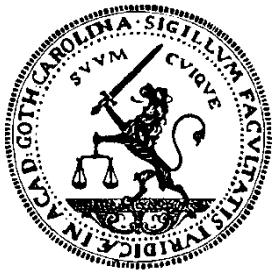

JURIDISKA FAKULTETEN
vid Lunds universitet

Anton Lucius

När personuppgifter korsar Atlanten

En analys av Safe Harbor-systemets ogiltigförklarande

LAGF03 Rättsvetenskaplig uppsats

Uppsats på juristprogrammet
15 högskolepoäng

Handledare: Moa De Lucia Dahlbeck

Termin: HT 2015

Innehåll

Summary

To various internet companies the collection, storage and use of personal data that has been transmitted through registration is an essential part of the companies business. Personal data refers to all information relating to a specific person and as a consequence of society's globalization this information has a considerable commercial value. The transfer of personal data from the EU to the US is a necessity to many companies but the transatlantic data flow is at the same time associated with the risk of privacy interference.

The right to privacy is guarantied EU citizens through a strong protection in convention and primary law. In order to protect the privacy of individuals, EU data protection law establishes a prohibition against third country transfers. However, derogations are provided to enable a transborder data flow.

In commercial terms, the Safe Harbor system was one of the most important derogations with thousands of member companies. After Edward Snowden's revelations, the systems compatibility with the right to privacy was questioned and in October 2015 the CJEU declared the system invalid. Consequently, former Safe Harbor member companies must implement alternative transfer methods. The privacy law discrepancy between the EU and the US remains however and even through the use of alternative mechanisms there is a risk of privacy interference.

The alternative transfer methods do not provide better guaranties that the fundamental rights of EU citizens are being protected and in the light of the reinforcement of the right to privacy which the CJEU case law demonstrates there is a strong likelihood that the alternatives will also be declared invalid.

Sammanfattning

En central del av många internetföretags verksamhet är insamlingen, lagringen och användningen av personuppgifter som överlämnats till bolagen genom registrering. Med personuppgifter avses all information som kan hänföras till en specifik person och i takt med samhällets globalisering har denna information kommit att få ett betydande kommersiellt värde. Överföringen av personuppgifter från EU till USA är för många företag en nödvändighet men detta transatlantiska dataflöde är samtidigt förenat med risken för att individens integritet inskränks.

Rätten till skydd för den personliga integriteten tillförsäkras EU-medborgarna genom ett starkt konventions- och primärrättsligt stadgat skydd. I syfte att skydda individernas integritet uppställs inom den EU-rättsliga dataskyddslagstiftningen ett generellt förbud mot tredjelandsöverföringar. Undantag från förbudet har emellertid inrättats för att möjliggöra ett gränsöverskridande dataflöde.

Safe Harbor-systemet var i kommersiellt hänseende ett av de viktigaste undantagen med tusentals anslutna företag. Efter Edward Snowdens avslöjanden kom systemets förenlighet med den personliga integriteten att ifrågasättas och i oktober 2015 ogiltigförklarades Safe Harbor av EU-domstolen. Konsekvensen är att de företag som tidigare varit anslutna till systemet måste implementera alternativa överföringsmetoder. Den integritetsrättsliga diskrepans som råder mellan EU och USA kvarstår dock och även genom tillämpning av alternativa metoder finns en risk för att integriteten åsidosätts.

De alternativa överföringsmetoderna ställer inte bättre garantier för att EU-medborgarnas grundläggande rättigheter skyddas och mot bakgrund av den personliga integritetens förstärkning som EU-domstolens praxis uppvisar är sannolikheten stor att även alternativen ogiltigförklaras.

Förkortningar

Art. 29-gruppen	Article 29 Data Protection Working Party
BCRs	Binding Corporate Rules
CJEU	Court of Justice of the European Union
Datalagringsdirektivet	Europaparlamentet och rådets direktiv 2006/24/EG av den 15 mars 2006 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
Dataskyddsdirektivet	Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter
EKMR	Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna
EU	Europeiska unionen
EU-domstolen	Europeiska unionens domstol
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
Europadomstolen	Europeiska domstolen för de mänskliga rättigheterna
FEUF	Fördraget om europeiska unionens funktionssätt
Kommissionen	Europeiska kommissionen
Lissabonfördraget	Lissabonfördraget om ändring av fördraget om Europeiska unionen och fördraget om upprättandet av Europeiska gemenskapen
NSA	National Security Agency

1 Inledning

1.1 Bakgrund

När ett användarkonto registreras på internet överlämnas personlig information som i kommersiellt hänseende kan ha ett betydande värde. Till följd av samhällets digitalisering har behandlingen av personuppgifter genom bl.a. insamling och lagring fått en allt större betydelse. Vissa integritetsrättsliga problem uppstår dock när personuppgifter överförs från EU till USA.

Det integritetsskydd som tillförsäkras unionsmedborgarna bortfaller när europeiska personuppgifter lämnar unionen och således uppställs ett generellt förbud mot tredjelandsöverföringar. I syfte att tillgodose företagens behov av ett gränsöverskridande dataflöde har undantag emellertid inrättats. Det s.k. Safe Harbor-systemet är ett av dessa undantag som tusentals företag anslutit sig till, däribland Facebook, Google och Microsoft.

Efter Edward Snowdens avslöjanden om amerikanska myndigheters insamling av underrättelseinformation väcktes frågor om Safe Harbor-systemets förenlighet med den personliga integriteten. Ett rättsligt efterspel inleddes som resulterade i att EU-domstolen ogiltigförklarade systemet i oktober 2015. Följaktligen har ett oklart rättsläge beträffande det transatlantiska dataflödet uppstått.

1.2 Syfte och frågeställningar

Syftet med denna uppsats är att, utifrån relevanta rättskällor, redogöra för överföringen av personuppgifter från EU till USA i förhållande till den personliga integriteten inom EU. Uppsatsen har även till syfte att analysera ogiltigförklarandet av Safe Harbor-systemet och exemplifiera tänkbara rättsliga konsekvenser i ljuset av den personliga integriteten. Följande frågeställningar kommer att utredas:

- Hur förhåller sig den transatlantiska personuppgiftsöverföringen till den personliga integriteten?
- Vilka alternativa överföringsmetoder kan företag tillämpa efter ogiltigförklarandet av Safe Harbor-systemet?
- Tillförsäkrar alternativen ett tillräckligt skydd för den personliga integriteten?

1.3 Avgränsningar

Framställningen utgår ifrån integritetsskyddets betydelse i förhållande till kommersiella intressen inom den europeiska dataskyddslagstiftningen. Överföringen av personuppgifter i brottsbekämpningsändamål kommer därmed inte att undersökas.

Då den inom EU-rätten reglerade dataskyddslagstiftningen och integritetsskyddet undersöks i förhållande till kommersiella intressen i en global kontext kommer nationella bestämmelser som implementerats till följd av exempelvis dataskyddsdirektivet inte att beröras.

Den ännu inte antagna allmänna dataskyddsförordningen och dess eventuella konsekvenser för dataskyddslagstiftningen inom EU kommer, av utrymmesskäl, inte att undersökas i någon fördjupande mening.

Vad beträffar rätten till skydd för den personliga integriteten kommer framställningen att avgränsas till EKMR och EU-stadgan då det för uppsatsen centrala dataskyddsdirektivet utgår ifrån dessa två instrument. Det integritetsskydd som är stadgat i Europarådets dataskyddskonvention kommer således inte att behandlas.

1.4 Metod och material

EU-rättslig metod kommer att användas för att besvara uppsatsens frågeställningar. I enlighet med den EU-rättsliga metoden kan EU-rätten

betraktas som en autonom rättsordning och metoden används som ett tillvägagångsätt för att hantera EU-rättsliga källor.[1] Lagstiftning, domstolspraxis och doktrin kommer att studeras utifrån ett internationellt perspektiv där överföringen av personuppgifter och dess förhållande till den personliga integriteten undersöks i en global kontext.

