Det tredje skiktet innehåller administrativa bestämmelser och är tänkt att bestå av regler om sekretess och tillsyn.[315]

De tre skikten tilldelas sedan en särskild tillämpningsbestämmelse där extraterritorialiteten är anpassad efter reglerna samt hur strikt reglerade de aktuella reglerna bör vara. Det första skiktet anser Svantesson ska regleras strikt och således ha en omfattande extraterritoriell tillämplighet.[316] Skikt två bör inte regleras lika strikt och bör tillämpas extraterritoriellt i de fall en aktör från tredjeland agerar på ett sätt där en form av minimumkontakt med

[310] Se Hon, Hörnle och Millard (2013), s. 220, Colonna (2014), s. 204 f och Svantesson, *The territorial scope of the proposed EU Data Protection Regulation*, blawblaw (2013).
[311] Kuner, Cate, Millard & Svantesson (2013), 147. Länder som antar nya dataskyddslagar är exempelvis Malaysia och Singapore, medan dataskyddslagar revideras i Australien och inom EU.
[312] Ibid, s. 147.
[313] Svantesson (2013), s. 278.
[314] Ibid, s. 280.
[315] Ibid, s. 281 ff.
[316] Ibid, s. 281 f.

den aktuella staten uppstår.[317] Det tredje skiktet kräver minst strikt reglering och således ska det endast tilldelas en extraterritoriell tillämplighet när ageranden vidtagna av en aktör i tredjeland är betydande, kontinuerliga och systematiska.[318]

Problem med tillämpning av denna metod kan dock uppstå, eftersom den innebär en uppdelning av en mänsklig rättighet. Beroende av vilken typ av agerande en aktör i tredjeland vidtar i en stat, leder detta till olika nivåer av integritetsskydd för en enskild individ. Svantesson menar dock att denna metod avsevärt skulle förbättra den nuvarande oklara situationen gällande extraterritoriell tillämpning av dataskyddslagar och att metoden bör tillämpas vid utformandet av EU:s nya dataskyddsförordning.[319]

6.2.3 Global överenskommelse – en multilateral lösning?

Trots att länder runt om i världen numera har närmat sig varandra vad gäller dataskyddslagstiftning, kvarstår det stora skillnader i lagstiftningen mellan olika länder, vilket problematiserar ett gränsöverskridande dataflöde. Framförallt har begreppet territorialitet bidragit till en ökad problematik, eftersom det används av de flesta stater för att fastställa tillämplig lag och jurisdiktion. Begreppet territorialitet är framförallt svårtillämpat när det gäller överföring av personuppgifter i molntjänster, som till sin karaktär är gränsöverskridande.[320]

Det finns en naturlig vilja att vid globala problem försöka nå en global lösning, och så även i detta fall. En önskan, och en möjlighet för EU att tillförsäkra skydd i tredjeländer, hade varit att åstadkomma en global reglering, som kan skydda enskildas rätt till personlig integritet, som inte överbelastar registeransvariga, som kan anpassas till en fortsatt teknisk utveckling och som möjliggör en smidig verkställighet av lagstiftningen över gränserna. Förslag har lagts fram för att skapa ett sådant, rättsligt bindande, globalt avtal som omfattar dataskydd och gränsöverskridande personuppgiftsöverföringar och skulle i sådant fall utgöra en konstitutionell rättslig ram.[321]

Att påstå att det endast bör finnas ett avtal eller en konvention på en internationell nivå är otillräckligt, eftersom detta kan hänvisa till många olika regionala eller globala gränsöverskridande samarbeten. Det finns vidare inte en tydlig hierarki mellan olika internationella institutioner och regelverk. Ett multilateralt avtal, eller något likvärdigt, bidrar således inte alltid till ett harmoniserat internationellt regelverk. I många länder måste ett

[317] Jfr argumentation i Svantesson (2013), s. 282 f. Svantesson tar utgångspunkt i amerikansk rätt där denna territoriella princip härleds ur framförallt två rättsfall från den amerikanska högsta domstolen: *International Shoe Co.* mot *Washington* och *Hanson* mot *Denckla*.
[318] Svantesson (2013), s. 283 f. Utgångspunkten även för denna tillämpningsbestämmelses utformning hämtar Svantesson från den amerikanska rätten och menar att inspiration bör hämtas från amerikansk rätt gällande territorialitetsprinciper.
[319] Ibid, s. 281 och 286.
[320] Kuner (2013), s. 158 f.
[321] Ibid, s. 162 och Burca (2010), s. 31 och 34 f.

sådant avtal implementeras i nationell rätt, vilket kan leda till stora skillnader i slutresultatet mellan de nationella lagarna.[322] Det har dock visat sig att implementering i nationell lagstiftning har varit det mest effektiva sättet för att ge praktisk effekt av konventioner och avtal om mänskliga rättigheter. Det finns däremot ingen garanti att ett avtal om skydd för personuppgifter vid gränsöverskridande överföringar hade implementerats på samma sätt.[323]

Inom EU kan en vilja att samarbeta internationellt för att åstadkomma ett gemensamt globalt skydd av personuppgifter utläsas ur kommissionens förslag till allmän dataskyddsförordning. I artikel 45(1)(a) föreskrivs att kommissionen och de nationella tillsynsmyndigheterna ska vidta lämpliga åtgärder för att utveckla ändamålsenliga rutiner gällande det internationella samarbetet för att underlätta en effektiv tillämpning av lagstiftningen om skydd av personuppgifter. Ett utvecklat samarbete med tredjeländer, särskilt de som erbjuder en adekvat skyddsnivå, förespråkas således av EU.[324]

Ett internationellt samarbete inom området för skydd av personuppgifter vid gränsöverskridande överföringar är av stort intresse, men troligtvis är ett internationellt bindande avtal ensamt inte hela lösningen på problemet.[325]

6.2.4 EU – en normativ makt på den internationella arenan?

Ytterligare en möjlighet för EU att sprida sina värderingar gällande respekt för privatlivet och skydd av personuppgifter vid behandling av dessa, är att agera som en normativ makt. En normativ makt är en aktörs makt att påverka normer, opinion och värderingar hos andra internationella aktörer. I detta avsnitt kommer två förespråkare och deras teorier om EU som en normativ makt att presenteras. Dessa förespråkare är Ian Manners, som menar att EU kan sprida sina normer genom att tillämpa olika spridningsstrategier, och Anu Bradford, som argumenterar för teorin om *Brysseleffekten* genom vilken EU har blivit en normativ makt.

6.2.4.1 Ett globalt ledarskap genom normspridning

En förespråkare för tesen att EU utgör en normativ makt på den internationella arenan är Manners. EU utgör, enligt Manners, en samlad aktör för flera nationalstater och besitter således makt att förändra normer och kan även påverka det som är en vedertagen norm i internationella sammanhang.[326] I den globaliserade värld som präglar dagens samhälle argumenteras det för att det finns andra sätt att vinna makt internationellt än endast genom militära och ekonomiska resurser. En aktör kan genom att

[322] Kuner (2013), s. 162 f.
[323] Heyns & Viljoen (2002), s. 5.
[324] Se förslag till allmän dataskyddsförordning, s. 12.
[325] Kuner (2013), s. 164.
[326] Manners (2002), s. 236.

agera som en ”civil” eller ”ideologisk” makt attrahera andra internationella aktörer genom sin kultur och värderingar.[327]

EU:s normativa utgångspunkt har utvecklats under de senaste 50 åren genom bl.a. internationella deklarationer, avtal och policys. Detta i kombination med att EU är grundat efter principerna om demokrati, rättsstaten och respekt för mänskliga rättigheter, gör unionen till en unik internationell aktör som normspridare enligt Manners. Genom att i sina externa relationer alltid beakta och följa dessa ideologiska grundvärderingar har EU skapat en specifik normativ karaktär, som många andra internationella aktörer saknar.[328]

Att EU utgår från denna normativa bas innebär inte att EU automatiskt blir en internationell normativ makt. Manners hävdar att EU utvecklat olika mekanismer för att sprida sina normer, vilka han kallar spridnings-strategier.[329] För att påvisa hur dessa strategier tillämpats av EU i praktiken, har Manners redovisat en studie om hur EU, genom sin normativa makt, har spridit normen om avskaffande av dödsstraffet. Studien visar att genom uppfattningen om avskaffandet av dödsstraffet som en värdenorm har EU lyckats sprida normen internationellt genom tillämpning av främst tre spridningsstrategier. Dessa strategier är *processuell spridning*[330], *informationsutbyte*[331] och *öppen närvaro*.[332] Processuell spridning handlar om spridning av normer genom att EU samarbetar och involverar sig med en tredje part, vilket kan åstadkommas genom bl.a. samarbetsavtal eller att EU blir medlem i en internationell organisation. Exempel på EU:s processuella spridning av normen om avskaffande av dödsstraff, är att det för medlemskap i unionen krävs ett avskaffande av dödsstraffet. Tillämpningen av informationsutbyte som strategi innebär att EU genom strategisk kommunikation sprider en norm. I studien hade spridning genom informationsutbyte skett genom att EU bl.a. utvecklat gemensamma strategier t.ex. genom upprättande av policys och medverkande i internationella deklarationer. Den sista spridningsstrategin som tillämpats av EU enligt Manners studie var öppen spridning, vilket innebär att EU genom att fysiskt närvara i tredjeländer och internationella organisationer har lyckats sprida normen om att avskaffa dödsstraff.[333]

6.2.4.2 Ett globalt ledarskap genom Brysseleffekten

Ytterligare en förespråkare för EU som en normativ makt är Bradford. Bradford menar att EU har förbisetts som en unilateral makt i diskussioner om globalisering och maktpolitik. EU har möjlighet att påverka regleringar på en internationell nivå inom en rad områden som t.ex. livsmedel, kemikalier, konkurrens och skydd för privatlivet. Det kan därmed hävdas att

[327] Jfr Manners (2002), s. 238 och Nye (2005), s. 75 f. Att som internationell aktör påverka andra aktörer genom att utöva civil makt, kallar Nye för ett utövande av ”*soft power*”. Detta skiljer sig således mot ett utövande av militär och ekonomisk makt, vilket istället benämns som ”*hard power*”.
[328] Manners (2002), s. 240 f.
[329] Följande stycke hänvisas från Manners (2002), s. 244 f.
[330] Svensk översättning av *procedural*.
[331] Svensk översättning av *informational*.
[332] Svensk översättning av *overt diffusion*.
[333] Manners (2002), s. 245 ff.

