Wictoria Lundén

BEAKTANDET AV ÄNDAMÅLSBEGRÄNSNING OCH SEKUNDÄR ÅTKOMST TILL PERSONUPPGIFTER I EU:S INTEROPERABILITETSRAMVERK INOM OMRÅDET MED FRIHET, SÄKERHET OCH RÄTTVISA

Pro gradu-avhandling i
offentlig rätt
Handledare: Markku Suksi
Fakulteten för
samhällsvetenskaper och
ekonomi
Åbo Akademi
Åbo 2020

ÅBO AKADEMI - FAKULTETEN FÖR SAMHÄLLSVETENSKAPER OCH EKONOMI
Abstrakt för avhandling pro gradu

Ämne: Offentlig rätt, Magisterprogram i utrikeshandel och kommersiell juridik

Författare: Wictoria Lundén

Arbetets titel: Beaktandet av ändamålsbegränsning och sekundär åtkomst till personuppgifter i EU:s interoperabilitetsramverk inom området med frihet, säkerhet och rättvisa

Handledare: Markku Suksi

Abstrakt:

Inom EU har ett flertal informationssystem upprättats för lagring av personuppgifter i anslutning till gränsförvaltning, migrationshantering och brottsbekämpning. Systemen har traditionellt utvecklats som separata enheter, s.k. silon, vilket har uppfyllt dataskyddets krav på ändamålsbegränsning. På senare tid har dessa silon dock ansetts bidra till informationsglapp. Genom upprättandet av en rättslig ram för interoperabilitet inom området med frihet, säkerhet och rättvisa har EU:s lagstiftare åtgärda detta problem. Interoperabilitet syftar på informationssystems förmåga att sinsemellan utbyta och använda sig av information för att uppnå en mer holistisk syn på information. Detta medför att den decentralisering av personuppgifter som tidigare tillämpats i syfte att säkerställa grundläggande rättigheter har frångåtts, bl.a. till följd av dess hämmande effekt vid utnyttjandet av ny teknologi för databehandling.

Upprättandet av interoperabla databaser medför en inskränkning av individens grundläggande rätt till privatliv i EU-stadgans artikel 7 och dataskydd i artikel 8 samt rätten till privatliv i artikel 8 i Europeiska konventionen om mänskliga rättigheter, särskilt avseende principen om ändamålsbegränsning. Principen utgör en del av skyddet av personuppgifter i EU:s allmänna dataskyddsförordning och polisdirektivet. Principens roll i bearbetning mellan regelverken är dock osäker. Skyddet av personuppgifter utgör emellertid inte en absolut rättighet utan kan inskränkas i enlighet med lagenliga begränsningar i stadgans artikel 52(1). Förutom att interoperabilitetsramverket måste iaktta gällande lagstiftning om personuppgifter måste det även uppfylla principer etablerade i EU-domstolens praxis, bland annat krav på genomförande av lämpliga skyddsåtgärder. Eftersom de berörda uppgifterna till stor del består av biometrisk data som till sin natur är särskilt känsliga blir kravet på adekvata skyddsåtgärder ännu påtagligare. Åtgärderna måste uppfylla ett strikt nödvändighets- och proportionalitetstest. Avhandlingen avser granska huruvida de nya förordningarna uppfyller dessa villkor, och om interoperabilitetsförordningarna uppfyller kravet på ändamålsbegränsning. I arbetet används en rättsdogmatisk metod för att besvara de huvudsakliga forskningsfrågorna.

Utredningen visar att interoperabilitetsramverket i verkligheten utgör en utvidgning av brottsbekämpande myndigheters åtkomsträttigheter, samtidigt som tidigare skyddsåtgärder har avvecklats. Denna utvidgning har inte följts av effektiva skyddsåtgärder, vilket går emot EU-domstolens praxis, och regleringen står därmed i strid med de registrerades dataskydd. Ytterligare påverkarar förordningarna de registrerades rätt till information och därtill kopplade rättigheter negativt, och försätter registrerade i en asymmetrisk position i jämförelse med de registeransvariga. Det står klart att interoperabilitet i grunden förändrar den nuvarande arkitekturen för EU:s storskaliga databaser och medföra ett skifte i tolkningen av principen om ändamålsbegränsning, särskilt avseende hur de normativa målen för principen ska uppfyllas.

Nyckelord: Interoperabilitet, dataskydd, personuppgifter, ändamålsbegränsning, brottsbekämpande myndigheter

Datum: 9.6.2020	Sidor: vi, 107, XVI

INNEHÅLLSFÖRTECKNING

Förkortningar

API-uppgifter	Avancerade passageraruppgifter
BMS	Biometriskt matchningssystem
CIR	Gemensam databas för identitetsuppgifter
Ecris-TCN	System för att identifiera de medlemsstater som innehar uppgifter om tidigare fällande domar mot tredjelandsmedborgare
EDPB	Europeiska dataskyddsstyrelsen
EDPS	Europeiska datatillsynsmannen
EES	In- och utresesystemet
EG	Europeiska gemenskapen
ESP	Europeisk sökportal
Etias	EU-system för reseuppgifter och resetillstånd
EU	Europeiska unionen
eu-LISA	Europeiska byrån för den operativa förvaltningen av stora it-system inom området med frihet, säkerhet och rättvisa
Eurodac	European Asylum Dactoscopy (databas där asylsökandes fingeravtryck förvaras)
Europadomstolen	Europeiska domstolen för de mänskliga rättigheterna
Europakonventionen	Europeiska konventionen om skydd för de mänskliga rättigheterna
Europol	Europeiska unionens byrå för brottsbekämpning
EUT	Europeiska unionens officiella tidning
FEU	Fördraget om Europeiska unionen (EU-fördraget)
FEUF	Fördraget om Europeiska unionens funktionssätt (EUF-fördraget)
FN	Förenta nationerna
FRA	EU:s byrå för grundläggande rättigheter
GDPR	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 (allmän dataskyddsförordning)

GL	Finlands grundlag (731/1999)
GrUU	Grundlagsutskottets utlåtande
HFD	Högsta förvaltningsdomstolen
ICS	EU:s importkontrollsystem
ICS2	EU:s reformerade importkontrollsystem
Interpol	Internationell organisation för kriminalpoliskårer
IOM	Internationella Migrationsorganisationen
JFT	Tidskrift utgiven av Juridiska föreningen i Finland
JK	Justitiekansler
JO	Justitieombudsman
MID	Multipel identitetsdetektor
PNR-uppgifter	Passageraruppgifter
Polisdirektivet	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
RP	Regeringens proposition
SIS	Schengens informationssystem
SIS II	Andra generationen av Schengens informationssystem
SLTD	Interpols databas över stulna och försvunna handlingar
Stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
SvJT	Svensk Juristtidning
TDAWN	Interpols databas för resehandlingar som är föremål för ett meddelande
VIS	Informationssystemet för viseringar
WP29	Artikel 29-gruppen

"There is a lot of wisdom in taking seriously
the political dimension of technical things."
- De Hert & Gutwin, 2006

1 INLEDNING

1.1 En interoperabel säkerhetsunion

Europeiska unionen (EU) har bedömts stå inför stora utmaningar relaterade till säkerhet och gränsförvaltning. Antalet illegala gränsöverskridningar har under de senaste åren ökat samtidigt som terroristhoten i Europa har tilltagit.[1] Dessutom överskrider dagens kriminella verksamhet traditionella gränser både i form av nationsgränser och sektorer av brottslighet. Inom EU har fokus lagts på behovet att stärka EU:s yttre gränser och informationssystem.[2] Medan medlemsstaterna fortfarande bär det främsta ansvaret för sin inre säkerhet,[3] kan staterna inte förväntas motverka dagens gränsöverskridande hot effektivt på egen hand, utan de är i behov av verktyg och infrastruktur på en gemensam europeisk nivå där nationella myndigheter kan samarbeta kring de kollektiva säkerhetsutmaningarna.[4] Detta arbete utförs inom ramen för EU:s gemensamma säkerhetsunion.[5] Inom EU regleras gemensamma säkerhetsrelaterade frågor som bekämpning av terrorism och brottslighet, gränsförvaltning men också behandling av asylansökningar och migration inom området med frihet, säkerhet och rättvisa. Området utgör ett relativt nytt och känsligt fält, som utvecklats till en europeisk knutpunkt för säkerhetssamarbete.[6] Området kännetecknas ofta av en spänning mellan säkerhet å ena sidan och frihet och rättvisa å andra sidan, där säkerhet betraktas som brottsbekämpning och skyddande av de europeiska medborgarna medan frihet och rättvisa betraktas som rättssäkerhet och skydd för individen.[7]

En av säkerhetunionens målsättningar är ett förbättrat informationsutbyte inom EU. Att effektivare kunna utnyttja de uppgifter som behöriga myndigheter har tillgång till genom

[1] Se bl.a. meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt regionkommittén, ”Europiska Säkerhetsagendan”, COM (2015) 185 final av den 28 april 2015 och meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt regionkommittén, ”En europeisk migrationsagenda”, COM (2015) 240 final av den 13 maj 2015.
[2] COM (2015) 240 final av den 13 maj 2015, s. 12.
[3] Artikel 72 FEUF.
[4] Meddelande från kommissionen till Europaparlamentet, Europeiska rådet och rådet, ”Att genomföra den europeiska säkerhetsagendan mot terrorism och bana väg för en säkerhetsunion”, COM (2016) 230 final av den 20 april 2016, s. 2.
[5] Se COM (2015) 185 final av den 28 april 2015.
[6] Herlin-Karnell 2017, s. 84.
[7] Suominen 2014, s. 6.

enskilda databaser inom respektive verksamhetsområde är starkt kopplat till detta mål. Insamlingen av biometriska uppgifter och registreringen av dessa i storskaliga informationssystem, i syfte att identifiera irreguljära migranter och brottslingar som passerar EU:s gränser,[8] har blivit ett viktigt element i unionens säkerhetspolitiska landskap. Sådana informationssystem innefattar huvudsakligen medborgare utanför EU, det vill säga tredjelandsmedborgare, inklusive korttidsresenärer, asylsökande och tredjelandsmedborgare med brottsregister.[9] Databaserna förlitar sig huvudsakligen på biometrisk teknologi, eftersom det ansetts vara en neutral och objektiv teknik med möjlighet att fånga upp individers unika personliga särdrag, såsom fingeravtryck, ansiktsbilder och DNA.[10] När biometriska uppgifter finns tillgängliga är risken att de används för andra ändamål än de som de samlats in för påtaglig. Sannolikheten att den registrerade inte kommer att känna till sådan användning är hög.[11] Därtill har dessa uppgifter tidigare lagrats i separata system som inte kommunicerat med varandra. De senaste årens utveckling har dock medfört en starkare sammankoppling av databaser och mer långtgående åtkomsträttigheter för olika brottsbekämpande myndigheter.

Genom upprättandet av en rättslig ram för interoperabilitet mellan EU:s befintliga och framtida storskaliga informationssystem inom området med frihet, säkerhet och rättvisa har man ansett målet med ett stärkt informationsutbyte och således även en stärkt gränsförvaltning uppfyllas. I och med antagandet av Europaparlamentets och rådets förordning (EU) 2019/817 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området gränser och viseringar, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 och (EU) 2018/1861 samt rådets beslut 2004/512/EG och 2008/633/RIF,[12] och antagandet av Europaparlamentets

[8] Enligt Internationella Migrationsorganisationen (IOM) inbegriper irreguljär migration ett brett spektrum av människor med skiftande rättslig ställning. Termen omfattar sådan mänsklig mobilitet som sker utanför lagar och författningar eller i internationella avtal reglerad gränsöverträdelse. Se IOM:s hemsida, illgänglig på: https://www.iom.int/key-migration-terms#Irregular-migration.

[9] EU-medborgare registreras huvudsakligen i nationella databaser och EU:s system inom området med frihet säkerhet och rättvisa täcker endast några specifika kategorier av EU-medborgare, bl.a. individer med dubbelt medborgarskap och EU-medborgare som blivit dömda eller misstänks för brott.

[10] Se bl.a. Liu 2011, ss. 29–31 samt Muller 2010, ss. 16–17.

[11] Brouwer 2011, s. 282.

[12] Europaparlamentets och rådets förordning (EU) 2019/817 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området gränser och viseringar, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU)

och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt samarbete, asyl och migration och om ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816[13] har laggrunden för detta informationsutbyte etablerats. Artiklarnas numrering liksom deras innehåll är huvudsakligen densamma i båda förordningarna. I avhandlingen hänvisas därför till båda förordningarna, såvida inget annat anges, när en specifik artikel nämns.[14]

Förordningarna trädde i kraft den 11 juni 2019. Det tekniska arbetet har ålagts eu-LISA,[15] och förväntas vara klart i slutet av år 2023.[16] Det enklare informationsutbytet har uppgetts bidra till att förbättra säkerheten inom unionen samt effektivisera kontrollen av gränser och bekämpa olaglig migration.[17] Förordningarna kan bidra till att ge behöriga användare som poliser, migrationstjänstemän och gränsbevakare snabbare och smidigare tillgång till information. Detta har setts som en möjlighet att förbättra effektiviteten i kampen mot allvarlig brottslighet, inklusive terrorism, och ramverket innebär i detta syfte ett värdefullt verktyg för de behöriga myndigheterna. Samtidigt som uppfyllandet av dessa brottsbekämpande mål är viktigt för unionens säkerhet måste regleringen respektera individers grundläggande rättigheter. På grund av de underliggande målen med interoperabilitet – att ge enklare och snabbare tillgång till information om tredjelandsmedborgare – innebär förordningarna utmaningar kopplade till rätten till privatliv i artikel 7 i EU:s stadga om grundläggande rättigheter (stadgan) och skyddet av

2018/1240, (EU) 2018/1726 och (EU) 2018/1861 samt rådets beslut 2004/512/EG och 2008/633/RIF. EUT 2019/L 135/27–84.

[13] Europaparlamentets och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt samarbete, asyl och migration och om ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816. EUT 2019/L 135/85–135.

[14] Innehållsmässigt består förordningarna av samma bestämmelser men eftersom medlemsstaterna deltar i samarbetet på olika nivåer och på grund av de olika rättsgrunderna för samarbetet inom sektorerna har förordningarna hållits åtskilda. Förordningarna har gemensamma rättsliga grunder i artiklarna 16(2) och 74 FEUF. Förordning 2019/817 bygger dessutom på artikel 77(2)(a), (b), (d) och (e) medan förordning 2019/818 bygger på artikel 78(2)(e), artikel 79(2)(c), artikel 82(1)(d), artikel 85(1), artikel 87(2)(a) och artikel 88(2). Se Europaparlamentet 2019, s. 12.

[15] Den Europeiska byrån för den operativa förvaltningen av stora it-system inom området med frihet, säkerhet och rättvisa.

[16] Hemsidan för eu-LISA, tillgänglig på: https://www.eulisa.europa.eu/Newsroom/News/Pages/Gaps-closed-between-information-systems-for-security-borders-and-migration-management.aspx.

[17] Förordning 2019/817 och 2019/818, skäl 9–10.

personuppgifter i artikel 8 i stadgan.[18] Från lagstiftares synvinkel har det funnits en stark vilja och agenda att presentera interoperabilitet som enbart en teknisk lösning med kompletterande komponenter framom ett politiskt ställningstagande med långtgående samhälleliga verkningar.[19] Detta förhållningssätt kopplar explicit bort de politiska och juridiska dimensionerna från interoperabilitetsbegreppet och förutsätter att de tekniska aspekterna är helt neutrala.[20] I själva verket är den tekniska utvecklingen varken oundviklig eller neutral, vilket också är fallet för interoperabilitet. Teknologi är sammanvävd med olika faktorer, bl.a. kulturella värderingar, rättslig reglering, beslut och konflikter och medför att teknologi i sig själv inte kan betraktas som isolerade frågor.[21] Avseende interoperabilitet innebär detta att teknisk framgång inte kan vara avgörande för antagandet av ny reglering, då det enbart representerar en av de många dimensionerna i frågan, parallellt med dess sociala, kulturella, juridiska, organisatoriska och semantiska dimensioner.[22] Teknik bör alltid tillkomma till stöd för policyer och legitima behov, inte tvärtom. Det som är tekniskt genomförbart behöver inte nödvändigtvis stå i linje med vad som är rättsligt motiverat eller etiskt önskvärt.[23] Således är ett förhållningssätt där ändamålet helgar medlen inte gångbart.

Faktum är att interoperabla informationssystem utmanar grundläggande data-skyddsprinciper och omdefinierar aktörers roller inom området med frihet, säkerhet och rättvisa. Därmed har interoperabiliteten inte enbart en djupgående och permanent inverkan på hur informationssystemens struktur och deras sätt att fungera ändras, utan systemet medför en förändring i sättet på vilket rättsliga principer inom området hittills har tolkats.[24] Europeiska datatillsynsmannen har kallat detta för en ”punkt utan återvändo”.[25]

1.2 Frågeställning och avgränsning

[18] Europeiska unionens stadga om de grundläggande rättigheterna av den 26 oktober 2012/C 326/02. EUT 2012/C 326/391–407.
[19] EDPS 2018 (b), skäl 30.
[20] de Hert & Gutwirth 2006, s. 23.
[21] de Hert & Gutwirth 2006, s. 23.
[22] de Hert & Gutwirth 2006, s. 23.
[23] EDPS 2017 (c), skäl 20.
[24] Se EDPS 2018 (b), skäl 25, 143.
[25] EDPS 2018 (b), skäl 25.

Sedan slutet av 1970-talet och parallellt med den teknologiska utvecklingen kan en tendens att revidera databaser inom EU:s område för frihet, säkerhet och rättvisa observeras.[26] Motiveringen har ofta angetts vara en högre grad av effektivitet, med följden att de berörda databaserna för varje revidering blivit allt mer inskränkande i förhållande till grundläggande friheter och rättigheter.[27] Genom ikraftträdandet av Lissabonfördraget fick grundläggande rättigheter en förstärkt ställning inom EU, och stadgan tillskrivs med stöd av artikel 6 FEU samma rättsliga värde som unionens fördrag. Tillämpningsområdet avgränsas genom stadgans artikel 51(1) som föreskriver att regleringen riktar sig till ”unionens institutioner, organ och byråer samt till medlemsstaterna endast när dessa tillämpar unionsrätten”. Rätten till privatliv i stadgans artikel 7 och dataskydd i artikel 8 tillsammans med rätten till privatliv i artikel 8 i Europeiska konventionen om mänskliga rättigheter anger villkoren under vilka personuppgifter får behandlas.[28] Är interoperabilitetsramverket förenligt med regleringen i dessa normer?

Rätten till dataskydd regleras mer specifikt i EU:s sekundärrätt. I det tidigare fragmenterade ramverket var reglerna fördelade mellan EU:s dataskyddsdirektiv[29] och ett lapptäcke av instrument tillämpliga på behandlingen av personuppgifter inom området för polisiärt och rättsligt samarbete, däribland rådets rambeslut från år 2008.[30] Dataskyddsdirektivet ersattes i maj 2018 av den allmänna dataskyddsförordningen (*General Data Protection Regulation*, GDPR) och samma år började även polisdirektivet för skydd av personuppgifter då sådana uppgifter används av brottsbekämpande myndigheter tillämpas, vilket ersätter det tidigare rambeslutet från år 2008. Förhållandet mellan förordningen och direktivet samt dess konsekvenser för de skyddsåtgärder som beviljas individer är ett centralt tema för avhandlingen. I båda rättsakterna uttrycks principen om ändamålsbegräsning som utgör en av dataskyddets centrala principer. Kravet på ändamålsbegränsning fungerar bl.a. som en skyddsåtgärd för individens rättigheter och det blir därmed väsentligt att besvara frågan huruvida tolkningen av

[26] Bunyan 2018, s. 14.
[27] Bunyan 2018, s. 2.
[28] Europeiska konventionen om skydd för de mänskliga rättigheterna, ändrad genom protokoll nr 11 och 14, November 1950, ETS 5.
[29] 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. EGT 1995/L 281/31-50.
[30] Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete. EUT 2008/L 350/60-71.

principen skiljer sig åt i de olika rättsakterna. Hur inverkar detta i så fall på de registrerades rättigheter? Avhandlingen fokuserar på behöriga brottsbekämpande myndigheters åtkomst till personuppgifter i de interoperabla databaserna och syftar till att besvara hur ändamålsbegränsning tolkas i denna specifika kontext. I avhandlingen ställs frågan hur dataskyddsförordningen och polisdirektivet förhåller sig till behandling av personuppgifter som samlats in under ett icke brottsbekämpande sammanhang men senare överförs till behandling i ett brottsbekämpande sammanhang. Innebär skiftet till interoperabla databaser i verkligheten en form av ny obehörig åtkomst och därmed en risk för maktmissbruk? Medför interoperabilitet i själva verket ett skifte i hur ändamålsbegränsning överhuvudtaget ska tolkas? I texten undersöks vad som avses med brottsbekämpande myndigheter och deras befogenheter. Hur skiljer sig denna definition åt mellan de olika medlemsländerna samt på vilket sätt påverkar detta skyddet av personuppgifter?

Eftersom Europeiska unionens domstol (EU-domstolen) övervakar efterlevnaden av grundläggande rättigheter i unionen, beror frågan huruvida lagstiftningen om interoperabilitet står i överensstämmelse med skyddet av personupgifter i slutändan på EU-domstolens bedömning. Dessutom bör lagstiftningen vara förenlig med den praxis om skyddet av privatliv som utvecklats av Europeiska människorättsdomstolen (Europadomstolen) med utgångspunkt i Europeiska människorättskonventionen (Europakonventionen). I avhandlingen ställs därför frågan om interoperabilitets-ramverket uppfyller kraven på proportionalitet och nödvändighet och ifall reglerna kan anses undergräva det väsentliga innehållet i rätten till privatliv och dataskydd. På grund av dataskyddets grundläggande karaktär och typen av känsliga uppgifter som samlas in är det legitimt att även undersöka de skyddsåtgärder som ges till de registrerade vars personuppgifter behandlas av brottsbekämpande myndigheter. Finns det en asymmetri i förhållandet mellan de ökade rättigheter som behöriga myndigheter tilldelas och avsaknaden av ökade rättigheter till information hos de registrerade?

