Sieps
Svenska institutet för europapolitiska studier
Mars 2021:4epa

EUROPAPOLITISK ANALYS

Fria dataflöden, EU:s integritetsskydd och nationell säkerhet

Maria Wiberg*

Sammanfattning

EU har skapat ett gemensamt regelverk för att ge enskilda ett starkt och tydligt integritetsskydd inom unionen. Men reglerna är inte enkla att få till eftersom EU:s syn på integritetsskydd samtidigt kräver att dataflöden till vissa tredjeländer begränsas när de inte upprätthåller samma skydd som EU gör. EU:s starka integritetsskydd innebär även att EU:s medlemsstater kan hindras att göra undantag från skyddet för att bekämpa grov brottslighet och skydda nationell säkerhet.

Enskilda länder har också olika syn på integritetsskydd, vilket påverkar företags och myndigheters möjligheter att använda exempelvis plattforms-, moln- och applikationstjänster som tillhandahålls över gränserna av olika leverantörer i olika länder. Frågan är hur EU ska upprätthålla balans mellan de tre målen: att säkerställa fria dataflöden på den inre marknaden och i resten av världen, att upprätthålla ett starkt skydd för den personliga integriteten och att tillåta undantag för att bekämpa grova brott och skydda nationell säkerhet.

Avvägningen kompliceras av att digitala tjänster är sammanflätade och globala samtidigt som brottsbekämpning och säkerhet är nära kopplat till den nationella självständigheten. För att undvika geografiska begränsningar av dataflöden krävs därmed en global samsyn kring hur en balans mellan de olika målen kan uppnås, skriver författaren. Den springande punkten är därför hur förtroende kan byggas upp mellan länder.

* Maria Wiberg är jurist med inriktning på EU-rätten. Som forskare i juridik vid Sieps har hon skrivit denna och andra analyser som berör den inre marknadens funktion. Från den 1 februari 2021 arbetar Maria Wiberg som jurist vid Polismyndigheten.

1. Inledning

Informations- och kommunikationstekniken utgör idag grunden för alla moderna samhällen och de flesta länder bygger sina samhällsstrukturer på innovativa ekonomiska system. Vi ser på TV, handlar, kommunicerar och hanterar ärenden med myndigheter, går till läkaren, söker efter och lagrar information digitalt. Under coronapandemin har vi kunnat använda digitala verktyg och tjänster till att jobba, handla och gå i skolan hemifrån, vilket har hjälpt till att bromsa spridningen av covid-19. Digitala tjänster är lättåtkomliga oavsett var i världen en tjänsteleverantör eller tjänstemottagare befinner sig, då allt man behöver är en uppkoppling och en mobiltelefon, dator eller liknande. Tjänster som vi använder är ofta så kallade plattforms-, moln- och applikationstjänster, vilka erbjuds av exempelvis Google, Amazon, Alibaba, Facebook, Twitter, Microsoft Onedrive och Klarna. De olika tjänsterna som vi använder kan vara till för exempelvis textbehandling, kalenderhantering, arkivering, kunddatahantering, betalningslösningar och e-posthantering utlagda på entreprenad. De olika tjänsterna kan också vara sammanlänkade eller vara en del av samarbeten mellan flera leverantörer av plattforms-, moln- och applikationstjänster.

När vi använder dessa tjänster uppkommer en stor mängd data som handlar om oss och vi lämnar olika digitala spår om vad vi gör på nätet, vilket ofta utgör så kallade persondata. Data har generellt ett stort värde för såväl företag som myndigheter. Detta eftersom den kan användas till att skapa och utveckla nya tjänster och effektivisera samhällsfunktioner och vad gäller just persondata beskrivs den till och med ibland som en av framtidens viktigaste tillgångar, eftersom den genererar tillväxt, innovation, konkurrenskraft och stor samhällsnytta.[1] Detta gör att många stater vill att data ska kunna flöda så fritt som möjligt över landsgränserna.

> ”Data har generellt ett stort värde för såväl företag som myndigheter.”

Samtidigt kan persondata vara känsliga och användarna kan vilja skydda sin personliga integritet. I mer allvarliga fall kan det handla om att skydda sig från övervakning, avlyssning och kartläggning av statsmakter medan det i mindre allvarliga fall kan handla om en önskan om att få slippa oönskad reklam. Det kan samtidigt vara viktigt att myndigheter och andra kan identifiera de digitala användarna för att kunna motverka brott och annan samhällsfarlig verksamhet. Digitala tjänster kan nämligen användas i planeringen av grov brottslighet såsom terrorism, bedrägerier och identitetsstölder. Brott som begås på internet ökar ständigt och elektronisk eller digital bevisning förekommer i de flesta utredningar av olika brott.[2] Därutöver kan tjänsterna användas för att sprida ”fake news” med potentiellt allvarliga effekter för det demokratiska systemet.

Det EU-rättsliga skyddet för persondata och integritet baseras på de rättigheter som uttrycks i EU:s stadga om de grundläggande rättigheterna (stadgan eller EU:s rättighetsstadga) vilka preciserats bland annat genom dataskyddsförordningen, i folkmun mer känd som GDPR,[3] och också det så kallade e-dataskyddsdirektivet.[4] Statlig verksamhet som rör medlemsstaternas nationella säkerhet omfattas dock inte av det EU-rättsliga integritetsskyddet eftersom det utgör verksamhet som faller utanför

---

[1] Olsson, E. Hårdare tag mot tech-jättarna även i Kina. ”I en tid där personliga data allt oftare beskrivs som framtidens viktigaste tillgångsslag innebär detta en enorm och växande maktposition.” (https://www.svd.se/hardare-tag-mot-tech-jattarna-aven-i-kina)

[2] BRÅ:s rapport, It-inslag i brottsligheten och rättsväsendets förmåga att hantera dem (BRÅ 2016:7) och regeringsuppdraget den 30 januari 2020 till Polismyndigheten att vidta åtgärder rörande kompetensförsörjning och kompetensutveckling avseende bekämpning av it-relaterad brottslighet (Ju2020/00378/PO).

[3] Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88.

[4] Europaparlamentets och rådets direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), EGT L 201, 31.7.2002, s. 37–47.

EU-rättens tillämpningsområde. EU:s regler handlar istället i första hand om att ge alla EU:s invånare ett enhetligt och likvärdigt skydd vid behandlingen av deras personuppgifter samt att ge skydd för juridiska personers berättigade intressen inom sektorn för elektronisk kommunikation, som används av privat och offentlig sektor. Skyddet innebär i princip att den som behandlar personuppgifter måste kunna peka ut en rättslig grund i lagstiftningen. Exempel på rättsliga grunder är avtal eller ett erhållet samtycke från en enskild om att uppgifterna får behandlas på ett visst sätt. Den som behandlar uppgifterna måste också uppfylla flera andra krav, exempelvis att tydligt informera om hur uppgifterna används samt erbjuda en möjlighet att rätta fel och att ta bort uppgifter på begäran. Syftet med lagstiftningen är att upprätta ett starkt gemensamt skydd som ska underlätta fria dataflöden på den inre marknaden.

Efter några år med dataskyddsförordningen börjar det nu gå att skönja vilka avvägningar EU-domstolen gör när den å ena sidan förhåller sig till behovet av att skydda enskildas integritet och å andra sidan behovet av att få del av personuppgifter för att bekämpa grov brottslighet och skydda nationell säkerhet. Domstolens praxis visar för det första att medlemsstaternas möjligheter att få tillgång till de integritetsskyddade uppgifterna i syfte att bekämpa vissa brott och skydda den nationella säkerheten är begränsad – trots att ansvaret för nationell säkerhet ligger på medlemsstaternas bord. För det andra visar rättspraxis att dataflöden till tredjeland helt kan behöva stoppas när det EU-rättsliga integritetsskyddet inte upprätthålls med hänvisning till skyddet för nationell säkerhet i det aktuella tredjelandet.

Sammanfattningsvis blir det ett problem för de fria dataflödena att olika länder – både inom och utanför EU – har olika syn på när de behöver göra avkall på integritetsskyddet i syfte att bekämpa vissa brott och skydda den nationella säkerheten. I ljuset av detta är syftet med denna Europapolitiska analys att identifiera och diskutera några målkonflikter som EU måste hantera i sin reglering av fria dataflöden och integritetsskydd.

Frågan är hur EU kan tillvarata fria dataflödens potential, utan att 1) göra avkall på enskildas personliga integritet, 2) begränsa ländernas möjligheter att använda vissa uppgifter i brottsbekämpande syfte och begränsa ländernas möjligheter att skydda den nationella säkerheten.

”Sammanfattningsvis blir det ett problem för de fria dataflödena att olika länder – både inom och utanför EU – har olika syn på när de behöver göra avkall på integritetsskyddet i syfte att bekämpa brott och skydda den nationella säkerheten.”