EU:s lagstiftning har en påtaglig inverkan på det dagliga livet för medborgare i hela världen. Få amerikaner är exempelvis medvetna om att EU, på något sätt har påverkat vilket smink de använder, vilka frukost-flingor de äter, vilken mjukvara som används på deras dator och vilken sekretessinställning de kan välja att ha på sitt Facebook-konto. Detta fenomen kallar Bradford för Brysseleffekten och avser att med denna teori förklara hur och varför lagar och regler, vilka härrör från Bryssel, har lyckats penetrera marknader både inom och utanför EU genom globalisering av unilaterala regelverk. En globalisering ett unilateralt regelverk uppstår när en stat lyckas exportera sina lagar och regler utanför dess jurisdiktion genom marknadsmekanismer som leder till en globalisering av standarder.[334] Enligt Bradford har EU genom detta tillvägagångssätt lyckats höja standardnivån på regler inom vissa rättsområden och således startat ett ”*race-to-the-top*”.[335]

Brysseleffektens teoretiska grund baserar sig på fem förutsättningar.[336] EU har lyckats uppfylla dessa förutsättningar och utgör således en global unilateral regelskapare inom vissa rättsområden. De fem förutsättningarna utgörs av följande. För att åstadkomma en globalisering av vissa regler, krävs det först och främst en makt över en stor ekonomisk marknad. Detta villkor uppfylls av många stater förutom EU, exempelvis USA och Kina.[337] Vidare måste staten ha en form av lagstiftningskapacitet för att kunna omsätta sin marknadsmakt till ett konkret reglerande inflytande. Utan en lagstiftande expertis samt resurser att driva igenom regelverk, kan en stat inte på ett effektivt sätt utöva en auktoritet över marknadsaktörer. Detta gäller både inom och utom statens jurisdiktion.[338] Inom EU har de olika interna institutionerna expertis, befogenheter och resurser att bevaka den gemensamma marknaden och samtidigt garantera de rättigheter och skyldigheter som är utfästa i EU:s fördrag.[339] Den lagstiftande kapaciteten måste dessutom kompletteras med en politisk vilja att genomföra ett strikt regelverk. En stat måste med andra ord ha en villighet att utfärda strikta regler.[340] De strikta reglerna kan endast fungera som globala standarder om reglerna är utformade på ett sätt som hindrar ett kringgående av dem genom att marknadens aktörer förflyttar sina verksamheter till andra jurisdiktioner,

[334] Bradford (2012), s. 3.
[335] Ibid, s. 4 ff. Ett *race-to-the-top* är motsatsen till ett *race-to-the-bottom*, och förklaras således enklast genom att först beskriva det sistnämnda begreppet. Ett race-to-the-bottom är en företeelse som åsyftar när stater väljer att stifta lagar och regler så förmånligt som möjligt inom en viss sektor för att skapa ett bättre företagsklimat och locka företag att etablera sig i landet. Detta kan leda till exempelvis lägre löner, sämre arbetsvillkor och sämre arbetsmiljö. Ett race-to-the-bottom uppstår främst när konkurrensen är hög inom ett visst geografiskt område eller inom en viss branch. Ett race-to-the-top är enligt Bradford motsatsen till ett race-to-the-bottom och uppstår när länder strävar efter att uppnå viss nivå på sina lagar och regler.
[336] De fem förutsättningar som måste vara uppfyllda för att uppnå en Brysseleffekt och som kommer redogöras för i följande stycke sammanfattar Bradford enligt följande: ”*... a single jurisdiction is able to supply global standards whenever that jurisdiction has a large domestic market, sufficient regulatory infrastructure, and a preference for regulating inelastic targets with strict and nondivisible standards.*”, Bradford (2012), s. 19.
[337] Ibid, s. 11 f.
[338] Ibid, s. 12 f.
[339] Ibid, s. 14.
[340] Ibid, s. 14 f.

d.v.s. genom s.k. forum shopping.[341] Slutligen kommer regler endast att bli globala när ett tredjelands exportör väljer att efterleva de strikta reglerna och tillämpa detta beteende vid sina affärer världen över och inte bara gentemot staten som utfärdat de strikta reglerna. Detta innebär att Brysseleffekten inträffar när t.ex. företag frivilligt väljer att följa de strängaste reglerna på marknaden och på så sätt höja standarden även på andra marknader där reglerna inte är lika strikta.[342]

Bradford menar att skyddet för privatlivet är ett rättsområde där EU:s regler till viss del har globaliserats genom Brysseleffekten. EU skyddar rätten till personlig integritet som en mänsklig rättighet och har till följd av detta strikta regler inom rättsområdet. Många länder har antagit liknande regler som EU, framförallt vad gäller skydd för personuppgifter vid automatiserad behandling.[343]

[341] Ibid, s. 16 f.
[342] Ibid, s. 17 f.
[343] Ibid, s. 22 ff. För liknande resonemang gällande skydd för privatlivet, se även Bach & Newman (2007), s. 833 ff. Exempel på länder vilka har ett högt dataskydd är Nya Zeeland, Argentina och i vissa delar Kanada. Ett land som dock valt att inte påverkas av EU:s höga skyddsnivåer är USA. Trots det påverkar EU:s regler amerikanska företag när de väljer att vara verksamma inom EU.

7 EU, regler om överföring av personuppgifter till tredjeland och rätt till personlig integritet – en analys

Denna uppsats syftar till att dels undersöka dataskyddsdirektivets och förslaget till allmän dataskyddsförordnings regler avseende överföring av personuppgifter till tredjeländer i förhållande till EU-medborgares rätt till personlig integritet, dels till att undersöka vilket ansvar EU har för att skydda EU-medborgarens fundamentala rättigheter. Vidare är avsikten att undersöka vilka möjligheter EU har att påverka skyddet av EU-medborgares rätt till personlig integritet i ett globalt sammanhang.

I följande kapitel är avsikten att knyta samman det tidigare i uppsatsen redovisade materialet, och utifrån detta söka besvara de i uppsatsen uppställda frågeställningarna. Första delen av analysen avser att diskutera om det nu gällande dataskyddsdirektivets bestämmelser om överföring av personuppgifter till tredjeländer är förenliga med Europakonventionens artikel 8 och EU-stadgans artikel 7 och 8, samt vilket ansvar EU har för att upprätthålla skyddet av EU-medborgarnas rätt till personlig integritet. I andra delen av analysen kommer det att diskuteras huruvida de reformerade reglerna om överföring av personuppgifter till tredjeländer, i förslaget till allmän dataskyddsförordning kommer att innebära ett förstärkt skydd för EU-medborgarna, eller om ifrågavarande skydd kommer att minskas till förmån för bl.a. molntjänstindustrin. Avslutningsvis kommer del tre av analysen att diskutera EU:s möjligheter att påverka skyddet av EU-medborgarnas rätt till personliga integritet på den internationella arenan.

7.1 Regler om överföring av personuppgifter till tredjeländer och deras förenlighet med rätten till personlig integritet

Det har i denna framställning redogjorts för de risker en EU-medborgares rätt till personlig integritet kan utsättas för vid användning av molntjänster där en överföring av personuppgifter sker från EU till ett tredjeland, eftersom det generellt sett finns ett svagare skydd för EU-medborgare när deras personuppgifter behandlas utanför EU:s jurisdiktion och territoriella gränser. Risker kan uppkomma vid behandling av personuppgifter av tredjelands privata aktörer och tredjelands offentliga myndigheter.

Huvudregeln i dataskyddsdirektivet artikel 25 är att överföring av personuppgifter till tredjeländer är förbjuden, om inte tredjelandet kan säkerställa en adekvat skyddsnivå. Bedömningen om skyddsnivån är adekvat sker på grundval av olika förhållanden och kan utföras av både kommissionen och den aktör som avser överföra personuppgifterna. Från detta krav på adekvat skyddsnivå, finns undantag som möjliggör en överföring till tredjeland som inte kan säkerställa en adekvat skyddsnivå. Undantag får följaktligen göras om det istället föreligger ett samtycke från den registrerade, eller om registerföraren tillämpar BCR:s, modellklausuler eller principerna angivna i Safe Harbor. I det följande analyserar och diskuterar jag dessa undantags förenlighet med rätten till respekt för privatlivet och skyddet av personuppgifter, såsom de stadgas i Europakonventionen artikel 8 och EU-stadgan artikel 7 och 8.

7.1.1 Ett hot från tredjeländer mot EU-medborgares personliga integritet?

För att utreda om dataskyddsdirektivets regler, vilka tillåter en överföring av personuppgifter till tredjeländer, strider mot rätten till respekt för privatlivet och skydd av personuppgifter såsom de stadgas och skyddas i Europakonventionen artikel 8 och EU-stadgan artikel 7 och 8, måste det först utredas om det finns en risk för att EU-medborgares rättigheter kränks när de behandlas i ett tredjeland.

I denna framställning har framförallt Snowden-avslöjandet om amerikanska underrättelsetjänsters tillgång till EU-medborgares personuppgifter utgjort exempel på vilka risker EU-medborgare kan utsättas för vid en överföring av personuppgifter till länder utanför EU:s territorium. PRISM-skandalen utgör dock bara ett exempel på förekomsten av tredjeländers regler om brottsbekämpning och ländernas säkerhetsmyndigheters tillgång till personlig information som lagras eller behandlas i molnet. Flertalet tredje-länder har lagstiftning som innebär en uppdelning mellan landets medborgare och utländska medborgare, där inhemska medborgare erhåller ett större skydd för den personliga integriteten, medan utlänningar erhåller ett mycket svagare, kanske näst intill obefintligt, skydd för den personliga integriteten. Det amerikanska regelverket FISA är ett exempel på hur EU-medborgares rätt till privatliv och skydd av personuppgifter behandlas annorlunda än de amerikanska medborgarnas rättigheter.

Det jag avser att diskutera i det följande är om det amerikanska regelverket FISA, och den däri föreskrivna § 1881a, kan utgöra ett otillåtet ingrepp i de rättigheter EU-medborgare är garanterade enligt Europakonventionen och EU-stadgan. Utgångpunkten enligt både Europakonventionen artikel 8 och EU-stadgan artikel 7 och 8, är att varje behandling av personuppgifter som innebär lagring, insamling eller användning av dessa uppgifter, faller inom begreppet privatliv. Personuppgifter är exempelvis information om den enskildes privata förhållanden, information om vederbörandes hälsa eller foton föreställande vederbörande. Rätten till privatliv och skydd av personuppgifter är dock inte en absolut rättighet, utan det är tillåtet för en stat att vidta åtgärder som innebär en inskränkning i dessa rättigheter. En sådan inskränkning är endast tillåten om vissa förutsättningar är uppfyllda.

Enligt både Europakonventionen och EU-stadgan gäller följande förutsättningar för att en inskränkning ska vara tillåten; (1) inskränkningen ska ha stöd i lag, (2) inskränkningen ska vara nödvändig i ett demokratiskt samhälle, samt avse att uppfylla mål av allmänt samhälleligt intresse, och (3) inskränkningen måste vara proportionerlig. I analysen om den amerikanska regeln FISA § 1881a uppfyller nämnda förutsättningar för att vara en tillåten inskränkning, kommer jag att utgå från de resonemang Europadomstolen och EU-domstolen har fört vid liknande bedömningar i de avgöranden som redogjorts för i framställningens avsnitt 5.1.4 och 5.2.4.

Sammanfattningsvis innebär FISA § 1881a en möjlighet för högre tjänstemän inom bl.a. amerikanska underrättelsetjänster att besluta om behörighet att, under en period upp till ett år, övervaka personer som misstänks befinna sig utanför USA för att erhålla utländsk underrättelse-information. En person som befinner sig utanför USA kan således utgöra en EU-medborgare. Detta beslut ska även godkännas av den amerikanska FISA-domstolen. Om FISA-domstolen tillåter sådan övervakning av en person som inte befinner sig i USA, kan detta medföra en skyldighet för amerikanska leverantörer av elektroniska kommunikationstjänster att förse underrättelsetjänsterna med information eller nödvändig hjälp som krävs för att förvärva sådan utländsk underrättelseinformation. Det föreligger dessutom en mycket begränsad insyn i de ärenden som FISA-domstolen handlägger. Möjlighet till skydd för personlig integritet i USA regleras främst genom det fjärde tillägget till förenta staternas konstitution. Detta skydd, som inte utgör ett renodlat skydd för den personliga integriteten, är dock inte tillämpligt på utländska medborgare.

Kan dessa amerikanska bestämmelser anses utgöra tillåtna inskränkningar i EU-medborgares garanterade rätt till personlig integritet? Jag gör i detta hänseende följande bedömning. Som utgångspunkt kan det konstateras att den information amerikanska underrättelsetjänster kan få tillgång till, från t.ex. IT-företag, utgör sådana personuppgifter vilka omfattas av skydd enligt både Europakonventionen och EU-stadgan. Att det således i lag föreskrivs en möjlighet att få tillgång till dessa personuppgifter, utgör därmed en inskränkning i rättigheten. Europadomstolen och EU-domstolen har i sin praxis, vad gäller bedömningen av om inskränkningen är begränsad till vad som är nödvändigt, angett att bestämmelsen måste föreskriva tydliga och precisa regler för räckvidden och tillämpningen av den aktuella åtgärden. Det kan då anses föreligga en tillräcklig garanti för att personuppgifterna inte kommer att missbrukas. FISA § 1881a föreskriver, enligt min åsikt, inte några tydliga riktlinjer för i vilka fall övervakning av en person får vidtas. Det föreligger inte heller en tillräcklig tydlighet kring hur FISA-domstolen gör sin bedömning. De begränsningar som föreskrivs i lagtexten gällande att övervakning endast får pågå under en period av ett år utgör inte tillräckliga riktlinjer för att uppnå kravet på en precis och tydlig reglering. Det kan således argumenteras för att bedömningen är alltför skönsmässig. Vid en bedömning av om FISA § 1881a är proportionerlig kan det mål och intresse som avses uppnås och tillgodoses med reglerna vara nationell säkerhet. Vad gäller nationell säkerhet är en större inskränkning i rätten till personlig integritet motiverad, men i detta fall är, enligt min åsikt, denna form av inskränkning är alltför ingripande, då amerikanska myndigheterna får tillgång till allt för stora mängder personuppgifter. I detta fall är min

personliga uppfattning att enskildas rätt till personlig integritet, väger tyngre än det samhälleliga intresse som avses uppfyllas.