I arbetet undersöks skyddet av personuppgifter i ett EU-rättsligt sammanhang. Internationella regelverk för behandling av personuppgifter, däribland Europarådets

dataskyddskonvention som påverkat utformningen av EU:s dataskyddslagstiftning,[31] behandlas således inte. Avhandlingens huvudsakliga fokus ligger på principen om ändamålsbegränsning och problematiseringen av den utvidgade sekundära åtkomsten till personuppgifter i samband med interoperabla databaser. Revideringen av befintliga databaser och utökade åtkomstmöjligheter till enskilda system som Eurodac, SIS och VIS behandlas enbart kortfattat och utgör inte kärnan för denna avhandlings frågeställning. Således undersöks inte hur långt ändringarna i de ursprungliga ändamålen bakom de berörda databaserna är förenliga med EU-domstolens krav på nödvändighet och proportionalitet, en aspekt som hittills inte behandlats av EU-domstolen. Vidare kommer den ursprungliga behandlingen av uppgifter under dataskyddsförordningens regelverk endast att behandlas ytligt.

Det bör understrykas att interoperabiliteten medför implikationer för flera av de grundläggande rättigheterna. Detta inkluderar bland annat diskrimineringsförbudet. Eftersom interoperabilitetsförordningarna i detta skede nästan uteslutande berör behandlingen av tredjelandsmedborgares personuppgifter riktar sig åtgärderna mot en specifik grupp människor. Speciellt irreguljära migranter utgör en målgrupp för de nya åtgärderna. Även rätten till asyl och internationellt skydd, skyddet av barn och grundläggande dataskyddsprinciper utöver ändamålsbegränsning som lagringstid, datakvalitet m.m. berörs av de nya reglerna. Dessa aspekter kommer på grund av platsbrist dock inte behandlas närmare i denna avhandling.

1.3 Material och metod

Avhandlingens frågeställning tar sin utgångspunkt i en EU-rättslig kontext och stöder sig huvudsakligen på EU-rättsligt material. Till följd av detta används en EU-rättslig tolkningsmetod i arbetet. Forskningsmetoden i avhandlingen är rättsdogmatisk vilket innebär att gällande rätt utreds, systematiseras och tolkas i enlighet med rättskälleläran.[32] EU-rätten utgör en autonom rättsordning med företräde över nationell rätt,[33] bestående av primärrätt, sekundärrätt, allmänna EU-rättsliga principer, rättspraxis från EU-domstolen

[31] Mäkinen 2016, s. 108.
[32] Peczenik 1990, s. 44.
[33] Företrädesprincipen utgör rättspraxis som utvecklats av EU-domstolen och den fastslogs ursprungligen i domstolens dom av den 15 juli 1964, *Flaminio Costa mot E.N.E.L.*, mål 6-64, ECLI:EU:C:1964:66.

samt internationell rätt. Avhandlingen stöder sig på primära rättskällor i form av EU- samt EUF-fördraget, EU-stadgans artikel 7 och 8 samt sekundärrätt i form av dataskyddsförordningen och polisdirektivet. Avhandlingen refererar i viss mån till finsk lagstiftning för att belysa reglering i medlemsstaternas lagstiftning. Därtill stöder sig avhandlingen på icke bindande rättsakter i form av förarbeten,[34] doktrin, riktlinjer och yttranden främst inom området för EU:s dataskydd.

Dataskyddsförordningen och polisdirektivet utgör båda viktiga utgångspunkter för analysen i avhandlingen. Bägge regelverken är bindande rättsakter inom sekundärrätten. Speciell vikt läggs vid principen om ändamålsbegränsning, en av dataskydds-bestämmelsernas grundprinciper, som fastställs i respektive regelverk. Förordningarna om interoperabilitet analyseras mot bakgrund av dessa rättskällor. Utöver lagstiftning utgör EU-domstolens och Europadomstolens rättspraxis en viktig rättskälla. I de fall sekundärrätten lämnar luckor i hur rättsläget bör tolkas blir utvecklingen av EU-rätten och dess enhetliga tillämpning avhängig av EU-domstolens avgöranden. EU-domstolen förlitar sig på en teleologisk tolkningsmetod med fokus på ändamålen vid utformningen av en rättsregel.[35] Arbetet bygger på domstolarnas praxis kopplad till behandling av personuppgifter, nödvändighets- och proportionalitetstest samt lagring av uppgifter och åtkomstmöjligheter för brottsbekämpande ändamål. Speciellt EU-domstolens avgöranden i fallen *Digital Rights Ireland* och *Tele2 Sverige* är av stor betydelse för utformningen av allmänna principer för brottsbekämpande myndigheters åtkomstmöjligheter. Eftersom interoperabilitet mellan de berörda databaserna utgör ett nytt och därmed tämligen outforskat område blir dessa principer vägledande för analysen. Monografier och artiklar används för att belysa centrala begrepp och ge läsaren en överblick över det tematiska området. I avhandlingen används både tryckt material och internetkällor.

Meddelanden från kommissionen som utgör icke-bindande rättsakter inom EU:s sekundärrätt utgör en viktig riktlinje för utvecklingen av området för frihet, säkerhet och rättvisa. Också den europeiska datatillsynsmannens yttranden har stor betydelse för

[34] Det bör påpekas att förarbeten inte tillskrivs samma rättskällevärde inom unionsrätten som inom den nordiska rättskälleläran.
[35] Saurugger & Fabien 2017, s. 119.

avhandlingen. Datatillsynsmannen har som uppgift att rådgiva EU:s institutioner och organ om aspekter rörande behandlingen av personuppgifter och därtill hörande lagstiftning, och utvärderar hur dessa uppfyller reglerna för uppgiftsskydd**.** I analyssyfte hänvisas även till artikel 29-arbetsgruppens (WP29) yttranden. Gruppen utgjorde en oberoende arbetsgrupp och behandlade frågor om integritetsskydd och skydd av personuppgifter fram till införandet av den allmänna dataskyddsförordningen i maj 2018. WP29 medverkade genom sitt arbete till en enhetlig tillämpning av personuppgiftsskyddet och har avgett flera yttranden och rekommendationer relaterade till dataskydd, också inom området för biometriska uppgifter och biometrisk teknologi. Både arbetsgruppen och datatillsynsmannen har avgett yttranden om de nya interoperabilitetsförordningarna. Även om karaktären av dessa dokument enbart är vägledande i form av s.k. *soft law* och därmed inte förpliktigar till åtgärder så har gruppen fått ett betydande inflytande.[36] Gruppen efterträddes av Europeiska dataskyddsstyrelsen (*European Data Protection Board*, EDPB), som består av Europeiska datatillsynsmannen samt en representant för datatillsynsmyndigheten i varje medlemsland. EDPB har godkänt utvalda dokument och handlingar av WP29 relaterade till GDPR.[37]

1.4 Disposition

Avhandlingen består av sju kapitel, vilket inkluderar en introduktion och en sammanfattning. Det andra kapitlet inleds med att presentera interoperabilitetsramverket inom EU:s område för frihet, säkerhet och rättvisa. I kapitlet diskuteras kort innebörden av interoperabiliteten mellan EU:s informationssystem och kapitlet introducerar de nya komponenter som möjliggör funktionen. Kapitlet behandlar såväl de existerande databaserna som databaser fortfarande under utveckling som berörs av de nya förordningarna. I det tredje kapitlet presenteras skyddet av personuppgifter som en grundläggande rättighet och analyseras utgående från artikel 16 FEUF, rätten till privatliv i artikel 8 i Europakonventionen samt rätten till privatliv i artikel 7 och rätten till dataskydd i artikel 8 i stadgan. Förhållandet mellan dessa rättigheter undersöks och personuppgiftsskyddets tillämpningsområde analyseras. I kapitlet presenteras EU:s sekundärlagstiftning där individers dataskydd regleras mer detaljerat. Först behandlas den

[36] Bygrave 2014, s. 174.
[37] Se EDPB 2018.

allmänna dataskyddsförordningen i from av *lex generalis*-reglering vid skyddet av personuppgifter, varefter polisdirektivet i form av *lex specialis*-reglering vid brottsbekämpande myndigheters behandling av personuppgifter presenteras. Fokus ligger på de aspekter som är av vikt för den senare analysen. Därtill presenteras EU:s normhierarki och förhållandet mellan direktiv och förordning som lagstiftningsdokument. I slutet av kapitlet analyseras balansen mellan rätten till privatliv och behovet av offentlig säkerhet. I anslutning till detta presenteras EU-domstolens samt Europadomstolen rättspraxis i frågan. Den rättspraxis som behandlas i avhandlingen fokuserar specifikt på situationer som berör brottsbekämpande myndigheters åtkomst till personuppgifter för att på så sätt staka ut allmänna principer inom detta område för dataskydd.

Det fjärde kapitlet behandlar principen om ändamålsbegränsning, fastställd i GDPR artikel 5(1)(b) och artikel 4(1)(b) i polisdirektivet, som en del av dataskyddet. Principens två element bestående av: (1) ändamålsspecifikation och (2) kompatibilitet behandlas separat. Ändamålsbegränsning och dess koppling till rättsstatsprincipen analyseras ytterligare. Därefter sker ett skifte i fokus till hur principen tar sig uttryck specifikt i brottsbekämpande sammanhang. I kapitel fem diskuteras allmänna trender inom brottsbekämpande myndigheters verksamhet och i kapitlet undersöks huruvida denna utveckling har lett till försvagandet av principen om ändamålsbegränsning. Detta inkluderar benägenheten att förena migrationshantering och säkerhetsändamål, skiftet mot ett centraliserat system och utvecklingen av ny teknologi samt olika sammankopplade aktörer inom området. I kapitel sex analyseras de nya förordningarna mot bakgrund av principen om ändamålsbegränsning som fastställts i kapitel fyra och relevant rättspraxis av Europadomstolen och EU-domstolen som diskuterats i kapitel tre. Asymmetrin mellan behöriga myndigheters åtkomsträttigheter och avsaknaden av information hos de registrerade analyseras ytterligare. Kapitlet undersöker ifall interoperabilitetsramverket kan anses utgöra en kränkning av individens dataskydd och utgör tyngdpunkten för avhandlingens analys tillsammans med tolkningen av ändamålsbegränsning i kapitel fyra. Slutligen kommer slutsatserna att sammanfattas, och förordningarnas effekt på grundläggande rättigheter fastställas.

2 INTEROPERABILITET INOM OMRÅDET MED FRIHET, SÄKERHET OCH RÄTTVISA

2.1 Interoperabla informationssystem

Ramverkets interoperabilitetsbegrepp syftar på informationssystems förmåga att sinsemellan utbyta och använda information på ett koordinerat sätt, utan slutanvändares egna insatser.[38] Genom interoperabilitet uppnås en högre effektivitet och en mer holistisk syn på information genom funktioner som inkluderar datatillgång, dataöverföring och samarbete mellan enheter, oavsett informationens ursprung. Sammankopplade system kan variera i graden av interoperabilitet. Informationssystemen i EU fungerar som verktyg i informationsdelning på olika nivåer och fastställer förfaranden för informationsutbyte både på medlemsstats- och EU-nivå. Till en början fungerade informationsutbytet inom brottsbekämpning på en *ad hoc* basis i form av ömsesidig rättshjälp men har genom utvecklingen av effektivare system för datorbaserat informationsutbyte gått över till mer strukturerade former av nätverk. Det samma gäller i ett brett spektrum av EU:s rättsområden.

Dagens rättsliga arrangemang för informationshantering skapar horisontella interaktioner mellan olika myndigheter i medlemsstaterna och vertikala interaktioner mellan nationella myndigheter och EU-organ.[39] Brottsbekämpning, gränsövervakning och migrationskontroll utgör idag dynamiskt sammankopplade områden inom EU.[40] Samtidigt är de existerande databaserna fragmenterade på grund av olika behov som funnits vid tidpunkten för upprättandet av databaserna samt olika institutionella, rättsliga och politiska strukturer i medlemsländerna.[41] Detta har medfört svårigheter i att effektivt iaktta sammankopplingar mellan olika datauppsättningar.[42] Interoperabiliteten inom området med frihet, säkerhet och rättvisa har därför prioriterats på högsta politiska nivå under de senaste åren.[43] Kommissionen har gått in för att stöda program för att utveckla och främja interoperabilitetslösningar inom hela EU och har uttryckt att interoperabilitet

[38] Se Institute of Electrical and Electronics Engineers 1990, s. 42.
[39] Galli 2019, s. 2.
[40] Meddelande från kommissionen till Europaparlamentet och rådet, ”Starkare och smartare informationssystem för gränser och säkerhet”, COM (2016) 205 final av den 26 april 2016, s. 2.
[41] EDPS 2017 (c), s. 2.
[42] FRA 2017 (b), s. 13.
[43] Se bl.a. kommissionens “Joint declaration on the EU’s legislative priorities for 2018-19” av den 14 december 2017, s. 2.

även borde beaktas vid utarbetningen av rättsakter.[44] En fungerande interoperabilitet, baserad på öppna plattformar och standarder, är av väsentlig betydelse för verkställandet av EU:s digitala agenda.[45]

Behovet att förbättra unionens uppgiftshanteringsstruktur för gränsförvaltning och säkerhet ledde till att kommissionen till följd av sitt meddelande ”Starkare och smartare informationssystem för gränser och säkerhet” i maj 2016 utnämnde en expertgrupp för utvecklande av informationssystem och interoperabilitet.[46] Arbetsgruppens huvuduppgift var att analysera de rättsliga, tekniska och operativa aspekterna i olika alternativ till interoperabilitet mellan informationssystemen inom området. En slutrapport utarbetades där expertgruppen granskade fyra alternativ för att uppnå detta mål. Mekanismerna bestod av en europeisk sökportal (ESP), en gemensam biometrisk matchningstjänst (BMS), en gemensam databas för identitetsuppgifter (CIR) samt en detektor för multipla identiteter (MID) som genom de ikraftträdda förordningarna inrättades som interoperabilitetskomponenter.[47] Dessa system förlitar sig till stor del på biometriska uppgifter, bl.a. fingeravtryck och ansiktsbilder, då de bearbetar data.[48] Biometriska kännetecken fungerar som en länk mellan individer och den lagrade informationen. Eftersom biometriska uppgifter är unika för varje person anses de vara den mest pålitliga källan med hänsyn till att identifiera en individ.[49] I själva verket är användningen av människokroppen för identifikation i sig inte ny, t.ex. har primitiva former av fingeravtryck sedan lång tid tillbaka använts för att identifiera och registrera individer för administrativa ändamål.[50]

---

[44] Se bl.a. meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt regionkommittén, ”Europeiska interoperabilitetsramen – genomförandestrategi”, COM (2017) 134 final av den 23 mars 2017 och meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt regionkommittén, “En digital agenda för Europa“, COM (2010) 245 final av den 19 maj 2010 och meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt regionkommittén, ”En EU-strategi för data”, COM(2020) 66 final av den 19 februari 2020.

[45] Se COM (2020) 66 final av den 19 februari 2020 och kommissionens kommunikation ” Shaping Europe’s digital future” av den 19 februari 2020.

[46] Kommissionens beslut om inrättande av en expertgrupp för informationssystem och interoperabilitet COM (2016) C 257/03 av den 17 juni 2016.

[47] Förordning 2019/817 och 2019/818, skäl 9.

[48] Exempel på biometriska kännetecken utgörs av fingeravtryck, näthinnemönster, irisigenkänning, ansiktsstruktur, röst, m.fl. Se FRA 2017 (b), s. 20.

[49] FRA 2017 (b), s. 20.

[50] Cole 2001 se van der Ploeg 2009, s. 85.

Statliga arrangemang för identifiering av individer har blivit viktiga styrmedel i demokratier och människor kan knappt leva sina dagliga liv utan ständiga krav på fastställande av identitet. Identifikation av tredjelandsmedborgare och införandet av dem i register är emellertid viktigt inte bara för upptäckande av irreguljär migration och situationer kopplade till olika former av exploatering och kriminalitet. Registrering av individer som tillhör utsatta grupper såsom flyktingar och asylsökande är ett viktigt verktyg eftersom det även kan säkerställa dessa individer tillgång till skydd i Europa och tillgång till grundläggande rättigheter. I själva verket existerar det en hel del individer i utvecklingsländer och krigszoner som aldrig blivit införda i någon folkbokföring och som således inte ”existerar” i samhället i dess juridiska betydelse och förblir osynliga inför lagen.[51] Sådana individer är mycket benägna att utsättas för olika former av exkludering i samhället och begränsningar av grundläggande rättigheter och friheter. Detta förhållningssätt inramar i hög grad juridisk identitet och registreringen av personer genom biometriska uppgifter i de olika databaserna som en fråga om mänskliga rättigheter, vilket skapar en stark koppling till var och ens rätt att överallt erkännas som en person i lagens mening, som fastställs i artikel 6 i FN:s människorättsförklaring och som upprepas i vissa andra människorättskonventioner, bl.a. artikel 16 i konventionen om medborgerliga och politiska rättigheter. Det kan alltså hända att registreringen i de europeiska databaserna är första gången en person erkänns juridiskt som en fysisk person med rättskapacitet.

Systemen som omfattas av interoperabilitetsförordningarna är de i nuläget verksamma databaserna Schengens informationssystem (SIS II, även känt som SIS), Informationssystemet för viseringar (VIS) samt Eurodac. I framtiden kommer dessa system kompletteras med in- och utresesystemet (EES), EU-systemet för reseuppgifter och resetillstånd (ETIAS) samt det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister avseende tredjelandsmedborgare (Ecris-TCN).[52] Interoperabiliteten innefattar även till viss del Europoluppgifter samt Interpols databaser. I denna kategori ingår Interpols databas över stulna och försvunna handlingar (*Stolen and Lost Travel Documents*, SLTD), Interpols databas för resehandlingar som är föremål för ett meddelande (*Travel Documents Associated with Notices*, TDAWN) och

[51] van der Ploeg 2009, s. 90.
[52] Se förordning 2019/817 och 2019/818, skäl 11.

Europoluppgifter, i den mån de är relevant för ETIAS.[53] Expertgruppen och kommissionen har även diskuterat möjligheten att i framtiden utvidga ramverket att inkludera ytterligare databaser och planer på att sammankoppla tullens egna informationssystem har framförts.[54] EU:s avancerade tullinformationssystem (ICS2) utvecklas för närvarande och en fasinföring är tänkt att ersätta det befintliga systemet ICS från år 2021.[55] Kommissionens expertgrupp föreslog till en början en integrering av tullens informationssystem i interoperabilitetsramverket.[56] I sin slutrapport rekommenderade expertgruppen att kommissionen genomför en genomförbarhetsstudie för att ytterligare undersöka de tekniska, juridiska och operativa aspekterna av interoperabilitet med tullsystemen.[57] Enligt expertgruppen bör interoperabilitet övervägas mellan SIS, Europoluppgifter och ICS2, med beaktande av att det senare ännu håller på att utvecklas.[58] Målet med interoperabilitet mellan tullsystemenen och övriga interoperabla system är således att bidra till att eliminera blinda fläckar och att hjälpa tullmyndigheter och andra brottsbekämpande myndigheter att förebygga säkerhetsrisker kopplade till varor och personer som rör sig över EU:s yttre gränser.[59] Förutsatt att nödvändigheten att inkludera systemen bevisas kan även vissa andra decentraliserade system, som de som drivs under Prümavtalet, PNR-direktivet och API-direktivet i ett senare skede kopplas till en eller flera av komponenterna.[60]

2.2 Från fysiska till digitala och biometriska gränser

Ökad insamling av personuppgifter tillhörande olika kategorier av tredjelandsmedborgare som överskrider unionens yttre gränser utgör en allmän utvecklingsriktning inom EU. Ett flertal storskaliga informationssystem har med tiden skapats för hantering av

[53] Se förordning 2019/817 och 2019/818, skäl 12, 15.
[54] Tullmyndigheterna omfattas av förordningarnas tillämpningsområde då de i egenskap av behöriga användare behandlar personuppgifter i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott.
[55] Se kommissionens hemsida (b), tillgänglig på: https://ec.europa.eu/taxation_customs/general-information-customs/customs-security/ics2_en.
[56] Slutrapport av expertgruppen för informationssystem och interoperabilitet ST 8434/1/17 REV 1 av den 15 Maj 2017, ss. 38–39.
[57] ST 8434/1/17 REV 1, ss. 38–39.
[58] ST 8434/1/17 REV 1, ss. 38–39.
[59] ST 8434/1/17 REV 1, ss. 38–39.
[60] Förslag till Europaparlamentets och rådets förordning om inrättande av en ram för interoperabilitet mellan EU-informationssystem (polissamarbete och rättsligt samarbete, asyl och migration), COM (2017) 794 final av den 12 December 2017. Se också Statewatch, "Automating the exchange of police data: Council looks to national databases", tillgänglig på: http://statewatch.org/news/2019/sep/eu-interop-national.htm.

gemensamma asyl-, migrations- och säkerhetsfrågor. Storskaliga informationssystem inom unionen kännetecknas bland annat av det stora antalet användare som har tillgång till systemen, mängden data som samlas in, lagras och kan tillträdas av användare samt antalet kopplingar som existerar mellan komponenterna.[61] Systemen inom området med frihet, säkerhet och rättvisa är antingen verksamma inom ramen för (1) gränskontroll i förhållande till EU-medborgare och tredjelandsmedborgare eller (2) brottsbekämpning.[62]

Inrättandet av de olika systemen är starkt sammankopplat med den grundläggande principen om fri rörlighet samt skapandet av en union utan inre gränser,[63] och kompenserar således för det faktum att gränserna inom Schengenområdet är öppna.[64] Av dessa system var SIS det första storskaliga informationssystemet inom EU som inrättades för att upprätthålla den inre säkerheten i avsaknad av inre gränskontroller.[65] Informationssystemet är den största och mest använda plattformen för informationsutbyte för migrations- och brottsbekämpningsändamål, och hjälper nationella brottsbekämpnings- och förvaltningsmyndigheter att skydda Schengenområdet, bekämpa brottslighet och lokalisera saknade personer.[66] Behöriga myndigheter med ansvar för områdets yttre och inre säkerhet, som gränsövervakare, poliser, tullmyndigheter och domstolsväsendet, har genom systemet åtkomst till uppgifter för att förhindra utvisade eller avvisade tredjelandsmedborgare från att tillträda området.[67] Genom SIS koordineras