Analysen inleds i avsnitt 2 med en beskrivning av hur man kan se på värdet av data och dataflöden med fokus på persondata. I avsnitt 3 ges en bild av EU:s digitala agenda som har sin utgångspunkt i att fria dataflöden har stor betydelse för innovation, utveckling och skapande av konkurrenskraft. I avsnitt 4 beskrivs det EU-rättsliga integritetsskyddet, vilket utgör en förutsättning för att data ska kunna röra sig fritt på den inre marknaden och också i resten av världen. I avsnitt 5 beskrivs de undantag som medges från integritetsskyddet i syfte att bekämpa brottslighet och för att skydda nationell säkerhet, och i avsnitt 6 beskrivs EU-domstolens praxis gällande detta. I avsnitt 7 ges en bild av under vilka faktiska förutsättningar persondata kan röra sig och vilka utmaningar som uppstår för regleringssystemen i förhållande till användandet av exempelvis plattformar och molntjänster. I avsnitt 8 diskuteras möjligheterna till dataöverföringar från EU till tredjeland, bland annat i ljuset av EU-domstolens senaste rättspraxis. I avsnitt 9 sammanfattas några viktiga skillnader som uppkommer som en effekt av det EU-rättsliga regelverket på fria dataflöden inom den inre marknaden jämfört med dataflöden till tredjeland.

Avslutningsvis presenteras några övergripande slutsatser och frågeställningar som uppstår i förhållande till målkonflikten: viljan att underlätta fria dataflöden och samtidigt upprätthålla integritetsskyddet, men utan att för den skull kringskära medlemsstaternas möjligheter att skydda nationell säkerhet eller bekämpa brottslighet.

2. Värdet av data

När vi använder olika digitala tjänster skapas stora mängder elektroniska data. Sådana data kan generellt sett delas in i antingen uppgifter som kan kopplas till en viss person, det vill säga persondata, eller icke-persondata. Alla elektroniska data genererar en stor mängd information som i sin tur kan utvinnas,[5] behandlas och användas av företag och myndigheter. När informationen analyseras eller kombineras med tjänster och produkter kan den skapa stora värden för företag i form av nya och innovativa tjänster och produkter som i sin tur skapar konkurrenskraft. Elektroniska data ger både företag och myndigheter möjlighet att förbättra och effektivisera sina verksamheter eftersom den kan läggas till grund för utvecklingen av digitala tjänster och funktioner anpassade till den aktuella marknaden och samhället.

De digitala spår i form av persondata som vi skapar när vi använder digitala tjänster kan användas av företag för att hitta rätt kunder på rätt tid och plats och för att individanpassa tjänsterna med hänsyn till vårt agerande, smak och preferenser. När vi använder digitala tjänster skapas en möjlighet att spåra var vi befinner oss och vilka preferenser vi har genom att exempelvis se till våra sökningar och digitala spår. Ibland lämnar vi även mer direkt namn, adress och betalningsinformation, exempelvis när vi köper något via internet. Detta kan resultera i att när vi sökt efter en ny cykel på internet dyker cykelannonser upp på annonsytor när vi läser dagens tidning digitalt. När vi använder en kartfunktion för att hitta en butik på vår shoppingrunda får vi automatiskt upp annonser från andra butiker som vi passerar i området eftersom vår position kan registreras via

Definitioner

Med **elektroniska data** och **digitala spår** avses här information/uppgifter som uppstår och skapas digitalt.

Med **kommunikationstjänst** avses här en tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät.

Persondata/uppgift används här synonymt och hänför sig till varje upplysning som avser en identifierad eller identifierbar person, vilket innebär att personen kan identifieras genom ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

När samlingsuttrycket **integritetsskydd** används här avses det skydd som föreskrivs för personuppgifter enligt dataskyddsförordningen (2016/679) och skydd för personuppgifter, integritet och juridiska personers berättigade intressen inom sektorn för elektronisk kommunikation enligt e-dataskyddsdirektivet (2002/58).

Icke-persondata används i syfte att beskriva andra data än personuppgifter – ett exempel kan vara aggregerade datamängder som används för stordataanalyser, uppgifter om precisionsjordbruk som gör det möjligt att övervaka och optimera hur man använder bekämpningsmedel, bevattning och vilka underhållsbehov det finns av till exempel jordbruksmaskiner.

Med **behandling av personuppgifter** menas här, i enlighet med dataskyddsförordningen (2016/679), en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Anm. **Personuppgiftsansvarig** är den organisation (till exempel aktiebolag, stiftelse, förening eller myndighet) som samlar in och bestämmer för vilka ändamål personuppgifter ska behandlas och hur behandlingen ska gå till. **Personuppgiftsbiträde** är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ.

[5] Se, Colonna, L., *Legal Implications of Data Mining – Assessing the European Union's Data Protection Principles in Light of the United States Government's National Intelligence Data Mining Practices*, Eddy.se AB, Tallinn, 2016.

mobilen. Även myndigheter har stor användning av den information som de kan få fram om sina medborgare när de exempelvis vill göra en kartläggning av hur människor rör sig, för att exempelvis kartlägga smittspridningen av covid-19. Informationen kan också användas av myndigheter i den brottsbekämpande verksamheten.

Det är sammanfattningsvis tydligt att icke-persondata, men kanske framförallt persondata har ett stort ekonomiskt och samhälleligt värde för såväl företag som myndigheter.

3. EU:s digitala agenda

Den snabba digitala utvecklingen har satt hårt tryck på EU att anpassa den inre marknaden så att den fria rörligheten av data inte urvattnas genom att medlemsstaterna tillämpar olika regler för datarörlighet eller för integritet vid användandet av digitala tjänster. Detta har gjort att EU har beslutat om en rad harmoniseringsåtgärder för att stärka och tydliggöra integritetsskyddet men även för att underlätta för fria dataflöden. I EU:s digitala agenda görs kopplingar mellan dataflöden och globalisering, industrialisering och EU:s möjligheter till innovation.

Arbetet med EU:s digitala agenda har pågått en tid och Lissabonstrategin[6] från år 2000 kan betecknas som startskottet. Strategin följdes senare upp 2010 med *en digital agenda för Europa*,[7] ett av sju huvudinitiativ i Europeiska kommissionens 2020-strategi.[8] Inom ramen för detta initiativ framhålls en strävan att inrätta en verklig inre marknad för onlineinnehåll och onlinetjänster. Här ingår mål som att säkra möjligheterna för webbtjänster och digitalt innehåll med hög tilltro och högt förtroende genom ett balanserat regelverk och tydliga rättighetssystem och att forma den globala styrningen av Internet.[9]

> ”Den snabba digitala utvecklingen har satt hårt tryck på EU att anpassa den inre marknaden så att den fria rörligheten av data inte urvattnas genom att medlemsstaterna tillämpar olika regler för datarörlighet […]”

I sina politiska riktlinjer för åren 2014–2019 uttryckte kommissionens ordförande, Jean-Claude Juncker, att ”… vi måste bli mycket bättre på att utnyttja de gränslösa möjligheter som den digitala tekniken erbjuder.”[10] 2015 antog kommissionen den digitala inremarknadsstrategin med fokus på skapandet av en sammankopplad digital inre marknad där konsumenter ska kunna få tillgång till tjänster, musik, film och sportevenemang oavsett plattform och var de befinner sig i EU och där rättvisa konkurrensvillkor gäller med samma dataskydds- och konsumentregler för alla företag.[11]

Det är också i kölvattnet av den digitala inremarknadsstrategin som EU stärkte och tydliggjorde integritetsskyddet när man antog dataskyddsförordningen och dataskyddsdirektivet.[12] Vidare är e-dataskyddsdirektivet under omförhandling. I november 2018 antogs också

---

6 Europeiska rådets slutsatser, 23–24 mars 2000, Lissabon.
7 Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén, En digital agenda för Europa, KOM(2010) 245 slutlig.
8 Meddelande från kommissionen, Europa 2020 – En strategi för smart och hållbar tillväxt för alla, KOM(2010) 2020 slutlig.
9 Ibid, s. 14.
10 Jean-Claude Junckers politiska riktlinjer – En ny start för EU: Mitt program för sysselsättning, tillväxt, rättvisa och demokratisk förändring (15 juli 2014), s. 4.
11 Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, En strategi för en inre digital marknad i Europa, COM(2015) 192 final.
12 Europaparlamentets och rådets direktiv (EU) 2016/680 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, EUT L 119, 4.5.2016, s. 89–131.

förordningen om fritt flöde av icke-persondata med sikte på att undanröja lokaliseringskrav och att se till att inlåsningseffekter inte uppstår inom EU gällande sådana data som inte är persondata.[13] Förordningen innebär att företag kan flytta icke-persondata fritt över gränserna inom den inre marknaden, i ett gemensamt dataområde. Sammantaget utgör dessa regleringar ett ramverk för att fria dataflöden ska kunna flöda så bra och säkert som möjligt inom EU.[14] Härutöver kan också nämnas NIS-direktivet[15] som syftar till att förbättra den inre marknadens funktion genom att skapa tillit och förtroende och uppnå en hög gemensam säkerhetsnivå i nätverk och informationssystem inom EU. Direktivet ska säkerställa kontinuitet i samhällsviktiga och digitala tjänster som omfattas.

När Ursula von der Leyens presenterade sina politiska riktlinjer hösten 2019 blev det tydligt att också den nuvarande kommissionen ser stor potential i digitaliseringen. Ett av de sex övergripande målen avser ”ett Europa som är rustat för den digitala tidsåldern”. En konkret åtgärd som återfinns i riktlinjerna är vad som kallas ”Digital Services Act package” som har resulterat i två rättsliga initiativ, Digital Services Act[16] och Digital Market Act,[17] båda från december 2020. Sammantaget ska paketet tillhandahålla ett modernt rättsligt ramverk för digitala tjänster och stärka den digitala inre marknaden. Den bärande tanken är att digitala tjänsteutövare i EU ska agera ansvarsfullt för att mildra riskerna som användandet av deras tjänster kan innebära. Onlineplattformar har ett gemensamt ansvar för att se till att användare inte utsätts för olagliga varor, innehåll och tjänster samt för att skydda användarnas grundläggande rättigheter online.[18] Till skillnad från tidigare politiska riktlinjer framträder nu en närmare hänvisning och koppling till att stärka industrin och möjligheterna till innovation, sett ur ett globalt perspektiv. Exempelvis poängteras särskilt att marknaden måste fungera bättre – inte bara för konsumenter, företag och samhället i stort – utan den ska också ge stöd till industrin så att den kan anpassa sig till globaliseringen i den förändring som just nu sker digitalt (och i förhållande till klimatet).