Jag menar därför, utifrån ovan förda argumentation, att den amerikanska bestämmelsen i FISA § 1881a, utgör en otillåten inskränkning i EU-medborgares rätt till respekt för privatliv och skydd av personuppgifter. Det föreligger följaktligen en stor risk att användande av molntjänster, där stora överföringar av personuppgifter sker till USA och andra tredjeländer med liknande lagstiftning, kan medföra en kränkning av EU-medborgares mänskliga rättigheter. Det ska återigen påpekas att USA och dess reglering har presenterats som ett exempel. Likvärdig risk kan därmed uppstå vid en överföring av personuppgifter till tredjeländer där en adekvat skyddsnivå inte kan garanteras.

Följdfrågan som uppstår är vilket ansvar som kan tillskrivas EU p.g.a. att det efter en överföring av personuppgifter till tredjeland kan uppkomma en risk, för att EU-medborgares personuppgifter behandlas på ett sätt som innebär ett otillåtet ingrepp i rätten till personlig integritet.

7.1.2 Är EU ansvarig för skydd av EU-medborgares personliga integritet i tredjeland?

I detta avsnitt kommer jag ta utgångspunkt i den territoriella tillämpligheten av Europakonventionen och EU-stadgan. Principerna jag avser att diskutera härleds från Europadomstolens praxis. Som redovisats i avsnitt 5.1.1. är EU inte part till Europakonventionen, men det pågår för närvarande förhandlingar kring ett sådant anslutande. EU-domstolen har dessutom i sin praxis angett att Europakonventionens principer och Europadomstolens praxis ska vara vägledande och respekteras av EU i deras arbete. Därav kommer Europakonventionen främst att beröras och hänvisas till i det följande, med antagandet att EU-stadgan troligen hade tolkats på ett likvärdigt sätt.

Utgångpunkten för Europakonventionens territoriella tillämplighet är enligt artikel 1 att konventionsstaten ska garantera rättigheter och friheter för var och en som befinner sig under statens jurisdiktion. Frågan är dock vad detta innebär. Eventuellt kan det tolkas på sådant sätt att en konventionsstat har en skyldighet att skydda en enskild så länge denne befinner sig inom statens jurisdiktion, oavsett var kränkningen av rättigheten sker geografiskt. Europadomstolen har genom olika uttalanden, bl.a. i målet *Soering* mot *Förenande Konungariket*, anfört att Europakonventionen inte kan göra en tredje part ansvarig för en åtgärd som vidtas i ett tredjeland mot en medborgare i en konventionsstat och som innebär en kränkning av en i Europakonventionen skyddad rättighet. Mer oklart är dock hur långt en konventionsstats ansvar för att skydda sina medborgares rättigheter sträcker sig. Europadomstolen har uttalat att artikel 3, om förbud mot tortyr och omänsklig eller förnedrande behandling eller bestraffning, har en extraterritoriell effekt. Denna extraterritoriella effekt innebär att en konventionsstat, som avser att utsända en enskild person till ett tredjeland där vederbörande riskerar att utsättas för tortyr eller nedvärderande

behandling, gör sig skyldig till brott mot konventionen. Detta p.g.a. av att konventionsstaten vidtar en åtgärd som innebär en risk för kränkning av mänskliga rättigheter.

Görs en analogisk tolkning av denna extraterritoriella tillämpning av artikel 3 till artikel 8 och rätten till respekt för privatlivet, kan det argumenteras för att en konventionsstat kan bli ansvarig i de fall det överförs personuppgifter till tredjeländer, där de behandlas på ett sätt som innebär en kränkning av rättigheten. Det kan dock ifrågasättas om det är rimligt att göra en sådan analogi.

Som utgångspunkt är tillämpligheten av Europakonventionen beroende av territorialitet. Jag är av uppfattningen att det kan finnas anledning att ifrågasätta den territoriella begränsningen av tillämpningen av skyddet av rätten till personlig integritet i den del rättigheten avser att utövas i molnet, eller på Internet. Det är nödvändigt att hänsyn tas till de skillnader som finns mellan händelser som sker i det verkliga livet och det som sker i den virtuella världen när vi är uppkopplade mot nätverk som Internet. I det verkliga livet är det till viss del lättare att prata om territoriella gränser och länders jurisdiktion. En person kan antingen befinna sig i land A, eller i land B och de handlingar som utförs kan oftast på ett enkelt sätt anknytas till något av länderna. Världen har dock förändrats och det går inte längre att förneka att stora delar av våra liv idag utspelar sig i en virtuell värld.

Ur ett molntjänstsammanhang, där personuppgifter varje sekund överförs från ett land till ett annat och där den geografiska platsen för uppgifterna är svår att fastställa, kan ansvar för skydd av mänskliga rättigheter komma att kringgås. Genom att territoriellt begränsa ansvaret för skydd av rättigheten, kan detta taktiskt utnyttjas av exempelvis företag. Ponera följande exempel. En enskild person som befinner sig i Sverige använder Facebook för att skicka meddelande till en vän. Detta meddelande överförs sedan från Facebook Irland, till moderbolaget i USA, vilket rättfärdigas av Safe Harbor-certifikatet. Moderbolaget i USA beläggs sedan med ett föreläggande om att utlämna dessa meddelanden, som är skickade av den enskilde personen, till amerikanska myndigheter, vilket vidtas på ett sätt som kränker den enskildes personliga integritet. Enligt den territoriella principen, som Europadomstolen uttalade i *Assanize* mot *Georgien*, skulle Sverige endast har ansvar för att skydda den enskilda personen inom Sveriges territorium. Det är därmed uppenbart att det uppstår ett hål i skyddet av den enskildes rätt till personlig integritet.

Det är av vikt att vi blir medvetna om att vi går mot ett samhälle med luddiga – eventuellt obefintliga – territoriella gränser när den virtuella världen integreras i det verkliga livet. Molntjänster utmanar vårt traditionella synsätt på territorialitet. En analogisk tillämpning av den extraterritoriella principen anser jag således vara nödvändig för att täppa till det hål i skyddet som annars uppstår vid en användning av molntjänster. Vid ett applicerande av principen om extraterritoriell effekt på Europakonventionens artikel 8, måste det även beaktas att rättigheten är både negativ och positiv. Det potentiella ansvar som således kan uppstå för EU vad gäller reglerna om överföring av personuppgifter till tredjeländer kan således argumenteras vara följande.

Vad gäller den negativa skyldigheten för en stat, kan ett ovan fört resonemang utmynna i ett ansvar för en stat, eller för EU i detta fall, att inte föreskriva bestämmelser vilka underlättar en överföring av personuppgifter till ett tredjeland, där uppgifter vid en senare tidpunkt riskerar att utsättas för en åtgärd som innebär ett otillåtet ingrepp i den personliga integriteten. Det kan även argumenteras för att det uppkommer en positiv skyldighet för EU att anta lagar som syftar till att förbjuda överföring av personuppgifter till tredjeländer där efterlevnad av rätten till personlig integritet inte kan säkras. Den positiva skyldigheten kan också tolkas så att den innebär en skyldighet för EU att instifta lagar som avser att skydda den personliga integriteten även i tredjeländer. Denna slutsats anser jag överensstämmer väl med den modell Milanovic presenterar gällande extraterritoriell effekt av mänskliga rättigheter.

Om en slutsats dras av ovan förda tes, skulle det innebära att EU kränker EU-medborgarnas rätt till privatliv och skydd av personuppgifter. EU:s negativa skyldighet enligt Europakonventionen innebär en skyldighet att inte föreskriva bestämmelser vars konsekvenser kan innebära en risk för kränkning av rättigheten i ett tredjeland. Dataskyddsdirektivet föreskriver idag som huvudregel att överföring av personuppgifter till tredjeländer är förbjudet, dock finns det undantag. Dessa undantag utgörs av den registrerades samtycke, användning av BCR:s, modellklausuler eller självcertifiering av Safe Harbor-principerna. Det handlar således om att säkra EU-medborgares mänskliga rättigheter genom civilrättsliga avtal. Det är ingen tvekan om att dessa avtal innehåller ett omfattande dataskydd. Det som dock inte beaktas är det faktum att det finns konkurrerande lagstiftning i tredjeland. Tredjelandslagstiftning kan, likt USA:s, innebära ett mycket svagare skydd och en skyldighet för företagen baserade i tredjelandet att följa tredjelandets regelverk och domstolsbeslut. Det blir således ett val för det i tredjelandsbaserade företaget att välja att antingen följa sina skyldigheter enligt avtalet med företaget etablerat i EU, eller att lyda under tredjelandets regelverk. Att lägga ansvaret för EU-medborgarnas skydd av mänskliga rättigheter, i händerna på privata aktörer är inte rimligt.

Att EU erbjuder denna möjlighet att överföra personuppgifter till länder som inte kan garantera en adekvat skyddsnivå, kan strida mot Europa-konventionen artikel 8 och rätten till privatliv, inkluderat skyddet av personuppgifter. Detta eftersom bestämmelserna möjliggör en överföring av personuppgifter till ett tredjeland, exempelvis USA, där det finns en risk att uppgifterna behandlas på ett sätt som kränker rättigheten.

Det kan uppfattas som djärvt att dra en sådan slutsats, men det är av vikt att lyfta problematiken och den eventuella kränkning EU:s regelverk kan medföra. Vidare kan det ifrågasättas huruvida en sådan drastisk ogiltigförklaring av reglerna hade kunnat vidtas i praktiken eller om det hade lett till ohanterliga konsekvenser. EU-domstolens avgörande i målet *Digital Rights Ireland* är ett av de första mål där EU-rättslig lagstiftning underkänts p.g.a. att de strider mot fundamentala rättigheter. Det är dock möjligt att en ogiltigförklaring av dataskyddsdirektivets regler som tillåter en överföring av personuppgifter till tredjeländer hade inneburit en alltför kraftig begränsning, samt medfört stora negativa ekonomiska konsekvenser. Som konstaterats i framställningen är frågan om extraterritoriell verkan av

skydd för personlig integritet en av de största utmaningarna inom den internationella rätten för tillfället och stora utmaningar väntar för att hitta en lösning som kan accepteras av medparten av världens länder.

Det kan däremot redan nu konstateras att oavsett om en analogi från *Soering* mot *Förenade Konungariket* är möjlig att göra till skyddet av EU-medborgares personuppgifter vilka behandlas i tredjeland, är det viktigt att EU upprätthåller ett så högt skydd som möjligt för medborgarnas rättigheter. Som presenterats i framställningen är EU nära att anta en ny förordning om dataskydd. Relevant för bedömningen av vilket skydd EU-medborgarna erhåller mot otillåten behandlingen av personuppgifter, är att även bedöma vilken konsekvens dessa nya regler kan komma att innebära för skyddet. En jämförelse mellan de nuvarande dataskyddsreglerna och kommissionens förslag till nya regler är därmed av stor betydelse för studien.

7.2 En ny allmän dataskyddsförordning och ett förstärkt skydd?

Dataskyddsdirektivet har länge ansetts vara en föråldrad lagstiftning med ett starkt behov av en ansiktslyftning. År 2012 presenterade kommissionen sitt förslag till allmän dataskyddsförordning, vilken avser ersätta dataskydds-direktivet. Förslagets väg fram tills idag har varit allt annat än rak. Det har utsatts för mycket kritik och varit föremål för lobbying, vilket har bidragit till en utdragen lagstiftningsprocess. Avsikten är att uppdatera och anpassa lagstiftningen till ny och föränderlig teknologi, men även att bygga upp ett förtroende hos EU-medborgarna för nätmiljön. Framförallt är avsikten att stärka skyddet av EU-medborgarnas personuppgifter. Frågan är om detta syfte uppfylls i förslaget till allmän dataskyddsförordning. I det följande avser jag analysera om reformen av reglerna om överföring av person-uppgifter till tredjeländer kan medföra ett förstärk skydd av EU-medborgarnas personliga integritet.