[61] EDPS hemsida, tillgänglig på: https://edps.europa.eu/press-publications/press-news/press-releases/2018/edps-calls-wider-debate-future-information-sharing_en.
[62] Tomaszycki 2019, s. 197.
[63] Se artikel 3(2) FEU, artikel 21 FEUF, avdelning IV och V FEUF och artikel 45 i Europeiska unionens stadga om de grundläggande rättigheterna.
[64] Schengensamarbetet regleras genom Schengenregelverket, en konvention antagen utanför ramarna för Europeiska gemenskaperna innan dess införlivande genom Amsterdamfördraget den 1 maj 1999. Per definition är Schengenområdet ett område med 26 EU-länder som delar gemensamma gränskontroller och där människor rör sig utan systematisk kontroll. Visum utfärdade av dessa stater är giltiga över hela territoriet. Se Schengenregelverket - Konvention om tillämpning av Schengenavtalet av den 14 juni 1985 mellan regeringarna i Beneluxstaterna, Förbundsrepubliken Tyskland och Franska republiken om gradvis avskaffande av kontroller vid de gemensamma gränserna. EGT 2000/L 239/19–62.
[65] Tillämpningsområdet för SIS definieras i följande rättsakter: Europaparlamentets och rådets förordning (EG) nr 1987/2006 av den 20 december 2006 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II). EUT 2006/L 381/4–23; rådets beslut 2007/533/RIF av den 12 juni 2007 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II). EUT 2007/L 205/63–84; Europaparlamentets och rådets förordning (EG) nr 1986/2006 av den 20 december 2006 om tillträde till andra generationen av Schengens informationssystem (SIS II) för de enheter i medlemsstaterna som ansvarar för att utfärda registreringsbevis för fordon. EUT 2006/L 381/ 1–3.
[66] Vavoula 2019, ss. 4–5.
[67] Kommissionens hemsida (a), tillgänglig på:

även efterspanandet av särskilda personer och föremål i brottsbekämpningssyfte och systemet innehåller en mängd olika möjligheter att utfärda registrerade varningar. Detta återspeglar systemets övergripande syfte att säkerställa en hög säkerhetsnivå inom Schengenområdet genom att underlätta arbetet inom både gränskontroll och polisutredningar.[68] Genom den senaste revideringen av SIS infördes flera nya funktioner i regelverket i form av nya registreringskategorier, typer av uppgifter och åtkomstmöjligheter. Dels innebär revideringen en ökad användning av biometriska uppgifter inklusive finger- och handavtryck samt ansiktsbilder och DNA, dels ökade åtkomstmöjligheter till uppgifter för EU:s byråer, bl.a. Europol.[69]

Schengenländernas gemensamma informationssystem för viseringar (VIS) stöder implementeringen av EU:s gemensamma visumpolitik och bearbetningen av data samt beslut kopplade till ansökningar om korttidsvisa för tredjelandsmedborgare inom Schengenområdet.[70] I VIS lagras ansökningsuppgifterna för visumsökande till EU:s centraliserade visumsystem. En del av ansökningsuppgifterna såväl som sökandes biometriska uppgifter överförs från det nationella VIS-systemet i varje medlemsstat till systemet på unionsnivå.[71] Även om det huvudsakliga ändamålet med VIS är att främja implementeringen av den gemensamma visumpolitiken har mekanismen också andra syften, bl.a. bekämpandet av bedrägeri, visa shopping samt att bidra till förhindrandet av hot mot medlemsstaternas inre säkerhet.[72]

Eurodac utvecklades först som ett renodlat instrument för hanteringen av asylansökningar.[73] Databasen utgör ett centraliserat register för bearbetning av

https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en.

[68] Vavoula 2019, s. 5.

[69] Vavoula 2019, s. 9.

[70] Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen). EUT 2008/L 218/60–81.

[71] Förordning 767/2008, skäl 7 samt artikel 28.

[72] Förordning 767/2008, skäl 5 samt artikel 2.

[73] Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (omarbetning) EUT 2013/L 180/1–30.

asylsökandes fingeravtryck i enlighet med de gemensamma Dublinreglerna om fastställande av vilken medlemsstat som är ansvarig för att behandla en asylansökan.[74] Genom att jämföra de lagrade fingeravtrycksuppgifterna är det möjligt att kontrollera om en asylsökande eller en tredjelandsmedborgare som vistas olagligt i ett EU-land redan har lämnat in en ansökan i en annan medlemsstat eller om en asylsökande har tillträtt EU irreguljärt. Ett pragmatiskt exempel på hur gränserna mellan migrations- och brottsbekämpningsdatabaser suddats ut är den gradvisa omställningen av Eurodac till ett verktyg i kampen mot terrorism och allvarlig brottslighet. Den reviderade Eurodacförordningen som antogs år 2013 öppnade bl.a. upp databasen för brottsbekämpande myndigheter och Europol.[75]

En ytterligare revidering av regelverken för både Eurodac och VIS är för närvarande under förhandling. Eurodac berörs av en utökad användning av biometriska uppgifter och registreringskategorierna kommer i framtiden att inkludera även tredjelandsmedborgare som vistas på EU:s område eller har passerat EU:s yttre gränser med oregelbunden status.[76] VIS kommer att förnyas för att adressera behovet att inkludera även uppgifter om innehavare av uppehållstillstånd, uppehållskort och långtidsvisum.[77] Parallellt med utvecklingen av interoperabilitetsramverket har helt nya system tagits fram, som in- och utresesystemet (EES),[78] och systemet för reseuppgifter och resetillstånd (ETIAS).[79] Medan EES berör in- och utresor av så gott som alla tredjelandsmedborgare fokuserar ETIAS på kontrollen av förhandsuppgifter för visafria tredjelandsmedborgare. EES fungerar alltså som en kontroll vid unionens gränser medan ETIAS möjliggör en extraterritoriell gränskontroll. Denna sammanslagning av olika ändamål återspeglas nu i

[74] Förordning 603/2013, skäl 13.
[75] Vavoula 2019, s. 10.
[76] Vavoula 2019, s. 15.
[77] Vavoula 2019, s. 16.
[78] Europaparlamentets och rådets förordning (EU) 2017/2226 av den 30 november 2017 om inrättande av ett in- och utresesystem för registrering av in- och utreseuppgifter och av uppgifter om nekad inresa för tredjelandsmedborgare som passerar medlemsstaternas yttre gränser, om fastställande av villkoren för åtkomst till in- och utresesystemet för brottsbekämpande ändamål och om ändring av konventionen om tillämpning av Schengenavtalet och förordningarna (EG) nr 767/2008 och (EU) nr 1077/2011. EUT 2017/L 327/20–82.
[79] Europaparlamentets och rådets förordning (EU) 2018/1240 av den 12 september 2018 om inrättande av ett EU-system för reseuppgifter och resetillstånd (Etias) och om ändring av förordningarna (EU) nr 1077/2011, (EU) nr 515/2014, (EU) 2016/399, (EU) 2016/1624 och (EU) 2017/2226. EUT 2018/L 236/1–71.

en sammankoppling av informationssystem som har skapats vid olika tidpunkter och för olika ändamål, men som idag förenas under en gemensam säkerhetsagenda.[80]

2.3 Interoperabilitetskomponenter

Grunden för interoperabiliteten mellan informationssystemen utgörs av den Europeiska sökportalen (ESP). Komponenten består av en central infrastruktur som säkrar kommunikationskanaler mellan sökportalen, nationella myndigheter och EU-organ samt alla relevanta databaser som ingår i systemet. Detta innebär att en slutanvändare genom en sökning i portalen får tillgång till de kombinerade resultaten från de olika systemen, det vill säga in- och utresesystemet, VIS, Etias, Eurodac, SIS och Ecris-TCN, samt Europoluppgifter och Interpols databaser, på en och samma skärm.[81] ESP möjliggör sökning av såväl biografisk som biometrisk data samtidigt. Sökportalen varken samlar eller bearbetar ny eller gammal data utan förmedlar enbart uppgifter som redan existerar i de bakomliggande databaserna. Ändamålet med ESP är ”att underlätta medlemsstaternas myndigheters och unionsbyråernas möjligheter att få snabb, kontinuerlig, effektiv, systematisk och kontrollerad åtkomst till EU-informationssystemen, Europoluppgifter och Interpols databaser som krävs för att de ska kunna utföra sina uppgifter i enlighet med sina åtkomsträttigheter”.[82] I förordningarna fastställs att ESP och de uppgifter som genom portalen tillhandahålls enbart får användas för de uttryckliga syften som har fastställts i den rättsliga grund som reglerar respektive databas.[83] Möjligheten att utföra sökningar i ett flertal databaser som ESP som brottsbekämpningsverktyg medför har väckt frågor ifall detta på längre sikt kan leda till att ytterligare utvidga befintliga användarrättigheter och ge myndigheter tillstånd att konsultera ett större antal databaser i framtiden.[84] Det har även ifrågasatts ifall införandet av ESP kan göra det lättare för myndigheter att missbruka redan befintliga åtkomsträttigheter, till exempel genom att göra förfrågningar på andras vägnar.[85] Regleringen innehåller skyddsåtgärder som är avsedda att förhindra och bestraffa sådant missbruk, men effektiv övervakning och

[80] Smith & LeVoy 2020.
[81] Förordning 2019/817 och 2019/818, artikel 6(2)(a).
[82] Förordning 2019/817 och 2019/818, artikel 6(1).
[83] Förordning 2019/817 och 2019/818, artikel 7(1).
[84] Jones 2019, s. 20.
[85] Jones 2019, s. 20.

verkställighet kommer att kräva noggrann granskning av nationella och europeiska dataskyddsmyndigheter, som måste förses med nödvändiga resurser.[86]

En gemensam biometrisk matchningstjänst (BMS) ger slutanvändare möjligheten att söka och jämföra biometrisk data som inhämtats från de bakomliggande informationssystemen som ingår i CIR och SIS. Syftet med BMS är att stödja funktionen av CIR samt MID och de olika målen i de bakomliggande databaserna.[87] Tidigare har varje centraliserat system använt sig av en egen biometrisk sökportal. Informationen lagras i biometriska mallar och ökar tillförlitligheten för identifiering av en person då man inte enbart förlitar sig på alfanumerisk data.[88] På så vis fungerar BMS som ett tekniskt verktyg för identifieringen av personer som har registrerats under olika identiteter. Det vill säga, medan ansiktsbilder och fingeravtryck behålls i de underliggande systemen kommer mallar som genereras från denna information att överföras till BMS, som kommer att användas för korsmatchning och jämförelse. Medan en mall i sig inte identifiera en individ tillåter den identifiering om dennes biometriska data matchar mallar i BMS som motsvarar data i ett eller flera av de underliggande systemen.

De olika personuppgifterna som registreras i de enskilda databaserna EES, VIS, Etias, Eurodac samt Ecris-TCN kommer i samband med introduktionen av den centraliserade databasen (CIR) ingå i en gemensam databas för identitetsuppgifter. Systemet kommer att innehålla upp till 300 miljoner individers personuppgifter.[89] Databasen innefattar såväl biografisk som biometrisk data. I CIR skapas en personakt för alla personer som registreras i databaserna som CIR har tillgång till.[90] Då en sökning i CIR utförs visas träffar enligt en tvåstegsmetod. Det första steget visar ifall det finns träffar för matchning av data i någon av de kopplade databaserna, så kallade ”flaggade träffar”, medan det senare steget kräver att myndigheter begär full åtkomst till de informationssystem i vilka en träff genererats.[91] ”Det svar som anger att uppgifter om personen i fråga förekommer i något av de EU-informationssystem som avses i punkt 1 får användas endast i syfte att

[86] Det finns alltså nationell lagstiftning som borde motverka dylikt handlande, men den skiljer sig åt mellan olika medlemsstater. För Finlands del, se bestämmelser om dataskyddsbrott i 38:9 § i strafflagen (29/1889).
[87] Förordning 2019/817 och 2019/818, artikel 12(1).
[88] Förordning 2019/817 och 2019/818, artikel 12–13.
[89] Jones 2019, s. 25.
[90] Förordning 2019/817 och 2019/818, artikel 17.
[91] Förordning 2019/817 och 2019/818, artikel 22.

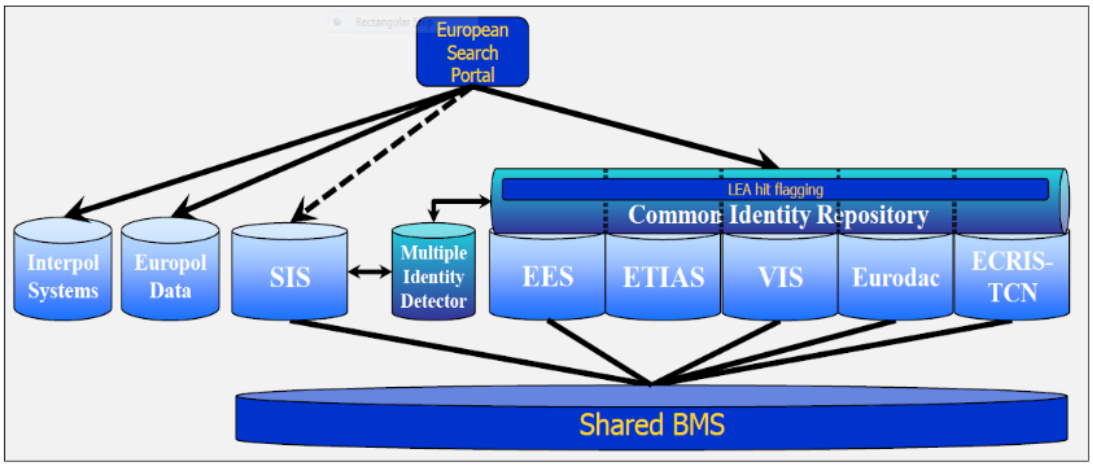
lämna in en begäran om full åtkomst som omfattas av de villkor och förfaranden som fastställs i respektive rättsliga instrument där sådan åtkomst regleras".[92] Detta innebär att informationen som en träff i CIR förmedlar inte får "tolkas eller användas som en grund för en slutsats om eller en anledning att vidta åtgärder med avseende på en person, utan bör användas uteslutande i syfte att lämna in begäran om åtkomst till de underliggande EU-informationssystemen".[93] Förordningarna adresserar dock inte hur det skulle gå att säkerställa att förbudet att dra slutsatser eller vidta åtgärder garanteras i praktiken.

Det första ändamålet bakom CIR är att "underlätta och bistå vid en korrekt identifiering av personer".[94] Artikel 20(1) i förordningarna tillåter sökningar i CIR utförda av polismyndigheter under olika omständigheter. Denna funktion och dess påverkan för dataskyddet analyseras mer djupgående i avhandlingens kapitel 6.1.2. Det andra syftet består av att stödja komponenten MID.[95] Det tredje syftet utgörs av att "underlätta och rationalisera de utsedda myndigheternas och Europols åtkomst [...] om det är nödvändigt för att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott".[96] Behöriga myndigheter samt Europol har rätt ifall det "i ett specifikt fall finns rimliga skäl att anta att en sökning i EU-informationssystem kommer att bidra till att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott, [...] söka i CIR för att få information om huruvida det finns uppgifter om en viss person"[97] i de bakomliggande systemen.

En detektor för multipla identiteter (MID) inrättas med uppgiften att skapa länkar mellan data i de informationssystem som ingår i CIR samt uppgifter från SIS, "med det dubbla syftet att underlätta identitetskontroller och bekämpa identitetsbedrägerier", samt "för att stödja CIR:s funktion" och målen i de bakomliggande databaserna.[98] Beroende på uppgifternas natur delas länkarna in i olika kategorier.[99] MID aktiveras ifall en ny fil skapas eller uppdateras i EES, VIS eller ETIAS, eller då en avisering om en person skapas

[92] Förordning 2019/817 och 2019/818 artikel 22.
[93] Förordning 2019/817 och 2019/818 skäl 33.
[94] Förordning 2019/817 och 2019/818 artikel 17.
[95] Förordning 2019/817 och 2019/818 artikel 17.
[96] Förordning 2019/817 och 2019/818 artikel 17.
[97] Förordning 2019/817 och 2019/818 artikel 22.
[98] Förordning 2019/817 och 2019/818 artikel 25.
[99] Förordning 2019/817 och 2019/818 artikel 30–33.

eller uppdateras i SIS, eller en ny uppgiftspost skapas eller ändras i ECRIS-TCN.[100] MID använder sig av de andra komponenterna för att jämföra biometriska uppgifter samt reseuppgifter mellan de olika EU-databaserna.



Figur 1 Interoperabilitetskomponenterna och de kopplade databaserna (källa: Kommissionen).

Genom interoperabilitetsförordningarna och sammankopplingen av befintliga och nya databaser skapas således tre nya storskaliga databaser i EU bestående av CIR, ESP samt BMS. Sammanlagt berör de nya åtgärderna sex centraliserade system. Det står tydligt att interoperabilitet har blivit ett dynamiskt begrepp inom EU:s olika rättsområden. Samtidigt saknar systemet konsekvens och tydliga indikationer på användningen av de utvecklade mekanismerna. Interoperabilitetsramen omspänner en komplex och fragmenterad arena, som inkluderar en mångfald inblandade aktörer på EU- och nationell nivå. Eftersom lag och teknik sammanflätas på detta sätt, kommer interoperabiliteten innebära utmaningarna med att överföra tekniska lösningar till en fungerande juridisk design.[101] Brottsbekämpande myndigheterna står inför ett flertal rättsliga grunder, kanaler, förfaranden och verktyg för olika kategorier av information, samtidigt som centraliserade databaser ökar risken för missbruk och väcker lättare önskemål om att använda systemen utöver de syften som de ursprungligen var avsedda för.[102]

[100] Förordning 2019/817 och 2019/818, artikel 27.
[101] Catanzariti 2020.
[102] EDPS 2018 (b), skäl 28.

3 SKYDDET AV PERSONUPPGIFTER

3.1 Rätten till privatliv och rätten till dataskydd

Värderingarna demokrati, rättsstatsprincipen och grundläggande rättigheter ligger till grund för EU:s existens. Artikel 2 FEU fastställer att ”unionen ska bygga på värdena respekt för människans värdighet, frihet, demokrati, jämlikhet, rättsstaten och respekt för de mänskliga rättigheterna”. EU:s stadga om de grundläggande rättigheterna inkluderar dessa värderingar.[103] Därmed är rätten till privatliv och rätten till dataskydd, vilka erkänns i artikel 16(1) FEUF och i artikel 7 och 8 i stadgan, som grundläggande rättigheter delar av unionens bredare ambitioner att främja de värden som fastställs i artikel 2 FEU. Respekten för dessa värden är avgörande för att EU:s åtgärder ska anses legitima. Tillsammans skapar de ett område med frihet, säkerhet och rättvisa inom unionen.[104]

Tillämpningsområdet *ratione personae* för skyddet av grundläggande rättigheter i stadgan är brett. Flera av stadgans rättigheter omfattar alla individer, oavsett nationalitet eller tredjelandsmedborgares migrationsstatus, då de berörs av unionslagstiftning. Detta inkluderar även artikel 7 och 8 i stadgan. Skyddet av privatliv och skyddet av personuppgifter är rättigheter som följer av stadgan. I stadgans artikel 51(1) fastställs att ”bestämmelserna i denna stadga riktar sig, med beaktande av subsidiaritetsprincipen, till unionens institutioner, organ och byråer samt till medlemsstaterna endast när dessa tillämpar unionsrätten”. Stadgan är således bara tillämplig för medlemsstater när de genomför EU-lagstiftning och nationella myndigheter är bara skyldiga att följa stadgan då de genomför EU-lagstiftning, t.ex. då de tillämpar EU:s förordningar. För EU:s institutioner och organ är stadgan alltid bindande. På liknande sätt har EU-domstolen enbart behörighet att avge förhandsavgöranden om grundfördragens tolkning samt om tolkningen och giltigheten av sådana rättsakter som utfärdats av någon av unionens institutioner.[105] EU-domstolen har dock utforskat gränserna för denna kompetens och fastställt att även åtgärder som inte direkt tillämpar EU-rätten också kan bli föremål för stadgans reglering.

[103] Ingressen till Europeiska Unionens stadga om de grundläggande rättigheterna.
[104] Ingressen till Europeiska Unionens stadga om de grundläggande rättigheterna.
[105] Artikel 267 FEUF.

Domstolen har i sin praxis valt att ge stadgans tillämpningsområde en extensiv tolkning. Detta illustreras i målen *Åkerberg Fransson*[106] samt *Melloni*.[107] I båda målen var ”tolkningsbehörigheten och följaktligen frågan huruvida tolkningsfrågorna rörande stadgan kunde tas upp till prövning [...] avhängiga av huruvida de aktuella nationella åtgärderna kunde anses utgöra åtgärder för att ”*tillämpa*” unionsrätten.”[108] I *Åkerberg Fransson* ansåg domstolen inte att detta innebar ett skäl att avstå från att granska nationell lagstiftning som inte hade antagits med stöd av bestämmelser i unionsrätten. I domen slog EU-domstolen fast att de nationella åtgärderna som var under prövning vid den nationella domstolen tryggade tillämningen av unionsrätten.[109] Generaladvokat Sharpston sammanfattar detta enligt följande: “Prövningen avser huruvida situationen är en sådan där unionsrätten *är tillämplig* (det vill säga en situation som omfattas av ”unionsrättens *tillämpningsområde*”) snarare än (kanske snävare) huruvida medlemsstaten ”tillämpar” unionsrätten genom att vidta specifika faktiska åtgärder.”[110] I *Melloni* fastställde domstolen att ”enligt fast rättspraxis följer det av principen om unionsrättens företräde, som är ett väsentligt kännetecken för unionens rättsordning [...], att den omständigheten att en medlemsstat hänvisar till bestämmelser i nationell rätt inte kan påverka unionsrättens verkan i den staten, även om de nationella bestämmelserna har grundlagsstatus”[111] men att medlemsstaterna, där en EU-rättsakt förutsätter nationella genomförandeåtgärder, förblir fria att tillämpa nationella standarder för skydd av grundläggande rättigheter i frågor som faller inom EU:s rättsområde, ”förutsatt att tillämpningen av dessa normer inte undergräver den skyddsnivå som föreskrivs i stadgan, såsom den tolkats av domstolen, eller unionsrättens företräde, enhetlighet och verkan”.[112] Rättspraxis tyder alltså på en bred tolkning av stadgans tillämpningsområde som omspänner alla ärenden som omfattas av EU:s behörighet.[113]

I stadgans artikel 7 fastställs respekten för privatliv enligt följande: ”Var och en har rätt

[106] Domstolens dom av den 26 februari 2013, *Åkerberg Fransson*, mål C-617/10, ECLI:EU:C:2013:105.
[107] Domstolens dom av den 26 februari 2013, *Melloni*, mål C‑399/11, ECLI:EU:C:2013:107.
[108] Ritleng 2014, s. 40. Se även domstolens dom av den 21 december 2011, *N.S. m.fl.*, förenade målen C-411/10 och C-493/10, ECLI:EU:C:2011:865.
[109] Ritleng 2014, s. 40.
[110] Förslag till avgörande av generaladvokat E. Sharpston föredraget den 14 november 2013 i mål C-390/12, *Pfleger*, EU:C:2013:747, p. 41.
[111] Mål C‑399/11, *Melloni,* p. 59.
[112] Mål C‑399/11, *Melloni,* p. 60.
[113] Boehm & Cole 2014, s. 44.

till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer." Artikeln avspeglar artikel 8 i Europakonventionen.[114] I EU-stadgans artikel 8 föreskrivs vidare om individers specifika rätt till skydd av personuppgifter. Artikel 8 i stadgan fastställer följande:

> 1. Var och en har rätt till skydd av de personuppgifter som rör honom eller henne.
> 2. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem.
> 3. En oberoende myndighet ska kontrollera att dessa regler efterlevs.