4. Integritetsskydd inom EU

Integritetsskyddet inom EU har förtydligats och förstärkts i digitaliseringens spår. Syftet är både att harmonisera medlemsstaternas lagar, för att underlätta fri rörlighet, och att förstärka det EU-rättsliga integritetsskyddet.

I artikel 8 i EU:s rättighetsstadga framgår att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Enligt bestämmelsen i stadgan ska uppgifterna behandlas lagenligt och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har dessutom rätt att få tillgång till de insamlade uppgifterna och att rätta dessa. Att reglerna efterlevs ska kontrolleras av en oberoende

[13] Europaparlamentets och rådets förordning (EU) 2018/1807 av den 14 november 2018 om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen (Text av betydelse för EES.), EUT L 303, 28.11.2018, s. 59–68, skäl 1.
[14] Se exempelvis Kommerskollegiums rapport, Data flows – a fifth freedom for the internal market? av Lindén, O. och Dahlberg, E., 2016.
[15] Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen, EUT L 194, 19.7.2016, s. 1–30.
[16] Förslag till Europaparlamentets och rådets förordning om en inre marknad för digitala tjänster (rättsakten om digitala tjänster) och om ändring av direktiv 2000/31/EG, COM(2020) 825 final.
[17] Förslag till Europaparlamentets och rådets förordning om öppna och rättvisa marknader inom den digitala sektorn (rättsakten om digitala marknader), COM(2020) 842 final.
[18] Se färdplan för utvärderingar/inledande konsekvensbedömning: Ares(2020)2877686, Combined evaluation roadmap/inception impact assessment, Digital Services Act package: deepening the Internal Market and clarifying responsibilities for digital services, indicative planning, Q4 2020, (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-Internal-Market-and-clarifying-responsibilities-for-digital-services), 4 juni 2020.

myndighet. Skyddet har vidare preciserats genom dataskyddsförordningen.[19]

Dataskyddsförordningen syftar till att skapa och upprätthålla ett enhetligt och likvärdigt skydd för personuppgifter för alla fysiska personer inom EU och att se till att det fria flödet av uppgifter inte hindras. Förordningen gäller om den som behandlar personuppgifter är etablerad inom EU,[20] men också vid behandling av den som är etablerad utanför EU om de aktuella personuppgifterna rör personer inom EU.[21] För att få behandla personuppgifter krävs att det finns en rättslig grund till detta, exempelvis ett avtal. En annan möjlighet är att man ger sitt samtycke till att de egna personuppgifterna behandlas på ett visst sätt. Förordningen ställer höga krav på att det ska finnas tydlig information om hur uppgifterna ska användas och syftet med användningen. Det måste också finnas möjlighet att rätta felaktiga uppgifter, att ta bort uppgifter på begäran, att flytta uppgifterna till någon annan aktör samt möjlighet att påverka automatiserade beslut som till exempel baseras på algoritmer.

Alla kommunikationstjänster som inte är offentliga eller utgör statlig verksamhet omfattas härutöver av e-dataskyddsdirektivet.[22] E-dataskyddsdirektivet syftar till att harmonisera skyddet för personuppgifter, integritet och juridiska personers berättigade intressen inom sektorn för elektronisk kommunikation med syftet att motverka hinder på den inre marknaden. Direktivet ger med andra ord ett skydd för både fysiska och juridiska personer och uppfyller på så sätt det skydd som eftersträvas i stadgan, i synnerhet artiklarna 7[23] och 8. Skyddet gäller i förhållande till åtgärder som vidtas av personer andra än användarna av en tjänst,[24] oavsett om det rör sig om privatpersoner, statliga eller privata aktörer. Detta innebär att skyddet gäller i förhållande till (bland andra) nätoperatörer oavsett om de är privatägda eller ägs av staten. Direktivets utgångspunkt är att åstadkomma en likvärdig skyddsnivå för den personliga integriteten samt för juridiska personers berättigade intressen för att underlätta det fria flödet inom EU. På så sätt kompletterar e-dataskyddsdirektivet dataskyddsförordningen.

Skyddet är inte absolut då det finns situationer när integritetsskyddet behöver stå tillbaka. En sådan situation är när stater behöver skydda den allmänna säkerheten, upprätthålla det nationella försvaret samt skydda den nationella säkerheten i förhållande till exempelvis terrorism. Som nämns ovan ligger ansvaret för nationell säkerhet på medlemsstaternas

---

[19] EU-domstolen framhåller i mål C-623/17, *Privacy International* mot *Secretary of State for Foreign and Commonwealth Affairs m.fl.*, ECLI:EU:C:2020:790, pp. 62–63 att ”[v]id tolkningen av artikel 15.1 i direktiv 2002/58 ska således betydelsen av såväl rätten till respekt för privatlivet, vilken garanteras i artikel 7 i stadgan, som rätten till skydd för personuppgifter, vilken garanteras i artikel 8 i stadgan, såsom denna betydelse framgår av domstolens praxis, samt betydelsen av rätten till yttrandefrihet beaktas. Denna grundläggande rättighet, som garanteras i artikel 11 i stadgan, utgör nämligen en av grundvalarna för ett demokratiskt och pluralistiskt samhälle och ingår i de värden som unionen enligt artikel 2 FEU bygger på … [men] … [d]e rättigheter som är stadfästa i artiklarna 7, 8 och 11 i stadgan är emellertid inte några absoluta rättigheter, utan måste bedömas utifrån deras funktion i samhället …” Detta i enlighet med artikel 52.1 i stadgan. Se även förenade målen C-511/18, C-512/18 och C-520/18, *La Quadrature du Net m.fl.* mot *Premier ministre m.fl.*, ECLI:EU:C:2020:791, pp. 106 och 109.

[20] Artikel 3.1 i dataskyddsförordningen.

[21] Artikel 3.2 i dataskyddsförordningen. Denna del är endast tillämplig på vissa sorters behandling, se punkterna a) och b).

[22] Statlig verksamhet omfattas av dataskyddsdirektivet (2016/680), vilket i princip innebär att sådan verksamhet måste iaktta nationell konstitutionell rätt och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen).Sse mål C-623/17, *Privacy International*, p. 43 och pp. 46–49 samt förenade målen C-511/18, C-512/18 och C-520/18, *La Quadrature du Net m.fl.*

[23] Artikel 7 i stadgan statuerar att ”[v]ar och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer.”

[24] En ”tjänst” i EU-rättslig mening innebär en prestation som normalt utförs mot ersättning (artikel 57 FEUF).

bord då säkerhetsfrågor är starkt kopplade till statssuveräniteten. Att medlemsstaterna kan åberopa nationell säkerhet som grund för att ta del av integritetsskyddade personuppgifter kan dock innebära att EU-rättens personuppgiftsskydd urvattnas.

5. Inskränkningar i persondataskyddet – nationell regleringskompetens

I artikel 5 i fördraget om Europeiska unionen (FEU) framgår att EU endast ska handla inom ramen för de befogenheter som medlemsstaterna har tilldelat unionen i fördragen. Det framgår också att varje befogenhet som inte har tilldelats unionen ska tillhöra medlemsstaterna. En befogenhet som inte har tilldelats EU är att reglera nationell säkerhet som fortsatt är varje medlemsstats eget ansvar. Samtidigt utgör en hänvisning till nationell säkerhet inte alltid en tillräcklig grund för att helt undanta en fråga från fördragets tillämpningsområde.

Medlemsstaterna har enligt artikel 4.2 FEU befogenhet att självständigt reglera frågor som rör exempelvis organisationen av försvarsmakten i syfte att försvara sitt territorium eller sina väsentliga intressen. Detta gäller dock i förhållande till medlemsstatens egen verksamhet för att säkra nationell säkerhet[25] där EU måste respektera medlemsstaternas ”väsentliga statliga funktioner”. Detta betyder att verksamhet som endast *kan* bedrivas av staten eller av statliga myndigheter (eller motsvarigheter till statliga myndigheter – som kan placeras i samma kategori) och som inte kan bedrivas av enskilda personer tillhör medlemsstaternas (exklusiva) regleringskompetens.[26] Sådan verksamhet kan EU därmed inte hitta stöd i fördraget för att reglera.[27]

Om, däremot, en nationell åtgärd påverkar den fria rörligheten på den inre marknaden, exempelvis genom nationella regleringar av leverantörer av digitala tjänster, kan den inte omfattas av undantaget om statlig verksamhet.[28] I dessa fall räcker det inte för medlemsstaterna att legitimera åtgärden med hänvisning till allmän säkerhet, nationellt försvar eller till att det rör sig om varor av strategisk betydelse.[29] EU-domstolen har nämligen konstaterat att det inte går att tolka medlemsstaternas möjlighet att göra undantag med stöd i nationell säkerhet som ett generellt förbehåll i fördraget, eftersom det skulle riskera att undergräva unionsrättens tvingande karaktär och dess enhetliga tillämpning.[30]

> ”En hänvisning till nationell säkerhet är med andra ord inte tillräcklig för att en medlemsstat ska kunna göra avsteg från EU-rättens integritetsskydd.”