Inledningsvis kan det konstateras att förslaget bibehåller de grundläggande utgångspunkterna för överföring av personuppgifter till tredjeländer så som de stadgas i dataskyddsdirektivet. Generellt sett har bestämmelserna utvecklats och specificerats för att underlätta dess tillämpning och tolkning. Möjligheterna att överföra personuppgifter till ett tredjeland som inte kan säkerställa en adekvat skyddsnivå ökas dock, vilket kan ifrågasättas ur ett människorättsperspektiv.

7.2.1 Samtycke – en frivillig viljeyttring?

Ett av undantagen när det anses vara tillåtet att överföra personuppgifter till ett tredjeland som inte utgör en garant för adekvat skyddsnivå, utgörs av ett samtycke från den registrerade, vilket regleras i det nuvarande dataskydds-direktivet artikel 26(1)(a). Möjligheten att lämna samtycke föreslås behållas även i förslaget till allmän dataskyddsförordning artikel 44(1)(a). I förslaget skärps dock kraven för att ett giltigt samtycke ska föreligga. Det stadgas att den registrerade ska bli informerad om de risker en överföring av personuppgifter kan innebära samt att samtycket ska lämnas särskilt, vara frivilligt och utgöra en informerad viljeyttring. Samtycket får således inte

omfatta återkommande och fortlöpande överföringar. Sett ur ett molntjänst-sammanhang är en sådan fortsatt begränsning problematisk, eftersom överföringar mellan olika länder kan ske varje sekund från en registeransvarig till en registerförare. En bestämmelse om samtycke kan däremot inte strida mot rätten till personlig integritet, eftersom det vid ett samtycke från den registrerade inte kan anses som ett påtvingat ingrepp i den enskildes rättighet.

Lämpligheten av att föreskriva samtycke som rättfärdigande för överföring till tredjeland kan ifrågasättas. Teknologin har utvecklats i en snabb takt de senaste åren och de registrerade som lämnar sitt samtycke utgörs av människor i alla åldrar, kön och samhällsklasser. Det finns därmed en stor risk att merparten de registrerade som lämnar samtycke till behandling av sina personuppgifter inte är medvetna om var, när eller hur uppgifterna kommer att behandlas och insamlas eller i vilken utsträckning och till vad uppgifterna kommer att användas. Att införa ett krav på att den registrerade ska göras medveten om vilka risker en överföring medför är definitivt ett steg i rätt riktning. Frågan är om det är tillräckligt.

Många registeransvariga använder sig idag av s.k. *opt-in*-samtycke, vilket är när en registrerad endast ombeds att bocka i en ruta där man godkänner den registeransvariges användarvillkor. Den information som den register-ansvarige lämnar om behandlingen av de registrerades personuppgifter och vilka risker en överföring av dem kan innebära, är således ofta obskyr eller gömd bland sällan lästa sekretessvillkor och liknande. Detta medför att registrerade sällan kan fatta ett välgrundat beslut när de samtycker till en överföring av deras personuppgifter. Internet och onlinetjänster som exempelvis sociala medier, är idag en stor integrerad del av våra liv. Vi håller kontakten, bestämmer möten och kommenterar varandras livs-händelser genom sociala medier och vi lever således i ett interaktions-samhälle. Vi lockas att dela med oss av det mesta på nätet, och riskerar därmed att förlora kontrollen över det som vi väljer att dela. Som nämnts i framställningen så använder sig många sociala medier sig av molntjänster. Ett talande exempel för ovanstående överföringar är Facebook, som för närvarande är ett av de största sociala medierna. Facebook är etablerade i Europa via sitt dotterbolag på Irland, men överför regelmässigt personuppgifter till moderbolaget i USA. Genom att godkänna Facebooks villkor när konto skapas hos dem, samtycker vi således till en överföring av våra uppgifter till USA.

Jag ifrågasätter om ett sådant samtycke är frivilligt, vilket är en förutsättning för att ett samtycke ska vara godkänt. Gör vi verkligen ett fritt val? Min åsikt är att det egentligen blir ett val mellan att vara delaktig i sociala interaktioner, eller att vid ett icke-samtycke, välja att stå utanför denna interaktion. Omvärldens påtryckningar gör att vi därför samtycker till en överföring till ett tredjeland, trots en medvetenhet om vilka risker vi då utsätter oss för. Det motiveras ofta av att personen ifråga inte har något att dölja för omvärlden. Ett sådant lämnat samtycke bör således, enligt min uppfattning, inte accepteras som ett informerat och frivilligt lämnat samtycke.

7.2.2 Modellklausuler och Binding Corporate Rules – lämpliga skyddsåtgärder?

Modellklausuler och BCR:s utgör avtalsreglerade möjligheter för EU-baserade molntjänstkunder och leverantörer att överföra personuppgifter till tredjeländer, där det inte föreligger en adekvat skyddsnivå. Dessa två möjligheter, om än något reviderade, kvarstår i förslaget till allmän dataskyddsförordning.

Möjligheten att överföra personuppgifter till ett tredjeland genom att tillämpa modellklausuler förblir ett alternativ även i förlaget till allmän dataskyddsförordning. Enligt dataskyddsdirektivet artikel 26(4) kunde endast kommissionen anta sådana modellklausuler. I förslagets artikel 42(2)(c) vidgas denna befogenhet, så att även nationella tillsynsmyndigheter tillåts anta modellklausuler, om det görs i enlighet med mekanismen för enhetlighet. Att vidga behörigheten är förmånligt för framförallt molntjänst-industrin, eftersom det avlastar kommissionen i deras arbete och fler avtal kan arbetas fram med hjälp av de nationella tillsynsmyndigheter, vilka standardiserar en överföring av personuppgifter till tredjeländer. En konsekvens av den utökade behörigheten kan emellertid bli att en viss diskrepans kan uppstå mellan de olika nationella tillsynsmyndigheternas antagna modellklausuler. Syftet med att införa en förordning om dataskydd inom EU var att harmonisera reglerna och att skapa en enhetlighet inom unionen. Att tillåta nationella tillsynsmyndigheter att anta modellklausuler kan leda till den raka motsatsen. Följden kan bli s.k. forum shopping, där exempelvis aktörer inom molntjänstindustrin kommer att etablera sig inom en viss EU-medlemsstat för att kunna utnyttja modellklausuler där de utformats på ett mer förmånligt sätt än i en annan medlemsstat. En mer förmånlig utformning av modellklausuler kan t.ex. innebära lättnader i skyddet av EU-medborgarnas personliga integritet. Det finns en risk att försöker utforma så fördelaktiga klausuler som möjligt för att locka företag till att etablera sig i landet. Konsekvensen blir ett race-to-the-bottom, där förlorarna är EU-medborgarna.

Vidare lagstadgas, i förslaget till allmän dataskyddsförordning artikel 42(2)(1), möjligheten att tillämpa BCR:s för att rättfärdiga en överföring. Detta kommer att innebära en viss harmonisering inom EU, vid ett införande av en allmän dataskyddsförordning, eftersom vissa medlemsstater idag inte tillåter ett användande av BCR:s. I förslaget anges att ett antal förutsättningar måste uppfyllas för att BCR:s ska godkännas, exempelvis att de ska specificera vilka överföringar som avses att utföras och att det ska anges vem av den registeransvarige eller registerföraren som ska ansvara vid brott mot företagsreglerna. Min uppfattning är att BCR:s är ett bra alternativ, i teorin, för att nå en hög skyddsnivå vid överföring till tredje-länder. Vid dess praktiska tillämning tillkommer dock många nyanser, som kan leda till ett ifrågasättande av dess rättssäkerhet. Den största risken för missbruk av BCR:s inom en företagsgrupp anser jag vara den bristande insynen i företagets efterlevnad av de interna reglerna. Det uppställs krav på rutiner för kontroll av efterlevnaden av företagsreglerna i förslaget till allmän data skyddsförordning, vilket även ska rapporteras till de nationella tillsynsmyndigheterna. Det som ska utföras är således en intern kontroll inom den aktuella företagsgruppen vad gäller företagsreglernas efterlevnad.

Stark kritik kan därmed redan nu riktas mot förslagets reglering vilken arbetar mot en transparens i företagens verksamheter. En enkel lösning, dock eventuellt mer kostsam, hade varit att föreskriva en årlig extern kontroll av företagsgruppens verksamhet och dess arbete kring gruppens BCR:s. På så sätt hade en större rättssäkerhet kunnat uppnås. Vidare avser jag även att kort nämna något kring de förutsättningar som ska uppfyllas i företagsreglerna. Vid utformandet av förslaget har kommissionen givits en stor möjlighet att utforma regler vilka kan garantera en hög skyddsnivå vid överföring av personuppgifter till tredjeländer, där det inte föreligger en adekvat skyddsnivå. Min uppfattning är att bestämmelsen om BCR:s är utformad på ett sätt som lämnar utrymme för alltför stora tolknings-möjligheter. Ett sådant utrymme för tolkning öppnar även upp möjligheter för företag att vända och vrida på reglerna för att utnyttja dem till dess yttersta gräns. Det kan mycket väl vara så att det är i denna bestämmelses utformning effekterna av lobbying visar sig. De parter som gynnas av oklara regler som lämnar utrymme för subjektiv tolkning är framförallt privata aktörer. Min mening är inte att argumentera för att EU-medborgares skydd för personlig integritet kommer att bli obefintligt p.g.a. oklara regler, men det är möjligt att skyddet inte når upp till den nivå som hade varit önskvärt.

Möjligheter till överföring genom civilrättsligt bindande instrument kan argumenteras för att tillgodose ett gott skydd vad gäller säkerställande av hur personuppgifterna kommer att behandlas av privata aktörer när de överförs till tredjeländer. Detta eftersom klausulerna ofta utformas i likhet med de bestämmer som återfinns i EU:s dataskyddslagstiftning, samt även genomgår en granskning av kommissionen eller nationell tillsynsmyndighet innan de tillåts tillämpas av t.ex. registeransvariga och registerförare. Ett problem som är ofrånkomligt är däremot frågan om verkställighet. I de fall den privata aktören i tredjelandet bryter mot godkända BCR:s eller modell-klausuler kan det ifrågasättas hur effektiv ett ansvarsutkrävande kommer att vara. En medlemsstats domstol kan döma ut böter mot aktören i tredjeland, men det kommer alltid kvarstå en viss ovisshet om en sådan bot kan komma att erkännas och verkställas i tredjelandet. Detta kommer att i slutändan vara beroende av utvecklingen av internationell processrätt och internationella avtal om erkännande och verkställighet av utländska domar. När en aktör i tredjeland inte längre är tillgänglig eller vägrar erkänna en dom, kommer ansvaret istället att falla på aktörer som är etablerade inom EU. Det är därför orimligt att placera ett så stort ansvar på aktörer inom EU.

Det är av vikt att återigen lyfta det faktum att en molntjänstaktör i ett tredje-land även är bunden av i tredjelandet föreliggande lagar och bestämmelser. Varje undantag som således görs från huvudregeln om att det ska garanteras en adekvat skyddsnivå i tredjelandet, innebär också en risk för ett tredje-lands inkräktande på EU-medborgares personuppgifter. Vid en bedömning av om adekvat skyddsnivå föreligger beaktas tredjelandets lagstiftning, möjligheter till rättslig prövning, m.m., vilket på så sätt, till en viss grad, kan garantera att EU-medborgares personuppgifter inte behandlas på ett otillåtet sätt i det aktuella landet p.g.a. av dess lagstiftning. En sådan skyddsnivå kan däremot inte garanteras när endast krav uppställs i ett civilrättsligt avtal mellan två privata aktörer, varav den ena är etablerad i ett tredjeland. Således kvarstår risken för att EU-medborgares personuppgifter, när de passerat EU:s gränser, kommer att vara tillgängliga för en tredje part p.g.a.

tredjelandets nationella lagar. En sådan situation hade kunnat undvikas genom ett bibehållande av den borttagna artikel 42 i förslaget till allmän dataskyddsförordning. Ett återinförande av denna artikel, vilken förbjöd erkännande och verkställighet av tredjelands beslut om utlämnande av personuppgifter inom unionen, hade inneburit en större rättssäkerhet för EU-medborgarna.