Respekten för privatliv i artikel 8 i Europakonventionen är mångfacetterad och inbegriper skydd för flera olika företeelser.[115] I Europakonventionen finns inte någon uttrycklig rättighet till dataskydd som motsvarar rättigheten i stadgan men Europadomstolen har tolkat artikel 8 i konventionen så att den inbegriper även frågor om dataskydd.[116] EU-domstolen har i sin rättspraxis i samband med hänvisning till skydd av personuppgifter i artikel 8 i allmänhet också hänvisat till respekt för privatliv i artikel 7.[117] EU-domstolen har vidare uttalat sig om att skyddet av personuppgifter bör tolkas enligt Europadomstolens praxis rörande rätten till respekt för privatliv.[118] Utformningen av stadgans artikel 8 bygger delvis på artikel 8 i Europakonventionen.[119] Därtill anger stadgans artikel 52(3) att i den mån stadgans rättigheter motsvarar en rättighet i Europakonventionen, ska dessa ges samma innebörd och räckvidd som i konventionen. Detta hindrar dock inte EU från att bevilja ett mer omfattande skydd i sin reglering än det som återfinns i Europakonventionen.[120]

---

[114] Förklaringar avseende stadgan om de grundläggande rättigheterna, förklaring till artikel 8, EUT 2007 C 303/02, *s. 17–35*.
[115] De Vries, 2018, s. 670.
[116] De Vries, 2018, s. 672.
[117] Se bl.a. domstolens dom av den 9 november 2010, *Volker*, förenade målen C-92/09 och C-93/09, ECLI:EU:C:2010:662 samt domstolens dom av den 8 april 2014, *Digital Rights Ireland och Seitlinger m.fl.* förenade målen C-293/12 och C-594/12, ECLI:EU:C:2014:238.
[118] Se domstolens dom av den 20 maj 2003, *Österreichischer Rundfunk m.fl.*, förenade målen C-465/00, C-138/01 och C-139/01, ECLI:EU:C:2003:294, p. 69.
[119] Förklaringar avseende stadgan om de grundläggande rättigheterna, förklaring till artikel 8, EUT 2007 C 303/02, ss. 17–35.
[120] Se domstolens dom av den 3 september 2008, *Kadi och Al Barkat International Foundation/ rådet och kommissionen*, C-402/05 P, ECLI:EU:C:2008:461 och domstolens dom av den 17 december 1970, *Internationale Handelsgesellschaft*, C-11/70, ECLI:EU:C:1970:114.

Rätten till privatliv och skyddet av personuppgifter är närbesläktade grundrättigheter som eftersträvar att skydda likartade värderingar, med fokus på individers självbestämmande och värdighet samt säkrandet av en personlig sfär för individen.[121] Trots likheterna utgör rätten till privatliv och skyddet av personuppgifter självständiga rättigheter som skiljer sig från varandra både till sin utformning och räckvidd. Rätten till privatliv är konstruerad som ett allmänt förbud mot ingripande i rättighetens sfär, och omfattar situationer där en individs privata intressen eller privata sfär blivit utsatt för en inskränkning, med förbehåll för vissa kriterier av allmänt intresse som kan motivera ingripandet i vissa fall.[122] Skyddet av personlig integritet innebär bland annat ett skydd från oönskad tillsyn från staten eller tredje parter, speciellt i koppling till brottsutredning.[123] Huruvida det anses finnas ett ingripande i individens privatliv eller inte är beroende av en *in casu* bedömning. Rätten till dataskydd betraktas som en aktiv rättighet, genom vilken ett system med kontrollmekanismer och balans inrättats för att skydda individer i sammanhang där deras personuppgifter behandlas.[124] Dataskyddet aktualiseras direkt då personuppgifter behandlas och erbjuder därmed ett bredare skydd än rätten till privatliv. All behandling av personuppgifter omfattas av kravet på lämpligt dataskydd, och rätten gäller alla typer av personuppgifter och databehandling, oavsett deras faktiska påverkan på individens integritet. Behandling av personuppgifter kan också konstateras kränka rätten till privatliv men det är emellertid inte nödvändigt att påvisa en kränkning av privatlivet för att reglerna för dataskydd ska aktualiseras.[125]

Det finns flera bakomliggande syften som ligger till grund för dataskyddet och det blir därför svårt att definiera dess yttersta intressen. Datarättigheter tenderar ofta att marginaliseras till ett snävt och individcentrerat intresse men deras skyddszon inkluderar även andra målsättningar och dataskyddet har bl.a. en stark koppling till legalitets-principen.[126] Brouwer identifierar tre olika mål för skyddet av personuppgifter.[127] Det första är det typiska skyddet av individuella rättigheter, mer specifikt skyddet av personlig integritet. Denna rättighet, som skyddas i artikel 8 i Europakonventionen och artikel 7 i

[121] FRA 2018 (c), s. 19.
[122] FRA 2018 (c), s. 19.
[123] De Vries 2018, s. 670.
[124] FRA 2018 (c), s. 19.
[125] FRA 2018 (c), s. 20.
[126] Brouwer 2011, s. 275.
[127] Brouwer 2011, ss. 275–276.

EU-stadgan, omfattar rätten att bli lämnad ifred, rätten till frihet och rätten till självbestämmande.[128] Det andra syftet bakom uppgiftsskyddet utgörs av skyddet av rättsstatsprincipen. Rätten till privatliv och dataskydd är väsentliga element i en demokrati eftersom ett demokratiskt samhälle inte kan existera om individer inte kan försäkra sig om att deras grundläggande rättigheter kan utövas fullt ut i enlighet med rättsstatsprincipen. Brouwer hänvisar till en bred tolkning av begreppet, vilket omfattar principen om maktfördelning i samhället, skyddet av de mänskliga rättigheterna och upprätthållandet av en demokratisk rättsordning, där statens befogenheter är begränsade till förmån för individers rättigheter och friheter samt jämlikhet och rättssäkerhet.[129] Detta mål har beskrivits som dataskyddets sociala funktion och utökar dataskyddets betydelse från ett skydd för den enskilda individen till ett skydd av individer som grupp.[130] Det tredje målet för dataskyddslagstiftningen gäller skyddet av god förvaltning. Om detta stadgas i artikel 15 FEUF samt stadgans artikel 41. Detta mål skyddar både den registrerades och den personuppgiftsansvarigas intressen genom att dels garantera integriteten och riktigheten i den information som lagras och dels genom att skydda säkerheten i informationssystem och tillförlitligheten när det gäller det lagrade datat.[131]

3.2 Regleringen av personuppgiftsskyddet

3.2.1 EU:s dataskyddsramverk

I artikel 16 FEUF fastställs det att EU ska agera för att säkerställa den grundläggande rätten till dataskydd:

> 1. Var och en har rätt till skydd av de personuppgifter som rör honom eller henne.
> 2. Europaparlamentet och rådet ska i enlighet med det ordinarie lagstiftningsförfarandet fastställa bestämmelser om skydd för enskilda personer när det gäller behandling av personuppgifter hos unionens institutioner, organ och byråer och i medlemsstaterna, när dessa utövar verksamhet som omfattas av unionsrättens tillämpningsområde, samt om den fria rörligheten för sådana uppgifter. Oberoende myndigheter ska kontrollera att dessa bestämmelser följs.
> De bestämmelser som antas på grundval av denna artikel ska inte påverka tillämpningen av de särskilda bestämmelser som anges i artikel 39 i fördraget om Europeiska unionen.

[128] Brouwer 2011, s. 275.
[129] Brouwer, 2011, s. 276.
[130] Brouwer, 2011, s. 276.
[131] Brouwer, 2011, s. 276.

Artikel 16 FEUF utgör grunden för EU:s lagstiftningsåtgärder inom området för dataskydd och ger EU ett specifikt mandat för att säkerställa denna rättighet,[132] utöver unionens allmänna ansvar – och medlemsstaterna när dessa agerar inom ramen för EU-lagstiftningen – att respektera de grundläggande rättigheterna i stadgan.[133] Artikel 16(1) FEUF, tillsammans med artikel 7 och artikel 8 i stadgan, anger rätten till dataskydd som unionen i slutändan bör garantera under kontroll av EU-domstolen.[134] Artikel 16(2) FEUF ger EU:s lagstiftare möjlighet att fastställa regler för dataskydd, vars kontroll bör säkerställas av oberoende myndigheter enligt artikel 16(2) FEUF och artikel 8(3) i stadgan.[135] Artikel 16 FEUF är tillämplig på all databehandling som äger rum inom EU:s lagstiftning, med undantag för de särskilda regler som antas av rådet inom ramen för den gemensamma utrikes- och säkerhetspolitiken enligt artikel 39 FEU. Artikel 16 FEUF beviljar därmed EU en brett formulerad roll för att säkerställa ett effektivt skydd av dessa grundläggande rättigheter för individen genom domstolsprövning, lagstiftning och tillsyn av oberoende myndigheter.

Därav fastställs skyddskravet på en fast grund, med två starka primärrättsliga pelare och en omfattande lagstiftningsram inom sekundärrätten. Den allmänna dataskyddsförordningen,[136] samt polisdirektivet,[137] utgör grundkomponenter för EU:s dataskyddsramverk. Detta ramverk blir tillämpligt då: (1) personuppgifter, (2) behandlas, (3) EU har kompetens och (4) inget undantag är tillämpligt.[138] Dataskyddet kan ses som en växande samling regler och principer som måste beaktas av lagstiftare och personuppgiftsansvariga vid utarbetandet av lagar och deras efterföljande. Denna tillväxt

[132] Den rättsliga grunden för dataskyddsförordningens föregångare, dataskyddsdirektivet, utgjordes av artikel 100(a) i fördraget om upprättandet av Europeiska gemenskapen, med målet att upprätta den inre marknaden och få den att fungera. Följaktligen skyddas personuppgifter inte längre genom regleringen av den inre marknaden utan som en grundläggande rättighet i stadgan och EU har ett uttryckligt mandat att reglera området för dataskydd som upprättats genom fördraget, vilket är unikt jämfört med andra grundläggande rättigheter.
[133] Hijmans 2016, s. 15.
[134] Hijmans 2016, s. 15.
[135] Hijmans 2016, s. 15.
[136] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 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). EUT 2016/L 119/1–88.
[137] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 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 2016/L 119/89–131.
[138] van der Sloot 2018, s. 6.

är konstant, eftersom utvecklingen av ny reglering aktualiseras då nya utmaningar uppstår i samband med tekniska framsteg.[139] Detta inkluderar bl.a. uppkomsten av ny teknik och den ökade användningen av biometri, vilket orsakar ett växande behov av mer detaljerade regler för att skydda individers personuppgifter. Både medlemsstaterna och EU:s organ måste se till att lagstiftningen är förenlig med regleringen i dessa regelverk.

I GDPR artikel 2(1) fastställs förordningens materiella tillämpningsområde omfatta ”sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register”. Inom EU har personuppgifter ansetts inbegripa en stor mängd olika uppgifter och information. Denna omfattning har vuxit väsentligt över tid. Enligt GDPR artikel 4(1) faller all information som rör en identifierad eller identifierbar levande fysisk person under begreppet personuppgift. WP29 har delat upp definitionen i fyra element, bestående av: (a) information, (b) avseende eller relaterat till (c) en identifierad eller identifierbar (d) fysisk person.[140] Flera uppgifter som tillsammans kan leda till att en enskild person kan identifieras, utgör likaså personuppgifter.[141] Begreppet inkluderar både direkt och indirekt identifierbar information.[142] I GDPR ingår en icke uttömmande lista på personuppgifter vilken inkluderar ”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”.[143] Det har till och med hävdats att all typ av uppgifter som berör en individ har potential att klassas som personuppgifter.[144] Detta beror på att uppgifter som inte direkt kan användas för att identifiera en person i allt högre grad kan sammankopplas med annan data, och kan då användas bl.a. för att skapa profiler.[145] WP29 har angett att dataskyddslagstiftningen omfattar både sanna och falska uppgifter, åsikter inkluderat. Arbetsgruppen har konstaterat att eftersom dataskyddsreglerna i sig tillåter möjligheten att informationen kan vara felaktig och förser individer med en rättighet att få tillgång till denna information och vidta lämpliga åtgärder

[139] Mäkinen 2016, s. 105.
[140] WP29 2007, s. 6.
[141] Dataombudsmannens byrå, tillgänglig på: https://tietosuoja.fi/sv/vad-ar-en-personuppgift.
[142] GDPR artikel 4 (1).
[143] GDPR artikel 4 (1).
[144] Purtova 2018 (b), s. 40.
[145] van der Sloot, 2018, s. 4.

för att bestrida den, innebär detta att felaktiga uppgifter också omfattas av dataskyddslagstiftningen.[146]

Regelverken identifierar även en särskild kategori av personuppgifter. I GDPR skäl 51 samt skäl 51 till polisdirektivet noteras att ”personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheterna och friheter bör åtnjuta särskilt skydd, eftersom behandling av sådana uppgifter kan innebära betydande risker för de grundläggande rättigheterna och friheterna”. Till denna kategori hänförs bl.a. genetiska uppgifter och biometriska uppgifter som används för att entydigt identifiera en person.[147] GDPR artikel 4(14) fastställer att biometriska uppgifter utgörs av ”personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person, såsom ansiktsbilder eller finger-avtrycksuppgifter”. Behandlingen av sådana känsliga uppgifter är bara tillåten under uppfyllandet av specifika kriterier. GDPR artikel 9(2)(g) anger att behandlingen ska vara ”nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen”. Förbudet att använda biometrisk data är dock inte kopplat till uppgifternas natur utan snarare till deras användningsändamål. Enbart i de fall biometrisk data kan användas för att entydigt identifiera en person kvalificerar de som känsliga uppgifter till skillnad från de andra uppräknade uppgifterna.[148]

För att reglerna ska vara tillämpningsbara krävs även att personuppgifterna behandlas. Behandling innebär enligt GDPR artikel 5:

> 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

[146] WP29 2007, s. 6.
[147] GDPR artikel 9 samt polisdirektivet artikel 10. Enligt skäl 9 till förordningen bör "behandling av foton inte systematiskt anses utgöra behandling av särskilda kategorier av personuppgifter, eftersom foton endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person”.
[148] Jasserand-Breeman 2018, s. 76.

> överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Avseende EU:s territoriella kompetens fastställs det att dataskyddsprinciperna inte bara gäller för ”behandlingen av personuppgifter inom ramen för den verksamhet som bedrivs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad i unionen, oavsett om behandlingen utförs i unionen eller inte”,[149] utan även för behandlingen av personuppgifter av registrerade som är i unionen, av en registeransvarig som inte är etablerad i unionen, om behandlingen av dessa är kopplade till övervakning av deras beteende i den mån deras beteende sker inom unionen.[150] GDPR artikel 4(7) definierar en personuppgiftsansvarig som:

> En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

Det finns undantag som faller utanför ramverkets tillämpningsområde. Personuppgifter som behandlas inom ramen för nationell säkerhet eller unionens gemensamma utrikes- och säkerhetspolitik tillhör denna grupp.[151] Också när databehandling är nödvändig för allmänintresset kan vissa delar av dataskyddet begränsas, även om majoriteten av dessa bestämmelser fortfarande måste respekteras. Polisdirektivet är utformat för att vara förenligt med dataskyddsförordningen och ger uttryck för flera av de principer som ingår i förordningen. Genom detta eftersträvas en balans mellan individers rättigheter och säkerhetsrelaterad bearbetning av personuppgifter. Den brottsbekämpande verksamhetens speciella karaktär medför dock att balansen mellan brottsbekämpande myndigheters behov och skyddet av registrerades uppgifter är något annorlunda än under GDPR.[152] Vid bearbetning av personuppgifter för säkerhetsrelaterade ändamål krävs en större mängd flexibilitet.[153] Vissa av principerna är speciellt problematiska, särskilt då data överförs från ett GDPR-sammanhang till behandling i ett brottsbekämpande

[149] GDPR artikel 3(1).
[150] GDPR artikel 3(2)(b).
[151] GDPR artikel 2(2)(a) och (b), artikel 23, 85–91 samt skäl 16.
[152] Leiser & Custers 2019, s. 3.
[153] de Hert och Papakonstantinou 2016, s. 9.

sammanhang. Ur ett rättsligt perspektiv medför detta problem med ändamåls-begränsningsprincipen, vilket granskas explicit senare i avhandlingen.[154]

3.2.2 EU:s rättsliga normhierarki

EU:s lagstiftning är baserad på primärrätt och sekundärrätt. De primära rättskällorna utgörs av grundfördragen, EU-stadgan, generella principer utvecklade av EU-domstolen samt internationella överenskommelser.[155] Den lagstiftning som bygger på principerna och målen i grundfördragen utgörs av sekundärrätt. Sekundärlagstiftning omfattar alla rättsakter som antagits av EU-institutionerna som gör det möjligt för EU att utöva sina befogenheter. I artikel 288 FEUF definieras de rättsakter som kan antas av unionen och här föreskrivs att endast rättsakter av dessa slag får antas. De rättsakter som definieras i artikeln är förordningar, direktiv, beslut, rekommendationer och yttranden. Det existerar ingen formell normativ hierarki mellan dessa rättsakter som mellan EU:s primärlagstiftning och sekundärlagstiftning.[156] Förordningar utgör direkt bindande lagstiftning som gäller automatiskt och enhetligt för alla EU-länder så snart de träder i kraft utan att behöva införlivas i nationell lagstiftning.[157] De är i sin helhet bindande för alla EU-länder. Förordningar är ett starkt lagstiftningsverktyg i unionen och medlemsstaterna kan inte välja att avstå från att delta eller välja att enbart tillämpa en del av en förordning. Förordningar har samma vikt som nationell lagstiftning. Direktiv är också bindande, men bara i utsträckningen för de resultat som de ska uppnå.[158] Medlemsstaterna kan välja form och metod för att nå de mål som anges i direktivet. Efter antagandet av ett direktiv måste medlemsstaterna införliva det i nationell lagstiftning. Detta innebär att medlemsstaterna måste skapa eller uppdatera nationella lagar för att uppnå direktivets mål. Överföringen till nationell lagstiftning måste ske inom den tidsfrist som fastställs när direktivet antas. Ifall en medlemsstat inte införlivar direktivet i nationell lagstiftning inom den utsatta tidsfristen förblir direktivet hursomhelst inte utan verkan.

[154] Se diskussionen om sekundär användning för brottsbekämpande ändamål i avhandlingens kapitel 4.2.
[155] Europaparlamentets hemsida (a), tillgänglig på: https://www.europarl.europa.eu/factsheets/en/sheet/6/sources-and-scope-of-european-union-law.
[156] Craig & de Búrca 2011, s. 104.
[157] Europaparlamentets hemsida (a), tillgänglig på: https://www.europarl.europa.eu/factsheets/en/sheet/6/sources-and-scope-of-european-union-law.
[158] Europaparlamentets hemsida (a), tillgänglig på: https://www.europarl.europa.eu/factsheets/en/sheet/6/sources-and-scope-of-european-union-law.

EU-domstolen har i sin rättspraxis fastställt att ett direktiv har vertikal direkt effekt när dess bestämmelser är ovillkorliga och tillräckligt tydliga och precisa samt när medlemsstaten inte har införlivat direktivet inom tidsfristen.[159] Vidare har EU-domstolen även fastställt en möjlighet för individer att väcka talan, genom vertikal effekt, om skadestånd mot en medlemsstat för underlåtenhet att genomföra EU-lagstiftning eller då den implementerats felaktigt av en medlemsstat.[160] I de flesta fall fastställer fördragen vilken typ av rättsakt som ska användas. Om så inte är fallet tillåter artikel 296 FEUF institutionerna att välja vilken typ av rättsakt som ska antas från fall till fall.