En hänvisning till nationell säkerhet är med andra ord inte tillräcklig för att en medlemsstat ska kunna göra avsteg från EU-rättens integritetsskydd.[31] Medlemsstaternas utrymme att införa nationella regler med anledning av nationell säkerhet som

---

[25] Mål C-186/01, *Alexander Dory* mot *Bundesrepublik Deutschland*, ECLI:EU:C:2003:146, p. 31.

[26] Mål C-623/17, *Privacy International*, pp. 46–49, se även förenade målen C-511/18, C-512/18 och C-520/18, *La Quadrature du Net m.fl.*, pp. 92–95 samt 98–99. Medlemsstaterna måste i dessa fall dock iaktta de regler som finns dataskyddsdirektivet, vilket innebär nationell konstitutionell rätt och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen).

[27] Se avseende e-dataskyddsdirektivet, mål C-623/17, *Privacy International*, p. 35. Se avseende dataskyddsförordningen, mål C-25/17, *Förfarande anhängiggjort av Tietosuojavaltuutettu* (dataombudsmannen, Finland), ECLI:EU:C:2018:551, p. 37 och mål C-311/18 *Data Protection Commissioner* mot *Facebook Ireland Limited och Maximillian Schrems*, (*Schrems II*), ECLI:EU:C:2020:559, p. 85.

[28] Se EU-domstolens resonemang i mål C-101/01, *Brottmål mot Bodil Lindqvist*, ECLI:EU:C:2003:596, pp. 37–44.

[29] Mål C-623/17, *Privacy International*, p. 44 med hänvisning till tidigare praxis och C-311/18, *Schrems II*, p. 86.

[30] Mål C-337/05, *Europeiska gemenskapernas kommission* mot *Republiken Italien*, ECLI:EU:C:2008:203, s. 2–3, p. 43.

[31] Mål C-623/17, *Privacy International*.

träffar verksamhet som inte i sig utgör statlig verksamhet måste därmed upprätthålla det EU-rättsliga integritetsskydd som föreskrivs. Detta torde dessutom inte förändras oavsett om undantagsgrunden ”nationell säkerhet” finns uttalad i några harmoniseringsåtgärder eller inte, då det i första hand handlar om en tolkning av artikel 4.2 FEU och fördragets tillämpningsområde.[32] Enligt EU-domstolens rättspraxis finns det dock ett litet utrymme att göra undantag från EU:s integritetsskydd i vissa fall och under en kortare tid om det finns ett verkligt, förevarande och förutsebart hot.[33] Åtgärden måste då vara strängt[34] nödvändig och proportionerlig. Detta både om syftet är att bekämpa brottslighet och skydda den nationella säkerheten[35] och om det finns möjlighet att få detta prövat av en oberoende domstol eller administrativ myndighet som kan komma fram till ett bindande beslut.[36]

6. Begränsade undantagsmöjligheter från integritetsskyddet

EU har satt en hög nivå för den personliga integriteten vilket inte minst framgår av EU-domstolens rättspraxis. En konsekvens är att medlemsstaternas utrymme att göra undantag från skyddet för att skydda sina nationella intressen, såsom att bekämpa brott och skydda sin nationella säkerhet, är begränsat. Som nämns ovan beror detta på att medlemsstaterna förvisso kan reglera frågor som rör nationell säkerhet inom statlig verksamhet, men däremot kan de inte omotiverat vidta åtgärder som träffar statliga eller privata aktörer och som får konsekvenser för den inre marknaden.

”EU har satt en hög nivå för den personliga integriteten vilket inte minst framgår av EU-domstolens rättspraxis.”

I de förenade målen *Tele2* och *Watson and Others*[37] (avgörande från 2016) ställdes frågan till EU-domstolen om en nationell reglering som innebar att leverantörer av elektroniska kommunikationstjänster skulle lagra generell och odifferentierad trafik- och lokaliseringsdata, vilket sedermera skulle användas till att bekämpa grov brottslighet, kunde anses förenlig med EU-rätten. I *Tele2* gällde frågan den svenska regleringen, som ställde krav på att leverantörer av elektroniska kommunikationstjänster systematiskt och kontinuerligt, utan undantag, lagrar samtliga trafik- och lokaliseringsuppgifter för samtliga abonnenter och registrerade användare avseende samtliga elektroniska kommunikationsmedel. I *Watson and Others* rörde frågan en motsvarande brittisk lagstiftning som gav inrikesministern en möjlighet att ålägga offentliga teleoperatörer att lagra alla uppgifter om kommunikation under högst tolv månader.[38]

---

[32] Ibid, se resonemanget avseende rättigheterna i stadgans artiklar 7 och 8 i p. 70.
[33] Ibid, pp. 44–49.
[34] Ibid, p. 67.
[35] Ibid, p. 75. EU-domstolen konstaterar i målet, att ”[b]etydelsen av målet att skydda nationell säkerhet, tolkad mot bakgrund av artikel 4.2 FEU, är dock mer omfattande än betydelsen av de övriga mål som anges i artikel 15.1 i direktiv 2002/58, bland annat målen att bekämpa brottslighet i allmänhet, även grov brottslighet, och att skydda allmän säkerhet. Sådana hot som avses i föregående punkt skiljer sig nämligen, till sin art och på grund av sitt särskilda allvar, från risken i allmänhet för oroligheter eller störningar, även allvarliga sådana, av den allmänna säkerheten. Under förutsättning att övriga krav i artikel 52.1 i stadgan iakttas, kan målet att skydda nationell säkerhet således motivera åtgärder som innebär mer långtgående ingrepp i de grundläggande rättigheterna än dem som dessa övriga mål skulle kunna motivera …”
[36] Förenade målen C-203/15 och C-698/15, *Tele2 Sverige AB och Secretary of State for the Home Department* mot *Post- och telestyrelsen m.fl.*, ECLI:EU:C:2016:970. EU-domstolen har ytterligare förtydligat intresseavvägningen genom mål C-746/18, Brottmål mot H.K., ECLI:EU:C2021:152. Domen meddelades den 2 mars 2021, efter det att denna analys färdigställts.
[37] Förenade målen, C-203/15 och C-698/15, *Tele2 Sverige AB och Secretary of State for the Home Department* mot *Post- och telestyrelsen m.fl.*, ECLI:EU:C:2016:970.
[38] Uppgifter skulle här lagras av leverantörer av elektroniska kommunikationstjänster och göras tillgängliga inte bara för säkerhets- och underrättelsetjänsterna, med hänsyn till den nationella säkerheten, utan även för andra myndigheter efter deras behov. Tele2-domen avsåg en brottsutredning och inte nationell säkerhet.

EU-domstolen konstaterade att medlemsstaterna inte får kräva att leverantörer av elektroniska kommunikationstjänster, på ett generellt och odifferentierat sätt, systematiskt lagrar trafik- och lokaliseringsdata i syfte att bekämpa grov brottslighet.[39] Det ansågs däremot tillåtet att föreskriva viss riktad lagring i syfte att bekämpa grov brottslighet förutsatt att lagringen begränsas till vad som är strängt nödvändigt vad gäller 1) vilka slags uppgifter som lagras, 2) vilka kommunikationsmedel som avses, 3) vilka personer som berörs. Därtill ställde domstolen krav på att regleringen skulle ange hur länge lagringen kan ske.[40] De nationella reglerna måste också grunda sig på objektiva omständigheter som gör det möjligt att ta sikte på en utpekad personkrets vars uppgifter kan avslöja en koppling till grov brottslighet. Ett ytterligare krav är att de lagrade uppgifterna inte lämnas ut utan att en domstol eller oberoende myndighet på förhand beviljar tillgång till uppgifterna samt att berörda personer underrättas av de myndigheter som fått tillgång till uppgifterna.

EU-domstolen har härefter i målen *Privacy International*,[41] (avgörande från oktober 2020) avseende Storbritanniens reglering om lagring och överföring av trafik- och lokaliseringsdata, och förenade målen *La Quadrature du Net m.fl.* mot *Premier ministre m.fl.*,[42] (avgörande från oktober 2020) avseende Frankrikes och Belgiens reglering av hanteringen av trafik- och lokaliseringsdata, ytterligare preciserat vilka möjligheter medlemsstaterna har att göra undantag från integritetsskyddet i förhållande till brottsbekämpning. Vidare har EU-domstolen i dessa mål också preciserat medlemsstaternas möjligheter att självständigt reglera frågor som rör skyddet för nationell säkerhet och under vilka förutsättningar som undantag får göras från integritetsskyddet i sådant syfte.