Material som varit av stor vikt för uppsatsen är även beslut och meddelanden från kommissionen vilka fungerat som riktlinjer i den rättsutveckling som dataskyddslagstiftningen genomgått inom EU.

1.5 Forskningsläge

Överföringen av personuppgifter från EU till USA som en del av den EU-rättsliga dataskyddslagstiftningen är ett begränsat undersökningsområde som under senare år fått ett allt större utrymme. Edward Snowdens avslöjanden och EU-domstolens avgöranden angående den personliga integriteten är bidragande orsaker till att ämnet fått stor uppmärksamhet. Rättsområdet har dock undersökts i liten omfattning vilket åskådliggörs av de förhållandevis få och återkommande författare som förekommer i doktrinen.

Då Safe Harbor-systemet ogiltigförklarades av EU-domstolen i oktober 2015 har de frågeställningar som är förenade med domen ännu inte undersökts i någon större utsträckning.

1.6 Disposition

I kapitel 2 redogörs för den europeiska dataskyddslagstiftningen och en beskrivning av Safe Harbor-systemet presenteras. I kapitel 3 behandlas rätten till skydd för den personliga integriteten utifrån EKMR samt EU-stadgan och därtill relevant domstolspraxis. Redogörelsen i kapitel 2 och 3 är nödvändig för att förstå *Schrems*-domen som behandlas i kapitel 4. Kapitel 5 berör vissa av de rättsliga konsekvenser som domen kan komma att ha ur ett kommersiellt

[1] Korling och Zamboni 2013, s. 109.

perspektiv genom att presentera de alternativa överföringsmetoder som företag kan tillämpa. I kapitel 6 avslutas uppsatsen med en analys av integritetsskyddets utveckling och förenlighet med de alternativa metoderna. Analysen kommer även att innehålla vissa framtidsaspekter.

2 Överföringen av personuppgifter från EU till USA

Den tekniska utvecklingen och samhällets digitalisering har under de två senaste decennierna i stor utsträckning påverkat det gränsöverskridande dataflödet. Internet och elektroniska kommunikationstjänster såsom molntjänster och sociala medier kännetecknas av gränslöshet och dess framväxt har bidragit till de digitala miljöernas globala karaktär.[2] En konsekvens av detta är att det skett en exponentiell tillväxt i behandlingen av personuppgifter i kommersiellt hänseende.[3] Möjligheten att exempelvis klarlägga digitala beteenden och individualisera marknadsföring är en av många orsaker till att EU-medborgarnas personuppgifter idag har ett betydande kommersiellt värde.[4]

Då världens största it-bolag befinner sig i USA är överföringen av personlig data utanför EU:s gränser av stor vikt för den internationella handelns utveckling. Ett transatlantiskt flöde av uppgifter som är hänförliga till specifika personer är emellertid inte helt oproblematiskt, i synnerhet med tanke på den personliga integriteten. I syfte att motverka en otillbörlig behandling av dessa uppgifter och att säkerställa ett starkt skydd för individer har det ansetts nödvändigt att reglera förfarandet inom EU.

2.1 Dataskyddsdirektivet

Redan 1990 argumenterade kommissionen för att upprätta ett enhetligt integritetsskydd i samband med behandlingen av personlig data.[5] Åtta år senare antogs dataskyddsdirektivet som ett resultat av en avvägning mellan individens behov av skydd beträffande personlig information och företagens behov av ett fritt dataflöde över gränserna.[6] Denna intressemotsättning illustrerar även

[2] Magnusson Sjöberg 2015, s. 33.
[3] Kommissionens meddelande COM(2013) 846 final, s. 3.
[4] Boston Consulting Group, The Value of our Digital Identity, 2012.
[5] Gonzáles Fuster 2014, s. 125.
[6] Rauhofer och Bowden 2013, s. 3.

direktivets syfte; att förbjuda begränsningar av det fria flödet mellan medlemsstater och samtidigt skydda individens grundläggande fri- och rättigheter.[7]

Ett fritt flöde av personuppgifter kan hänföras till EU:s inre marknad som förutsätter en fri rörlighet av varor, personer, tjänster och kapital. En gemensam reglering på området effektiviserar flödet av personlig information vilket bidrar till att upprätthålla en ekonomisk integration inom unionen.[8] Utan restriktioner uppstår dock en risk för att den personliga integriteten inskränks när uppgifter inhämtas, överförs eller lagras. I direktivet betonas därför att rätten till privatlivet är en grundläggande rättighet som inte får åsidosättas när informationen behandlas.[9] Denna rättighet återfinns både i EKMR och i EU:s rättighetsstadga. Följaktligen framställer direktivet goda förutsättningar för en hög skyddsnivå av personuppgifter inom EU.

I syfte att säkerställa efterlevnaden av uppgiftsskyddet har nationella och oberoende tillsynsmyndigheter inrättats. Dessa dataskyddsmyndigheter har en övervakande funktion med befogenhet att ingripa och inleda rättsliga förfaranden vid eventuella överträdelser av dataskyddsreglerna.[10] Direktivets antagande resulterade även i etablerandet av den s.k. art. 29-gruppen, en oberoende och rådgivande arbetsgrupp som består av representanter från medlemsstaternas tillsynsmyndigheter. Genom yttranden och rekommendationer har gruppen som mål att bidra till en enhetlig tillämpning av reglerna inom EU och samtidigt se till att integritetsskyddet inte åsidosätts.[11]

2.1.1 En allmän dataskyddsförordning

Dataskyddsdirektivet är idag rättsligt bindande för EU:s samtliga medlemsstater samt staterna inom EES.[12] Implementeringen av dataskyddslagstiftningen har

[7] Jfr. dataskyddsdirektivet art. 1.
[8] Lebeck 2013, s. 142.
[9] Jfr. dataskyddsdirektivet skäl 10.
[10] Jfr. dataskyddsdirektivet skäl 62-63 och art. 28.
[11] Jfr. dataskyddsdirektivet skäl 65 och art. 29-30.
[12] Kuner 2013, s. 41.; EES-kommitténs beslut nr. 83/1999.

dessvärre resulterat i en fragmentarisk nationell reglering inom unionen. Möjligheten att utöva de rättigheter som framgår av direktivet varierar och således har en splittrad rättslig miljö uppstått.[13] Till följd av denna bristande enhetlighet bland medlemsstaterna presenterade kommissionen 2012 ett förslag till en allmän dataskyddsförordning i syfte att effektivisera skyddet av personuppgifter på den inre marknaden.[14] Eftersom att en förordning, till skillnad från ett direktiv, enligt art. 288 FEUF är direkt tillämplig kan harmoniserade kärnbestämmelser inrättas vilket med stor sannolikhet kommer att öka rättssäkerheten.[15] Förordningen har ännu inte antagits men belyser vissa av dataskyddsdirektivets svagheter.

2.2 Safe Harbor

Överföringen av personuppgifter från EU till USA är en viktig del av de transatlantiska förbindelserna, i synnerhet för växande digitala affärsverksamheter.[16] Det skydd som dataskyddsdirektivet tillförsäkrar enskilda sätts dock ur spel när uppgifterna lämnar den inre marknaden. Då ett ur EU-rättsligt perspektiv godtagbart skydd för personlig information inte kan garanteras i tredje länder uppställer direktivet ett generellt förbud mot sådana överföringar.[17]

Mot bakgrund av de gränsöverskridande dataflödenas vikt för den ekonomiska utvecklingen inom unionen har ett undantag emellertid gjorts genom principen om adekvat skyddsnivå som återfinns i direktivets art. 25.1. Principen innebär att personuppgifter får överföras till ett tredje land under förutsättning att en adekvat skyddsnivå för dessa uppgifter säkerställs i det landet. Huruvida skyddsnivån är adekvat, i direktivets mening, avgörs av kommissionen utifrån det tredje landets interna lagstiftning eller på grund av internationella förpliktelser.[18]

[13] Kommissionens meddelande COM(2012) 9 final, s. 4ff.
[14] Kommissionens förslag till förordning COM(2012) 11 final, s. 3ff.
[15] Ibid, s. 5f.
[16] Kommissionens meddelande COM(2013) 846 final, s. 2.
[17] Millard 2013, s. 254f.
[18] Jfr. dataskyddsdirektivet art. 25.6.