Jag ska även kort kommentera de nya undantagen i artikel 44 i förslaget till allmän dataskyddsförordning. I denna artikel anges det när en överföring får ske trots att det varken föreligger en adekvat skyddsnivå eller lämpliga skyddsåtgärder. Artikel 44 innebär en utvidgning av möjligheterna till överföring av personuppgifter till tredjeländer. Jag ställer mig frågande till varför kommissionen ansåg det vara nödvändigt att införa dessa ytterligare möjligheter att överföra uppgifter. De utgör breda undantag, vilka innebär en stor risk för missbruk av de privata aktörerna. Genom att ha så pass breda och vaga regler för undantag, finns det en risk att registeransvariga eller registerförare väljer att endast förlita sig på att deras överföring av personuppgifter faller in under dessa undantag, istället för att använda sig av modellklausuler eller utforma BCR:s. De kan således kringgå vissa skyldigheter som annars hade behövt uppfyllas enligt de lämpliga skyddsåtgärderna.

De förändringar som förslaget till allmän dataskyddsförordning innebär är ur ett molntjänstsammanhang sammanfattningsvis förmånliga, eftersom det för företag möjliggör en ökad användning molntjänster vilket är både ekonomiskt och organisatoriskt gynnsamt. Om förslaget blir verklighet, föreligger det dock en stor risk för en massöverföring av personuppgifter till tredjeländer. I de fall tredjeland kan garantera en adekvat skyddsnivå, kan det inte argumenteras för att utgöra något problem eller stort hot mot EU-medborgarnas rätt till personlig integritet. I de fall tredjeland däremot inte kan säkerställa en adekvat skyddsnivå kan risker för otillåten behandling och tillgång till EU-medborgarnas personuppgifter uppstå, liknande de som argumenterades för ovan i avsnitt 7.1.1, och således innebära en kränkning av EU-medborgares rätt till personlig integritet. Reformen av EU:s dataskyddslagstiftning är en unik möjlighet för EU att ta dessa problem på allvar, och att framförallt bekräfta värdet av den personliga integriteten i en globaliserad värld.

7.2.3 Safe Harbor – en säker hamn?

Även det föreliggande Safe Harbor-ramverket mellan EU och USA lämnas oförändrat vid en reform av dataskyddslagstiftningen. Detta är uppseendeväckande med tanke på det senaste årets avslöjanden. I framställningen redogjordes det för det irländska rättsfallet *Schrems* mot *Data Protection Commissioner*, genom vilket den irländska domaren ställde frågan till EU-domstolen huruvida kommissionens beslut om Safe Harbor ska omvärderas i ljuset av EU-stadgan artikel 7 och 8 samt med beaktande av Snowden-avslöjandena. Något förhandsavgörande i frågan har inte avdömts av EU-domstolen. Vi går således en spännande framtid tillmötes, där utfallet i förhandsavgörandet kan resultera i ett ogiltigförklarande av Safe Harbor-ramverket.

Min uppfattning är att Safe Harbor-principerna brister i tre väsentliga delar, närmare bestämt (1) dess transparens, (2) dess verkställighet, och (3) information om amerikanska myndigheters tillgång till personuppgifter. Så som principerna idag är utformade och tillämpas, krävs det en förbättring vad gäller insynen i de certifierade företagens policys gällande skydd för personlig integritet. Jag hade önskat ett föreliggande krav på offentliggörande av företagens policys på deras hemsidor eller likande, så det finns en möjlighet för enskilda individer att undersöka de riktlinjer företaget har gällande integritet. Med bakgrund av bl.a. undersökningar och Snowden-avslöjandena vet vi idag att en Safe Harbor-certifiering inte alltid innebär att företaget har policys gällande integritet och behandling av personuppgifter eller för den delen efterlever de fastställda principerna. Detta leder även in oss på frågan kring ramverkets verkställighet, för vilken FTC bär det främsta ansvaret. Hårdare sanktioner måste införas mot de företag som bryter mot principerna och FTC måste allt oftare fullfölja utredningar kring brott mot Safe Harbor. Någon form av årlig kontroll av företagens efterlevande av principerna hade kunnat utgöra en påtryckningsmetod och motiverat amerikanska företag att ta principerna på allvar. Med beaktande av amerikanska underrättelsetjänsters lagstadgade möjligheter till tillgång till bl.a. EU-medborgares personuppgifter, anser jag det även vara av vikt att de certifierade amerikanska företagen förpliktas att informera enskilda användare av deras tjänster om vilka skyldigheter företaget har enligt amerikansk nationell lagstiftning att utlämna personuppgifter till nationella myndigheter eller andra tredje parter. Jag menar att en förbättrad tydlighet kring dessa delar hade utgjort ett steg i rätt riktning för att stärka skyddet för EU-medborgare, samt även för att skapa en medvetenhet hos EU-medborgare som väljer att nyttja tjänster som tillhandahålls av amerikanska företag anslutna till Safe Harbor.

EU-domstolen har för tillfället en möjlighet att påverka den fortsatta tillämpningen av Safe Harbor, eftersom domstolen nu handlägger målet *Schrems* mot *Data Protection Commissioner*. Jag anser att EU-domstolen nu står vid ett vägskäl. Det finns flera alternativa vägar domstolen kan välja att gå. Ett alternativ är att tolka Safe Harbor mot bakgrund av EU-stadgans artikel 7 och 8. En sådan tolkning bör medföra en möjlighet för de nationella tillsynsmyndigheterna att i varje enskilt fall bedöma huruvida det föreligger en adekvat skyddsnivå när överföring sker till USA. En sådan tolkning av den ställda frågan kan medföra en period där stor rättsosäkerhet kan uppstå. Detta eftersom de nationella tillsynsmyndigheterna kan göra egna tolkningar och således finns det en stor risk att det inom EU uppstår en splittrad rättstillämpning vad gäller överföringar av personuppgifter till USA. En annan alternativ väg EU-domstolen kan välja, är att tolka den ställda frågan vidare och även välja att bedöma lagligheten av Safe Harbor mot bakgrund av de garanterade rättigheterna i Europarätten, d.v.s. rätten till respekt för privatlivet och skydd av personuppgifter enligt Europakonventionen och EU-stadgan. En sådan bedömning bör, enligt min åsikt, leda till ett ogiltigförklarande av Safe Harbor-ramverket mot bakgrund av ett beaktande av FISA-regelverket och Snowden-avslöjandena.

Det är av vikt att EU-domstolen inser allvaret och betydelsen av denna tolkningsfråga, eftersom deras avgörande kommer att få betydande konsekvenser för det framtida transatlantiska dataflödet.

7.3 EU – skyldigheter och möjligheter externt

När det gäller reglering av behandling av personuppgifter i molnet, problematiseras förhållandet avsevärt p.g.a. dess globala karaktär. Vad gäller rätt till privatliv och skydd för personuppgifter är det tydligt att detta är rättigheter vilka värderas olika runt om i världen, där Europa kan anses utgöra den världsdel där rättigheterna skyddas allra högst. När det från EU överförs personuppgifter till tredjeländer uppstår det en risk, vilket har presenterats ovan, att det där föreligger ett lägre skydd för privatlivet och personuppgifter, vilket kan leda till en kränkning av EU-medborgares fundamentala rättigheter i tredjeland. Detta innebär att det finns en diskrepans i integritetsskyddet vilket måste lösas på nationell, regional eller internationell nivå. Om reglerna för dataskydd inte överensstämmer i olika länder störs det internationella utbytet av personuppgifter, vilket påverkar både offentliga myndigheter och privata aktörer inom bl.a. molntjänst-industrin negativt.

I analysens första del, avsnitt 7.1.2, redogjorde jag för det eventuella ansvar EU har för att agera på ett sätt som innebär att någon kränkning av EU-medborgares personliga integritet inte sker i ett tredjeland. Där diskuterades ansvaret utifrån EU:s negativa skyldighet. I detta avsnitt avser jag att istället diskutera EU:s eventuella positiva skyldighet enligt Europakonventionen och EU-stadgan. En sådan positiv skyldighet innebär att EU bär ett ansvar för att anta lagar och regler, inklusive internationella avtal och fördrag, vilka har till syfte att skydda rätten till personlig integritet från inblandning av tredjeländers offentliga myndigheter. EU har även, enligt FEU artikel 3(5) och 21, en skyldighet att i sina externa relationer arbeta för att främja de mänskliga fri- och rättigheternas universalitet.

Vilka möjligheter har EU att i ett sådant fall uppnå ett likvärdigt skydd för den personliga integriteten när personuppgifterna överförts till ett tredjeland och således befinner sig utanför EU:s territorium? Jag har i denna framställning argumenterat för tre alternativa lösningar vilka är följande; (1) en unilateral lösning genom att utvidga EU:s dataskyddslagstiftning till att ha en extraterritoriell effekt, (2) en bilateral eller multilateral lösning genom att förhandla fram avtal med andra länder eller arbeta fram ett internationellt avtal, eller (3) en multilateral lösning genom EU-ledarskap och norm-spridning. Det är dock oklart hur lämpliga dessa lösningar är och om det i praktiken är möjligt att genomföra dem.

7.3.1 Extraterritoriell lagstiftning – en lämplig unilateral lösning?

För att nå en bred tillämpning av en eventuell framtida dataskydds-förordning är en lösning att vidga regleringens territoriella räckvidd. Såsom bestämmelsen om territoriell räckvidd idag är utformad i både dataskydds-direktivet och förslaget till allmän dataskyddsförordning, finns det ett stort tolkningsutrymme och deras territoriella räckvidd är oklar. Det positiva med en vid territoriell tillämpning av EU:s dataskyddslagstiftning är dock att det tvingar externa aktörer att leva upp till en högre standard vad gäller

behandling av personuppgifter och således även skydd för EU-medborgares personliga integritet.

Svantesson har presenterat en metod för extraterritoriell tillämpning av dataskyddslagstiftningen, där de olika materiella reglerna i lagstiftning delas upp i tre olika skikt; bestämmelser om förebyggande av missbruk, rättighetsbestämmelser och administrativa bestämmelser. Beroende på vilket skikt den materiella regeln klassificeras inom tilldelas den en viss territoriell tillämpning. De tre skikten har således olika extraterritoriell effekt och tilldelar därför en aktör från tredjeland olika stort ansvar beroende på vilken behandling aktören utför på personuppgifterna. Min uppfattning är att teorin är välgenomtänkt och kan underlätta tillämpningen av dataskyddslagar runt om i världen. Det modellen dock gör, vilket även Svantesson påpekar, är att dela upp rätten till personlig integritet i tre delar och tilldela dem olika högt skyddsvärde. Jag anser att detta utgör en betydande brist i modellen.