3.2.3 Två uppsättningar regler: GDPR och polisdirektivet

Den allmänna dataskyddsförordningen, GDPR, utgör *lex generalis* vid behandling av personuppgifter. Varje person, unionsmedborgare eller inte, som faller under EU:s jurisdiktion, kvalificerar som en digital medborgare i unionen. Dataskyddsförordningen innehåller grundläggande principer som utgör kärnan i skyddet av dessa individers uppgifter. All behandling av personuppgifter som faller under förordningen måste således uppfylla dessa grundläggande principer, som ska beaktas i alla skeden av uppgifternas behandling. Dessa utgörs av laglighet, korrekthet och öppenhet; ändamålsbegränsning; uppgiftsminimering; riktighet; lagringsminimering; integritet och konfidentialitet samt ansvarsskyldighet.[161]

En annan typ av uppgiftsskydd blir tillgängligt då personuppgifter används inom brottsbekämpningssektorn. Då regleras uppgiftsbehandlingen genom specifika regler i polisdirektivet som *lex specialis* i förhållande till den annars allmänt gällande dataskyddsförordningen. Som namnet avslöjar berör direktivet behandlingen av personuppgifter för brottsbekämpningsändamål vilket faller utanför ramen för GDPR.[162] Brottsbekämpning utgör alltså ett område av sektorspecifik reglering som kräver mer specifika bestämmelser. Medan den allmänna dataskyddsförordningen fastställer de

[159] Se domstolens dom av den 4 december 1974, *van Duyn*, mål 41–74, ECLI:EU:C:1974:133.
[160] Se domstolens dom av den 9 augusti 1993, *Marshall*, mål C-271/91, ECLI:EU:C:1993:335 och domstolens dom av den 9 november 1995, *Francovich*, mål C-479/93, ECLI:EU:C:1995:372.
[161] GDPR artikel 5.
[162] Brottsbekämpande ändamål bör i kontexten av denna avhandling förstås referera till de ändamål som faller innanför polisdirektivets tillämpningsområde. Se GDPR artikel 2(1)(d) som utesluter polisdirektivets tillämpningsområde från förordningen reglering.

allmänna reglerna som gäller till skydd för ”fysiska personer med avseende på behandling av personuppgifter och att säkerställa det fria flödet av personuppgifter inom unionen”, fastställer polisdirektivet ”särskilda regler som syftar till att skydda fysiska personer med avseende på behandlingen av personuppgifter och att säkerställa det fria flödet av personuppgifter inom unionen på området för straffrättsligt samarbete och polissamarbete”.[163] Ibruktagandet av ett sektorspecifikt regelverk för behandling av personuppgifter inom brottsbekämpande myndigheters verksamhet är motiverat för att uppnå tydlighet och balans mellan dataskydd och andra legitima säkerhetspolitiska intressen. Detta dubbla tillvägagångssätt har uppstått på grund av brottsbekämpningens särskilda behov vid förebyggande, utredning och lagföring av brott, och på grund av EU:s pelarstruktur före Lissabon.[164] EU:s kompetens fördelades tidigare mellan tre pelare, varav den första inkluderade ärenden gällande den inre marknaden, den andra utrikes- och säkerhetsfrågor och den tredje området för frihet, säkerhet och rättvisa vilket också omfattade brotts- och polissammarbetsärenden. Innan var ”lagstiftningen om uppgiftsskydd på området med frihet, säkerhet och rättvisa uppdelad mellan den första pelaren (uppgiftsskydd för privata och kommersiella ändamål, med beslutsfattande enligt gemenskapsmetoden) och den tredje pelaren (uppgiftsskydd i brottsförebyggande syfte, med beslutsfattande på mellanstatlig nivå)”.[165]

I Finland regleras det allmänna dataskyddet genom dataskyddslagen (1050/2018) som är en allmän lag. Lagen trädde i kraft den 1 januari 2019 och kompletterar och preciserar EU:s dataskyddsförordning i nationell lagstiftning.[166] Dataskyddslagen utgör inte en självständig och samlad lagstiftningshelhet, utan lagen bör tillämpas parallellt med GDPR som är direkt tillämplig i medlemsstaterna.[167] Dataskyddslagen tillämpas dock inte på frågor som regleras enligt lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018), som trädde i kraft samtidigt

[163] Förordning 2018/1725, skäl 3.
[164] Porcedda 2012, s. 210.
[165] Europaparlamentets hemsida (b), tillgänglig på: https://www.europarl.europa.eu/factsheets/sv/sheet/157/varstvo-osebnih-podatkov.
[166] RP 9/2018, s. 1.
[167] RP 9/2018, s. 1. I RP 2/2020 fastställs att “Grundlagsutskottet tog uttrycklig ställning i frågan när det behandlade dataskyddslagen, som kompletterar dataskyddsförordningen, och dataskyddslagen avseende brottmål. Utskottet konstaterade att skyddet för personuppgifter härefter i första hand bör tillgodoses med stöd av dataskyddsförordningen och den nya nationella allmänna lagstiftningen och att vi i fortsättningen bör förhålla oss restriktiva när det gäller att införa nationell speciallagstiftning“. Se GrUU 14/2018, ss. 4–5 samt GrUU 26/2018, ss. 2–3.

som dataskyddslagen.[168] I Finland genomförs polisdirektivets reglering i första hand genom lagen om behandling av personuppgifter i brottmål (1054/2018) som ”har karaktären av allmän lag som ska iakttas inom dataskyddet vid behandling av brottmål”.[169] I RP 31/2018 fastställs att ”eftersom de myndigheter som tillämpar lagen, i synnerhet polisen, Gränsbevakningsväsendet, Försvarsmakten och Tullen har olika uppgifter, befogenheter och informationssystem, behöver lagstiftningen kompletteras med särskilda bestämmelser för de olika förvaltningsområdena”.[170] Lagen är således subsidiär i förhållande till annan speciallagstiftning. Sådan speciallagstiftning utgörs bl.a. av lagen om behandling av personuppgifter i polisens verksamhet (616/2019), lagen om behandling av personuppgifter vid Gränsbevakningsväsendet (639/2019), lagen om behandling av personuppgifter inom Tullen (650/2019) och lagen om behandling av personuppgifter inom Försvarsmakten (332/2019). I praktiken har det upprättats speciallagstiftning om behandlingen av personuppgifter för så gott som alla behöriga myndigheter som lagen omfattar, vilket medför att speciallagstiftning ska tillämpas i dessa fall.[171] Lagen om behandling av personuppgifter i brottmål (1054/2018) tillämpas också på behandling av personuppgifter när denna utförs av behöriga myndigheter vid upprätthållandet av den nationella säkerheten men då grundar sig lagens tillämpningsområde inte på genomförandet av polisdirektivet, utan det är då frågan om en nationell lösning.[172]

För att polisdirektivets regler ska vara tillämpliga måste både kriterierna för dess materiella samt personliga tillämpningsområde uppfyllas. Behandlingen ska för det första i enlighet med direktivets artikel 1(1) utföras ”i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten”. För det andra ska

[168] Se 2 § i dataskyddslagen (1050/2018).
[169] RP 31/2018, s. 19.
[170] RP 31/2018, s. 19. Se även 2 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018).
[171] I RP 2/2020, s. 6 fastställs att ”orsaken till de många bestämmelserna om behandling av personuppgifter kan i hög grad härledas till kravet i 10 § 1 mom. i grundlagen att närmare bestämmelser om skydd för personuppgifter ska utfärdas genom lag och i grundlagsutskottets tidigare tolkningspraxis när det gäller detta och skyddet för privatlivet. Dessutom grundar sig bestämmelserna om utlämnande av personuppgifter i anslutning till myndigheternas verksamhet delvis på ett behov av att göra det möjligt att lämna ut personuppgifter trots sekretessbestämmelserna i lagen om offentlighet i myndigheternas verksamhet (621/1999)”.
[172] RP 31/2018, s. 19.

behandlingen utföras av behöriga myndigheter. Artikel 1(1) fastställer dessa bestå av offentliga myndigheter eller andra organ som genom nationell rätt påförts befogenheter att behandla personuppgifter för de ovannämnda ändamålen. Beroende på olika strukturer och reglering i medlemsländerna kan direktivet tillämpas på olika sätt. Formuleringen i polisdirektivet begränsar inte tillämpningsområdet till typiska brottsbekämpande myndigheter utan till all behandling för brottsbekämpande ändamål som utförs av ett offentligt eller privat organ som passar definitionen av behörig myndighet.[173] Skäl 11 i direktivet anger att ”sådana behöriga myndigheter kan omfatta inte bara offentliga myndigheter såsom rättsliga myndigheter, polis eller andra brottsbekämpande myndigheter, utan också alla andra organ eller enheter som genom medlemsstaternas nationella rätt har anförtrotts myndighetsutövning enligt detta direktiv”. Det går alltså inte automatiskt att anta att all behandling av personuppgifter som utförs av brottsbekämpande myndigheter omfattas av direktivet, eller att en enhet inom den privata sektorn inte skulle omfattas. Då medlemsstaterna anförtror dessa myndigheter andra uppgifter som inte omfattas av tillämpningsområdet för direktivet, omfattas de av den allmänna dataskyddsförordningen, i den mån dessa omfattas av unionsrätten.[174] Därmed faller inte alla personuppgifter som hanteras av behöriga brottsbekämpande myndigheter inom ramen för polisdirektivet, utan behandlas då normalt under dataskyddsförordningen. Detta gäller även för behandling av personuppgifter relaterad till gränsbevakning, migrations- och asylärenden. Enheter inom den privata sektorn kan ha anförtrotts, i enlighet med medlemsstaternas nationella lagstiftning, offentliga myndighetsuppgifer eller ålagts att utföra databehandling för brottsbekämpande ändamål. I finsk lagstiftning begränsas överföringen av förvaltningsuppgifter på andra aktörer än myndigheter i och med GL 124 § som fastställer att ”uppgifter som innebär betydande utövning av offentlig makt får dock ges endast myndigheter”. Sammanfattningsvis innebär detta att ett potentiellt mycket stort antal olika organ kan omfattas av tillämpningsområdet, och tillämpligheten av detta system måste bedömas från fall till fall. Direktivets tillämpningsområde inkluderar även nationell behandling av personuppgifter och gäller således inte uteslutande för utbyte av personuppgifter mellan medlemsstaterna.

[173] Se Purtova 2018 (a), s. 52–68, för uppgifts- och informationsdelning mellan privata och statliga enheter.
[174] Polisdirektivet artikel 9. Se även skäl 11–12 i direktivet.

Nationell säkerhet hör enligt artikel 4(2) FEUF till medlemsstaternas exklusiva kompetensområde och faller således utanför EU:s behörighet. Sådan behandling regleras av varje medlemsstats nationella lagstiftning.[175] Begränsningen av EU:s tillämpningsområde med hänvisning till nationell säkerhet är dock inte helt entydig. Enligt EU-domstolens rättspraxis är möjligheten att avvika från tillämpningen av unionslagstiftningen i detta avseende endast acceptabel i ett begränsat antal situationer. Annars skulle denna möjlighet riskera att undergräva lagstiftningens bindande karaktär och enhetliga tillämpning i unionen. Följaktligen blir unionens rättsordning och EU-domstolens praxis i viss mån även relevant i frågor med anknytning till nationell säkerhet, däribland frågor relaterade till nationell underrättelselagstiftning.[176]

Likaså faller behandlingen av personuppgifter som utförs av unionens institutioner, organ och byråer utanför direktivets tillämpningsområde,[177] eftersom dessa enheter regleras skilt genom förordning 2018/1725.[178] Förordningen upphäver förordning 45/2001 och beslut 1247/2002/EG som daterar tillbaka till tiden innan Lissabonfördraget, och i linje med GDPR antar den en principbaserad dataskyddsstrategi. Även denna förordning innehåller undantag. I enlighet med dess artikel 2(2) fastställs att ”endast artikel 3 och kapitel IX i denna förordning är tillämpliga på behandling av operativa personuppgifter som utförs av unionens organ och byråer när dessa utövar verksamhet som omfattas av tredje delen avdelning V kapitel 4 eller kapitel 5 i EUF-fördraget”. Skäl 11 fastställer att ”sådana särskilda regler bör betraktas som *lex specialis* till bestämmelserna i kapitlet i

[175] I polisdirektivets skäl 14 fastställs att ”eftersom detta direktiv inte bör tillämpas på behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten, bör verksamhet som rör nationell säkerhet, verksamhet som utförs av byråer och organ som hanterar nationella säkerhetsfrågor och medlemsstaternas behandling av personuppgifter när de utför verksamhet som omfattas av del V kapitel 2 i fördraget om Europeiska unionen (EU-fördraget) inte betraktas som verksamhet som omfattas av detta direktivs tillämpningsområde”.

[176] Se bl.a. domstolens dom av den 7 juni 2012, *Insinööritoimisto InsTiimi*, mål C-615/10, ECLI:EU:C:2012:324, p. 35, samt domstolens dom av den 15 december 2009, *Commission / Finland*, mål C-284/05, ECLI:EU:C:2009:778, p. 45. I det pågående målet C-623/17, *Privacy International,* har en begäran om förhandavgörande angående säkerhets- och underrättelseorganens möjligheter att använda stora mängder data (s.k. mängddata) i anknytning till nationell säkerhet hänskjutits domstolen med frågan om detta kunde anses falla utanför EU-lagstiftningens tillämpningsområde och därmed undgå att uppfylla de stränga kraven på skyddsåtgärder som fastställts i förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*, samt förenade målen C-203/15 och C-698/15, *Tele2 Sverige*.

[177] Polisdirektivet artikel 2(3)(b).

[178] Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG. EUT 2018/L 295/39–98.

denna förordning om behandling av operativa personuppgifter". Det bör emellertid noteras att förordningen inte gäller för Europol eller för Europeiska åklagarmyndigheten innan de rättsakter som inrättat Europol och Europeiska åklagarmyndigheten har reviderats.[179] Huruvida dessa institutioners rättsliga grund måste anpassas till förordningen kommer att bedömas i en tillsynsprocess år 2022.[180]

Till skillnad från dataskyddsförordningen som är direkt tillämplig i alla medlemsstater sedan dess ikraftträdande och därav säkerställer ett rätt effektivt genomförande av dataskyddsregleringen, måste polisdirektivet införlivas i respektive medlemsstats nationella lagstiftning. I enlighet med skäl 7 i direktivet "bör skyddet för fysiska personers rättigheter och friheter i samband med behöriga myndigheters behandling av personuppgifter [...] vara likvärdigt i alla medlemsstater". Eftersom direktivet ger medlemsstaterna en viss tolkningsmarginal när det gäller dess införlivande, och eftersom medlemsstaternas straffrättsliga system inte är harmoniserade, kan tillämpningen av direktivet variera beroende på olika definitioner av straffbara handlingar och behöriga myndigheter i medlemsländerna, samt de olika befogenheter som tilldelats de sistnämnda. Då kan t.ex. såväl brottsutredningsändamål som underrättelseändamål omfattas av direktivet. Huruvida syftet med direktivet, som är att öka det ömsesidiga förtroendet och effektiviteten för datautbyte i brottsutredning, kommer att uppnås beror till stor del på hur bestämmelserna i direktivet genomförs i de olika medlemsländerna.[181]

3.3 Privatliv, personuppgifter och säkerhet – en avvägning

3.3.1 Dataskyddets icke-absoluta karaktär

Skyddet av personuppgifter utgör inte en absolut rättighet utan måste balanseras och betraktas i ljuset av andra samhällsfunktioner.[182] Denna balansering ser i enlighet med EU-domstolens praxis olika ut från fall till fall.[183] Enligt stadgan kan grundläggande rättigheter inskränkas under vissa villkor. En sådan omständighet utgöras av EU:s inre

[179] Förordning 2018/1725, artikel 2.
[180] Förordning 2018/1725, artikel 98.
[181] Kędzior 2019, s. 509.
[182] GDPR skäl 4. Se även förenade målen C-92/09 och C-93/09, *Volker*, p. 48, samt domstolens dom av den 17 oktober 2013, *Schwarz*, C-291/12, ECLI:EU:C:2013:670 p. 33.
[183] Brkan 2016, s. 825.

säkerhet, där medlemsstaterna antar gemensamma åtgärder för att bekämpa terroristhot, men mer generellt för att stärka det rättsliga och polisiära samarbetet i kriminella (främst straffprocessuella) frågor inom området med frihet, säkerhet och rättvisa.[184] Mifsud Bonnici identifierar fem olika aspekter som ställer upp gränser för dataskyddets räckvidd. Dessa utgörs av: (a) beaktandet av dataskyddets funktion i samhället; (b) den positiva avgränsningen av rättigheten som härrör sig från formuleringen i artikel 8 i stadgan; (c) begränsningen av rättigheten enligt artikel 52 i stadgan; (d) den nära förbindelsen mellan artikel 7 i stadgan och artikel 8 i Europakonventionen; (e) bestämmelser i nuvarande sekundärlagstiftning om dataskydd.[185]

Dataskyddets funktion i samhället har diskuterats ovan i ett tidigare avsnitt av kapitel 3.[186] I avsnittet formuleras tre mål, bestående av en individuell, en social och en administrativ dimension av dataskyddet. Trots EU-domstolens uttryckliga hänvisningar till 'dataskyddets funktion i samhället',[187] har domstolen inte ännu definierat innebörden av detta begrepp. Detta skulle innebära ett behov att besvara mer grundläggande fråga kopplade till vad rätten till dataskydd består av och i nuläget finns det ingen överenskommen definition av rättigheten.[188] En balansering av rättighetens gränser är således svår att utföra på dessa grunder trots domstolens uttalanden. Vidare anger en granskning av formuleringen i stadgans artikel 8(2) och 8(3) den positiva avgränsning för skyddet av personuppgifter som fastställs i artikel 8(1).[189] Den registrerades kontroll över sina personuppgifter kan antingen åsidosättas genom den registrerades samtycke,[190] eller när lagstiftaren anser det nödvändigt att samla in, lagra eller behandla personlig information för att uppnå ett legitimt mål.[191] Även under dessa omständigheter åtnjuter den registrerade fortfarande vissa aspekter av kontroll över sina personuppgifter, detta illustreras bl.a. genom kraven på ändamålsspecifikation och den registrerades rätt till tillgång och rättelse av felaktiga uppgifter.[192] Den registrerade garanteras även extern

[184] EU har kompetens i ärenden som rör unionens inre säkerhet, polisiärt och rättsligt samarbete inkluderat, i enlighet med artikel 4 FEU och kapitel 4 och 5 FEUF.
[185] Mifsud Bonnici 2014, s. 133.
[186] Se avhandlingens kapitel 3.1.
[187] Se bl.a. förenade målen C-92/09 och C-93/09, *Volker,* p. 48 samt mål C-291/12, *Schwarz*, p. 33.
[188] Mifsud Bonnici 2014, s. 133.
[189] Mifsud Bonnici 2014, s. 133.
[190] GDPR artikel 8(2).
[191] GDPR artikel 8(2).
[192] Mifsud Bonnici 2014, s. 135.

övervakning genom kontroll av en oberoende myndighet.[193] Vad beträffar dataskyddets reglering i sekundärlagstiftningen avgör varje regelverk skilt vilka begränsningar och principer som gäller för åtnjutandet av dataskydd. Sekundärlagstiftningen besitter en dubbel karaktär, där den å ena sidan realiserar innehållet i artikel 16 FEUF som fastställer EU:s befogenheter i frågor som rör dataskydd, samt innehållet i rättigheterna i artiklarna 8 och 7 i stadgan och i artikel 8 i Europakonventionen, men å andra sidan också kan ligga till grund för en laglig inskränkning av rättigheterna.[194]

Den nära kopplingen mellan artikel 7 och 8 i stadgan kan både vara till fördel och nackdel vid tolkningen av dataskyddet, då kopplingen medför att de begränsningar som identifierats rörande behandlingen av personuppgifter inom ramen för rätten till privatliv i artikel 7 i stadgan samt artikel 8 i Europakonventionen fungerar riktgivande även för dataskyddet i stadgans artikel 8.[195] Nackdelen är naturligtvis att denna nära koppling kan medföra en hämmande effekt på utvecklingen av rätten till dataskydd som en självständig rättighet. EU-domstolen har dock i sin senare rättspraxis visat en tendens att tolka artikel 8 i stadgan som en egen rättighet och således har utvecklingen av en gradvis distansering mellan de två rättigheterna påbörjats.[196] Genom att i Lissabonfördraget ge stadgan bindande kraft och införa en uttrycklig rättslig grund för lagstiftning om dataskydd i artikel 16 FEUF har EU-domstolen erhållit de nödvändiga rättsliga verktygen för att utarbeta innehållet och betydelsen av en oberoende rätt till dataskydd.[197] Detta innebär en positiv utveckling eftersom rättigheterna skiljer sig till sin omfattning och skyddsnivå.

Tydligast framgår begränsningen av dataskyddet i artikel 8(2) i Europakonventionen och artikel 52(1) i stadgan. Trots olika uttryckssätt förmedlar de båda regelverken liknande krav på lagenliga begränsningar. Dessa begränsningar har vidare utformats och tolkats genom rättspraxis från Europadomstolen och EU-domstolen. EU-domstolen har i sin rättspraxis fastställt att ”konventionen utgör emellertid inte något rättsligt instrument som formellt har införlivats med unionsrätten, så länge som unionen inte har anslutit sig till

[193] GDPR artikel 8(3).
[194] Mifsud Bonnici 2014, s. 140.
[195] Mifsud Bonnici 2014, s. 137.
[196] von Grafenstein 2018, s. 214.
[197] Lynskey 2014, s. 579.

denna konvention".[198] Sedan ikraftträdandet av Lissabonfördraget har EU-stadgan blivit den viktigaste referensen för att bedöma om EU:s sekundärlagstiftning uppfyller grundläggande rättigheter.[199] EU-domstolen har i sin rättspraxis fastställt att en bedömning av giltigheten i en bestämmelse i sekundärlagstiftningen endast måste göras mot bakgrund av de grundläggande rättigheter som garanteras i stadgan.[200] I enlighet med artikel 6(3) FEU har EU-domstolen emellertid också fastställt att de specifika bestämmelserna i Europakonventionen måste beaktas för att tolka motsvarande bestämmelser i stadgan.[201] Detta framgår även i artikel 52(3) i stadgan som uttrycker att rättigheterna i stadgan ska ges samma innehåll och räckvidd i den mån de korresponderar mot Europakonventionens rättigheter:

> I den mån som denna stadga omfattar rättigheter som motsvarar sådana som garanteras av europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna ska de ha samma innebörd och räckvidd som i konventionen. Denna bestämmelse hindrar inte unionsrätten från att tillförsäkra ett mer långtgående skydd.