Kommissionen har hittills endast erkänt ett fåtal länder och flera av dessa utgör mindre territorier i Europa, däribland Andorra och Isle of Man.[19]

Vad gäller USA konstaterade kommissionen i samband med antagandet av dataskyddsdirektivet att en adekvat skyddsnivå inte förelåg. Detta innebar ett handelshinder som gav upphov till förhandlingar mellan kommissionen och amerikanska handelsdepartementet med målet att inrätta ett förfarande som skulle möjliggöra ett fritt flöde av personlig data från EU till USA.[20] Genom kommissionens beslut 2000/520 resulterade förhandlingarna i det s.k. Safe Harbor-systemet som innefattar särskilda regler om integritetsskydd enbart tillämpliga på amerikanska företag som tar emot personuppgifter från EU.

Safe Harbor-systemet bygger huvudsakligen på frivilligt anslutande från enskilda amerikanska organisationer som vill åtnjuta ett fritt dataflöde över Atlanten. För att motverka en behandling av personuppgifter som inskränker den personliga integriteteten måste företag som lagrar, använder eller sprider europeiska uppgifter vidta vissa säkerhetsåtgärder. Safe Harbor uppställer därmed regler som tar sikte på dels det materiella skyddet av personuppgifter, dvs. principer för dataskydd och integritet, dels processuella rättigheter som ger enskilda tillgång till rättsmedel för att kunna framställa invändningar mot uppgifternas hantering.[21] För att ytterligare skydda den personliga integriteten måste företagen även underställa sig en tillsynsmyndighet som ser till att reglerna efterlevs.[22]

Anslutningsförfarandet enligt Safe Harbor-systemet utgår ifrån självcertifiering vilket innebär att amerikanska företags interna integritetsskyddspolicy utgör grunden för en eventuell anslutning.[23] När ett i USA etablerat företags policy överensstämmer med systemets skyddsregler skapas en presumtion om adekvat skyddsnivå som i sin tur rättfärdigar fri överföring av personuppgifter från EU

[19] Millard 2013, s. 254.; kommissionens beslut 2010/625/EU och 2004/411/EG.
[20] Gonzáles Fuster 2014, s. 138f.
[21] Kommissionens meddelande COM(2013) 847 final, s. 3.
[22] Kommissionens beslut 2000/520, skäl 5.
[23] Bilaga I till kommissionens beslut 2000/520, 3st.

till USA.[24] Konsekvensen, utifrån en integritetsrättslig aspekt, blir att de organisationer som anslutit sig till systemet betraktas som ”trygga hamnar” i en annars otrygg rättsordning. I slutet av 2013 uppgick antalet Safe Harbor-certifierade organisationer till 3 246, inklusive välkända internetföretag som Facebook och Google.[25]

[24] Bilaga I till kommissionens beslut 2000/520, 2st.
[25] Kommissionens meddelande COM(2013) 847 final, s. 5.

3 Den personliga integriteten

Det internationella flödet av personlig information har under senare år intensifierats med följden att individernas integritet blivit utsatt för nya och ökade risker.[26] Rätten till skydd för den personliga integriteten är en grundläggande mänsklig rättighet och betraktas vara ett utflöde av skyddet för privatlivet som återfinns i både EKMR och EU:s rättighetsstadga.[27] Integritetsskyddet är samtidigt en relativ rättighet vilket ger utrymme för vissa inskränkningar. I vilken utsträckning det är motiverat att skyddet begränsas är en svår fråga som, i ljuset av samhällets digitalisering, har fått en allt större betydelse.

3.1 Europakonventionen

Europadomstolen betraktar EKMR som ett levande instrument där samhällets utveckling ska iakttas vid rättigheternas tillämpning.[28] Denna inställning har bidragit till en extensiv tolkning av rätten till respekt för privatlivet som tillförsäkras var och en genom konventionens art. 8.1. Begreppet privatliv är svårdefinierat och dess avgränsning varierar utifrån omständigheterna i det enskilda fallet.[29] Ett integritetsskydd vad beträffar behandlingen av personuppgifter kan dock härledas ur skyddet för privatlivet, vilket bekräftas av Europadomstolens praxis.

Målet *S och Marper* illustrerar den variation av grunder som kan berättiga viss information som anknytande till privatlivet. Rättsfrågan i målet berörde huruvida brittiska myndigheters lagring av den klagandes fingeravtryck och DNA-profil efter nedlagt åtal stod i strid med art. 8 i EKMR. Domstolen ansåg att skyddet för privatlivet är av särskild vikt när personuppgifter är föremål för automatisk

[26] Kuner 2013, s. 1ff.
[27] Gonzáles Fuster 2014, s. 22f.
[28] Ibid, s. 94f.
[29] Peers m.fl. 2014, s. 156.

behandling där det föreligger stor risk för otillåten tillgång till uppgifterna.[30] Mot bakgrund av den identifierbara informationens ytterst personliga natur fann domstolen att myndigheternas förvarande innebar en inskränkning av art. 8.[31] Det kan därmed konstateras att personlig information kan ha olika skepnader och dess skydd är av stor betydelse för individens åtnjutande av rätten till respekt för privatlivet.

Förutom lagring av personuppgifter kan även myndigheters vägran att tillgängliggöra uppgifterna till den individ som informationen avser utgöra ett åsidosättande av art. 8.[32] Detta har framhållits i bl.a. målet *Leander* där en snickares jobbansökan nekades till följd av den information om honom som återfanns i ett sekretessbelagt polisregister.[33] Det faktum att snickaren inte fick tillgång till hans personuppgifter och därmed inte heller möjlighet att bemöta informationen innebar enligt domstolen att en inskränkning av konventionsskyddet förelåg.[34]

Rättigheten är emellertid inte absolut och av art. 8.2 framgår att en inskränkning av integritetsskyddet kan rättfärdigas under förutsättning att åtgärden har stöd i lag samt syftar till att tillvarata ett berättigat intresse som är nödvändigt i ett demokratiskt samhälle. I det här hänseendet har konventionsstaternas myndigheter ett utrymme för en skönsmässig bedömning vad gäller inskränkningarnas förenlighet med undantaget.[35] Denna bedömning varierar beroende på bl.a. rättighetens beskaffenhet, ingreppets allvar och syftet med inskränkningen.[36]

Bedömningsmarginalen är dock begränsad då Europadomstolen har uttalat att art. 8.2 ska tolkas restriktivt.[37] Detta innebär att nationella lagar som möjliggör

[30] *S och Marper mot Förenade kungariket* [2008] nr. 30562/04, p. 103.
[31] Ibid, p 73.
[32] Gonzáles Fuster 2014, s. 102.
[33] *Leander mot Sverige* [1987] nr. 9248/81, p. 10-13.
[34] *Leander mot Sverige* [1987] nr. 9248/81, p. 48.
[35] *Connors mot Förenade kungariket* [2004] nr. 66746/01, p. 82.
[36] Ibid.
[37] *Klass mot Tyskland* [1978] nr. 5029/71, p. 42.

ett ingrepp i den personliga integriteten måste vara förutsebara och ge effektiva garantier mot orättfärdigt utnyttjande av undantaget.[38] Lagarna måste dessutom vara proportionerliga i förhållande till det berättigade intresset och tillförsäkra individer en behandling av personuppgifter som inte går utöver vad som är nödvändigt för att uppnå syftet med behandlingen.[39]

Rätten till respekt för privatlivet som garanteras av EKMR är även relevant vid tolkningen av dataskyddsdirektivet, vilket kan utläsas ur hänvisningen till konventionen i direktivets ingress.[40] EU-domstolen har också bekräftat detta och anser att art. 8 i konventionen är nödvändig att beakta då direktivet tillämpas.[41] Europadomstolens praxis har således betydelse för den personliga integritetens omfattning även inom ramen för EU-rättsliga bedömningar, detta trots att unionen i sig inte anslutit till konventionen.