För att exemplifiera det jag ovan försöker förklara kan följande situation illustreras. Företag A och B är båda etablerade i ett tredjeland. Företag A utbjuder tjänster till medborgare inom EU regelbundet och uppfyller kravet för att klassificeras i skiktet vilket innehåller bestämmelser om förebyggande av missbruk. Detta skikt är enligt Svantessons modell det mest skyddsvärda och företag A är därmed skyldigt att efterfölja EU:s regler gällande ett förebyggande av missbruk. Företag B har dock en minimal marknad i EU och uppfyller endast kraven för att klassificeras i rättighetsskiktet, vilket enligt modellen är mindre skyddsvärt än skiktet för bestämmelser om förebyggande av missbruk. Anta att Axel och Bertil, vilka båda är EU-medborgare, väljer att handla från företag A och B. Axel väljer att inhandla en SaaS-tjänst från företag A, och Bertil inhandlar en SaaS-tjänst från företag B. Konsekvenserna av tillämpandet av modellen i detta fall blir att Axel åtnjuter ett högre skydd för sin rätt till personlig integritet än vad Bertil gör. Detta p.g.a. att företag A och B klassificerades in i olika skikt. Axel och Bertil, i sin roll som konsumenter, är troligtvis omedvetna om vilken interaktion företag A och B har inom EU:s marknad och vilket skydd företagen är skyldiga att upprätthålla vid behandling av EU-medborgares personuppgifter. Modellen kan således i praktiken innebära en lättnad för företagen, men en risk för EU-medborgarna eftersom de riskerar att behandlas olika beroende på vilka företag i tredjeländer som behandlar deras personuppgifter. I en värld där molntjänster används i större utsträckning kan en ännu större osäkerhet uppstå, då konsumenten oftast inte vet vilken aktör i tredjeland som behandlar deras personuppgifter. Detta eftersom en EU-medborgare oftast endast överför uppgifter till en registeransvarig inom EU, som sedan i sin tur överför uppgifter till en registerförare i tredjeland.

Det som blir avgörande för modellens tillämpande är huvudsakligen vilket värde lagstiftaren väljer att tilldela rättigheten. Jag anser att utgångpunkten bör vara att var och en har rätt till sina garanterade mänskliga rättigheter. Att dela upp rättigheten och tilldela de uppdelade skikten ett visst skyddsvärde riskerar att både göra skyddet svagare och att i längden urholka det. Ytterligare problematik som uppstår vid ett tillämpande av extraterritoriell lagstiftning, vilket jag dock inte kommer att gå närmare in på, är hur EU ska

kunna garantera lagstiftningens effektivitet, genomslag och verkställighet utanför EU.

7.3.2 En möjlig bilateral eller multilateral lösning?

Ett självklart alternativ och kanske även en utopi, är att utarbeta ett internationellt avtal eller fördrag vilken reglerar behandling av personuppgifter där stor hänsyn tas till de enskildas rätt till personlig integritet. Ett globalt, rättsligt bindande, avtal hade löst alla problem som uppkommer vid överföringar av personuppgifter till tredjeländer, eller? Det har i framställningen presenterats vilka problem som kan uppstå vid processen att utarbeta ett sådant avtal, vid dess införlivande och vid dess verkställighet.

Svårigheter som ofta uppstår vid upprättande av avtal, oavsett om det rör stater eller privata aktörer, är skillnaden i storlek på parterna och deras påverkan på avtalet. Vid förhandlingar om ett internationellt avtal för dataöverföring kan det tämligen lätt bli så att stora stater som exempelvis USA lyckas förhandla fram ett för dem gynnsamt avtal, medan mindre parter kan komma att bli lidande då deras röst inte uppfattas som lika kraftig eller betydelsefull. I en sådan situation är det dock positivt att EU, som en representant för 28 suveräna stater, kan föra en talan där den personliga integriteten ses som det mest skyddsvärda vid en reglering om överföringar av personuppgifter internationellt.

Ett av de största problemen som måste övervinnas, för att kunna åstadkomma en global överenskommelse, är de kulturella skillnaderna. Dessa skillnader gäller både synsätt och värdering av personlig integritet, men även tillvägagångsättet hur rättigheten regleras inom olika rättsområden. Om ett tredjeland har regler vilka exempelvis möjliggör för offentliga myndigheter att få tillgång till personuppgifter från företag, kan det antas att landet exempelvis värderar nationens säkerhet högre än enskildas rätt till personlig integritet. Enligt det landets uppfattning utgör dessa lagar och regler en integrerad del av deras nationella regelverk, vilket syftar till att skydda och tillvarata samhällets värderingar, snarare än att de kränker fundamentala rättigheter.

Min uppfattning i denna fråga, är att det för närvarande kommer att förbli en utopi att nå en global lösning på problemet. Det är däremot möjligt att EU genom bilaterala avtal kan vidga antalet länder till vilka det är relativt säkert att överföra personuppgifter. Det viktiga är dock att det runt om i världen uppstår en vilja att bygga partnerskap för att försöka åstadkomma en lösning på detta gemensamma problem.

7.3.3 EU – en potentiell internationell ledare och förebild?

Om det nu framstår som alltför svårt att utarbeta en lämplig modell för extraterritoriell effekt av dataskyddslagstiftningar, samt även en näst intill omöjlig uppgift att upprätta ett internationellt avtal för att åstadkomma en multilateral överenskommelse, är frågan vilka andra möjliga åtgärder som kvarstår för EU att vidta, för att förstärka skyddet för den personliga

integriteten vid behandling av personuppgifter när de överförts till ett tredjeland. En möjlighet jag har valt att presentera i denna uppsats under avsnitt 6.2.4 är EU:s möjligheter att som en normativ makt på den internationella arenan påverka stater och internationella organisationer att anta en likvärdig reglering som EU. Två teorier framförda av Manners och Bradford presenterades.

Manners var en av de första att argumentera för EU som normativ makt internationellt. Genom att tillämpa olika strategier är det möjligt för EU att sprida normer till resten av världen. EU är en unik organisation på många sätt varav ett är EU:s ideologiska ursprung i de mänskliga rättigheterna. Manners har genom en studie påvisat hur EU exempelvis lyckats sprida normen om förbud mot dödsstraff runt om i världen. Det kan därför argumenteras för att liknande spridning kan åstadkommas vad gäller rätten till personlig integritet. De spridningsstrategier Manners presenterar anser jag vara applicerbara inom många rättsområden. Inom rättsområdet för dataskydd finns det möjligheter för EU att påverka omvärlden genom att bl.a. tillämpa strategier som processuell spridning, informationsutbyte och spridning genom öppen närvaro. Exempel på den processuella spridningen kan redan återses i Safe Harbor-ramverket mellan USA och EU. Det finns dock mer kvar att sträva efter i det avtalet, men det är likväl ett steg på vägen mot att sprida ett krav på högre skydd för personers personliga integritet. Denna spridningsstrategi kan och bör utvecklas, då EU i sina externa relationer ska sträva efter att utveckla förbindelser och bygga partnerskap med tredjeländer för att främja lösningar på gemensamma problem. På samma sätt bör således strategin om informationsutbyte kunna bidra till en spridning av normen. Genom att EU deltar i internationella samarbeten kan utarbetning av olika policys påverkas, vilket i sin tur kan bidra till att stärka skyddet för den personliga integriteten vid behandling av personuppgifter.

Bradford har presenterat teorin om Brysseleffekten, där EU har en möjlighet att bli en normativ makt inom vissa rättsområden genom att uppfylla specifika förutsättningar. Om dessa förutsättningar uppfylls, kommer effekten att kunna bli att länder runt om i världen väljer att anpassa sin lagstiftning till EU:s lagar och regler inom området. På så sätt uppstår det ett race-to-the-top, där lagstiftning når en generellt högre standard.

Inom området för dataskydd anser jag att EU är på god väg att uppfylla Brysseleffektens förutsättningar för att bli en global normativ makt. EU har inflytande över en stor marknad och har inom denna marknad lagstiftnings-kapacitet inom området för dataskydd. Det finns en vilja hos EU att skapa strikta regler för behandling av personuppgifter, vilket framförallt grundar sig i en skyldighet enligt EU-stadgan att skydda EU-medborgarnas rätt till respekt för privatlivet och skydd av personuppgifter. Avsikten inom EU är dessutom att utforma reglerna på ett sätt som gör att det inte går att kringgå dem. Detta kan tydligt ses i förslaget till allmän dataskyddsförordning där förordningens territoriella tillämpning vidgas ytterligare jämfört med dataskyddsdirektivet. Vidare kan det urskiljas en trend att det bland privata aktörer, vilka är etablerade utanför EU, antar policys och regelverk för hantering av personuppgifter som lever upp till EU:s högre standard. Privata aktörer utformar sådana policys för att kunna verka inom EU:s marknad,

och väljer sedan att tillämpa dessa standarder även vid behandling av personuppgifter vilka tillhör personer som inte är EU-medborgare.

Länder runt om i världen har redan nu påverkats att revidera och förstärka sina dataskyddslagstiftningar. Ett land som däremot inte ännu påverkats av EU:s normativa makt vad gäller dataskydd är USA. Som nämnts i framställning pågår det en stark lobbying mot förslaget till allmän dataskyddsförordning från amerikanska företag, då de inte vill drabbas av mer ansvar eller högre krav på deras behandling av EU-medborgares personuppgifter. Det som är intressant ur ett Brysseleffektperspektiv är hur de amerikanska företagen kommer att agera vid ett antagande och ikraftträdande av dataskyddsförordningen, vilken skärper reglerna för behandling av personuppgifter. Kommer företagen sluta att verka inom EU:s marknad, p.g.a. att de inte vill eller kan efterfölja EU:s striktare regler? Eller kommer de att anpassa sig och höja sin egen standard, inte bara vid ageranden inom EU:s marknad, utan även på världens alla marknader? Om följden blir det sistnämnda anser jag det vara möjligt att även USA kommer att vakna upp ur en dvala och inse värdet av att erbjuda enskilda ett starkt skydd för sin personliga integritet. De står annars eventuellt inför en risk att privata aktörer i USA i värsta fall kommer att förbjudas från att verka inom EU:s marknad, vilket kan leda till stora ekonomiska konsekvenser för aktörer både i USA och EU.

Ett genomslag av endera teorierna om normspridning och Brysseleffekten inom området för dataskydd skulle med stor sannolikhet kunna innebära en lösning på problemet gällande skydd för personlig integritet vid överföring av personuppgifter från EU till tredjeland. Om standarden höjs runt om i världen gällande dataskydd, skulle det inte längre innebära en risk för kränkning av EU-medborgares rätt till personlig integritet när uppgifter överförs till tredjeland. Om konsekvenserna i praktiken faller ut enligt vad som förutspås i teorin återstår att se i en inte allt för avlägsen framtid.

7.4 Avslutande reflektion

Denna uppsats tar avstamp i ett växande problem avseende personlig integritet i ett gränslöst informations- och kommunikationssamhälle. Det är uppenbart att den överföring av personuppgifter som idag sker från EU till tredjeländer innebär ett hot för den rätt till personlig integritet som EU-medborgare är garanterade, genom både Europakonventionen och EU-stadgan.

I denna uppsats argumenteras det för att EU har en negativ skyldighet att inte föreskriva regler vilka tillåter en överföring av EU-medborgares personuppgifter till tredjeländer vars lagar och regler utgör en otillåten inskränkning i rätten till personlig integritet. Det EU-rättsliga dataskydds-direktivet och den föreslagna allmänna dataskyddsförordningen innehåller båda regler vilka tillåter en sådan ovan nämnd överföring.

Vid författandet av det nya förslaget till allmän dataskyddsförordning har EU haft möjlighet att genomlysa detta problem och utforma regler som tillförsäkrar ett tillräckligt skydd av EU-medborgares personuppgifter när dessa överförs till tredjeländer. Denna möjlighet har inte tillvaratagits och

skyddet för den personliga integriteten vid en överföring till tredjeländer har sammanfattningsvis försvagats med hänsyn till hur EU valt att utforma reglerna i förslaget till allmän dataskyddsförordning.

Det argumenteras i uppsatsen för att EU har tre alternativa vägar att ta för att försöka åstadkomma en lösning på problemet. Dessa tre alternativa lösningar är (1) en unilateral lösning genom att utvidga EU:s dataskydds-lagstiftning till att ha extraterritoriell verkan, (2) en bilateral eller multilateral lösning genom att förhandla fram avtal med andra länder, eller (3) en multilateral lösning genom EU-ledarskap och normspridning. Effektivast och störst påverkan på lösningen av problematiken kanske EU kan erhålla vid en kombination av de tre nämnda alternativen.

Det kan avslutningsvis ifrågasättas om den bästa lösningen gällande gränsöverskridande överföring av personuppgifter är lagstiftning. Eventuellt kan dessa problem, vilka har skapats genom användande av ny teknologi, även behöva lösas genom ännu nyare teknologi, d.v.s. genom en förändring i den digitala världens arkitektur.