I *Privacy International* hade EU-domstolen att bedöma huruvida Storbritanniens säkerhets- och underrättelseorgans inhämtning och användning av stora mängder uppgifter om kommunikation, så kallade mängddata, stred mot EU-rättens integritetsskydd. I förenade målen *La Quadrature du Net m.fl.* mot *Premier ministre m.fl.* och *Ordre des barreaux francophones et germanophone and Others* rörde frågorna istället fransk samt belgisk reglering avseende nationella krav om lagring av data som kunde göras tillgänglig för myndigheterna. Domstolen kom i dessa mål i huvudsak fram till att:

1. nationell lagstiftning om lagring, eller direktöverföring av, data till en nationell säkerhetstjänst från en leverantör av elektroniska kommunikationstjänster i syfte att skydda nationell säkerhet omfattas av EU-rättens integritetsskydd och faller under fördragets tillämpningsområde,

2. undantag från EU:s integritetsskydd ska tolkas restriktivt och uppfylla den allmänna EU-rättsliga principen om proportionalitet. Detta innebär i princip att:

   a. lagring eller direktöverföring av trafik- och lokaliseringsdata endast får ske under en begränsad tid som är strängt nödvändig,[43]

   b. en målinriktad lagring eller överföring måste föreskrivas vilken är begränsad i förhållande till objektiva och odifferentierade faktorer gällande kategorier av personer eller genom användning av geografiska kriterier.[44]

Utöver möjligheten att med hänvisning till nationell säkerhet göra dessa begränsade undantag från integritetsskyddet öppnade EU-domstolen även upp för vissa begränsade möjligheter att

[39] Se mål C-623/17, *Privacy International*, p. 59 med hänvisningar.
[40] Förenade målen C-511/18, C-512/18 och C-520/18, *La Quadrature du Net m.fl.*, pp. 146–147.
[41] Mål C-623/17, *Privacy International*.
[42] Förenade målen C-511/18, C-512/18 och C-520/18, *La Quadrature du Net m.fl.*
[43] Ibid, p. 151.
[44] Mål C-623/17, *Privacy International*, pp. 65–68 och förenade målen C-511/18, C-512/18 och C-520/18, *La Quadrature du Net m.fl.*, p. 147.

göra undantag i förhållande till att bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet.[45] Härutöver finns också ett visst utrymme att utföra realtidsinsamling av trafik- och lokaliseringsdata om den begränsas till personer som man har en uppenbar anledning att misstänka håller på med terroristverksamhet. Inskränkningar i skyddet måste dock alltid kunna prövas av en domstol eller oberoende myndighet.[46] EU-domstolen är slutligen tydlig med att det inte är tillåtet att upprätthålla temporära effekter av en sådan nationell åtgärd och låta detta fortgå under en förlängd eller obegränsad tid. EU:s rigida skydd ska ses mot bakgrund av unionens syn att personlig integritet är en mänsklig rättighet och att ett gemensamt skydd inom EU underlättar det fria flödet av data på den inre marknaden genom att det skapar trygghet och förtroende för digitala tjänster.

> ”EU:s rigida skydd ska ses mot bakgrund av unionens syn att personlig integritet är en mänsklig rättighet och att ett gemensamt skydd inom EU underlättar det fria flödet av data på den inre marknaden [...]”

Men frågan återstår hur elektroniska data och digitala spår på internet förhåller sig till EU:s yttre gränser och den inre marknaden, och därmed vad som händer med skyddet för personuppgifter om de hamnar i tredjeland. Hur ser EU på fria dataflöden till tredjeland om de mottagande länderna inte upprätthåller EU:s eget integritetsskydd?

För att lite närmare förstå hur elektroniska data, inklusive persondata, kan röra sig inom EU och i resten av världen krävs en kort beskrivning av kommunikationstjänster, plattformar och molntjänster.

7. Plattformar och molntjänster

Kommunikationstjänster är i praktiken möjliga att tillhandahålla och använda så länge man kan koppla upp sig på ett fast eller mobilt nätverk (genom master, fiber, koppar med mera) oavsett var man befinner sig i världen. Det finns vissa tekniska möjligheter att begränsa den faktiska åtkomsten genom olika typer av spärrar och blockeringar (till exempel brandväggar), vilket används av vissa stater för att generellt begränsa åtkomsten till informations- och kommunikationstjänster utanför nationens gränser.[47] I avsaknad av sådana blockeringar är det upp till staterna att genom nationell och internationell reglering styra hur kommunikationstjänster och persondata ska hanteras inom och mellan staterna.

Nätoperatörer – statliga eller privata – driver och säljer kapacitet i de fasta och mobila nätverken och ser till att trafiken mellan fasta telefoner och mobiltelefoner finns och fungerar samt kan erbjuda exempelvis IP-telefoni och bredband. All typ av tillgång till fasta eller mobila nät sker genom någon form av nätoperatör med vilken personer, fysiska eller juridiska, tecknar ett avtal för att kunna använda ett nät eller en uppkoppling. Genom ett abonnemang med en nätoperatör kan vi med andra ord få tillgång till olika digitala tjänster. Operatören har därmed stor insyn i den trafikdata som rör sig i nätet i förhållande till deras kunder, vilket bland annat är nödvändigt för att kunna fakturera kunderna för den kapacitet de använder.

Användandet av olika digitala tjänster såsom plattformar och molntjänster ökar med stor hastighet eftersom sådana tjänster ger möjligheter till större, bättre och mer avancerade resurser när informationsmängd och funktionskrav ständigt ökar.

I princip, och mycket förenklat, innebär en plattformstjänst en affärsmodell som möjliggör enklare användning av mer eller mindre komplexa funktioner. Tekniskt sett är en plattform en plats

---

[45] Se förenade målen C-511/18, C-512/18 och C-520/18, *La Quadrature du Net m.fl.* p. 168 där det framgår i detalj vad som krävs för undantag från integritetsskyddet i förhållande till brottsbekämpning och skydd för den nationella säkerheten.

[46] Ibid, p. 189.

[47] I Nordkorea finns en sluten version av internet som fungerar som ett nationellt ”intranät”. Om du kopplar upp dig från en nordkoreansk IP-adress spärrar en gigantisk brandvägg så att du inte kommer ut på den öppna delen av internet, https://www.soi2017.se/hur-fungerar-internet-i-nordkorea/.

där det går att placera eller köra olika tillämpningar eller applikationer. En plattform kan vara ett operativsystem, återanvändbara kodbibliotek och mjukvarukomponenter såsom spelmotorer och databasmotorer och även infrastruktur som uppfyller vissa specifikationer. Ofta står plattformar ovanpå varandra och internet kan betraktas som den grundläggande kommunikationsplattformen. En plattform kan därför beskrivas som både en arkitektur och en affärsmodell.

En molntjänst ger möjlighet till lagring och behandling av information genom internet. Tjänsten är en typ av plattform som kan köpas som en IT-resurs. Resurser kan beställas efter behov och är enkla att konfigurera, bygga ut och komma åt via internet. Företag – och andra aktörer – kan på så sätt till marginella kostnader köpa in teknik av högsta kvalitet, som annars skulle vara för dyr.[48] Att använda sig av molntjänster från en tredje part, som exempelvis Microsoft eller Amazon, innebär alltså att man slipper bygga en egen IT-infrastruktur.[49] Datacenter byggs runtom i världen och sammankopplas för att skapa skalbarhet, driftsäkerhet och lokal kapacitet.[50]

Plattformar och molntjänster erbjuder ett brett spektrum av tjänster: från virtuella behandlingssystem till tjänster som stöder applikationsutveckling och avancerade värdtjänster, samt webbaserade programlösningar som kan ersätta konventionellt installerade applikationer på slutanvändarnas persondatorer. Detta omfattar en stor mängd applikationer såsom exempelvis textbehandlingsapplikationer, kalendrar, arkiveringssystem för onlinebaserade dokumentarkiv, kunddatasystem och e-postlösningar utlagda på entreprenad.[51] Olika tjänster kan dessutom bestå av sammanlänkningar eller samarbete mellan flera leverantörer av plattforms- och molntjänster.

Mot denna bakgrund kan det konstateras att det är svårt att avgöra exakt vilka data som kan komma att finnas och behandlas var, av vem och i vilket land vid användandet av olika plattformar och molntjänster. Inom EU kan data röra sig fritt eftersom det finns gemensamma och rigida regler för integritetsskyddet. Medlemsstaternas möjligheter att avvika från skyddet är, som vi sett ovan, relativt begränsade. Men vad händer med EU:s integritetsskydd om persondata som genereras inom EU behandlas eller blir tillgängliga på en plattform eller i en molntjänst som tillhandahålls av ett företag som är etablerat i tredjeland? Eller när ett europeiskt företag använder sig av dellösningar som tillhandahålls av ett företag etablerat i tredjeland? Vem kan då få tillgång till data och vilka regler gäller? Den generella frågeställningen blir alltså hur det EU-rättsliga integritetsskyddet ska kunna upprätthållas i förhållande till tredjeland och vilka konsekvenser det får om EU:s skydd inte sträcker sig dit?

> ”[...] det är svårt att avgöra exakt vilka data som kan komma att finnas och behandlas var, av vem och i vilket land vid användandet av olika plattformar och molntjänster.”

I målet *Privacy International*, som nämns ovan, konstaterade EU-domstolen att Storbritanniens nationella regler inte upprätthåller EU:s integritetsskydd. Innebär detta att det fria dataflödet mellan EU och Storbritannien måste stoppas när de tillfälliga reglerna som man har kommit överens om upphör att gälla den 30 juni 2021?[52]

---

[48] Yttrande 5/2012 om datormoln (cloud computing), artikel 29-gruppen för skydd av personuppgifter, 01037/12/SV, WP 196, 1 juli 2012, s. 4.
[49] Se även beskrivning av molntjänster i SOU 2021:1, delbetänkande, Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering, avsnitt 2.2.4.
[50] För att säkra kunders data byggs systemen redundant, det vill säga alla funktioner dubbleras dels inom ett datacenter, dels mellan datacenter. Det innebär att kundernas data måste vara uppdaterade på flera ställen, med andra ord förflyttas data runt hela tiden.
[51] Yttrande 5/2012 om datormoln (cloud computing), artikel 29-gruppen, s. 4.
[52] Avtal om handel och samarbete mellan Europeiska unionen och Europeiska atomenergigemenskapen, å ena sidan, och Förenade konungariket Storbritannien och Nordirland, å andra sidan, EUT L 444, 31.12.2020, s. 14–1462.