3.2 EU-stadgan

Skyddet för den personliga integriteten i EU-stadgan tillförsäkras unionsmedborgarna dels genom art. 7 som reglerar respekten för privatlivet, dels genom art. 8 som reglerar skyddet av personuppgifter. Stadgan innehåller många likheter med EKMR och har som syfte att stärka skyddet av de grundläggande fri- och rättigheterna i ljuset av samhällsutvecklingen.[42]

Genom Lissabonfördraget, som trädde i kraft 2009, infördes en ny primärrättslig grund för skyddet av personuppgifter, nämligen art. 16 FEUF. Denna bestämmelse gör det möjligt att inom EU fastställa heltäckande dataskyddsregler som syftar till att garantera ett starkt integritetsskydd.[43] Lissabonfördraget innebar även en konstitutionell reform som resulterade i att EU:s rättighetsstadga

[38] Rauhofer och Bowden 2013, s. 19f.
[39] Peers m.fl. 2014, s. 236.
[40] Jfr. dataskyddsdirektivet skäl 10.
[41] De förenade målen C-465/00, C-138/01 och C-139/01 *Österreichischer Rundfunk m.fl.,* p. 70-72.
[42] Jfr. EU-stadgans ingress, 4st.
[43] Kuner 2012, s. 2.

blev rättsligt bindande för EU:s organ samt för medlemsstaterna då dessa tillämpar unionsrätten.[44]

3.2.1 Artikel 7

Enligt EU-domstolen ska rätten till respekt för privatlivet som återfinns i art. 7 överensstämma med art. 8 i EKMR.[45] I enlighet med stadgans art. 52.3 ska de rättigheter i stadgan som motsvarar rättigheterna i Europakonventionen anses ha samma innebörd och räckvidd. Skyddet angående respekten för privatlivet som Europadomstolen utvecklat genom sin praxis utgör dock ett minimiskydd vid tillämpning av art. 7.[46] Detta har sin förklaring i att unionsrätten inte hindras från att säkerställa ett mer långtgående skydd.

Till skillnad från EKMR är respekten för privatlivet och skyddet av personuppgifter reglerade i två separata bestämmelser i stadgan. Då båda dessa rättigheter innefattar ett integritetsskydd har EU-domstolen ansett att det finns en tydlig korrelation, något som även kan utläsas ur Europadomstolens praxis.[47] Konsekvensen, vad avser behandlingen av personlig information, är att respekten för privatlivet blir viktig att beakta tillsammans med skyddet av personuppgifter. I det här hänseendet överlappar bestämmelserna varandra och ett gemensamt tillämpningsområde kan påvisas. Detta har motiverats av EU-domstolen med att båda rättigheter omfattar all information som rör en fysisk namngiven person eller som på annat sätt kan identifieras.[48]

3.2.2 Artikel 8

Skyddet av personuppgifter i art. 8 utformades utifrån dataskyddsdirektivets regler och Europadomstolens praxis under art. 8 i EKMR med syftet att möta den tekniska utvecklingen på det digitala området.[49] Bestämmelsens struktur skiljer

[44] Barnard och Peers 2014, s. 240.
[45] Mål C-256/11 *Dereci*, p. 70.
[46] Peers m.fl. 2014, s. 195.
[47] De förenade målen C-92/09 och C-93/09 *Volker und Markus Schecke och Eifert*, p.47.
[48] Ibid, p. 52.
[49] Peers m.fl. 2014, s. 228f.

sig från flera av stadgans rättigheter då den, istället för att vara formulerad i generella ordalag, innehåller specifika rekvisit som tillsammans konstituerar skyddets omfattning. Rekvisiten återspeglar vissa av de principer som uppställs i dataskyddsdirektivet, däribland skyldigheten att behandla personuppgifter på grundval av personens samtycke eller en annan legitim grund och att en oberoende myndighet ska kontrollera efterlevnaden av rättigheten.[50] En koppling till Europadomstolens praxis kan även noteras genom rätten att få tillgång till insamlade uppgifter som rör en.[51]

Valet att reglera skyddet av personuppgifter avskilt från respekten för privatlivet belyser rättighetens angelägenhet, inte minst i dess moderna digitala kontext. Den separata regleringen innebär att det finns en distinktion men som framhållits ovan är båda bestämmelser, i praktiken, av vikt för den personliga integriteten. Skyddet av personuppgifter utgör *lex specialis* i förhållande till det allmänna skyddet för privatlivet.[52] I jämförelse med art. 7 är art. 8 tänkt att ge ett mer detaljerat och långtgående skydd avseende insamlingen, lagringen och användningen av information hänförligt till den enskildes privatliv.[53] När personlig information är föremål för behandling ges ett mer specifikt skydd som syftar till att individen ska få en ökad kontroll över sina personuppgifter.[54]

Som konstaterats ovan är rätten till skydd för den personliga integriteten en relativ rättighet. Enligt art. 52.1 i stadgan får en inskränkning i rättigheterna endast rättfärdigas under förutsättning att begränsningarna är nödvändiga och svarar mot ett mål av allmänt samhällsintresse. Proportionalitetsprincipen måste även beaktas i det enskilda fallet vilket får till följd att behandlingen av personuppgifter är förenad med ett krav på avvägningar mellan intresset av att skydda personlig information och motstående intressen av olika slag.[55] EU-domstolen har dock klargjort att det utrymme till rättfärdigande som kan motivera ett åsidosättande av integritetsskyddet ska inskränkas till vad som är

[50] Gonzáles Fuster 2014, s. 203f.
[51] Se art. 8.2 i EU-stadgan.
[52] Lebeck 2013, s. 141.
[53] Lynskey 2014, s. 588f.
[54] Ibid, p. 591.
[55] Lebeck 2013, s. 137.

strängt nödvändigt.[56] Stadgans bestämmelse om skydd för personuppgifter innebär därmed, i en EU-rättslig kontext, ett konstitutionellt skydd som endast undantagsvis kan begränsas.[57]

3.2.3 Praxis

Den personliga integriteten, så som den kommer till uttryck i EU-stadgan, och dess förhållande till den digitala utvecklingen har klargjorts av EU-domstolen i uppmärksammade mål de senaste åren. Två av dessa presenteras nedan.

3.2.3.1 Google Spain

I fallet *Google Spain* hade domstolen att ta ställning till huruvida Google, i egenskap av sökmotorleverantör, har ett ansvar vad avser de personuppgifter som tillgängliggörs genom hemsidan.[58] Bakgrunden till målet var den spanska dataskyddsmyndigheten, AEPD, som efter klagomål från en spansk privatperson ålade företaget att ta bort individens personuppgifter från sökresultaten.[59] EU-domstolen konstaterade att Google, genom att på ett automatiskt och systematiskt sätt samla in, registrera och organisera personuppgifter för att sedan lagra och tillhandahålla dem för sina användare, ägnar sig åt behandling av personuppgifter i den mening som avses i dataskyddsdirektivet.[60] Följaktligen uppställs krav på en hög integritetsrättslig skyddsnivå i enlighet med direktivet och de grundläggande fri- och rättigheter som återfinns i stadgan.