Det som kommer att vara avgörande för den framtida utvecklingen av skyddet för den personliga integriteten vid behandling av personuppgifter i molnet, är om vi även fortsättningsvis kommer att betrakta och värdesätta vår rätt till ett privatliv som en av de viktigaste fundamentala rättigheterna, eller om vi i framtiden kommer att se på privatlivet som något föråldrat och som vi får lära oss inte längre existerar.

Käll- och litteraturförteckning

Källor

Offentligt tryck

Sverige

SOU 2008:3 *Skyddet för den personliga integriteten – bedömningar och förslag*

Ds 2014:23 *Datalagring, EU-rätten och svensk rätt*

USA

FCT, FCT Charges Deceptive Privacy Practices in Google´s Rollout of Its Buzz Social Network, FCT File No. 102 3136, 2011, <http://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz>, hämtad 14 oktober 2014

EU

Beslut och förslag

Kommissionens beslut av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (*Safe Harbor Privacy Principles*) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat (2000/520/EG), L 251/7, 25 augusti 2000

Kommissionens beslut av den 15 juni 2001 om standardavtalsklausuler för överföring av personuppgifter till tredje land enligt direktiv 95/46/EG (2001/479/EG), OJ L 181/19
[cit. KOM (2001/479/EG)]

Kommissionens beslut av den 27 december 2004 om ändring av beslut 2001/479/EG om standardavtalsklausuler för överföring av personuppgifter till tredje land (2004/915/EG), OJ L 385/74
[cit. KOM (2004/915/EG)]

Kommissionens beslut av den 5 februari 2010 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland i enlighet med Europaparlamentets och rådets direktiv 95/46/EG (2010/87/EU), OJ L 39/5
[cit. KOM (2010/87/EU)]

European Commission, Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Version 56, (29/11/2011), <http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf>
[cit. Utkast 56 om förslag till allmän dataskyddsförordning]

Kommissionens förslag av den 25 januari 2012 om förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän dataskyddsförordning), COM(2012) 11 final
[cit. Förslag till allmän dataskyddsförordning]

Europaparlamentets betänkande av den 21 november 2013 om förslaget till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän dataskyddsförordning), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), A7-0402/2013
[cit. Europaparlamentets betänkande]

Europeiska rådet, Förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän dataskyddsförordning), 2012/0011 (COD), Bryssel, 16 december 2013, <http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2017831%202013%20INIT>

Rekommendationer och yttranden

Article 29 Data protection Working Party, Working document: Transfers of personal data to third countries: Applying Atricle 26(2) of the EU Data Protection Directive to Binding Corprate Rules, WP 74, 3 juni 2003, <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_en.pdf>
[cit. WP 74]

Article 29 Data Protection Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of October 1995, WP 114, 25 november 2005, <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf>
[cit. WP 114]

Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, WP 179, 1 juli 2012, <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf>
[cit. WP 179]

European Parliament, Directorate general for Internal Policies, Policy Department C: Citizens´ Rights and Constitutional affairs, *Implementation of the EU Charter of Fundamental Rights and its Impact on EU Home Affairs Agencies*, Frontex, Europol and the European Asylum Support Office, 2011, <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/02_study_fundamental_rights_/02_study_fundamental_rights_en.pdf>
[cit. *Implementation of the EU Charter of Fundamental Rights and its Impact on EU Home Affairs Agencies* (2011)]

Article 29 Data Protection Working Party, Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 195, 6 juni 2012, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf>
[cit. WP 195]

Article 29 Data Protection Working Party, Opinion 5/2012 on Cloud Computing, WP 196, 1 juli 2012, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf>
[cit. WP 196]

Article 29 Data Protection Working Party, Opinion 07/2012 on the level of protection of personal data in the Principality of Monaco, WP 198, 19 juli 2012, <http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2012/wp198_en.pdf>
[cit. WP 198]

Meddelande från kommissionen till Europaparlamentet, rådet, europeiska ekonomiska och sociala kommittén samt regionskommittén, ”*Att frigöra de molnbaserade datortjänsternas potential i Europa*”, COM(2012) 529 final, 27 september 2012, <http://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52012DC0529&rid=1>
[cit. COM(2012) 529 final]

Pressmeddelande, Europeiska kommissionen: Kommissionen föreslår en genomgripande reform av reglerna om uppgiftsskydd för att öka användarnas kontroll över sina uppgifter och sänka företagens kostnader, IP/12/46, 25 januari 2014, <http://europa.eu/rapid/press-release_IP-12-46_sv.htm>
[cit. Pressmeddelande, EU-kommissionen: Förslag om genomgripande reform av reglerna om uppgiftsskydd]

Press release, European Commission: Data Protection Day 2014: Full Speed on EU Data Protection Reform, Memo/14/60, 27 january 2014, <http://europa.eu/rapid/press-release_MEMO-14-60_en.htm>
[cit. Pressmeddelande, EU-kommissionen: Data Protection Day 2014: Full Speed on EU Data Protection Reform]

Litteratur

Agell, Anders, *Rationalitet och värderingar i rättevetenskap – med en exkurs om rättsvetenskapen i Sverige*, Svensk Juristtidning, 2002, s. 243 – 260
[cit. Agell (2002)]

Bach, David & Newman, Abraham L., *The European regulatory state and global public policy: micro-institutions, macro-influence*, Journal of European Public Policy, 14:6, 2007, s. 827 – 846
[cit. Bach & Newman (2007)]

Bradford, Anu, *The Brussels Effect*, Northwestern University Law Review, vol. 17, nr. 1, 2012, s. 1 – 68
[cit. Bradford (2012)]

Burca, Gráinne de, *The European Court of Justice and the International Legal Order after Kadi*, Harvard International Law Journal, vol. 51, nr. 1, 2010, s. 1 – 50
[cit. Burca (2010)]

Colonna, Liane, *Article 4 of the EU Data Protection Directive and the irrelevance of the EU – US Safe Harbour Program?*, International Data Privacy Law, Oxford University Press, Vol. 4, No. 3, 2014, s. 203 – 221
[cit. Colonna (2014)]

Danelius, Hans, *Mänskliga rättigheter i europeisk praxis: en kommentar till Europakonventionen om de mänskliga rättigheterna*, 4 [uppdaterade] uppl., Norstedts juridik, Stockholm, 2012
[cit. Danelius (2012)]

Eckes, Christina, *European Legal Methods – Moving Away from Integration*, I: *European legal method: towards a new European legal realism*, Neergaard, Ulla & Nielsen, Ruth (red.), DJØF Publishing, Copenhagen, 2013
[cit. Eckes (2013)]

Edvardsson, Tobias & Frydlinger, David, *Molntjänster: juridik, affär och säkerhet*, Norstedts juridik, Stockholm, 2013
[cit. Edvardsson & Frydlinger, (2013)]

Edwards, Lilian, *Protection Online: The Laws Don´t Work?*, I: *Law and the Internet: a foundation for electronic commerce*, Edwards, Lilian & Waelde, Charlotte (red.), 3. uppl., Hart, Oxford, 2009
[cit. Edwards (2000)]

Gilbert, Francoise, *Proposed EU Data Protection Regulation: The Good, The Bad, and The Unknown*, Journal of Internet Law, Vol. 15, Nr. 10, 2012, s. 20 – 34
[cit. Gilbert (2012)]

Gräns, Minna, *Användningen av andra* vetenskaper, I: *Juridisk metodlära*, Korling, Fredric & Zamboni, Mauro (red.), Studentlitteratur, Lund, 2013
[cit. Gräns (2013)]

Hellström, Roger, *På molnfronten intet nytt? Vissa rättsliga aspekter på molntjänster*, Ny Juridik, 2:11, 2011, s. 37 – 51
[cit. Hellström (2011)]

Hettne, Jörgen & Otken Eriksson, Ida (red), *EU-rättslig metod: teori och genomslag i svensk rättstillämpning*, 2 omarb. uppl., Norstedts juridik, Stockholm, 2011
[cit. Hettne & Otken Eriksson (2011)]

Heyns, Christof & Viljoen, Frans, *The impact of the United Nations human rights treaties on the domestic level*, Kluwer Law International, The Hague, 2002
[cit. Heyns & Viljoen (2002)]

Hon, W. Kuan, Hörnle, Julia & Millard, Christopher, *Which Law(s) Apply to Personal Data in Clouds?*, I: *Cloud computing law*, red. Millard, Christopher, Oxford University Press, Oxford, 2013
[cit. Hon, Hörnle och Millard (2013)]

Hon, W. Kuan, Kosta, Eleni, Millard, Christopher, Stefanatou, Dimitra, *Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation*, Queen Mary University of London, School of Law, Legal Studies Research Paper, nr. 172, 2014
[cit. Hon m.fl. (2014)]

Hon, W. Kuan & Millard, Christopher, *Cloud Technologies and Services*, I: *Cloud computing law*, red. Millard, Christopher, Oxford University Press, Oxford, 2013
[cit. Hon & Millard, *Cloud Technologies and Services* (2013)]

Hon, W. Kuan & Millard, Christopher, *How Do Restrictions on International Data Transfers Work in Clouds?*, I: *Cloud computing law*, red. Millard, Christopher, Oxford University Press, Oxford, 2013
[cit. Hon & Millard (2013)]

Jareborg, Nils, *Rättsdogmatik som vetenskap*, Svensk Juristtidning, 2004, s. 1 – 10
[cit. Jareborg (2004)]

Kokott, Juliane & Sobotta, Christoph, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, International Data Privacy Law, Oxford University Press, Vol. 3, Nr. 4, 2013, s. 222 – 228
[cit. Kokott & Sobotta (2013)]

Koops, Bert-Jaap, *Criminal Law and Cyberspace as a Challenge for Legal Research*, Scripted, vol. 9, nr. 3, 2012
[cit. Koops (2012)]

Kuner, Christopher, *Transborder data flows and data privacy law*, Oxford University Press, Oxford, 2013
[cit. Kuner, (2013)]

Kuner, Christopher, Cate, Fred H., Millard, Christopher, Svantesson, Dan Jerker B., *The end of the beginning*, International Data Privacy Law, Oxford University Press, vol. 2, nr. 3, 2012, s. 115 – 116
[cit. Kuner m.fl. (2012)]

Kuner, Christopher, Cate, Fred H., Millard, Christopher, Svantesson, Dan Jerker B., *The extraterritoriality of data privacy laws – an explosive issue yet to detonate*, International Data Privacy Law, Oxford University Press, vol. 3, nr. 3, 2013, s. 147 – 148
[cit. Kuner, Cate, Millard & Svantesson (2013)]

Lebeck, Carl, *EU-stadgan om grundläggande rättigheter: en introduktion*, Studentlitteratur, Lund, 2013
[cit. Lebeck (2013)]

Lynskey, Orla, *Deconstructing data protection: The ”added-value” of a right to data protection in the EU legal order*, International and Comparative Law Quarterly, vol. 63, nr. 3, 2014, s. 569 – 597
[cit. Lynskey (2014)]

Manners, Ian, *Normative Power Europe: A Contradiction in Terms?*, Journal of Common Market Studies, vol. 40, nr. 2, 2002, s. 235 – 258
[cit. Manners (2002)]

Milanovic, Marko, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, Harvard International Law Journal, Forthcoming, 31 mars, 2014
[cit. Milanovic (2014)]

Mowbray, Alastair, *Cases, materials, and commentary on the European Convention on Human Rights*, 3 uppl, Oxford University Press, Storbritannien, 2012
[cit. Mowbray (2012)]

Nowak, Karol, *Oskyldighetspresumtionen*, Norstedts juridik, Diss. Göteborg: Handelshögskolan, 2003, Stockholm, 2003
[cit. Nowak (2003)]

Nye, Joseph S., *On the Rise and Fall of American Soft Power*, New Perspectives Quarterly, vol. 22, nr. 3, 2005, s. 75 – 77
[cit. Nye (2005)]

Rainey, Bernadette, Wicks, Elizabeth & Ovey, Clare, *Jacobs, White and Ovey: the European Convention on Human Rights*, 6. uppl., 2014
[cit. Rainey m.fl. (2014)]