I sin rättspraxis hänvisar EU-domstolen och Europadomstolen ofta till varandras domar, som en del av en ständig dialog mellan de två domstolarna för att söka en harmonisk tolkning av reglerna om dataskydd.[202] Artikel 52(3) i stadgan avser innehållet och omfattningen av de rättigheter som skyddas av varje rättsordning, snarare än villkoren för deras begränsningar. Med tanke på det bredare sammanhanget av dialogen och samarbetet mellan de två domstolarna kan EU-domstolen dock i sina analyser ta hänsyn till kriterierna för laglig begränsning enligt artikel 8 i Europakonventionen, såsom de tolkats av Europadomstolen, och Europadomstolen å sin sida kan också hänvisa till villkoren för laglig begränsning enligt stadgan.[203] Som konstaterats tidigare i kapitlet har stadgans artikel 8 om dataskydd inte en direkt motsvarighet i Europakonventionens

[198] Se mål C-617/10, *Åkerberg Fransson*, p. 44, domstolens dom av den 3 september 2015, *Inuit Tapiriit Kanatami*, mål C‑398/13 P, ECLI:EU:C:2015:535, p. 45, förenade målen C-203/15 och C-698/15, *Tele2 Sverige*, p. 127–129.
[199] EDPS 2017 (a), s. 6. Se också Hijmans 2016, s. 183.
[200] Se domstolens dom av den 15 februari 2015, *N.*, mål C-601/15 PPU, ECLI:EU:C:2016:84, p. 46, domstolens dom av den 6 november 2012, *Otis m.fl.*, mål C-199/11, ECLI:EU:C:2012:684, p. 47, mål C‑398/13 P, *Inuit Tapiriit Kanatami*, p. 46.
[201] Se mål C-601/15 PPU, *N.*, p. 77.
[202] FRA 2018 (c), s 51. Se t.ex. förenade målen C-92/09 och C-93/09, *Volker*, p. 59 samt mål C-291/12, *Schwarz*, p. 33, förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*, p. 35, förenade målen C-203/15 och C-698/15, *Tele2 Sverige*, p. 119–120 och Europadomstolens dom av den 12 januari 2016 i mål *Szabó och Vissy mot Ungern*, 37138/14, p. 23.
[203] FRA 2018 (c), s. 52.

rättigheter, men det framgår att rättigheten har baserats på bland annat artikel 8 i Europakonventionen.[204] Det bör även påpekas att det endast finns ett begränsat antal domar från EU-domstolen angående dataskydd innan Lissabonfördragets ikraftträdande vilket motiverar hänvisningar till Europadomstolens praxis. Därför är Europadomstolens rättspraxis angående artikel 8 också relevant, men inte nödvändigtvis avgörande, vid bedömningen av om en begränsning överensstämmer med stadgan.[205] Således är den viktigaste hänvisningen när man bedömer åtgärder som begränsar utövandet av de rättigheter som garanteras i artikel 8 i stadgan artikel 52(1) i stadgan och EU-domstolens rättspraxis. Dessutom bör kriterierna i artikel 8(2) i Europakonventionen, såsom de tolkats i Europadomstolens rättspraxis, också beaktas i en sådan bedömning.[206] EU-domstolen har uppmärksammat att EU-lagstiftningen ofta är skyldig att uppfylla flera mål av allmänt intresse som ibland kan vara motstridiga och därmed krävs en rättvis balans mellan de olika allmänna intressena och grundläggande rättigheter som skyddas av EU:s rättsordning.[207] När en inskränkning av en individs rätt till dataskydd föreligger är det nödvändigt att undersöka om inskränkningen är motiverad med beaktande av artikel 52(1) i stadgan. I förklaringarna till stadgan anges att ordalydelsen i artikel 52(1) är hämtad från EU-domstolens rättspraxis.[208]

Europadomstolen har behandlat många fall med koppling till personuppgifter och har i sin praxis bekräftat att brottsbekämpande myndigheters övervakning och systematiska insamling av personuppgifter faller innanför ramen för artikel 8 och därmed utgör en inskränkning i den enskildes rätt till privatliv.[209] Både Europadomstolen och EU-domstolen har upprepade gånger varnat för en massartad och oproportionell insamling och behandling av individers personuppgifter. Syftet med en sådan inskränkning måste därför övervägas noggrant. EU-domstolen har uttalat att en rättsakt utgör ett intrång i den

[204] Se avhandlingens kapitel 3.1.
[205] EDPS 2017 (a), s. 6.
[206] EDPS 2017 (a), s. 7.
[207] Se t.ex. domstolens dom av den 29 januari 2008, *Promusicae*, mål C-275/06, ECLI:EU:C:2008:54, p. 68, domstolens dom av den 6 november 2003, *Lindqvist*, mål C-101/01, ECLI:EU:C:2003:596, p. 87.
[208] Förklaringar avseende stadgan om de grundläggande rättigheterna, förklaring till artikel 51, EUT 2007 C 303/02, ss. 17–35.
[209] Se t.ex. Europadomstolens dom av den 26 mars 1987 i mål *Leander mot Sverige*, 9248/81; dom av den 4 maj 2000 i mål *Rotaru mot Rumänien*, 28341/95; dom av den 29 juni 2006 i mål *Weber och Saravia mot Tyskland*, 54934/00; dom av den 1 juli 2008 i mål *Liberty m.fl. mot Storbritannien*, 58243/00; dom av den 4 december 2008 i mål *S. och Marper mot Storbritannien*, 30562/04 och 30566/04; dom av den 18 april 2013 i mål *M.K. mot Frankrike*, 19522/09.

grundläggande rätten till skydd av personuppgifter som garanteras i artikel 8 i stadgan, då den föreskriver behandling av personuppgifter.[210] Därmed utgör i princip all databehandling, såsom insamling, lagring, användning och överföring av personuppgifter, som fastställs enligt lagstiftning, en begränsning av rätten till skydd av personuppgifter som ska beakta kriterierna i artikel 52(1). EU-domstolen har betonat att ett mål av allmänt intresse inte i sig är tillräckligt för att motivera en sådan inskränkning.[211] I artikel 52(1) fastställs:

> Varje begränsning i utövandet av de rättigheter och friheter som erkänns i denna stadga ska vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa rättigheter och friheter. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

De begränsningar som åläggs i artikel 8 i stadgan måste för det första föreskrivas i lag. Denna begränsning återfinns i artikel 8(2) i Europakonventionen. Europadomstolen har i sin rättspraxis gett en omfattande reflektion över vad som kan betraktas vara i enlighet med lagen. I målet *M.M. mot Storbritannien* fastställde Europadomstolen kriterier som måste uppfyllas för att ett ingripande i en rättighet ska anses ha skett med stöd av lag.[212] En begränsning måste ha en grund i nationell lagstiftning och vara förenlig med rättsstatsprincipen, och lagen måste vara tillgänglig och förutsebar, det vill säga formulerad med tillräcklig precision för att göra det möjligt för individen att anpassa sitt beteende efter den.[213] Sådana regler bör också, i tillämpliga fall, tydligt ange omfattningen av en eventuell bedömningsmarginal som ges brottsbekämpande myndigheter och ange vägledning i hur denna bedömning ska utövas samt ge tillräckliga rättsliga skyddsåtgärder åt de berörda individerna.[214]

För det andra krävs det att begränsningarna är förenliga med det väsentliga innehållet i stadgans rättigheter och friheter. EU-domstolen har ännu inte undersökt denna aspekt av artikel 52(1) i samband med rätten till dataskydd. Kravet härrör från EU-domstolens äldre

[210] Se förenade målen C-92/09 och C-93/09, *Volker*, p. 58, förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*, p. 34–36.
[211] Se förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*, p. 51 samt förenade målen C-203/15 och C-698/15, *Tele2 Sverige*, p. 103.
[212] Europadomstolens dom av den 13 november 2012 i mål *M.M. mot Storbritannien*, 24029/07.
[213] Europadomstolens dom i mål *M.M. mot Storbritannien* och dom av den 24 april 1990 i mål *Huvig mot Frankrike*, 11105/84.
[214] Europadomstolens dom i mål *M.M. mot Storbritannien* och dom i mål *Huvig mot Frankrike*.

rättspraxis om att själva innehållet i rättigheterna inte bör undergrävas.[215] Även om det inte existerar ett överflöd av rättspraxis avseende villkoren under vilka en rättighets väsentliga innehåll påverkas, kan man säga att detta skulle vara fallet om begränsningen går så långt att den fråntar rättigheten dess grundelement och därmed förhindrar utövandet av rättigheten.[216] Det väsentliga innehållet sträcker sig endast över ett begränsat omfång eftersom någon form av proportionalitets- och balanseringstest inte alls är möjlig på detta område.[217] I *Schrems* fann EU-domstolen i sin granskning att det ”väsentliga innehållet i den grundläggande rätten till effektivt domstolsskydd” inte respekterades.[218] I *Digital Rights Ireland* fann domstolen att det väsentliga innehållet i rätten till respekt för privatlivet inte påverkades av begränsningen. Domstolen fastställde att ”även om den lagring av uppgifter som föreskrivs i direktiv 2006/24 utgör ett synnerligen allvarligt ingrepp i dessa rättigheter kan det inte kränka deras väsentliga innehåll” då man inte kunde skaffa sig kännedom om själva innehållet i uppgifterna.[219] På liknande sätt fann EU-domstolen att det väsentliga innehållet i rätten till skydd av personuppgifter i fallet inte påverkades på grund av att datalagringsdirektivet föreskrev en grundläggande regel där ”medlemsstaterna ska säkerställa att det antas lämpliga tekniska och organisatoriska åtgärder för att skydda mot oavsiktlig eller olaglig förstöring och mot oavsiktlig förlust eller oavsiktlig ändring av uppgifterna”.[220] Det faktum att en åtgärd respekterar det väsentliga innehållet i en grundläggande rättighet betyder dock inte automatiskt att den överensstämmer med proportionalitetsprincipen.[221] Avsaknaden av en oberoende myndighet som granskar efterlevnaden av skyddsnivån som garanteras i EU-lagstiftningen kan också påverka det väsentliga innehållet i dataskyddet. I *Tele2 Sverige* fastställde EU-domstolen följande:

> En sådan kontroll krävs uttryckligen enligt artikel 8.3 i stadgan och utgör enligt domstolens fasta praxis en grundläggande beståndsdel i skyddet för enskilda i samband med behandlingen av personuppgifter. Annars skulle de personer vars personuppgifter har lagrats berövas sin rätt enligt artikel 8.1 och 8.3 i

[215] Se domstolens dom av den 13 juli 1989, *Wachauf*, mål C-5/88, EU:C:1989:321, p. 18, och domstolens dom av den 13 april 2000, *Karlsson m.fl.*, mål C-292/97, EU:C:2000:202, p. 45.
[216] EDPS 2017 (a), s. 4. Se även Lenaerts 2019, s. 781.
[217] Lenaerts 2019, s. 786.
[218] Domstolens dom av den 6 oktober 2015, *Schrems*, mål C‑362/14, EU:C:2015:650, p. 95.
[219] Förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*, p. 39.
[220] Förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*, p. 40.
[221] Lenaerts 2019, s. 781 och 786–788.

> stadgan att vända sig till de nationella tillsynsmyndigheterna med begäran om skydd för sina personuppgifter.[222]

Begränsningen måste enligt artikel 52(1) kunna motiveras i förhållande till ett allmänt samhälleligt intresse. Denna begränsning ger nationella myndigheter en viss prövningsmarginal, vars omfattning beror inte bara på det eftersträvade legitima målets art utan också på inskränkningens specifika karaktär.[223] Målet med ett allmänt samhälleligt intresse agerar som en bakgrund mot vilken åtgärdens nödvändighet kan bedömas. Det är därför viktigt att identifiera målet i tillräcklig detalj för att senare möjliggöra bedömningen av åtgärdens nödvändighet. Alternativt kan en inskränkning även vara berättigad vid behov av skydd för andra människors rättigheter och friheter och EU-domstolen har t.ex. behandlat situationer där den balanserat dataskyddet mot andra rättigheter.[224] Individens säkerhet erkänns inte i stadgan, men utgör ett gemensamt mål för EU, och bl.a. artikel 67(3) FEUF föreskriver att:

> Unionen ska verka för att säkerställa en hög säkerhetsnivå genom förebyggande och bekämpning av brottslighet, rasism och främlingsfientlighet, genom åtgärder för samordning och samarbete mellan polismyndigheter och straffrättsliga myndigheter och andra behöriga myndigheter samt ömsesidigt erkännande av domar och beslut i brottmål och, vid behov, genom tillnärmning av den straffrättsliga lagstiftningen.

Nödvändighet och proportionalitet är väsentliga kumulativa krav som all behandling av personuppgifter måste uppfylla. Ifall nödvändighetstestet uppfylls kan man gå vidare till att bedöma proportionaliteten i en åtgärd. Det bör understrykas att nödvändighet och proportionalitet, även om villkoren är nära kopplade till varandra och bägge kriterierna måste uppfyllas i lagstiftningen, innebär två separata test. Domstolen kan dock bedöma kriterierna parallellt.[225] I det fall utvärderingen av en åtgärd inte uppfyller nödvändighets-testet finns det ofta inget behov av att undersöka dess proportionalitet. EU-domstolen har i sina senaste avgöranden inte gått vidare till att bedöma proportionaliteten i en begränsning av stadgans artikel 7 och 8 efter att ha konstaterat att begränsningen inte har

[222] Domstolens dom av den 21 december 2016, *Tele2 Sverige*, förenade målen C-203/15 och C-698/15, ECLI:EU:C:2016:970, p. 123. För ett liknande resonemang se förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*, p. 68, och mål C‑362/14, *Schrems*, p. 41 och 58.
[223] Europadomstolens dom i mål *Leander mot Sverige*, p. 59.
[224] Mifsud Bonnici 2014, ss. 136–137.
[225] EDPS 2017 (a), s. 5.

varit strikt nödvändig.[226] I artikel 8(2) i Europakonventionen föreskrivs utöver detta kriterium att begränsningen också måste vara ”nödvändig i ett demokratiskt samhälle”. Även om artikel 52(1) inte använder samma språkbruk, är kriteriet på ett demokratiskt samhälle en beståndsdel av EU:s rättsordning eftersom det härrör sig från EU:s grundläggande värderingar, som inkluderar respekten för demokrati i artikel 2 FEU.[227]

Nödvändighetstestet innebär en kombinerad, faktabaserad bedömning av åtgärders effektivitet i förhållande till det eftersträvade målet och en övervägning om den valda åtgärden är mindre påträngande i jämförelse med andra alternativa åtgärder som kunde uppnå samma mål.[228] Dessa punkter bör tydligt framgå i en konsekvensbedömning.[229] Nödvändighet utgör också en datakvalitetsprincip och är ett återkommande villkor i krav på laglighet i behandlingen av personuppgifter i EU:s sekundärlagstiftning.[230] EU-domstolen har uttalat ett krav på strikt nödvändighet vid varje undantag eller begränsning av skyddet av personuppgifter vilket illustreras i målet *Digital Rights Ireland*: ”Enligt domstolens fasta praxis kräver skyddet av den grundläggande rätten till respekt för privatlivet under alla omständigheter att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt.”[231] Det följer av EU-domstolens rättspraxis att villkoren för strikt nödvändighet är horisontella, och gäller oavsett det aktuella området, även för den brottsbekämpande sektorn.[232] Även om det antagits sektorspecifika regler, bl.a. genom polisdirektivet, motiverar detta inte en annorlunda bedömning av nödvändighet. Europadomstolen tillämpar ett strikt nödvändighetstest enligt en *in casu* bedömning.[233] Kravet på strikt nödvändighet har ytterligare konsekvenser eftersom domstolsprövningen av åtgärderna följaktligen också

[226] Se t.ex. domstolens resonemang i förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*, p. 46, 65, 69 och mål C‑362/14, *Schrems*, p. 92–93, 98.
[227] EDPS 2017 (a), s. 6.
[228] EDPS 2017 (a), s. 5.
[229] En konsekvensbedömning ingår i förarbetet till kommissionens lagförslag för initiativ som kan få stora effekter för ekonomin, samhället eller miljön och bidrar således till beslutsunderlaget.
[230] EDPS 2017 (a), s. 5. Se GDPR artikel 5(1)(c) och 6(1) samt skäl 49, polisdirektivet artikel 8(1), förordning 45/2001 artikel 4(1)(c) och 5.
[231] Förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*, p. 52. Se även mål C‑362/14, *Schrems*, p. 92 och förenade målen C-92/09 och C-93/09, *Volker*, p. 86.
[232] EDPS 2017 (a), s. 7.
[233] EDPS 2017 (a), s. 7. Europadomstolens dom av den 12 januari 2016 i mål *Szabó och Vissy mot Ungern*, 37138/14, p. 73.

är strikt, med beaktande av ingreppets beskaffenhet och allvar, vilket medför att lagstiftarens skönsmässiga bedömning begränsas.[234]

Sammanfattningsvis kan det konstateras att inskränkningar i dataskyddet bör stödjas av bevis som beskriver problemet som åtgärden avser adressera, hur detta kommer genomföras och varför befintliga eller mindre påträngande åtgärder inte räcker till för att behandla problemet. En analys av domstolarnas rättspraxis indikerar att nödvändighet i dataskyddslagstiftningen är ett faktabaserat begrepp snarare än ett abstrakt rättsligt begrepp, och att det bör beaktas mot bakgrund av de specifika omständigheterna kring ett mål liksom det konkreta syftet det ämnar uppnå.[235]

Proportionalitet utgör en allmän princip i EU-rätten. I artikel 5(4) FEU fastställs: ”Enligt proportionalitetsprincipen ska unionens åtgärder till innehåll och form inte gå utöver vad som är nödvändigt för att nå målen i fördragen.” Proportionalitet kräver i huvudsak att en åtgärd som inskränker en grundläggande rättighet inte ska gå längre än nödvändigt för att uppnå det legitima mål som eftersträvas. Kärnan i proportionalitetsbegreppet utgörs av en balansövning där en avvägning mellan styrkan av en begränsning och vikten eller legitimiteten av det mål som ska uppnås i det givna sammanhanget sker.[236] I *Volker* fastställde domstolen att ”åtgärder som medför mindre långtgående ingrepp i denna grundläggande rättighet för fysiska personer, men vilka ändå på ett effektivt sätt bidrar till att målen med unionslagstiftningen i fråga uppnås”[237] ska eftersträvas. Detta begränsar således myndigheterna i utövandet av deras befogenheter genom att kräva en balans mellan de använda medlen och det avsedda målet.[238] I målen *Z. mot Finland* och *S. & Marper mot Storbritannien* behandlade Europadomstolen frågan om proportionalitet inom området för personlig integritet. I *S. & Marper* ansåg sökandena att polisens lagrande av deras biometriska uppgifter utgjorde en orättfärdig begränsning av artikel 8 i Europakonventionen.[239] I *Z. mot Finland* handlade begränsningen om att den sökandes

[234] Förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*, p. 47–48.
[235] EDPS 2017 (a), s. 8.
[236] EDPS 2019, s. 11.
[237] Förenade målen C-92/09 och C-93/09, *Volker*, p. 86.
[238] Se förenade målen C-92/09 och C-93/09, *Volker*, p. 74 samt förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*, p. 47.
[239] Europadomstolens dom av den 4 december 2008 i mål *S. och Marper mot Storbritannien*, 30562/04 och 30566/04.

personliga information offentliggjorts.[240] De faktorer som Europadomstolen beaktade i fallen visar på ett brett spektrum av faktorer som kan vara relevanta vid bedömningen av en åtgärds proportionalitet. I *S. & Marper* fastställde domstolen att lagligheten för åtgärderna krävde förekomsten av tydliga, detaljerade regler, som reglerar omfattningen och tillämpningen av åtgärder, liksom förekomsten av minimisäkerhetsåtgärder som hänför sig till bland annat varaktighet, lagring och användning av uppgifter och därmed tillhandahåller tillräckliga garantier mot risken för missbruk och godtycke.[241] Domstolens tolkning i synnerhet i *S. & Marper* tyder på att massövervakning, även om den kan visa sig uppfylla ett legitimt mål, troligtvis inte uppfyller proportionalitetsaspekten av att vara nödvändigt i ett demokratiskt samhälle.[242]

Ett proportionalitetstest innebär i allmänhet en bedömning av vilka skyddsåtgärder som ska åtföljas av en åtgärd för att minimera de risker som den planerade åtgärden innebär för de berörda rättigheterna till en proportionell nivå.[243] En annan faktor som ska beaktas vid bedömningen av proportionaliteten hos en föreslagen åtgärd är, i likhet med nödvändighetstestet, effektiviteten hos befintliga åtgärder utöver den föreslagna åtgärden.[244] Utan en sådan bedömning av effektiviteten hos befintliga åtgärder som strävar efter samma eller ett liknande syfte kan proportionalitetstestet för en ny åtgärd inte anses ha utförts vederbörligen.[245]

3.3.2 EU-domstolens minimikrav på skyddsåtgärder

Förutom att såväl EU:s institutioner som medlemsstater måste ta hänsyn till den omfattande regleringen av dataskydd som tryggas individer inom unionen måste allt agerande också vara förenligt med de principer som utvecklats i rättspraxis från EU-domstolen och Europadomstolen. Unionen har en aktiv skyldighet att säkerställa allas rätt till integritet och dataskydd inom dess område och ansvarar för att detta resultat uppfylls. EU-domstolen blir en viktig aktör för att övervaka denna uppgift. Domstolens handlande särskilt inom området med frihet, säkerhet och rättvisa bör belysas. Sedan Lissabon-

[240] Europadomstolens dom av den 25 februari 1997 i mål *Z. mot Finland*, 22009/93.
[241] Harris & O'Boyle & Bates & Buckley 2014, s. 560.
[242] Europadomstolens dom i mål *S. och Marper mot Storbritannien*, p. 119.
[243] EDPS 2019, ss. 10–11.
[244] Se WP29 2014, s. 9.
[245] EDPS 2019, s. 11.

fördragets ikraftträdande utgör också EU-domstolen en av de institutioner vars befogenheter har ökat. Tidigare hade domstolen en begränsad roll i de frågor som föll inom området för EU:s mellanstatliga pelare, medan domstolen idag besitter behörighet även i tolkningen av frågor som förut tillhörde den tredje pelaren, numera området för frihet, säkerhet och rättvisa.[246] EU-domstolen är den slutliga tolkaren av EU:s rättsakter och har redan före Lissaboneran varit den största bidragande faktorn till framväxten av grundläggande rättigheter i EU-lagstiftningen. Domstolen är således inte bara en instans för tvistelösning, utan bär även drag av en konstitutionell domstol, vars roll innebär en balansering mellan unionens och medlemsstaternas befogenheter och utvecklandet av konstitutionella principer för domstolsprövning.[247] Vid utövandet av denna roll har domstolen ofta uppfattats som aktivistisk.[248] Denna aktivistiska roll kvalificerar domstolen som en lämplig aktör för tolkningen av skyddet av integritet och datarättigheter inom området med frihet, säkerhet och rättvisa där de grundläggande rättigheterna utmanas bl.a. av aktiviteternas gränsöverskridande karaktär.