Google yrkade på att ett ansvar för behandlingen inte förelåg eftersom att leverantören inte hade kännedom om uppgifterna och därmed inte möjlighet att utöva kontroll över dem.[61] Trots denna invändning ansåg domstolen att sökmotorernas organisering av personuppgifter kan innebära ingrepp i privatlivet och skyddet för personuppgifter eftersom att sökresultatet över en fysisk person

[56] Mål C-473/12 *IPI*, p. 39.
[57] Lebeck 2013, s. 141f.
[58] Mål C-131/12 *Google Spain och Google mot AEPD*, p. 1-2.
[59] Ibid, p. 14-17.
[60] Ibid, p. 28.
[61] Ibid, p. 22.

kan innehålla känsliga aspekter av personens privatliv.[62] Internets globala karaktär medför dessutom en risk för att ingreppet blir allvarligt. Stadgans betydelse i det här hänseendet betonades av domstolen med förklaringen att dataskyddsdirektivets bestämmelser ska tolkas mot bakgrund av de rättigheter som är stadfästa i stadgan.[63]

Efter en avvägning mellan företagets intresse av uppgiftsbehandlingen och individens integritetsskydd utifrån artiklarna 7 och 8 i stadgan slog domstolen fast att Google är skyldig att avlägsna personlig information från sökresultaten efter begäran från den berörda individen.[64] Stadgans rättigheter väger således tyngre än både leverantörens ekonomiska intressen och allmänhetens intressen av att få tillgång till personuppgifterna.[65]

3.2.3.2 Digital Rights Ireland

EU-domstolens dom i fallet *Digital Rights Ireland* berörde giltigheten av datalagringsdirektivet i förhållande till det integritetsskydd som tillerkänns unionsmedborgarna i stadgan.[66] Direktivet föreskrev leverantörer av elektroniska kommunikationstjänster en skyldighet att lagra personuppgifter i brottsbekämpande syfte genom att tillgängliggöra dessa för nationella myndigheter vid utredning och åtal av allvarliga brott.[67] Genom att identifiera en individs elektroniska kommunikationer kunde detaljerade uppgifter om personers privatliv inhämtas, såsom namn, IP-adress, uppringda telefonnummer och från vilka platser kommunikationen skett.[68]

Domstolen konstaterade inledningsvis att lagringsskyldigheten i sig utgör ett intrång i stadgans art. 7 och därmed har det föga betydelse om de uppgifter som

[62] Mål C-131/12 *Google Spain och Google mot AEPD*, p. 36-38.
[63] Ibid, p. 68.
[64] Ibid, p. 74 och 88.
[65] Ibid, p. 97.
[66] De förenade målen C-293/12 och C-594/12 *Digital Rights Ireland m.fl.*, p. 23.
[67] Ibid, p. 24.
[68] Ibid, p. 26-27.

avser privatlivet är av känslig art eller inte.[69] Det faktum att lagringen även innefattade en behandling av personuppgifter aktualiserade samtidigt en tillämpning av stadgans art. 8.[70] En försvårande omständighet i sammanhanget var att förfarandet skedde utan att de berörda personerna var underrättade vilket kunde bidra till en känsla av att privatlivet ständigt stod under övervakning.[71]

Trots ingreppet i integritetsskyddet ansåg domstolen att direktivet utgjorde ett värdefullt verktyg för att förebygga och bekämpa organiserad brottslighet vilket innebar att begränsningen svarade mot ett mål av allmänt samhällsintresse som avses i art. 52.1 i stadgan.[72] Ett eventuellt rättfärdigande måste dock alltid föregås av proportionalitetsprincipens tillämpning, med visst utrymme för en skönsmässig bedömning. I förevarande fall var bedömningsmarginalen begränsad till följd av dels den stora betydelse som skyddet av personuppgifter har för rätten till respekt för privatlivet, dels det allvarliga integritetsingrepp som direktivet innebar.[73]

Med hänvisning till Europadomstolens praxis konstaterade domstolen att ett effektivt skydd av personuppgifter mot risker för otillåten tillgång eller användning inte säkerställdes eftersom att direktivet omfattade samtliga personer, kommunikationsmedel och trafikuppgifter utan undantag.[74]. Då begränsningar av skyddet för personuppgifter endast ska inskränkas till vad som är strängt nödvändigt överskred datalagringsdirektivet proportionalitets-principens gränser och ogiltigförklarades.[75]

[69] De förenade målen C-293/12 och C-594/12 *Digital Rights Ireland m.fl.*, p. 33-34.
[70] Ibid, p. 29.
[71] Ibid, p. 37.
[72] Ibid, p. 41-44.
[73] Ibid, p. 48.
[74] Ibid, p. 54-57.
[75] Ibid, p. 52, 69-71.

4 Schrems-domen

4.1 Bakgrund

Safe Harbor-systemet hade varit föremål för kritik under en längre tid och rapporter från kommissionen visade på en ofullständig införlivning av dataskyddsreglerna hos ett flertal amerikanska företag.[76] Självcertifieringsprocessen och tillsynsmyndigheternas kontroll ifrågasattes därmed och systemets förenlighet med den personliga integriteten diskuterades. Ytterligare en ifrågasättbar aspekt var ett undantag i Safe Harbor som gav amerikanska myndigheter möjligheten att begränsa systemets integritetsskydd till vad som är nödvändigt för den nationella säkerheten.[77] Dessa bekymmer till trots fortgick systemet att tillämpas i över ett decennium och antalet Safe Harbor-certifierade företag ökade i takt med tillväxten av den digitala ekonomin.

Under 2013 väcktes nytt liv i debatten om Safe Harbor i samband med Edward Snowdens avslöjanden om amerikanska program för insamling av underrättelseinformation.[78] Nästintill samtliga företag anslutna till Safe Harbor-systemet deltog i det s.k. Prism-programmet som gav USA:s säkerhetsmyndighet NSA tillgång till europeiska personuppgifter.[79] Safe Harbor medgav förvisso ingrepp i integritetsskyddet i syfte att värna den nationella säkerheten men de amerikanska underrättelseorganens omfattande insamling av personuppgifter som överförts från EU riskerade att undergräva rätten till skydd för den personliga integriteten som tillförsäkras unionsmedborgarna.[80]

Snowdens avslöjanden utmynnande i ett EU-rättsligt efterspel som inleddes när den österrikiske medborgaren Maximillian Schrems gjorde en anmälan till den irländske dataskyddsmyndigheten DPC om att förbjuda Facebook Ireland från att

[76] Kommissionens meddelande COM(2013) 847 final, s. 7ff och kommissionens arbetsdokument SEC(2002) 196 och SEC(2004) 1323.
[77] Bilaga I till kommissionens beslut 2000/520, 4st.
[78] Kommissionens meddelande COM(2013) 846 final, s. 3.
[79] Kommissionens meddelande COM(2013) 847 final, s. 17.
[80] Ibid, s. 17f.

överföra personuppgifter till USA.[81] Samtliga personer med hemvist inom unionen som registrerar sig på Facebook måste nämligen godkänna att användarens personuppgifter överförs från dotterbolaget Facebook Ireland till företagets servrar i USA.[82] Med hänvisning till kommissionens beslut 2000/520 ansåg DPC att USA säkerställde en adekvat skyddsnivå och avslog därmed Schrems anmälan.[83] Beslutet överklagades till irländsk domstol som i sin tur begärde förhandsavgörande från EU-domstolen.[84]

4.2 Ogiltigförklarandet av Safe Harbor

Fallet *Schrems* berör två aspekter beträffande överföringen av personuppgifter från EU till USA. Den ena tar sikte på de nationella tillsynsmyndigheternas befogenheter vid uppgiftsöverföringen i förhållande till dataskyddsdirektivets och EU-stadgans processuella rättigheter. Den andra handlar om Safe Harbor-systemets giltighet med utgångspunkt i direktivets materiella innehåll och de grundläggande rättigheterna avseende den personliga integriteten.