8. Integritetsskyddad data i tredjeland

Det EU-rättsliga integritetsskyddet gäller oavsett var persondata med ursprung från EU behandlas, det vill säga oavsett om det sker inom medlemsstaterna eller i tredjeland. Det säger sig dock självt att det är svårt att kontrollera att EU:s regler upprätthålls av tredjeland. Persondata får därför endast överföras till tredjeland i det fall en adekvat skyddsnivå upprätthålls i det aktuella tredjelandet. EU:s krav är att det mottagande landet har en skyddsnivå som är väsentligen likvärdigt med EU:s integritetsskydd. En överföring mellan EU och tredjeland omfattas av EU-lagstiftningens begrepp ”behandling”. Behandling i detta hänseende definieras enligt dataskyddsförordningen som en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, exempelvis utlämning eller avslöjande genom överföring, spridning eller tillhandahållande på annat sätt. Ingen åtskillnad görs beroende på om verksamheten utförs inom unionen eller har samband med ett tredjeland.[53]

a. Adekvat och väsentligen likvärdig skyddsnivå

Överföringar[54] av integritetsskyddade uppgifter till organisationer som är etablerade i tredjeland[55] kan med andra ord enligt EU-rätten ske under förutsättning att det går att säkerställa en adekvat och väsentligen likvärdig skyddsnivå som finns inom EU för sådana uppgifter i det aktuella tredjelandet. Detta kan uppnås på olika sätt.

- *Adekvat skyddsnivå*
  Kommissionen kan enligt artikel 45 i dataskyddsförordningen besluta att ett tredjeland generellt uppfyller kraven om en adekvat skyddsnivå vilket innebär att skyddet ska vara väsentligen likvärdigt med det som finns i EU.[56] Detta kan även gälla för ett visst territorium, en internationell organisation eller en eller flera sektorer i ett tredjeland.[57] När kommissionen fattar ett sådant beslut tittar den bland annat på mottagarlandets lagar och internationella åtaganden, vilka möjligheter den registrerade (vars uppgifter överförs) har att få en rättslig prövning och om landet respekterar de mänskliga rättigheterna och de grundläggande friheterna. Kommissionen kontrollerar också att det finns oberoende tillsynsmyndigheter som ansvarar för att dataskyddsreglerna följs och som kan hjälpa de registrerade.[58]

- *Standardklausuler*
  När kommissionen inte har fattat ett generellt beslut om adekvat skyddsnivå kan överföring endast ske om lämpliga skyddsåtgärder vidtagits av personen som är ansvarig för överföringen av personuppgifterna. Här kan aktörer istället använda sig av standardiserade dataskyddsbestämmelser, så kallade standardklausuler, som antagits av kommissionen. Skyddet måste då genom standardklausulerna, tillsammans med eventuellt övriga åtaganden, uppnå ett skydd som är väsentligt likvärdigt med det som finns

---

[53] C-311/18, *Schrems II*, p. 82. Jfr resonemanget i SOU 2021:1, där motsatt tolkning synes framföras: ”Det är också vår bedömning att det inte är fråga om en tredjelandsöverföring när personuppgifter behandlas uteslutande inom EU, även om den personuppgiftsansvarige eller personuppgiftsbiträdet som behandlar personuppgifterna är bunden av tredjelands lagstiftning som innebär att denne kan åläggas att lämna ut uppgifter direkt till ett tredjelands myndigheter. Tredjelandsöverföringen sker först i samband med att uppgifterna överförs till myndigheter eller annan mottagare i tredjeland.”

[54] Att låta överföra personuppgifter från en medlemsstat till ett tredjeland är i sig en behandling av personuppgifter, se mål C-362/14, *Maximillian Schrems* mot *Data Protection Commissioner*, ECLI:EU:C:2015:650 (*Schrems I*), p. 45.

[55] Ibid, p. 79.

[56] C-311/18, *Schrems II*, p. 176.

[57] Se Integritetsskyddsmyndighetens information på https://www.imy.se/lagar--regler/dataskyddsforordningen/tredjelandsoverforing/hur-vet-vi-om-ett-tredje-land-har-adekvat-skyddsniva/

[58] Länder som enligt kommissionens beslut för närvarande har en adekvat skyddsnivå är: Andorra, Argentina, Bailiwick of Guernsey, Färöarna, Isle of Man, Israel, Japan, Jersey, Nya Zeeland, Schweiz, Uruguay. Se Integritetsskyddsmyndigheten, (https://www.imy.se/lagar--regler/dataskyddsforordningen/tredjelandsoverforing/hur-vet-vi-om-ett-tredje-land-har-adekvat-skyddsniva/).

inom EU. Utöver detta måste det finnas vissa lagstadgade rättigheter och effektiva rättsmedel i det aktuella tredjelandet i förhållande till de uppgifter som överförs.[59]

- *Undantag i särskilda situationer*
  Om varken kommissionen har fattat ett generellt beslut eller det finns fastställda standardklausuler att tillgå, kan överföringar till tredjeland ändå ske om man följer bestämmelserna som gäller vid överföringar i särskilda situationer. Detta innebär i korthet att den registrerade på förhand samtycker till överföringen eller att överföringen är nödvändig; 1) för att fullgöra ett avtal i den registrerades intresse, 2) i förhållande till ett allmänintresse eller 3) i förhållande till ett rättsligt anspråk. Ytterligare möjligheter till överföring är om det är nödvändigt i förhållande till den registrerades eller andra personers grundläggande intressen eller om överföringen görs från ett register som är avsett för att ge allmän information.[60] Undantagen som kan användas i särskilda situationer får dock aldrig tillämpas om de riskerar att undergräva nivån på skyddet för personuppgifter. Detta innebär att utnyttjande av undantagen i särskilda situationer aldrig får leda till att grundläggande rättigheter kan komma att kränkas.[61]

En viss vägledning för hur de tre här ovan beskrivna undantagen bör tolkas kan hittas i EU-domstolens avgöranden i *Schrems I* och *II* i förhållande till USA.[62] I *Schrems I* ifrågasatte EU-domstolen kommissionens beslut om att USA:s så kallade *Safe Harbor*-regler kunde betraktas som att de garanterade en adekvat skyddsnivå, det vill säga en som var accepterad av EU. *Safe Harbor*-reglerna består av en samling frivilliga regler framtagna av USA:s handelsdepartement om hur företag och organisationer ska behandla personuppgifter för att respektera skyddet för personlig integritet. EU-domstolen ogiltigförklarade kommissionens beslut om att *Safe Harbor* uppfyllde kraven om integritetsskydd. Detta i första hand eftersom USA:s lagstiftning och rättspraxis ger den amerikanska underrättelsetjänsten ett brett handlingsutrymme att övervaka enskilda med utgångspunkt i enskildas personuppgifter.[63]

Eftersom EU-domstolen ogiltigförklarade kommissionens beslut antog kommissionen ett nytt beslut, baserat på det så kallade *Privacy Shield*,[64] som skulle garantera en adekvat skyddsnivå för uppgifter som överförs från EU till USA. *Privacy Shield* innebär att företag som är etablerade i USA, genom ett förfarande om självcertifiering, förklarar att de följer vissa principer som utfärdats av USA:s handelsministerium vilka garanterar en adekvat skyddsnivå för de personuppgifter som överförs.[65] Genom *Privacy Shield*-beslutet infördes också en ombudsmansmekanism för att säkerställa kraven om rättslig prövning för överförda uppgifter, vilket saknades i förhållande till *Safe Harbor*. På samma grunder som i *Schrems I* (myndigheternas möjligheter till övervakning) konstaterade dock

---

[59] C-311/18, *Schrems II*, p. 103.
[60] Se Europeiska dataskyddsstyrelsens riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679, antagna den 25 maj 2018, där det framgår att ”[v]id tillämpning av artikel 49 måste man komma ihåg att enligt artikel 44 ska den dataexportör som överför personuppgifter till tredjeländer eller internationella organisationer även uppfylla villkoren i övriga bestämmelser i GDPR. Varje behandling måste följa de relevanta dataskyddsbestämmelserna, särskilt artiklarna 5 och 6. Följaktligen måste ett tvåstegstest användas: för det första måste det finnas en rättslig grund för behandlingen av uppgifter som sådan, tillsammans med alla relevanta bestämmelser i GDPR. Som ett andra steg måste bestämmelserna i kapitel V följas.” I artikel 29-gruppens arbetsdokument, WP 114 s. 9 och WP 228 s. 39, framgår att undantagen i artikel 49 i dataskyddsförordningen aldrig får leda till en situation där grundläggande rättigheter kan komma att kränkas.
[61] Ibid, s. 3.
[62] Mål C-362/14, *Schrems I* och C-311/18, *Schrems II*.
[63] Se mål C-362/14, *Schrems I*, pp. 60–64 för en beskrivning av omfattningen av möjligheterna för USA att utöva vad man brukar kalla massövervakning.
[64] Privacy Shield – Skölden för skydd för privatlivet i EU och USA utgörs av principer som utfärdats av USA:s handelsministerium och som organisationer i USA kan ansluta sig till.
[65] Förslag till avgörande av generaladvokat H. Saugmandsgaard Øe, föredraget den 19 december 2019 i mål C-311/18, *Schrems II*, pp. 33–38.