Genom förhandsavgöranden har EU-domstolen fastställt vägledande principer angående processuella och materiella villkor för brottsbekämpande myndigheters åtkomst-möjligheter och behandling av personuppgifter. Speciellt domstolens uttalanden i avgörandet *Digital Rights Ireland*, vilka senare upprepats och preciserats i den efterföljande domen *Tele2 Sverige*, har utstakat tydliga ramar som behöver uppfyllas för att brottsbekämpande myndigheters behandling av personuppgifter kan anses vara befogad och i enlighet med etablerade dataskyddsprinciper. I rättsfallen har EU-domstolen integrerat principer som utformats av Europadomstolen i dess tidigare avgöranden rörande dataskydd. I båda avgörandena har kraven på proportionalitet och nödvändighet haft en vägande påverkan i domstolens slutsats att fastställa en inskränkning av dataskyddet.[249] Inom ramen för proportionalitetsanalysen försökte EU-domstolen i målen säkerställa jämvikten mellan å ena sidan allmän säkerhet och å andra sidan integritet och dataskydd och beslutade slutligen att balansen skulle lutas mot det

[246] Hijmans 2016, s. 56.
[247] Hijmans 2016, s. 169.
[248] Hijmans 2016, s. 170.
[249] Jasserand-Breeman 2019, s 160. Till liknande slutsatser har EU-domstolen kommit även i sitt yttrande 1/15 om avtalet om PNR-uppgifter mellan EU och Kanada. Se EU-domstolens yttrande 1/15 av den 26 Juli 2017, ECLI:EU:C:2017:592.

senare.[250] I *Digital Rights Ireland* och *Tele2 Sverige* undersökte EU-domstolen lagenligheten i lagstiftning som förpliktade teleoperatörer att lagra och möjliggöra sekundär åtkomst till personuppgifter i form av metadata som samlats in för teleoperatörers eget bruk. För avhandlingens frågeställning ligger fokuset inte på datalagringens laglighet utan snarare på vilka regler och principer som styr brottsbekämpande myndigheters åtkomstmöjligheter till sådana uppgifter. Dessa uttalanden återspeglar grundläggande principer som måste beaktas för alla typer av jämförbara åtgärd i EU-lagstiftning.[251] Domstolen fastställde att även i fall med kopplingar till terrorism och grov brottslighet kan grundläggande rättigheter inte kompromissas till den grad att data lagras på ett allmänt och massartat sätt i syfte att erbjuda brottsbekämpande myndigheter tillgång till uppgifterna.[252]

I båda rättsfallen tog domstolen fasta vid att behandlingen av personuppgifterna innebar ett ingrepp i de grundläggande rättigheterna för ett mycket stort antal individer.[253] Allvaret i inskränkningen härrör sig från mängden uppgifter som lagras i storskaliga databaser.[254] Enligt EU-domstolen kan ”den omständigheten att lagringen av uppgifterna och den senare användningen av dem sker utan att abonnenten eller den registrerade användaren är underrättad om detta ge de berörda personerna en känsla av att deras privatliv står under ständig övervakning”.[255] I samstämmighet med Europadomstolens praxis ansåg EU-domstolen att varje insamling, användning och överföring av personuppgifter till en annan myndighet utgör en ny inskränkning av grundläggande rättigheter och ska därför också motiveras med en separat orsak.[256] Insamlingen av personuppgifter utgör alltså en första inskränkning men varje påföljande aktivitet måste också motiveras. Behandlingen av uppgifter för brottsbekämpande ändamål är en mycket känslig fråga och kan ha en allvarlig inverkan på de berörda individernas liv. Risken för stigmatisering till följd av införandet av uppgifter i databaser för brottsbekämpningsändamål, som var föremål för Europadomstolens granskning i fallet *S.*

[250] Brkan 2016, s. 825.
[251] Boehm & Cole 2014, s. 27.
[252] För ett liknande resonemang se mål C-362/14**,** *Schrems.*
[253] Förenade målen C-293/12 och C-594/12*, Digital Rights Ireland*, p. 56 samt förenade målen C-203/15 och C-698/15, *Tele2 Sverige*, p. 97.
[254] Boehm & Cole 2014, s. 31.
[255] Förenade målen C-293/12 och C-594/12*, Digital Rights Ireland*, p. 37.
[256] Förenade målen C-293/12 och C-594/12*, Digital Rights Ireland*, p. 35.

och Marper, måste övervägas och bör beaktas vid granskning av andra befintliga eller planerade åtgärder för datalagring på EU- och medlemsstatsnivå.

EU-domstolen har i sin praxis utvecklat krav på specifika skyddsåtgärder. Detta balanserande element är en del av domstolens proportionalitetstest. Domstolen har yttrat ett krav på att det ska finnas en skälig misstanke om delaktighet i terroristbrott eller allvarlig brottslighet.[257] Domstolen fastställde också att åtkomsten till uppgifter måste vara explicit begränsad till ändamålet att bekämpa grov brottslighet.[258] Samtidigt måste nationell lagstiftning erbjuda objektiva kriterier för att avgränsa behöriga nationella myndigheters tillgång till uppgifter och deras senare användning.[259] Med beaktande av kravet på ändamålsbegränsning utgör en allmän hänvisning till allvarliga brott en otillräcklig åtgärd eftersom detta inte definieras i EU-lagstiftningen utan lämnas till medlemsstaterna att reglera.[260] Domstolen har uttalat att ”nödvändigheten av sådana garantier är av än större betydelse när personuppgifterna [...] är föremål för automatisk behandling och risken för otillåten tillgång till uppgifterna är stor”.[261] Följaktligen måste all databehandling inte bara begränsas till det som är absolut nödvändigt utan måste också följa regler som garanterar ett effektivt skydd av uppgifterna. Domstolen förväntar sig regler som ”gör det möjligt att säkerställa ett effektivt skydd av de lagrade uppgifterna mot riskerna för missbruk och otillåten tillgång eller användning” och de ska ”på ett tydligt och strängt sätt reglera skyddet av uppgifterna och deras säkerhet i syfte att säkerställa fullständig integritet och konfidentialitet för uppgifterna”.[262] Domstolen lyfte fram kravet på att uppgifter är underkastade förhandskontroll av en domstol eller en oberoende myndighet.[263] I *Tele2 Sverige* införde domstolen ytterligare en skyddsåtgärd i from av krav på att behöriga brottsbekämpande myndigheter informerar de berörda

[257] Förenade målen C-293/12 och C-594/12*, Digital Rights Ireland,* p. 57–58 samt förenade målen C-203/15 och C-698/15, *Tele2 Sverige*, p. 60. Se även EU-domstolens yttrande 1/15, p. 172.
[258] Förenade målen C-293/12 och C-594/12*, Digital Rights Ireland,* p. 59 samt p. 61 och förenade målen C-203/15 och C-698/15, *Tele2 Sverige*, p. 102.
[259] Förenade målen C-293/12 och C-594/12*, Digital Rights Ireland*, p. 60 samt förenade målen C-203/15 och C-698/15, *Tele2 Sverige*, p. 117.
[260] Förenade målen C-293/12 och C-594/12*, Digital Rights Ireland*, p. 60
[261] Förenade målen C-293/12 och C-594/12*, Digital Rights Ireland*, p 55. Se även Europadomstolens dom i mål *S. och Marper mot Storbritannien*, p. 103 och Europadomstolens dom i mål *M.K. mot Frankrike*, p. 35.
[262] Förenade målen C-293/12 och C-594/12*, Digital Rights Ireland*, p. 66.
[263] Förenade målen C-293/12 och C-594/12*, Digital Rights Ireland*, p. 62 samt förenade målen C-203/15 och C-698/15, *Tele2 Sverige*, p. 120 och EU-domstolens yttrande 1/15, p. 202.

personerna om behandlingen av deras personuppgifter, i enighet med nationella förfaranden, så fort en sådan upplysning inte längre riskerar att skada myndigheternas utredningar.[264]

Kravet på en koppling till allvarlig brottslighet klargjordes i EU-domstolens avgörande *Ministerio Fiscal* där definitionen av allvarlig brottslighet utvecklades ytterligare.[265] Domstolen fastställde att då brottsbekämpande myndigheters tillgång till personuppgifter inte kan anses innebära ett allvarligt ingrepp i de grundläggande rättigheterna för de registrerade, kan ingreppet och tillgång till sådana uppgifter motiveras av målet att förebygga, utreda, upptäcka och lagföra brottsliga gärningar i allmänhet, utan att det är nödvändigt att dessa brott definieras som allvarliga.[266] ”Syftet med en lagstiftning måste stå i proportion till hur allvarligt ingrepp i de grundläggande rättigheterna i fråga åtgärden innebär”.[267]

EU-domstolens rättspraxis visar en tydlig hållning i fråga om brottsbekämpande myndigheters åtkomsträttigheter vid sekundär användning av personuppgifter. Förutom att domstolen har varit tydlig med att uttala faror och risken för stigmatisering i koppling till dessa fall har domstolen utstakat strikta krav för att dessa processer skall anses lagliga. Domstolen har fastställt tydliga krav på specifika skyddsåtgärder som bör betraktas som allmängiltiga principer vid behandling av personuppgifter för brottsbekämpande ändamål. För att summera omfattar dessa principer följande punkter:

1. All typ av behandling såsom insamling, lagring och användning av personuppgifter innebär sådana åtgärder som utgör en inskränkning av rätten till dataskydd och kräver därför uppfyllandet av ett strikt nödvändighets- och proportionalitetstest.

2. Domstolen förkastar tydligt massinsamling av oskyldiga individers personuppgifter och ser ett känsligt problem i att uppgifter som ursprungligen samlats in för andra ändamål senare används för brottsbekämpningsändamål.

[264] Förenade målen C-203/15 och C-698/15, *Tele2 Sverige*, p. 121.
[265] Domstolens dom av den 2 oktoker 2018, *Ministerio Fiscal,* mål C-207/16, *ECLI:EU:C:2018:788.*
[266] Mål C-207/16, *Ministerio Fiscal*, p. 54–61.
[267] Mål C-207/16, *Ministerio Fiscal*, p. 54–61. För ett liknande resonemang, se förenade målen C-203/15 och C-698/15, *Tele2 Sverige*, p. 115.

3. Det krävs en koppling mellan ett hot mot den allmänna säkerheten och de personuppgifter som lagras för sådana ändamål. Brottsbekämpande myndigheter har enbart tillåtelse till åtkomst för personuppgifter som samlats in för andra ändamål i särskilda fall.

4. Domstolen kräver uttryckligen effektiva skyddsåtgärder som oberoende tillsyn och rätt till information, åtkomst och rättelse av felaktiga uppgifter för den registrerade.

4 ÄNDAMÅLSBEGRÄNSNING SOM SKYDDSÅTGÄRD FÖR DE REGISTRERADES RÄTTIGHETER

4.1 Principen om ändamålsbegränsning

Ändamålsbegränsning utgör en av dataskyddets hörnstenar och innebär en väsentlig skyddsåtgärd mot missbruk av personuppgifter.[268] Med ökade möjligheter att använda data på multifunktionella sätt förstärks rollen och betydelsen av ändamålsbegränsning vid uppgiftsbehandling. Detta är inte minst fallet för de ökade och förenklade möjligheterna till uppgiftsåtkomst som interoperabilitetsramen medför. Principens exakta innehåll och de kriterier som bör tas i beaktande är svår att fastställa på ett schablonartat sätt. En väsentlig fråga utgörs av under vilka förhållanden den sekundära behandlingen av dessa uppgifter är kompatibel eller oförenlig med det första behandlingsändamålet. Både EU-domstolen och Europadomstolen har varit fåordiga vad beträffar uttalanden om ändamålsbegränsningens faktiska innebörd. För att förstå ändamålsbegränsningens funktion i ett interoperabilitetssammanhang krävs en djupare förståelse av principens innebörd. Mot bakgrund av detta blir det nödvändigt att undersöka vilka krav som fastställs i EU:s sekundärlagstiftning, vilken juridisk funktion ändamålsbegränsning har i vårt digitala samhälle och särskilt hur WP29 har tolkat principens innebörd. Arbetsgruppen har uttryckt att en av de farligaste fallgroparna kopplad till ändamålsbegränsning är att avvisa eller försvaga konceptet bara för att den databehandlingsmiljö som vi lever i har förändrats och för att det innebär en utmaning för registeransvariga att tillämpa ett giltigt koncept på en förändrad verklighet.[269] Eftersom behandlingen av personuppgifter påverkar inskränkande på individers grundläggande rättigheter bör den begränsas, vilket även innebär ett krav på begränsning av behandlingens ändamål.

Ändamålsbegränsning skyddar registrerade genom att sätta gränser för hur personuppgiftsansvariga kan använda deras data, samtidigt som principen erbjuder en viss grad av flexibilitet för de personuppgiftsansvariga.[270] Principen syftar till att säkerställa att skälen för personuppgifters användning är tydliga redan från deras

[268] WP29 2013, s. 4.
[269] WP29 2013, s. 13.
[270] WP29 2013, s. 3.

insamlingstidpunkt och att behandlingen av uppgifterna ligger i linje med de registrerades rimliga förväntningar. På så vis bidrar ändamålsbegränsning till upprätthållandet av allmänhetens förtroende och rättssäkerhet, samtidigt som den utgör en förutsättning för andra dataskyddsprinciper.[271] Genom att tillämpa principen förebyggs funktionskryp, där tillgängliga uppgifter används utöver de syften som de initialt samlats in för. Enbart det faktum att personuppgifter finns tillgängliga rättfärdigar därmed inte att de kan användas för nya ändamål, eftersom en sådan ny behandling kan innebära en större inverkan på individers rättigheter.[272] Principen är starkt kopplat till kraven på öppenhet, förutsebarhet och användarkontroll, eftersom då syftet med behandlingen är tillräckligt specifikt och tydligt utstakat, vet individer också vad de kan förvänta sig och öppenheten och rättssäkerheten förbättras.[273] Samtidigt är en tydlig avgränsning av syftet viktig för att göra det möjligt för de registrerade att effektivt utöva sina rättigheter, bl.a. genom rätten att invända mot behandlingen.[274] Eftersom ändamålsbegränsningen ligger till grund för andra principers effektiva efterföljande medför principen en samling olika standarder som personuppgiftsansvariga bör ta hänsyn till, inklusive tidsbegränsningar för lagring av data och begränsningar med avseende på kvaliteten och relevansen av den information som samlas in eller lagras.[275]

Principen finns uttryckt både i dataskyddsförordningen och polisdirektivet. I regelverken fastställs i identiska termer i artikel 5(1)(b) GDPR respektive artikel 4(1)(b) i polisdirektivet att personuppgifter ”ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål”. Ändamålsbegränsning har fastställts bestå av två olika element. För det första måste data samlas in inom ramen för särskilda, uttryckligt angivna och berättigade ändamål, vilket utgör ett krav på ändamålsspecifikation.[276] Dessa ändamål utgör databehandlingens *raison d’être*.[277] För det andra får data inte i ett senare skede behandlas på ett sätt som är oförenligt med dessa ändamål, vilket utgör ett krav på kompatibilitet.[278]

[271] Hit hör bl.a. kraven på laglighet, korrekthet och öppenhet i GDPR, artikel 5(1)(a), korrekthet i artikel 5(1)(d) samt lagringsminimering i artikel 5(1)(e).
[272] EDPS 2017 (c), skäl 33.
[273] FRA 2018 (c), s. 122.
[274] FRA 2018 (c), s. 122.
[275] Brouwer 2011, s. 273.
[276] WP29 2013, s. 11.
[277] WP29 2013, s. 11.
[278] WP29 2013, s.12.

Dessa krav är kumulativa till sin natur vilket innebär att både kravet på specifikation och kravet på kompatibilitet bör uppfyllas för att behandlingen av personuppgifter ska anses lagenlig.

Det första kravet på särskilda ändamål föreskriver att databehandlingens syften specificeras tillräckligt noggrant. Detta innebär att ändamålen är tillräckligt definierade för att kunna avgöra vilken typ av behandling som ingår och inte ingår i det angivna syftet, och för att möjliggöra att överensstämmelse med lagen kan bedömas och nödvändiga skyddsåtgärder tillämpas.[279] Specifikationen bör ske senast vid den tidpunkt då insamlingen av personuppgifter sker. Detta framkommer bl.a. i GDPR skäl 39 som fastställer att ”de specifika ändamål som personuppgifterna behandlas för bör vara tydliga och legitima och ha bestämts vid den tidpunkt då personuppgifterna samlades in”. Ändamålet för uppgiftsbehandlingen ska inte stå klart enbart för den personuppgiftsansvariga utan det ska även vara tydligt uttryckt samt otvetydigt till sitt innehåll. Detta innebär att bearbetningen inte bör innehålla några dolda syften.[280] Kravet är dock distinkt från individens rättighet till information av den personuppgifts-ansvariga.[281] Personuppgifter kan samlas in för fler än ett ändamål. I vissa fall är dessa ändamål, även om de är distinkta, relaterade till varandra. I de fall där olika syften existerar från början och olika typer av data samlas in och behandlas samtidigt för växlande ändamål måste datakvalitetskraven följas upp separat för varje ändamål.[282] Således bör det understrykas att alla uppgifter som samlats in för ett specifikt ändamål och uppfyller de uppställda kraven inte alltid kan anses vara relevanta och nödvändiga i förhållande till andra ändamål, definierade vid tidpunkten för den ursprungliga insamlingen eller vid ett senare tillfälle.

Slutligen kräver ändamålsspecifikation att personuppgifter samlas in för ett legitimt ändamål, vilket förutsätter att behandlingen i alla stadier baseras på åtminstone en av de rättsliga grunder som föreskrivs i GDPR artikel 6. Kravet på legitimitet är emellertid bredare än räckvidden för artikeln, och inbegriper att syftet är i överensstämmelse med

[279] WP29 2013, s. 15.
[280] WP29 2013, s. 17.
[281] För information som ska tillhandahållas om personuppgifterna samlas in från den registrerade se GDPR, artikel 13(1)(c), 13(3), 14(1)(c) samt 14(4). För individens rätt till information se artikel 15(1)(a).
[282] WP29 2013, s. 16.

alla bestämmelser i tillämplig dataskyddslagstiftning samt andra tillämpliga lagar.[283] Legitimitetskravet innebär därmed att ändamålen måste vara förenliga med lagen i dess vidare mening. Det är möjligt att legitimiteten för ett visst ändamål förändras över tid, beroende på vetenskaplig och teknisk utveckling samt förändringar i samhället och kulturella attityder.[284] I regel är en individ i en svagare position i förhållande till en myndighet då denna verksamhet baseras på lagstiftning och kräver således inte individens samtycke. Individers uppfattning av offentliga myndigheters legitimitet är dock en viktig funktion av lagligheten som gäller även för staters befogenheter kopplade till uppgiftsbehandling. Allmänheten tenderar att acceptera den offentliga maktens befogenheter i den mån denna makt inte anses missbrukas.[285] Denna aspekt av legitimitet är nära besläktad med kriterierna som formulerats i Europadomstolens rättspraxis med avseende på lagens förutsebarhet.[286]

Kravet på kompatibilitet utgör den andra delen av principen och innebär att personuppgifter inte senare får behandlas på ett sätt som är oförenligt med de initiala ändamålen. Principen skiljer således mellan den första behandlingsoperationen, som består av insamling av uppgifter, och andra efterföljande bearbetningsoperationer. All bearbetning efter den initiala insamlingen, vare sig den sker för de ursprungligen angivna ändamålen eller för ytterligare ändamål, måste betraktas som vidare bearbetning och bör därmed uppfylla kravet på kompatibilitet.[287] Förbudet är formulerat på ett sätt där lagstiftaren inte ställer ett direkt krav på förenlighet med de initiala ändamålen utan istället föreskriver ett förbud mot oförenlighet. WP29 menar att lagstiftaren, genom att föreskriva att all ytterligare behandling är godkänd så länge den inte klassas som oförenlig, avser ge personuppgiftsansvariga en viss flexibilitet när det gäller sekundär användning av personuppgifter, och understryker att den ytterligare behandlingen som utförs för ett annat syfte inte nödvändigtvis innebär att behandlingen automatiskt skulle vara oförenlig.[288] Detta måste bedömas från fall till fall. EU:s dataskyddslagstiftning förbjuder således inte fullständigt användningen av uppgifter för andra ändamål än de

[283] WP29 2013, ss. 19–20.
[284] WP29 2013, s. 20.
[285] Brouwer 2011, s. 290.
[286] Brouwer 2011, s. 290. Se Europadomstolens krav på förutsebarhet i avhandlingens kapitel 3.3.1.
[287] WP29 2013, s. 21.
[288] WP29 2013, s. 21.

som de samlats in för, men ställer vissa begränsningar på sådan användning. I vissa situationer kan extra flexibilitet behövas för att möjliggöra en förändring av räckvidd eller fokus i situationer där samhällets eller de registrerades förväntningar har förändrats.[289]

Ändamålsbegränsningen kan endast begränsas i enlighet med de villkor som anges i artikel 23 GDPR. I artikel 23(1) föreskrivs att ”det ska vara möjligt att i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige eller personuppgiftsbiträdet omfattas av införa en lagstiftningsåtgärd som begränsar tillämpningsområdet för de skyldigheter och rättigheter som föreskrivs”. Begränsningen måste dock ske ”med respekt för andemeningen i de grundläggande rättigheterna och friheterna” samt utgöra ”en nödvändig och proportionell åtgärd i ett demokratiskt samhälle”,[290] med syftet att säkerställa bl.a. allmän säkerhet,[291] ”förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten”,[292] samt skydd av den registrerade eller andras rättigheter och friheter.[293] Artikel 23(2) föreskrivs dock krav på specifika bestämmelser i lagstiftningsåtgärderna.

Ovan utförda granskning visar att ändamålsbegränsningen uppfyller både en autonom och en villkorlig funktion. Den autonoma funktionen fungerar som en förutsättning för den villkorliga funktionen och ställer krav på att personuppgifter samlas in för specifika, uttryckliga och legitima syften och inte behandlas vidare på ett sätt som är oförenligt med dessa syften. Principens villkorliga funktion utgörs av dess koppling till andra dataskyddsprinciper och blir då en förutsättning för andra skyddsåtgärder som datakvalitet, uppgiftsminimering och ansvarsskyldighet. Som en följd av denna dubbla funktion resulterar urvattningen av principen om ändamålsbegränsning i en urvattning av flera relaterade dataskyddsprinciper.

4.2 Ändamålsbegränsning och rättsstatsprincipen

[289] WP29 2013, s. 21.
[290] GDPR, artikel 23(1).
[291] GDPR, artikel 23(1)(c).
[292] GDPR, artikel 23(1) (d).
[293] GDPR, artikel 23(1) (i).