I enlighet med både dataskyddsdirektivets art. 28 och stadgans art. 8.3 är de oberoende tillsynsmyndigheterna ansvariga för kontrollen av efterlevnaden av unionsbestämmelserna om skyddet vid behandlingen av personuppgifter.[85] Mot denna bakgrund konstaterade EU-domstolen att myndigheterna har befogenhet att kontrollera huruvida tredje länder säkerställer en adekvat skyddsnivå och ett kommissionsbeslut, såsom beslut 2000/520, får varken hindra personer från att vända sig till myndigheten eller inskränka myndighetens befogenheter som framgår av unionens primärrätt.[86]

Domstolen slog således fast att kommissionens beslut som möjliggör för organisationer i USA att uppnå en adekvat skyddsnivå inte utgör ett hinder för en medlemsstats tillsynsmyndighet att pröva en persons begäran om skydd för sina

[81] Mål C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, p. 28
[82] Ibid, p. 27.
[83] Ibid, p. 29.
[84] Ibid, p. 30-36.
[85] Ibid, p. 45-47.
[86] Ibid, p. 50-53.

fri- och rättigheter.[87] Av denna anledning var den irländske dataskyddsmyndighetens beslut att avslå Schrems anmälan felaktigt. Finns det fog för de argument som anförs i anmälan ska dataskyddsdirektivets och stadgans processuella rättigheter respekteras.

Vad beträffar Safe Harbor-systemets förenlighet med den personliga integriteten erinrade EU-domstolen om att det huvudsakliga syftet med systemet är att en hög skyddsnivå vidmakthålls när personuppgifter överförs från unionen till ett tredje land.[88] Vad som utgör en adekvat skyddsnivå enligt direktivet är inte tydligt definierat men enligt domstolen ska begreppet förstås som att det krävs att länder utanför EU säkerställer ett skydd av grundläggande fri- och rättigheter som är väsentligen likvärdigt det skydd som garanteras inom unionen.[89]

Till följd av de amerikanska myndigheternas generella, omfattande och ospecifika åtkomst av europeiska personuppgifter uppstod en, i jämförelse med EU-rätten, integritetsrättslig diskrepans. Med hänsyn till det stora antalet personer som riskerade att få sin integritet kränkt vid uppgiftsöverföringen till USA ansåg domstolen att behandlingen av dessa uppgifter gick utöver vad som var strängt nödvändigt och proportionerligt för att skydda den nationella säkerheten.[90]

Domstolen hänvisade till *Digital Rights Ireland*-målet och konstaterade att en lagstiftning som tillåter behandling av samtliga personuppgifter som överförs från unionen utan att det görs några åtskillnader eller begränsningar utifrån det eftersträvade syftet och samtidigt ger myndigheter åtkomst till innehållet kränker rätten till den i stadgan stadfästa respekten för privatlivet.[91] Genom att anta beslut 2000/520 hade kommissionen överskridit sin befogenhet och domstolen fann att beslutet var ogiltigt, följaktligen ogiltigförklarades även Safe Harbor-systemet.[92]

[87] Mål C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, p. 66.
[88] Ibid, p. 72.
[89] Ibid, p. 70 och 73.
[90] Ibid, p. 90.
[91] Ibid, p. 93-94.
[92] Ibid, p. 103-106.

5 Tänkbara rättsliga konsekvenser efter Schrems-domen

Ur ett kommersiellt perspektiv har EU-domstolens ogiltigförklarande av Safe Harbor den 6 oktober 2015 medfört vissa utmaningar. Företag som tidigare varit anslutna till systemet kan inte längre förlita sig på det för att tillförsäkra en skyddsnivå som överensstämmer med EU-rätten vid transatlantisk personuppgiftsöverföring. I detta hänseende har *Schrems*-domen inneburit en begränsning av det gränsöverskridande dataflödet till förmån för skyddet för den personliga integriteten. I en globaliserad värld där europeiska personuppgifter ständigt lämnar EU:s gränser riskerar förutsättningarna att försämras för företag vars affärsverksamhet är avhängig av att personuppgifter behandlas genom insamling, lagring och liknande förfaranden. I syfte att förhindra en inskränkning av individens integritet måste de tusentals Safe Harbor-certifierade organisationer nu övergå till alternativa lösningar.

5.1 Alternativ till Safe Harbor

Till följd av *Schrems*-domen har kommissionen utfärdat ett meddelande innehållande riktlinjer för hur de berörda företagen kan agera i den situation som uppstått. I meddelandet framhålls att företagen måste använda sig av alternativa metoder till Safe Harbor på så vis att överföringen av personuppgifter från EU till USA kan genomföras i enlighet med dataskyddsdirektivets princip om adekvat skyddsnivå.[93] Trots att rättsläget ännu är oklart beträffande alternativens förenlighet med det europeiska integritetsskyddet har art. 29-gruppen bedömt dessa som lagenliga.[94]

5.1.1 Binding corporate rules

Överföringar av personuppgifter utanför EU får som huvudregel endast genomföras om en skyddsnivå som motsvarar den unionsrättsliga

[93] Kommissionens meddelande COM(2015) 566 final, s. 3f.
[94] Ibid, s. 15.

dataskyddslagstiftningen säkerställs i det tredje landet. Kommissionens återhållsamhet angående erkännanden av tredje länders adekvata skyddsnivå har resulterat i upprättandet av alternativa mekanismer för att, under särskilda omständigheter, möjliggöra ett fritt gränsöverskridande dataflöde.[95] Dessa alternativ har utformats med stöd i dataskyddsdirektivets art. 26 och utgör undantag från det generella förbudet mot tredjelandsöverföringar.[96]

Ett av de alternativa överföringsförfarandena är Binding Corporate Rules som har utvecklats av art. 29-gruppen. BCRs är bindande företagsinterna dataskyddsregler som multinationella koncerner kan upprätta i syfte att åstadkomma ett fritt dataflöde inom koncernen, oavsett var bolagen är etablerade.[97] Reglerna grundar sig i dataskyddsdirektivets art. 26.2 som tillåter överföring av personuppgifter till tredje länder som inte säkerställer en adekvat skyddsnivå under förutsättning att företaget ställer tillräckliga garantier för att privatlivet och enskildas grundläggande fri- och rättigheter skyddas.

BCRs utformas av företagen själva men för att tillförsäkra ett godtagbart skydd av individens integritet måste reglernas implementering föregås av ett godkännande från berörda nationella dataskyddsmyndigheter inom EU.[98] I syfte att åstadkomma tillräckliga garantier till skydd för individens rättigheter ges företagen en begränsad frihet vid reglernas utformning då innehållet måste överensstämma med riktlinjer som art. 29-gruppen sammansatt.[99] I likhet med Safe Harbor-systemet är syftet med dessa interna dataskyddsregler att skapa en, i integritetsrättsligt hänseende, trygg hamn. Genom antagandet av BCRs får koncerner således en rättslig grund för export av personuppgifter från EU och ett obegränsat dataflöde inom koncernen möjliggörs.[100]

Trots att bindande företagsinterna regler kan fungera som alternativ till Safe Harbor är ansökningsprocessen för godkännande både tidskrävande och

[95] Lynskey 2015, s. 41f.
[96] Art. 29-gruppens arbetsdokument WP 74, s. 5f.
[97] Ibid, s. 9.
[98] Millard 2013, s. 267.
[99] Art. 29-gruppens arbetsdokument WP108, s. 2f.
[100] Kuner 2013, s. 43.

kostsam.[101] Ytterligare en försvårande omständighet är det faktum att de nationella dataskyddsmyndigheternas villkor för godkännande av BCRs inte är identiska i samtliga medlemsstater.[102] Denna bristande enhetlighet exemplifierar den fragmentering som den europeiska dataskyddslagstiftningen har inneburit, vilket medfört praktiska komplikationer för kommersiella aktörer. Vissa dataskyddsmyndigheter anser dessutom att reglerna inte tillgodoser de krav på integritetsskydd som uppställs inom EU och är således ovilliga att erkänna BCRs som alternativ.[103]