Rauhofer, Judith, *Privacy is dead, get over it! Information privacy and the dream of a risk-free society*, Information & Communications Technology Law, Vol, 17, Nr. 3, 2008, s. 185 – 197
[cit. Rauhofer (2008)]

Rauhofer, Judith, *Round and Round the Garden? Big Data, Small Government and the Balance of Power in the Information Age*, Edinburgh School of Law Research Paper Series, University of Edinburgh, nr 6, 2014
[cit. Rauhofer (2014)]

Rauhofer, Judith & Bowden, Casper, *Protecting their own: Fundamental rights implications for EU data sovereignty in the cloud*, Edinburgh School of Law Research Paper Series, University of Edinburgh, nr 28, 2013
[cit. Rauhofer & Bowden (2013)]

Reichel, Jane, *EU-rättslig metod*, I: *Juridisk metodlära*, Korling, Fredric & Zamboni, Mauro (red.), Studentlitteratur, Lund, 2013
[cit. Reichel (2013)]

Rubinstein, Ira S., Lee, Ronald D., Schwartz, Paul M., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, University of Chicago Law Review, vol. 75, 2008, s. 261 – 285
[cit. Rubinstein m.fl. (2008)]

Sandgren, Claes, *Är rättsdogmatiken dogmatisk?*, Tidsskrift for rettsvittenskap, 2005, s. 648 – 656
[cit. Sandgren (2005)]

Sandgren, Claes, *Rättsvetenskap för uppsatsförfattare – Ämne, material, metod och argumentation*, 2 uppl., Norstedts Juridik, Stockholm, 2007
[cit. Sandgren (2007)]

Solove, Daniel J., *The Digital Person: Technology and Privacy in the Information Age*, New York University Press, 2004
[cit. Solove (2004)]

Svantesson, Dan Jerker B, *A "layered approach" to the extraterritoriality of data privacy laws*, International Data Privacy Law, Oxford University Press, vol. 3, nr. 4, 2013, s. 278 – 286
[cit. Svantesson (2013)]

Tzanou, Maria, *Data protection as a fundamental right next to privacy? "Reconstructing" a not so new right*, International Data Privacy Law, Oxford University Press, vol. 3, nr. 2, 2013, s. 88 – 99
[cit. Tzanou (2013)]

van Dijk, Pieter (red.), *Theory and practice of the European Convention on Human Rights*, 4. ed., Intersentia, Antwerpen, 2006
[cit. van Dijk (2006)]

van Gestel, Rob, Micklitz, Hans-W., Poiares Maduro, Miguel, *Methodology in the new legal world*, EUI Working Papers, Department of Law, 2012/13
[cit. van Gestel, Micklitz & Poiares Maduro (2012/13)]

van Hoboken, Joris V.J., & Rubinstein, Ira S., *Privacy and security in the cloud: some realism about technical solutions to transnational surveillance in the post-snowden era*, Maine Law Review, vol. 66, nr. 2, 2014, s. 487 – 534
[cit. van Hoboken & Rubinstein (2014)]

van Vooren, Bart, Blockmans, Steven & Wouters, Jan, *The Legal Dimension of Global Governance: What Role for the European Union? An Introduction*, I: *The EU's role in global governance: the legal dimension*, red. Van Vooren, Bart, Blockmans, Steven & Wouters, Jan, Oxford University Press, Oxford, 2013
[cit. van Vooren m.fl. (2013)]

Elektroniska källor

Amazon Webservice, *Amazon S3*,<http://aws.amazon.com/s3/>, hämtad den 19 oktober 2014

Brandel, Tobias, *Vem ska äga makten över dig på nätet?*, Svenska Dagbladet, 27 maj 2013, <http://www.svd.se/nyheter/utrikes/vem-ska-aga-makten-over-dig-pa-natet_8211028.svd>, hämtad den 14 oktober 2014
[cit. Brandel, Svenska Dagbladet: *Vem ska äga makten över dig på nätet?*]

Dropbox, ”*Dina saker, var du än är*”, <https://www.dropbox.com/>, Hämtad den 19 oktober 2014

Europe v. Facebook, *Complaints against Facebook Ireland Ltd*, Wien, 18 augusti, 2011, <http://europe-v-facebook.org/Complaint_07_Messages.pdf>, hämtad den 13 december 2014
[cit. Complaint against Facebook Ireland Ltd. (2011)]

Europeiska kommissionen, *Commission decisions on the adequacy of the protection of personal data in third countries*, senast uppdaterad den 24 juni 2014, <http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm>, hämtad den 14 oktober 2014
[cit. *Commission decisions on the adequacy of the protection of personal data in third countries*, senast uppdaterad den 24 juni 2014]

Europeiska kommissionen, dataskydd, *Information om Artikel 29-gruppen,* <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm>, hämtad den 14 oktober 2014
[cit. EU-kommissionen, *Information om Artikel 29-gruppen*]

Facebook Inc, Facebooks villkor, *Policy om rättigheter och skyldigheter*, uppdaterat 15 november 2013,<https://www.facebook.com/legal/terms>, hämtad den 13 december 2014
[cit. Facebook Inc., Policy om rättigheter och skyldigheter]

Facebook Inc, Facebooks villkor, *Privacy Policy*, träder ikraft den 1 januari 2015, <https://www.facebook.com/about/privacy/update/>, hämtad den 15 december 2014
[cit. Facebook, *Privacy policy*, 1 januari 2015]

Google, *Google App Engine: Platform as a Service,* <https://cloud.google.com/appengine/docs>, hämtad den 19 oktober 2014

Greenwald, Glenn, *NSA collecting phone records of millions of Verizon customers daily*, The Guardian, 6 juni 2013, <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>, hämtad den 1 december 2014
[cit. Greenwald, *The Guardian*, 6 juni 2013]

Kopstein, Joshua & Sottek, T.C., *Everything you need to know about PRISM – A cheat sheet for the NSA´s unprecedented surveillance programs*, 17 juli 2013, <http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet>, hämtad den 18 september 2014
[cit. Kopstein & Sottek (2013)]

Kuner, Christopher, *Extraterritoriality and the Fundamental Right to Data Protection*, EJIL:Talk!, 16 december, 2013, <http://www.ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/#more-10092>, hämtad den 2 december 2014
[cit. Kuner, *EJIL:Talk!* (2013)]

Mell, Peter, Grance, Timothy, *The NIST Definition of Cloud Computing*, NIST Special Publication 800-145, Gaitherburg, 2011, <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>, hämtad den 2 oktober 2014
[cit. Mell & Grance, *NIST:s definition av molntjänster* (2011)]

Microsoft, *Office Online*, <https://office.com/start/default.aspx>, hämtad den 19 oktober 2014

Milanovic, Marko, *Foreign Surveillance and Human Rights, Part 5: The Substance of an Extraterritorial Right to Privacy*, EJIL:Talk!, 29 november, 2013, <http://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-5-the-substance-of-an-extraterritorial-right-to-privacy/>, hämtad den 3 december 2014
[cit. Milanovic, *EJIL:Talk!* (2013)]

Padova, Yann, *EU: Will the Court of Justice of the EU invalidate "Safe Harbor" agreement because of the PRISM scandal?*, GlobalComplianceNews: A new platform moderated by Baker & McKenzie, 8 november, 2014, <http://globalcompliancenews.com/cjeu-safe-harbor-20141109/>, hämtad den 10 december 2014
[cit. Padova (2014)]

Svantesson, Dan, *The territorial scope of the purposed EU Data Protection Regulation*, blawblaw-blogg, Institutet för Rättsinformatik, Juridiska institutionen vid Stockholms universitet, 24 mars 2013, <*http://blawblaw.se/2013/03/the-territorial-scope-of-the-proposed-eu-data-protection-regulation/*>, hämtad den 17 november 2014
[cit. Svantesson, *The territorial scope of the proposed EU Data Protection Regulation*, blawblaw (2013)]

US – EU Safe Harbor, Overview, <http://export.gov/safeharbor/eu/eg_main_018476.asp>, hämtad den 17 oktober 2014
[cit. US – EU Safe Harbor, Overview]

Övriga källor

Milanovic, Marko, Lecture: *The Extraterritorial Application of Human Rights Treaties*, UN WEB TV, Audiovisual Library of International Law, 28 oktober, 2014, <http://webtv.un.org/news-features/audiovisual-library-of-international-law-avl/watch/marko-milanovic-on-the-extraterritorial-application-of-human-rights-treaties/3875099482001>, hämtad den 3 december 2014
[cit. Milanovic, Föreläsning om extraterritoriell effekt av människorätts-konventioner (2014)]

Rättsfallsförteckning

Internationell praxis

EU-domstolen

Mål C-238/99 P, *Limburgse Vinyl Maatschappij m.fl.* mot *kommissionen*, EU:C:2002:582

Mål C-244/99 P, *DSM och DSM Kunststoffen* mot *kommissionen*, EU:C:2002:582

Mål C-101/01, *Lindqvist*, EU:C:2003:596

Mål C-301/04, *Europeiska kommissionen* mot *SGL Carbon AG*, EU:C:2006:432

Mål i de förenade målen C-92/09 och 93/09, *Volker und Markus Schecke GbR och Hartmut Eifert* mot *Land Hessen*, EU:C:2010:662

Mål C-324/09, *L'Oréal SA m.fl.* mot *eBay International AG m.fl.*, EU:C:2011:474

Mål C-283/11, *Sky Österreich GmbH* mot *Österreichischer Rundfunk*, EU:C:2013:28

Mål C-101/12, *Herbert Schaible* mot *Land Baden-Württemberg*, EU:C:2013:661

Mål i de förenade målen C-293/12 och 594/12, *Digital Rights Ireland Ltd* mot *Minister for Communications, Marine and Natural Resources m.fl. och Kärntner Landesregierung m.fl.*, EU:C:2014:238

Mål C-131/12, *Google Spain SL och Google Inc.* mot *Agencia Española de Protección de Datos (AEPD) och Mario Costeja González*, EU:C:2014:317

Mål C-362/14, *Schrems* mot *Data Protection Commissioner*, [målet pågår]

Generaladvokatens förslag till avgörande

De förenade målen C-293/12 och 594/12, *Digital Rights Ireland Ltd* mot *Minister for Communications, Marine and Natural Resources m.fl. och Kärntner Landesregierung m.fl.*, förslag till avgörande av generaladvokat Pedro Cruz Villalón, EU:C:2013:845

Europadomstolen

Handyside mot *Förenade Konungariket*, dom den 7 december 1976, ans. nr. 5493/72

Malone mot *Förenade Konungariket*, dom den 2 augusti 1984, ans. nr. 8691/79

Niemietz mot *Tyskland*, dom den 16 december 1992, ans. nr. 13710/88

Chahal mot *Förenade Konungariket*, dom den 15 november 1996, ans. nr. 22414/93

Z mot *Finland*, dom den 26 februari 1997, ans. nr. 22009/93

Amann mot *Schweiz*, dom den 16 februari 2000, ans. nr. 27798/95

Rotaru mot *Rumänien*, dom den 4 maj 2000, ans. nr. 28341/95

Jabari mot *Turkiet*, dom den 11 juli 2000, ans. nr. 40035/98

Bensaid mot *Förenade Konungariket*, dom den 6 februari 2001, ans. nr. 44599/98

Peck mot *Förenade Konungariket*, dom den 28 januari 2003, ans. nr. 44647/98

Dangeville SA mot *Frankrike*, dom den 16 april 2003, ans. nr. 45036/98

Assanidze mot *Georgien*, dom den 8 april 2004, ans. nr. 71503/01

Sciacca mot *Italien*, dom den 11 januari 2005, ans. nr. 50774/99

Segerstedt-Wiberg m.fl. mot *Sverige*, dom den 6 juni 2006, ans. nr 62332/00

S. och Marper mot *Förenade Konungariket*, dom den 4 december 2008, ans. nr. 30562/04 och 30566/04

M.M. mot *Förenade Konungariket*, dom den 13 november 2012, ans. nr. 24029/07

Nationell praxis

Irland

Schrems mot *Data Protection Commissioner* [2014] IEHC 310

USA

International Shoe Co. mot *Washington*, 326 U.S. 310 (1945)

Hanson mot *Denckla*, 357 U.S. 235 (1958)