EU-domstolen att inte heller *Privacy Shield-beslutet* uppfyllde kraven på att USA:s lagstiftning säkerställde en adekvat skyddsnivå, eftersom USA:s lagstiftning och praxis inte hade förändrats sedan *Schrems I*-målet. Sedan *Schrems-målen* ser USA:s lagstiftning ut att ha gått i motsatt riktning, sett EU:s skyddsintressen, eftersom landet 2018 antog ”the CLOUD Act”.[66] Denna lag ger amerikanska myndigheter möjlighet att begära ut data från amerikanska molntjänstleverantörer – oavsett var data finns lagrad rent geografisk.

”Exportören av uppgifterna och mottagaren av överföringen måste i förväg kontrollera att den skyddsnivå som krävs enligt EU-rätten iakttas i det aktuella tredjelandet.”

I *Schrems II* konstaterade EU-domstolen vidare att också användandet av standardklausuler kan ifrågasättas. Detta gör den eftersom standardklausuler inte per automatik innebär att en överföring av persondata är laglig. Om den kan betraktas som laglig beror helt och hållet på om det aktuella tredjelandet kan leva upp till ett skydd som är väsentligt likvärdigt med det som finns inom EU. Om förhållandena i tredjeland är sådana att standardklausulerna inte kan efterlevas av mottagarna av persondata ska överföringar inte tillåtas och avbrytas.[67] Exportören av uppgifterna och mottagaren av överföringen måste i förväg kontrollera att den skyddsnivå som krävs enligt EU-rätten iakttas i det aktuella tredjelandet. Mottagaren är skyldig att informera exportören om mottagaren inte kan iaktta de standardiserade skyddsklausulerna, varmed exportören i så fall måste avbryta överföringen av uppgifter och/eller häva avtalet med mottagaren.

b. Grunder för adekvat skyddsnivå i enlighet med EU:s rättspraxis

För att en adekvat skyddsnivå ska anses föreligga måste skyddet i tredjeland vara väsentligt likvärdigt med det som garanteras enligt EU-rätten.[68] Enligt EU-rätten krävs i princip att:

- det måste finnas en legitim och laglig grund för hur personuppgifter behandlas,
- var och en ska ha rätt att få tillgång till insamlade uppgifter som rör honom eller henne,
- ett förbud gäller mot generell och odifferentierad lagring eller överföring till myndigheter – även i syfte att bekämpa grov brottslighet och/eller skydda den nationella säkerheten,[69]
- realtidsinsamling av trafik- och lokaliseringsdata är begränsad till situationer där det finns ett allvarligt hot mot nationell säkerhet och får endast röra personer där det finns en uppenbar anledning till misstanke om terroristverksamhet,[70]
- målinriktad lagring av trafik- och lokaliseringsdata är tillåten endast under en strikt begränsad tidsperiod och måste vara begränsad i förhållande till objektiva och odifferentierade faktorer med avseende på kategorier av personer eller genom användning av geografiska kriterier,[71]
- det måste finnas effektiva rättsmedel för att upprätthålla integritetsskyddet.

---

[66] Clarifying Lawful Overseas Use of Data Act, https://www.congress.gov/bill/115th-congress/house-bill/4943.
[67] *Schrems I*, p. 68. Se även Europeiska dataskyddsstyrelsen, Vanliga frågor om EU-domstolens dom i mål C-311/18 – Data Protection Commissioner mot Facebook Ireland och Maximillian Schrems, 24 juli 2020, (https://edpb.europa.eu/our-work-tools/our-documents/ohrajn/frequently-asked-questions-judgment-court-justice-european-union_sv).
[68] C-311/18, *Schrems II*, p. 96. För kopplingen mellan vad som kan anses acceptabelt inom EU med de krav som ställs på regleringen i tredjeland för att tillåta överföring till tredjeland, se Europeiska dataskyddsstyrelsens rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder, 10 november 2020, p. 34.
[69] Ibid, jfr resonemanget i pp. 172–173.
[70] Förenade målen C-511/18, C-512/18 och C-520/18, *La Quadrature du Net m.fl.*, pp. 172 och 192.
[71] Mål C-623/17, *Privacy International*, p. 65–68.

c. Rekommendationer från Europeiska dataskyddsstyrelsen

Mot bakgrund av *Schrems II*-avgörandet presenterade Europeiska dataskyddsstyrelsen i början av november 2020 nya rekommendationer avseende internationella överföringar av personuppgifter till tredjeland.[72] Europeiska dataskyddsstyrelsen är ett oberoende europeiskt organ bestående av företrädare för nationella dataskyddsmyndigheter och Europeiska datatillsynsmannen som bland annat kan utfärda rekommendationer för att ge hjälp och vägledning till dataexportörer. Dataskyddsstyrelsen ska bidra till en enhetlig tillämpning av dataskyddsregler inom hela EU samt främja samarbete mellan EU:s dataskyddsmyndigheter.

I korthet innebär dataskyddsstyrelsens rekommendationer att det krävs en hög kunskapsnivå hos dataexportörer. De har i sin tur ett stort ansvar för att kontrollera att det EU-rättsliga skyddet för personuppgifter upprätthålls om personuppgifter hamnar i tredjeland.

Rekommendationerna är uppbyggda i sex steg där dataexportören är skyldig att:

1. ”känna till sina överföringar” genom att kartlägga alla överföringar av personuppgifter till tredjeländer, inklusive vidarebefordran till underbiträden och minimera överföringar,

2. välja lämplig skyddsmetod från kapitlet om tredjelandsöverföringar i dataskyddsförordningen, hålla uppsyn över att adekvansbeslut upprätthålls, om inget sådant beslut finns,

   a. kompensera med exempelvis standardklausulavtal, bindande företagsregler, uppförandekoder, certifieringsmekanismer eller ad hoc-avtalsbestämmelser, eller

   b. använda de undantag som finns i artikel 49 i dataskyddsförordningen (samtycke och fullgörande av avtal, vilket dock ska tolkas restriktivt och får inte undergräva skyddet),

3. bedöma om något i det aktuella tredjelandets lagar eller praxis kan påverka effektiviteten av vald skyddsåtgärd. Detta innebär att skyddet i huvudsak måste vara likvärdigt med det som garanteras i EU (särskilt bör uppmärksammas om det finns lagar som gör det möjligt för myndigheter att begära ut överförda personuppgifter, i förhållande till exempelvis nationell säkerhet, brottsbekämpning eller myndighetstillsyn),[73]

4. genom kompletterande åtgärder säkerställa EU:s skyddsnivå för personuppgifter såsom av teknisk, avtalsmässig natur eller av organisatorisk karaktär,

5. implementera skyddsåtgärderna,

6. löpande omvärdera och uppmärksamma lagstiftning som kan påverka effektiviteten av åtgärderna.

Sammanfattningsvis kan konstateras att EU-rätten är tillämplig vid överföring av persondata, i kommersiellt syfte, mellan ett företag i EU till ett företag som är etablerat i tredjeland. Tredjeland behöver dock inte förhålla sig till om en åtgärd avser att skydda nationell säkerhet inom ramen för statlig verksamhet. Detta faller sig naturligt eftersom artikel 4.2 FEU, som fördelar ansvaret mellan EU och medlemsländerna, bara gäller för EU:s medlemsstater. Tredjeland måste alltid uppfylla kraven om att en nationell åtgärd är strikt nödvändig och proportionerlig i förhållande till undantag från det EU-rättsliga integritetsskyddet för att överföringar ska få ske. I det fall kommissionen inte antagit ett beslut om adekvat skyddsnivå i förhållande till ett tredjeland kan fastställda standardklausuler användas eller undantag i särskilda situationer. För att dataexportörer ska kunna använda denna möjlighet måste de dock uppfylla de strikta krav

[72] Europeiska dataskyddsstyrelsens rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter, antagna den 10 november 2020.

[73] I länder där myndigheter kan begära ut personuppgifter är det avgörande huruvida sådana befogenheter är begränsade till vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle. Detta måste bedömas enligt EU-standard med beaktande av artiklarna 47 och 53 i stadgan.

som satts upp i Europeiska dataskyddsstyrelsens rekommendationer.

Gällande situationen i *Schrems I och II* och möjligheterna till fortsatta överföringar till företag etablerade i USA återstår för den nationella domstolen i målet att avgöra om de amerikanska reglerna kan anses som strikt nödvändiga och proportionerliga i förhållande till nationell säkerhet. Om så inte är fallet måste överföringarna till amerikanska företag stoppas. I enlighet med EU-domstolens dom i *Privacy International* synes detsamma gälla i förhållande till överföringar av persondata till Storbritannien efter den 30 juni 2021, då avtalet mellan EU och Storbritannien anses innebära ett säkerställande av fria dataflöden mellan parterna.[74]

9. Skillnader vid överföring mellan medlemsländerna och mellan EU och tredjeland

EU-domstolen har i sin rättspraxis konstaterat att nivån avseende integritetsskyddet för uppgifter härrörande från personer i EU måste kunna upprätthållas och vara väsentligen likvärdigt med det inom EU oavsett var persondata hanteras i världen. Förenklat uttryckt innebär detta att uppgifter som faller under det EU-rättsliga integritetsskyddet, som hanteras både inom EU eller i tredjeland, ska vara skyddade från nationella åtgärder som innebär att tjänsteutövare på ett generellt och odifferentierat sätt tvingas att systematiskt lagra eller överföra integritetsskyddade uppgifter som därmed kan användas av myndigheter.[75] Lagring och överföring kan i undantagsfall under en mycket begränsad tid tillåtas om den är målinriktad, strikt nödvändig och begränsad till vissa utpekade personer i syfte att bekämpa brottslighet och/eller skydda nationella säkerhet. I princip får det inte förekomma någon form av allmän massövervakning av personer även om det rör nationell säkerhet.