5.1.2 Standardavtalsklausuler

Utöver BCRs har kommissionen tagit fram särskilda standardavtalsklausuler för överföring av personuppgifter till tredjeländer.[104] Dessa avtalsklausuler är bindande för medlemsstaterna och grundar sig i dataskyddsdirektivets art. 26.4.[105] Liksom BCRs utgör reglerna en alternativ överföringsmetod som företag frivilligt kan använda sig av för att säkerställa en adekvat dataskyddsnivå. Klausulerna har utformats med den personliga integriteten i åtanke och anses ge tillräckliga garantier för att enskilda personers privatliv och grundläggande fri- och rättigheter skyddas.[106] Genom att infoga klausulerna i avtal förhindras ett åsidosättande av integritetsskyddet då företagen åtar sig att behandla personuppgifter i enlighet med EU-rätten.[107] Som incitament för klausulernas efterlevnad är eventuell överträdelse förenad med skadeståndsansvar.[108]

Till skillnad från de bindande företagsinterna reglerna har standardavtalsklausuler ett bredare tillämpningsområde då dessa kan användas av andra företag än multinationella koncerner. I jämförelse med BCRs måste klausulerna däremot undertecknas vid varje överföring vilket kan bli betungande

[101] Millard 2013, s. 267.
[102] Kuner 2013, s. 44.
[103] Ibid.
[104] Rauhofer och Bowden 2013, s. 7.
[105] Art. 29-gruppens arbetsdokument WP 12, s. 28.
[106] Kommissionens beslut 2001/497, art. 1.
[107] Bilaga till kommissionens beslut 2001/497, klausul 4 och 5.
[108] Ibid, klausul 6.

för organisationer där överföringen av personuppgifter utanför EU utgör en central del av verksamheten.[109] I de flesta fall kan personuppgiftsöverföringar med klausulerna som rättslig grund genomföras utan godkännande från relevant dataskyddsmyndighet. Vissa nationella myndigheter uppställer emellertid krav på en föregående granskning av avtalen likt den kontroll som fordras ifråga om BCRs, en omständighet som kan försvåra klausulernas användning.[110]

[109] Kuner 2013, s. 93.
[110] Millard 2013, s. 266f.

6 Analys

6.1 En förstärkning av den personliga integriteten

Den europeiska dataskyddslagstiftningen präglas av en intressemotsättning mellan skyddet för den personliga integriteten och det fria flödet av personuppgifter. När information hänförlig till unionsmedborgarna samlas in och lagras i tredje länder sätts individernas grundläggande fri- och rättigheter ur spel. Samtidigt är ett fritt gränsöverskridande dataflöde nödvändigt i kommersiellt hänseende, inte minst mot bakgrund av den betydelse som de transatlantiska handelsförbindelserna har för den ekonomiska utvecklingen. *Schrems*-domen illustrerar denna inom integritetsrätten centrala konfliktlinje genom att uppmärksamma de risker som är förenade med behandlingen av personuppgifter när dessa lämnar unionens trygga sfär.

I samband med samhällets digitalisering har personuppgifternas omfattning och tillgänglighet ökat. Följaktligen har skyddet för den personliga integriteten fått en större betydelse, något som även kan utläsas ur EU-domstolens praxis. De senaste åren har domstolens bedömningar vad gäller avvägningen mellan integritetsrättsliga och kommersiella intressen fått stor uppmärksamhet. I *Google Spain*-målet konstaterade domstolen att individens kontroll över sina personuppgifter väger tyngre än både företagets ekonomiska intressen och allmänhetens intresse av att få ta del av informationen. Ogiltigförklarandet av datalagringsdirektivet i *Digital Rights Ireland*-målet är även det ett exempel på en betoning av integritetsskyddets betydelse i det digitala informationssamhälle som den tekniska utvecklingen givit upphov till.

Genom Safe Harbor-systemets ogiltigförklarande understryker EU-domstolen återigen att skyddet för den personliga integriteten är en grundläggande mänsklig rättighet som måste respekteras av såväl företag som statliga myndigheter. Trots de begränsningsmöjligheter som kan rättfärdiga en inskränkning av både privatlivet och skyddet av personuppgifter är dessa av undantagskaraktär.

Integritetsskyddet får nämligen endast inskränkas till vad som är strängt nödvändigt. Även proportionalitetsprincipen måste iakttas vilket medför ytterligare en tröskel som ska klivas över i syfte att åstadkomma ett rättfärdigat åsidosättande.

Den personliga integriteten har givits stor tyngd av EU-domstolen och en förstärkning av integritetsskyddet i digitala miljöer kan noteras. Mot bakgrund av Snowdens avslöjanden och den godtyckliga massövervakning som Prism-programmet innebar är domstolens ställningstagande angeläget. Samtidigt innebär *Schrems*-domen ett oklart rättsläge för de tusentals företag som tvingas hitta alternativa metoder för tredjelandsöverföringar. Huruvida en balans i avvägningen mellan kommersiella och integritetsrättsliga intressen har uppnåtts är svårt att säga men EU-domstolens senare praxis visar tydligt på att behandlingen av EU-medborgarnas personuppgifter är förenad med ett starkt konventions- och primärrättsligt stadgat skydd.

6.2 Alternativens förenlighet med integritetsskyddet

Redan i samband med dataskyddsdirektivets antagande konstaterades att den amerikanska dataskyddslagstiftningen inte uppfyller det krav på adekvat skyddsnivå som EU-rätten uppställer. Utifrån ett kommersiellt perspektiv är den transatlantiska överföringen av personuppgifter emellertid oundviklig. Undantag från det generella förbudet mot tredjelandsöverföringar har således skapats i syfte att kringgå den i dataskyddshänseende integritetsrättsliga diskrepans som råder mellan EU och USA. I och med Safe Harbor-systemets ogiltigförklarande försvann ett av de viktigaste undantagen och berörda företag tvingas nu tillämpa alternativa överföringsmetoder.

Övergången till bindande företagsinterna regler och standardavtalsklausuler är dock inte oproblematisk. BCRs kan endast användas av multinationella koncerner och utesluter därmed många mindre företag som är beroende av tredjelandsöverföringar. Mot bakgrund av de kostnader som är förenade med BCRs riskerar ansökningsförfarandet dessutom att inverka avskräckande. En

utdragen process kan även resultera i att företagens skydd av personuppgifter hamnar i ett rättsligt vakuum då möjligheten ett implementera överföringsmekanismen hindras under en längre tid. Användningen av standardavtalsklausuler framstår som det mest rimliga alternativet men till skillnad från både BCRs och Safe Harbor skapas ingen bestående trygg sfär där ett fritt dataflöde möjliggörs.

Schrems-domen ger även anledning att ifrågasätta alternativens förenlighet med den personliga integriteten. Trots att EU-domstolen inte uppmärksammar överföringen av personuppgifter utifrån andra rättsliga grunder än Safe Harbor finns det en risk för att integriteten inskränks även genom tillämpning av de alternativa metoderna. Varken BCRs eller standardavtalsklausuler ställer bättre garantier för att EU-medborgarnas grundläggande rättigheter skyddas. Samtidigt kvarstår risken för att amerikanska underrättelseprogram åsidosätter respekten för privatlivet och skyddet av personuppgifter.

I kommersiellt hänseende måste undantag från förbudet mot tredjelandsöverföringar finnas men dessa kan endast rättfärdigas under förutsättning att en adekvat skyddsnivå uppnås. Oavsett överföringsmetod består det faktum att USA inte säkerställer en skyddsnivå av personuppgifter som är väsentligen likvärdig den nivå som garanteras inom unionen. Det kan därmed ifrågasättas om integritetsskyddet överhuvudtaget kan vidmakthållas när europeiska personuppgifter överförs till USA. Det råder onekligen en osäkerhet beträffande de alternativ till Safe Harbor som tusentals företag nu tvingas vända sig till. Mot bakgrund av den personliga integritetens förstärkning som bekräftas genom *Schrems*-domen är sannolikheten stor att även BCRs och standardavtalsklausuler kommer att ogiltigförklaras av EU-domstolen vid en framtida prövning.

6.3 En oviss framtid

I en global kontext uppställer EU-rätten höga krav på skydd av personuppgifter vilket medför utmaningar för det gränsöverskridande dataflödet. När

kommersiella intressen får ge vika till förmån för individernas grundläggande rättigheter blir integritetsfrågor allt viktigare att beakta även utanför EU:s gränser. Genom förtydligandet av begreppet adekvat skyddsnivå i *Schrems*-domen slår EU-domstolen fast att tredje länder måste ha ett skydd som är väsentligen likvärdigt det som tillförsäkras inom unionen för att ett fritt dataflöde ska uppnås. Den europeiska dataskyddslagstiftningen förflyttas därigenom utanför unionens gränser och påtvingas tredje länder.

Integritetsskyddet inom EU får en extraterritoriell effekt där tredje länder måste anpassa sin lagstiftning till EU-rätten för att möjliggöra överföringen av personuppgifter. I ett alltmer globaliserat och digitalt informationssamhälle kommer behandlingen av EU-medborgarnas personuppgifter med all sannolikhet att öka. I ett långsiktigt perspektiv kommer företagens behov av ett fritt transatlantiskt dataflöde eventuellt leda till en anpassning av amerikansk lagstiftning till EU-rätten.

En annan oviss framtidsaspekt är de nationella tillsynsmyndigheternas verksamhet. Dataskyddsdirektivets implementering i nationell rätt har givit upphov till fragmentariska lagar inom unionen. Den rättsliga splittring som den europeiska dataskyddslagstiftningen har resulterat i åskådliggörs av tillsynsmyndigheternas oberoende. När vissa medlemsstaters dataskyddsmyndigheter inte erkänner BCRs och uppställer krav på granskning av avtal där standardavtalsklausuler infogats försvåras förutsättningarna för tredjelandsöverföringar. I *Schrems*-domen framhävs myndigheternas ställning då domstolen konstaterar att dessa har befogenhet att tolka kommissionsbeslut.

En förstärkning av myndigheternas oberoende riskerar dessvärre att öka fragmenteringen inom EU, inte minst beträffande de alternativa överföringsmetodernas förenlighet med integritetsskyddet. Till följd av oenhetliga bedömningar från dataskyddsmyndigheterna finns en risk för att ytterligare oförutsebarhet beträffande överföringen av personuppgifter till USA skapas. I syfte att tillgodose företagens behov av ett fritt dataflöde över gränserna krävs reformer. En ny allmän dataskyddsförordning kan medföra en

harmonisering genom att säkerställa gemensamma dataskyddsregler men det kan ta lång tid innan förordningen antas. De företag som tidigare varit anslutna till Safe Harbor-systemet går en oviss framtid till mötes.

Käll- och litteraturförteckning

EU-dokument

Beslut, meddelanden och förslag

Gemensamma EES-kommitténs beslut nr 83/1999 av den 25 juni 1999 om ändring av protokoll 37 och bilaga XI (Teletjänster) till EES-avtalet

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

Kommissionens beslut av den 15 juni 2001 om standardavtalsklausuler för överföring av personuppgifter till tredje land enligt direktiv 95/46/EG, 2001/497/EG

Kommissionens beslut av den 28 april 2004 om skyddsnivån för personuppgifter på Isle of Man, 2004/411/EG

Kommissionens beslut av den 19 oktober 2010 i enlighet med Europaparlamentets och rådets direktiv 95/46/EG om adekvat skydd för personuppgifter i Andorra, 2010/625/EU

Kommissionens förslag till Europarlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning), COM(2012) 11 final, 25 januari 2012

Meddelande från kommissionen till Europaparlamentet, rådet, europeiska ekonomiska sociala kommittén samt regionkommittén, ”*Skydd av den personliga integriteten i en uppkopplad värld, En europeisk ram för personuppgiftsskydd för tjugohundratalet*”, COM(2012) 9 final, 25 januari 2012

Meddelande från kommissionen till Europaparlamentet och rådet, ”*Återskapande av förtroendet för dataflöden mellan EU och Förenta staterna”*, COM(2013) 846 final, 27 november 2013

Meddelande från kommissionen till Europaparlamentet och rådet *”om hur principerna om integritetsskydd (safe harbour) fungerar när det gäller EU:s medborgare och företag som är etablerade i EU”*, COM(2013) 847 final, 27 november 2013

Meddelande från kommissionen till Europaparlamentet och rådet ”*om överföring av personuppgifter från EU till Amerikas förenta stater enligt direktiv 95/46/EG med anledning av domstolens dom i mål C-362/14 (Schrems)*”, COM(2015) 566 final, 6 november 2015

Yttranden och rekommendationer

Article 29 Data Protection Working Party, ”*Working Document: Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive*”, WP 12, 24 juli 1998

Kommissionens arbetsdokument, ”*The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce*”, SEC(2002) 196, 13 februari 2002

Article 29 Data Protection Working Party, ”*Working document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*”, WP 74, 3 juni 2003

Kommissionens arbetsdokument, ”*The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce*”, SEC(2004) 1323, 20 oktober 2004

Article 29 Data Protection Working Party, ”*Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules*”, WP108, 14 april 2005

Direktiv

Europaparlamentet och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter

Artiklar

Kuner, Christopher, *The European Commission’s Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, Privacy and Security Law Report, Bloomberg BNA, 2 juni 2012

Rauhofer, Judith & Bowden, Casper, *Protecting their own: Fundamental rights implications for EU data sovereignty in the cloud*, University of Edinburgh School of Law Research Paper Series, nr 28, 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, s. 569 – 597, 2014

Litteratur

Korling, Fredric & Zamboni, Mauro (red.), *Juridisk metodlära*, 1. uppl., Studentlitteratur, Lund, 2013

Kuner, Christopher, *Transborder data flows and data privacy law*, Oxford University Press, Oxford, 2013

Lebeck, Carl, *EU-stadgan om grundläggande rättigheter: en introduktion*, 1. uppl., Studentlitteratur, Lund, 2013

Millard, Christopher J. (red.), *Cloud computing law*, Oxford University Press, Oxford, 2013

Barnard, Catherine & Peers, Steve (red.), *European Union law*, 2014

González Fuster, Gloria, *The emergence of personal data protection as a fundamental right of the EU*, 2014

Peers, Steve, Hervey, Tamara, Kenner, Jeff & Ward, Angela (red.), *The EU Charter of fundamental rights: a commentary*, Hart Pub Ltd, Oxford, 2014

Magnusson Sjöberg, Cecilia (red.), *Rättsinformatik: juridiken i det digitala informationssamhället*, 1. uppl., Studentlitteratur, Lund, 2015

Lynskey, Orla, *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, 2015

Elektroniska källor

Boston Consulting Group, The Value of our Digital Identity, publicerad 20 november 2012. Hämtad den 11 november 2015 från: https://www.bcgperspectives.com/content/articles/digital_economy_consumer_insight_value_of_our_digital_identity/

Rättsfallsförteckning

EU-domstolen

C-465/00, C-138/01 och C-139/01 Rechnungshof mot Österreichischer Rundfunk m.fl. och Christa Neukomm och Joseph Lauermann mot Österreichischer Rundfunk, REG 2003 s. I-04989

C-92/09 och C-93/09 Volker und Markus Schecke GbR och Hartmut Eifert mot Land Hessen, REU 2010 s. I-11063

C-256/11 Murat Dereci m.fl. mot Bundesministerium für Inneres, ännu ej publicerad i REU

C-131/12 Google Spain SL och Google Inc. mot Agencia Española de Protección de Datos (AEPD) och Mario Costeja González, ännu ej publicerad i REU

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., ännu ej publicerad i REU

C-473/12 Institut professionnel des agents immobiliers (IPI) mot Geoffrey Englebert m.fl., ännu ej publicerad i REU

C-362/14 Maximillian Schrems mot Data Protection Commissioner, ännu ej publicerad i REU

Europadomstolen

Klass mot Tyskland, dom från den 6 september 1978, nr. 5029/71

Leander mot Sverige, dom från den 26 mars 1987, nr. 9248/81

Connors mot Förenade kungariket, dom från den 27 maj 2004, nr. 66746/01

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