Det finns vissa skillnader mellan hur regleringen och EU-domstolens praxis slår å ena sidan inom den inre marknaden och å andra sidan i förhållande till tredjeland. Reglering av statlig verksamhet tillhör uteslutande varje medlemsstats eget ansvar och faller utanför fördragets tillämpningsområde. Medlemsstaternas eventuella undantag från skyddet behöver därför inte beakta dataskyddsförordningen eller e-dataskyddsdirektivet eller uppfylla det EU-rättsliga proportionalitetskravet för att dataflöden ska vara tillåtna enligt EU-rätten mellan medlemsstaterna.

För att överföringar ska få ske till tredjeland måste däremot alla eventuella undantag som görs från det EU-rättsliga integritetsskyddet i det landet uppfylla den EU-rättsliga proportionalitetsbedömningen, oavsett om det rör statlig verksamhet. Detta innebär att integritetsskyddade uppgifter med ursprung i EU exempelvis har ett uttalat skydd mot oproportionerlig signalspaning i tredjeland, men inte i medlemsstaterna. En annan tydlig skillnad är att medlemsstaterna kan ställas inför EU-domstolen och i förlängningen dömas till att betala böter och/eller vite när de bryter mot det EU-rättsliga integritetsskyddet, medan överföringar till tredjeland istället måste stoppas[76] om ett väsentligen likvärdigt skydd med det som finns inom EU inte upprätthålls.

> ”I princip får det inte förekomma någon form av allmän massövervakning av personer även om det rör nationell säkerhet.”

[74] Se information från Integritetsskyddsmyndigheten, (https://www.imy.se/lagar--regler/dataskyddsforordningen/tredjelandsoverforing/) och Europeiska dataskyddsstyrelsen, Statement on the withdrawal of the United Kingdom from the European Union, adopted on 15 December 2020, updated on 13 January 2021. Avtalet utgör inte ett beslut om adekvansnivå utan en tillfällig lösning i avvaktan på ett sådant beslut.

[75] Förenade målen C-511/18, C-512/18 och C-520/18, *La Quadrature du Net m.fl.*, p. 138.

[76] Av relevant nationell myndighet i den medlemsstat där persondataskyddet ifrågasätts, se Mål 311/18, *Schrems II*, p. 121.

10. Slutsats

Dataflöden, en av framtidens viktigaste tillgångar, har idag antagit nya former. Det innebär att data inte alltid ”flödar” eller skickas mellan företag över nationella gränser utan snarare ”existerar” i obestämd form på en obestämd plats och kan vara tillgänglig och användas av flera aktörer samtidigt. Vidare är digitala värdekedjor ofta globala: plattforms-, moln- och applikationstjänster med ursprung i olika länder är nära sammankopplade och beroende av varandra. Hinder mellan länder för fria dataflöden kan därmed hämma utvecklingen och utbytet av digitala tjänster som skapar tillväxt, innovation och konkurrenskraft. Det kan samtidigt vara svårt att avgöra vilket företag i vilken stat som ansvarar och/eller hanterar specifika data, vilket i sin tur skapar osäkerhet avseende vilket land som reglerar tillgången till exempelvis integritetsskyddade data. Tillgång till integritetsskyddade data kan vara enormt viktig för stater i deras brottsbekämpande verksamhet och för att skydda nationell säkerhet. Målkonflikter mellan fria dataflöden, integritetsskydd och möjligheter att göra undantag från skyddet har uppstått när EU måste begränsa dataflöden till vissa utpekade tredjeländer som inte upprätthåller samma integritetsskydd som EU. Vidare hindras medlemsstaterna från att göra vissa undantag från skyddet för att bekämpa grov brottslighet och skydda nationell säkerhet.

När exempelvis länder som USA och i framtiden kanske Storbritannien inte upprätthåller ett integritetsskydd som är väsentligt likvärdigt med det inom EU – eftersom de är mer tillåtande än EU vad gäller tillgång till integritetsskyddade data i syfte att bekämpa grov brottslighet och skydda nationell säkerhet – kräver EU-rätten att dataflöden till dessa länder begränsas eller helt stoppas. För att detta inte ska ske måste antingen EU sänka sina krav på integritetsskyddet eller tredjeland höja sitt skydd. Alternativet skulle annars vara att EU skapar sitt eget dataområde, med någon form av barriär mot tredjeland, vilket exempelvis kommissionär Thierry Breton har framhållit som en möjlighet vid flera tillfällen.[77]

Den springande punkten synes här vara hur förtroende mellan länder kan byggas upp gällande avvägningen mellan integritetsskydd och möjligheterna att använda integritetsskyddade uppgifter i syfte att bekämpa grov brottslighet och för att skydda nationell säkerhet, vilket är nära kopplat till nationellt självstyre och identitet. En lösning verkar ligga i att komma fram till en gemensam global syn på hur balans kan uppnås mellan integritetsskydd och undantag i syfte att bekämpa grov brottslighet och skydda nationell säkerhet, allt för att skapa förtroende mellan länderna och undvika geografiska begränsningar av dataflöden.

EU:s integritetsskydd bör inte heller utarma möjligheterna för medlemsstater att bekämpa brottslighet och skydda nationell säkerhet. EU-domstolen har konstaterat att fördraget omfattar och begränsar nationella regler som innebär undantag från integritetsskyddet i syfte att bekämpa grov brottslighet och skydda nationell säkerhet när de är riktade mot tjänsteutövare. Brottslig och samhällsfarlig verksamhet på internet ökar ständigt och det måste finnas effektiva metoder att kunna stoppa detta. Det är därför viktigt att EU tar ansvar för att göra en tydlig, relevant och väl balanserad avvägning mellan integritetsskyddet och möjligheterna för medlemsstaterna att utöva en effektiv brottsbekämpning och skydda nationell säkerhet.

> ”Höga och ibland nästintill ouppnåeliga krav ställs på företag som är ansvariga för integritetsskyddade uppgifter.”

Så som EU-rätten utvecklats har målkonflikterna – mellan fria dataflöden, integritetsskydd och undantag från skyddet med hänvisning till brottsbekämpning och skydd av nationell säkerhet – skapat stora svårigheter för både företag och medlemsstaterna. Höga och ibland nästintill ouppnåeliga krav ställs på företag som är ansvariga för integritetsskyddade uppgifter.

---

[77] Scott, M. och Manancourt, V., *Facebook to stop moving data from EU to US: 5 things you need to know – Here's what the pending decision means for transatlantic relations*, POLITICO, 2 september 2020, https://www.politico.eu/article/facebook-data-ireland-privacy/

Företag som exempelvis använder olika plattforms- och molntjänster måste enligt EU-rätten ha full kontroll gällande när, hur och vilka uppgifter som kan komma att hanteras var, eftersom det finns olika förutsättningar för behandling av integritetsskyddade data inom och utanför EU. Företagen måste kunna säkerställa att beslut om adekvat skyddsnivå finns och upprätthålls i alla länder där olika uppgifter kan komma att behandlas av olika inblandade företag eller, om ett sådant generellt beslut inte finns, använda standardklausuler och se till att de upprätthåller rätt nivå eller, om varken ett generellt beslut eller standardklausuler finns, använda undantag i särskilda situationer. Detta gäller i förhållande till varje aktuell uppgift i varje aktuellt land. Integritetsskyddade uppgifter från EU får inte hamna hos ett företag etablerat i ett tredjeland som utövar någon form av massövervakning.

Med tanke på hur plattforms-, molns-, och applikationstjänster är uppbyggda och sammanvävda med varandra, och genom olika samarbete mellan företag i olika länder, kan detta bli ytterst svårt. För medlemsstaterna innebär uttolkningen av EU-rätten att utrymmet för att göra undantag från integritetsskyddet starkt begränsar deras möjligheter att få tillgång till skyddade uppgifter i syfte att bekämpa grov brottslighet och skydda nationell säkerhet. De kriterier som medlemsstaterna måste uppfylla enligt EU-domstolens praxis är snäva, snåriga och inte alltid effektiva för att uppnå önskat syfte.

Om regelverket ska fungera för önskat syfte måste EU ta ansvar för att skapa tydlighet, balans och effektivitet för både företag och medlemsstater. För det första måste EU säkerställa fria dataflöden både inom EU och till tredjeland genom att driva fram en gemensam syn med andra länder avseende integritetsskyddet. Företag som utvecklar och använder digitala tjänster behöver kunna förlita sig på tydliga och enkla regelverk som inte i onödan begränsar fria dataflöden. För det andra måste EU ge tydlig vägledning och tillräckligt utrymme för medlemsstaterna när de vill göra undantag från integritetsskyddet för att bekämpa grov brottslighet och skydda nationell säkerhet.