Rättsstatsprincipen utgör ett av EU:s mest grundläggande värden som hela unionssamarbetet grundas på. Dess betydelse fastställs bland annat i artikel 2 FEU samt i stadgan. Principen innebär att myndigheter i sitt agerande styrs av bindande regler som fastslagits på förhand i enlighet med etablerade lagstiftningsförfaranden, vilket möjliggör för individer att med skälig säkerhet förutspå hur myndigheter kommer att använda sig av offentlig makt och därmed planera sitt agerande efter denna vetskap.[294] En kränkning av rättsstatsprincipen innebär ett minskande förtroende hos individer för att deras rättigheter tillgodoses. Rättsstatsprincipen kräver inte bara att en uppsättning formella principer efterföljs, utan i de flesta, om inte alla europeiska konstitutionella traditioner, tolkas rättsstatsprincipen av domstolar som ett krav på att offentlig maktutövning är föremål för såväl processuella som materiella begränsningar.[295]

Ändamålsbegränsning som dataskyddsprincip bygger på värderingar som transparens och att binda ansvarspersoner som registeransvariga till förutbestämda regler. Principen kräver genom ändamålsspecifikation på förhand insyn i planerade avsikter och genom kompatibilitet bundenhet till förutbestämda villkor. Ändamålsbegränsning främjar tanken om maktdelning genom åtskiljandet av olika databehandlingsprocesser. Dessa krav visar därmed en nära koppling till rättsstatsprincipen. På samma sätt som det finns en befogad förväntning att de offentliga myndigheternas funktionella befogenheter beskrivs i lagregler är det också nödvändigt att ha tydliga regler för vilken myndighet som kan samla in eller använda sig av vilken slags information. Detta blir av synnerlig vikt i ett interoperabelt sammanhang med ett flertal aktiva aktörer. I nära anslutning till idén om maktfördelning inom den statliga förvaltningen ligger begreppet ’informativ maktfördelning’ (jämför engelskans *informational division of powers*).[296] Konceptet är av tyskt ursprung och förankrar sig i den administrativa organisationens oro för konsekvenserna av den tidiga informationsteknologin i förvaltningens ömsesidiga relationer.[297] Den informativa maktfördelningen reflekteras i dataskyddets princip om ändamålsbegränsning. Ett av de viktigaste syftena med ändamålsbegränsning är begränsningen av befogenheter genom informativ maktfördelning och att skydda

[294] Se Europarådet 2016, Venedigkommssionens rapport.
[295] Pech 2019, s. 54.
[296] Brouwer 2008, s. 201.
[297] Brouwer 2008, s. 201. Se även von Grafenstein 2018, s. 145.

individer mot missbruk av makt och godtycklighet. Att i förväg definiera de syften för vilka personuppgifter kan användas förhindrar att personlig information som förvärvas i ett specifikt sammanhang blir tillgänglig hos andra myndigheter, för andra syften.

Brouwer har gjort en koppling mellan dataskyddets ändamålsbegränsning och förbudet av *détournement de pouvoir* som utgör en del av EU:s förvaltningsrätt, samt rätten till god förvaltning.[298] Rätten till god förvaltning garanteras i stadgans artikel 41 och återspeglar enligt EU-domstolen en allmän princip som medlemsstaterna ska tillämpa i alla förfaranden.[299] Med beaktande av god förvaltning som ett av målen för dataskyddet bör individer ha en försäkran om att information som ges till en myndighet inte automatiskt är tillgänglig för andra myndigheter.[300] Med andra ord bör denna princip i viss utsträckning skydda den informativa maktfördelningen. Ett problem med regleringen av myndigheters befogenheter kopplad till den informativa maktfördelningen är att även om det ganska långt råder samstämmighet om substansen och vikten av dataskyddet, tillåter de tillämpliga reglerna många undantag. Detta innebär en risk att flera bestämmelser om dataskydd betraktas som icke bindande regler eller s.k. *soft law*. Det faktum att ändamålsbegränsning kan uppfattas på olika sätt i olika medlemsländer kan förstärka detta problem. Principen om ändamålsbegränsning motsvaras i Finland av ändamålsbundenhetsprincipen, och här betraktas ändamålsbundenhet som en så stark princip, att man med hänvisning till den kan få ett förvaltningsbeslut upphävt.[301] I övriga nordiska länder finner man också en motsvarighet till principen om ändamålsbegränsning, som verkar ha sitt ursprung i fransk förvaltningsrätt och principen om *détournement de pouvoir*.[302]

4.3 Sekundär användning av uppgifter för brottsbekämpande syften

Ändamålsbegränsning tolkas olika i ett brottsbekämpande sammanhang. Situationen blir ytterligare komplicerad då personuppgifter har samlats in i ett sammanhang som faller under dataskyddsförordningens reglering och sedan behandlas vidare för ett annat,

[298] Brouwer 2008, ss. 201–202. Se även Suksi 2015, ss. 528–531, angående *détournement de pouvoir* inom EU:s förvaltningsrätt.
[299] Förklaringar avseende stadgan om de grundläggande rättigheterna, förklaring till artikel 41, 51, EUT 2007 C 303/02, ss. 17–35. Se mål C‑604/12, *N.*, p. 49–50 och 52.
[300] Brouwer 2008, s. 202.
[301] Se Suksi 2015, s. 507.
[302] Suksi 2015, s. 532.

brottsbekämpande ändamål, under polisdirektivets reglering. Reglerna om dataskydd fördelas då mellan två distinkta rättsakter. Eftersom detta stycke fokuserar på den sekundära behandlingen av personuppgifter för brottsbekämpande ändamål och inte på deras initiala behandling, kan vi här anta att syftet med den första behandlingen uppfyller kriterierna för ändamålsspecifikation vilket diskuterats tidigare i texten.

I en situation där brottsbekämpande myndigheter får åtkomst till personuppgifter som i grunden samlats in för ett annat än ett brottsbekämpande syfte har det nya brottsbekämpande syftet oftast ingen länk till det initiala ändamålet. I dessa fall regleras ändamålsbegränsningen av polisdirektivets artikel 4(2). Enligt polisdirektivet följer den sekundära användningens legitimitet inte av ett kompatibilitetsavvägande baserat på flera olika faktorer, utan direktivet föreskriver att behandlingen är tillåten för andra ändamål då den baseras på unionens eller nationell lagstiftning, samt uppfyller kraven på nödvändighet och proportionalitet. I den finska lagstiftningen fastställer lagen om behandling av personuppgifter i brottmål (1054/2018) uttryckligen principen om ändamålsbegränsning i dess 5 § i enlighet med polisdirektivets artikel 4(2). I speciallagstiftningen inom området fastställs också ett krav på ändamålsbundenhet.[303]

Jasserand-Breeman har tagit fasta vid två problem kopplade till polisdirektivets artikel 4(2).[304] I artikeln stadgas i samband med sekundär användning för brottsbekämpande syften om när ”behandling som utförs av samma eller en annan personuppgiftsansvarig för något annat ändamål [...] än det för vilket personuppgifterna samlas in” är tillåten.[305] Formuleringen i artikeln har ansetts vara tvetydig och möjliggöra för en bred tolkning som innefattar all initial behandling av data vare sig den faller innanför eller utanför polisdirektivets tillämpningsområde. Det framkommer nämligen inte ifall den sekundära användningen av uppgifter som samlats in under dataskyddsförordningens regim innebär en första bearbetning eller en sekundär bearbetning vid dess vidare behandling under

[303] Se 46 § i lagen om behandling av personuppgifter i polisens verksamhet (616/2019); 3 § i lagen om behandling av personuppgifter vid Gränsbevakningsväsendet (639/2019); 3 § i lagen om behandling av personuppgifter inom Tullen (650/2019); 4 § i lagen om behandling av personuppgifter inom Försvarsmakten (332/2019).
[304] Jasserand-Breeman 2019, s 101.
[305] En lika otydlig formulering återfinns i motivet till polisdirektivet, skäl 29, som fastställer att ”om samma eller en annan personuppgiftsansvarig behandlar personuppgifter för ett ändamål som omfattas av detta direktiv men som inte är det ändamål som uppgifterna insamlades för”

polisdirektivet.[306] Därmed förblir det oklart ifall artikel 4(2) är tillämplig på sekundär behandling av sådana uppgifter som initialt samlats in för brottsbekämpande ändamål och sedan behandlas för ett ytterligare brottsbekämpande ändamål, eller om regeln ska tillämpas på uppgifter som från början samlats in för vilket som helst syfte, vilket inkluderar uppgifter som regleras av dataskyddsförordningen. Ifall artikeln tillämpas på uppgifter i det andra scenariot kan ändamålsbegränsningen fortfarande spela en roll som skyddsåtgärd. Ifall artikeln enbart tillämpas på uppgifter som samlats in för ett brottsbekämpande syfte tappar ändamålsbegränsningen sitt syfte.

Det andra problemet är att artikel 4(2) inte skapar någon som helst koppling mellan syftet med den första behandlingen och syftet med den sekundära behandlingen i enlighet med ändamålsbegränsningens krav på kompatibilitet.[307] Detta innebär en annan utgångspunkt än vad AW29 förespråkat i sitt yttrande 03/2013 där arbetgruppen även avseende brottsbekämpande myndigheters sekundära användning av personuppgifter utförde ett kompatibilitetstest, med beaktande av flera olika faktorer.[308] Hursomhelst innebär arbetsgruppens yttranden bara vägledande uttalanden och är inte bindande till sin natur. Det samma gäller dataskyddsstyrelsens ställningstaganden. I avsaknad av mer specifika föreskrifter verkar dessa regler i artikel 4(2) gälla oberoende av kompatibiliteten mellan de ursprungliga och sekundära syftena med behandlingen, förutsatt att de uppfyller kraven på nödvändighet och proportionalitet. Artikeln har i och med detta ansetts utgöra ett undantag från principen om ändamålsbegränsning i artikel 4(1)(b).[309]

Det faktum att EU har antagit en förordning som fastställer de allmänna reglerna för behandling av personuppgifter och ett direktiv med specifika regler som gäller för brottsbekämpande syften, innebär att det inte existerar några enhetliga skyddsregler inom området för EU:s dataskyddslagstiftning.[310] En förordning är effektivare för att uppnå harmonisering än ett direktiv, även om en förordning inte heller behöver lyckas med att uppnå fullständig harmonisering, om regler och principer, däribland ändamålsbegräsning, tolkas och tillämpas olika i medlemsstater.[311] Avsaknaden av uttryckliga regler i frågorna

[306] Jasserand-Breeman 2019, s.100.
[307] Jasserand-Breeman 2019, s. 101.
[308] WP29 2013, annex 4 exempel 17–20 och 67–69.
[309] Se de Busser och Vermeulen 2010, s. 102.
[310] Caruana 2019, s. 252.
[311] Caruana 2019, s. 252.

och det faktum att regleringen inom brottsbekämpningen utgörs av ett minimidirektiv, vilket endast är bindande vad gäller resultatet som ska uppnås, lämnar således över problemet till medlemsstaterna själva med risk för skiljaktigheter mellan lagstiftning.[312] Inom ramen för direktivet är harmonisering beroende av en konsekvent tolkning och tillämpning i medlemsstaterna. Om syftet med databehandlingen och den grupp myndigheter som har tillgång till uppgifter definieras mycket allmänt, kommer ändamålsbegränsning inte att erbjuda något extra skydd för registrerade. I praktiken kan det bli svårt för individer och dataskyddsmyndigheter att verkställa eller verifiera att principen faktiskt efterlevs. Därför kan eventuella oklarheter, till exempel när det gäller tillämpningsområdet för polisdirektivet, innebära ytterligare fragmentering av dataskyddet inom området med frihet, säkerhet och rättvisa.[313] Frågor om direktivets reglering faller under nationella domstolars prövning fram till att de prövas av EU-domstolen. På sikt kan ett sådant problem framtvinga mera ovillkorlig reglering från EU:s håll. Fragmenteringen återspeglar emellertid utvecklingen av medlemsstaternas polissamarbete som ett specialområde, vilket också kan göra potentiell framtida harmonisering utmanande.

Europadomstolen har inte i sin praxis fastställt exakta kriterier för ändamålsbegränsning genom att specificera ändamålen för uppgiftsbehandling och följaktligen genomföra en kompatibilitetsbedömning. I stället har domstolen i anknytning till artikel 8 fokuserat på att den senare användningen av data måste vara i enlighet med individens ”rimliga förväntningar”.[314] Kraven på ändamålsspecifikation och kompatibilitet kan ses som delelement i bedömningen av huruvida användningen av data uppfyller individens rimliga förväntningar.[315] EU-domstolen följer inte en strikt tillämpning av Europadomstolens praxis i förhållande till artikel 8 i konventionen. I stället har domstolen utarbetat sin rättspraxis baserat på de särdrag i dataskydd som föreskrivs i artikel 7 och 8 i stadgan samt unionens sekundärlagstiftning.[316]

Coudert har uttryckt att ändamålsbegränsning till viss mån motsvaras av konceptet

[312] Polisdirektivet, artikel 1(3).
[313] Caruana 2019, s. 252.
[314] von Grafenstein 2018, s. 182.
[315] von Grafenstein 2018, s. 182.
[316] Se närmare avhandlingens kapitel 3.3.1.

"inbyggt dataskydd och dataskydd som standard" i dataskyddsförordningens artikel 25.[317] Ett grundläggande antagande är att en personuppgiftsansvarig bör genomföra tekniska och organisatoriska åtgärder, i ett tidigt stadie i utformningen av bearbetningsverksamheten, på ett sådant sätt att de skyddar principerna om integritet och dataskydd redan från början (s.k. "inbyggt dataskydd").[318] Personuppgiftsansvariga bör dessutom se till att personuppgifter behandlas i enlighet med det högsta integritetsskyddet, till exempel så att endast de nödvändiga uppgifterna får behandlas och med begränsad åtkomst, så att personuppgifter som standard inte görs tillgängliga för ett obestämt antal personer (s.k. "dataskydd som standard").[319] Det är således upp till varje personuppgiftsansvarig att definiera vilka åtgärder som ska genomföras för att hantera de risker som uppstår av databehandlingen.[320] Genom principen förflyttas fokusen på ändamålsbegränsning från datainsamlingen till de enskilda behandlingsprocesserna. Samtidigt utgör ändamålsbegränsning fortfarande en komponent i den grundläggande rätten till dataskydd som uttryckligen hänvisar till principen som ett av dess grundläggande element.[321] Som sådan utgör principen en garanti för skyddet av personuppgifter. EU-domstolen har också erkänt att principen utgör en del av det väsentliga innehållet i rätten till skydd för personuppgifter.[322] Detta talar emot uppfattningen att principen enbart skulle utgöra *soft law,* enligt vilken ändamålsbegränsning endast skulle behöva behandlas som en riktlinje för databehandling, vilket gör det möjligt för personuppgiftsansvariga eller lagstiftare att avvika från principen eller modifiera dess innehåll när det anses lämpligt.[323] Varje inskränkning i principen om ändamålsbegränsning bör också uppfylla villkoren formulerade i artikel 52(1) i stadgan. Det faller då i sista hand på EU-domstolens ansvar att tolka kraven på nödvändighet och proportionalitet för att säkerställa detta skydd.

Implementeringen av ändamålsbegränsningsprincipen har fått en dubbel, för att inte säga

[317] Coudert 2017, s. 323.
[318] GDPR, artikel 25(1).
[319] GDPR, artikel 25(2).
[320] Se EDPB 2019.
[321] I artikel 8(2) i stadgan anges att personuppgifter "måste behandlas rättvist för specifika ändamål".
[322] EU-domstolens yttrande 1/15, p. 150. Se även förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*, p. 39–40 och mål C-362/14, *Schrems*, p. 94 angående det väsentliga innehållet i de grundläggande rättigheter.
[323] Brouwer 2011, s. 274.

motstridig inverkan inom EU.[324] Å ena sidan stärker den europeiska lagstiftningen och domstolarnas rättspraxis betydelsen av ändamålsbegränsning genom att betona dess funktion och förutsättning för andra rättigheter. Å andra sidan är det oundvikligt att notera en tydlig tendens att undergräva betydelsen av ändamålsbegränsningen i EU:s politik och lagstiftning, genom att tillhandahålla vaga definitioner för den avsedda användningen av personuppgifter, upprättandet av multifunktionella databaser och genom att utvidga användningen av befintliga databaser för nya ändamål, så kallade funktionskryp.[325] Diskussionen om ändamålsbegränsning och brottsbekämpande myndigheters sekundära behandling av personuppgifter blir högst aktuell i diskussionen om ändamålen för de nya reglerna om interoperabilitet och storskaliga databaser. Den oklara regleringen av ändamålsspecifikation och kompatibilitet inom polisdirektivets tillämpningsområde tyder på en urvattning av principens normativa innehåll, speciellt inom brottsbekämpande verksamhet, och skalar av ändamålsbegränsningen på sitt huvudsakliga innehåll. Det som återstår är kravet på nödvändighet och proportionalitet i polisdirektivets artikel 4(2) för beaktandet av ändamålsbegränsning i ett brottsbekämpande sammanhang. I enlighet med EU-domstolens rättspraxis bör alla beslut om inrättande av nya EU-informationsverktyg, centraliserad lagring av uppgifter om tredjelandsmedborgare eller utvidgningen av ändamålsbegränsning baseras på en strikt bedömning av nödvändigheten och proportionaliteten i åtgärderna innan en sådan begränsning antas. Nödvändighet och proportionalitet utgör som tidigare understrukits en avgörande faktor under EU-domstolens prövning eftersom den centraliserade användningen av storskaliga databaser måste baseras på transparenta och harmoniserade regler med tillgång till effektiv övervakning och tillgängliga skyddsåtgärder för de registrerade.

[324] Brouwer 2011, s. 293.
[325] Brouwer 2011, s. 293.

5 EN FÖRSVAGAD BETYDELSE AV DATASKYDD OCH ÄNSAMÅLSBEGRÄNSNING INOM OMRÅDET MED FRIHET, SÄKERHET OCH RÄTTVISA?

5.1 Säkerhetsunionens sektorövergripande strävan – mot en sammanslagning av EU:s rättsområden

Möjligheten för brottsbekämpande myndigheter att använda sig av personuppgifter som lagras i de enskilda databaserna är i sig inte ny. De utmaningar som genom åren orsakats av förändringar i kriminalitetens natur samt utvecklingen av nya teknologier och tillvägagångssätt hos brottsbekämpande myndigheter har lett till att kompetensområden gradvis har expanderat och tillgången till de enskilda databaserna har utvidgats. Som konstaterats tidigare i arbetet utvecklades både VIS och Eurodac till en början som redskap i gränsförvaltningen inom EU och först vid ett senare skede har man infört åtkomstmöjligheter för brottsbekämpande myndigheter till dessa databaser i syfte att bekämpa terrorism och andra allvarliga brott.[326] Av de berörda databaserna är det enbart SIS och ECRIS-TCN som upprättats huvudsakligen för brottsbekämpande ändamål. Det bör understrykas att de berörda databaserna, förutom SIS och ECRIS-TCN, enbart innehåller uppgifter om personer som inte misstänks ha begått några brott.

Både på unions- och nationell nivå verkar principen om ändamålsbegränsning undergrävas av den pågående utvecklingen av datainsamling samt den s.k. ’säkerhetiseringen’ av migrationsfrågor (jämför engelskans *securitization*), det vill säga en stegvis normalisering av en viss fråga som ett säkerhetsproblem.[327] Denna säkerhetisering kan också användas för att bygga hotbilder genom politiska diskurser. Debatten om hotbilder och deras allvarlighetsgrad faller till stor del inom området för den samhälleliga och politiska debatten. Den väsentliga rättsliga kopplingen uppstår emellertid av det faktum att medlen för att svara på de nya hoten kan ha en betydande inverkan på individers grundläggande rättigheter. Detta är också fallet med utvidgningen av myndigheters åtkomsträttigheter till tredjelandsmedborgares personuppgifter.

[326] År 2013 genomfördes en revidering av Eurodac i och med antagandet av förordning 603/2013, där åtkomsmöjligheter för brottsbekämpande myndigheter infördes. I VIS infördes åtkomstmöjligheter till brottsbekämpande myndigheter genom antagande av rådets beslut 2008/633/RIF. Se närmare avhandlingens kapitel 2.2 om utökningen av databasers åtkomsträttigheter till brottsbekämpande myndigheter.
[327] Se Jaskulowski 2019, ss. 710–720.

För att skilja mellan önskade och oönskade tredjelandsmedborgare som har för avsikt att passera EU:s yttre gränser introduceras regelbundet ny teknik och befintlig teknik kopplas samman i allt högre grad. Detta kan leda till funktionskryp, där teknologi som utvecklats för ett specifikt syfte över tid också används för andra ändamål.[328] I EU:s säkerhetsagenda har stark betoning lagts vid behovet av en sammankopplad och sektorövergripande strategi för säkerhet.[329] Detta förhållningssätt bygger på synergier mellan säkerhet och migration i syfte att stärka både gränsförvaltning och brottsbekämpning.[330] Detta förenande av agendor återspeglas nu i en sammanslagning av databaser som har uppstått vid olika tidpunkter och för olika syften, men som idag förenas under en gemensam säkerhetsagenda. Det nya ramverket för interoperabilitet förstärker på detta vis kopplingen mellan oregelbunden status och brottslighet.[331] Kontrollen av tredjelandsmedborgares mobilitet över och inom unionens gränser har inte bara ökat i omfattning, utan har även tydligt ändrat karaktär. Idag beskrivs migration i allt större grad i termer av risk och kriminalitet. Då migration i allt högre grad ses som en säkerhetsfråga, verkar migrationskontroll och brottsbekämpning smälta samman, en process som hänvisats till som ’krimmigration’ (jämför engelskans *crimmigration*).[332] Parkin identifierar en diskursiv och en sektorövergripande dimension av detta fenomen.[333] En betydande påverkan av kriminalisering av migration äger rum utanför området för straffrättslig och administrativ lagstiftning och praxis, och sker inom den diskursiva dimensionen av kriminalisering.[334] Detta omfattar sättet på vilket diskurser om invandring, avvikelse och säkerhet tillsammans hjälper till att konstruera idén om ett kriminellt hot som starkt kopplas till migranter som avvikande karaktärer och invandring som ett tecken på säkerhetsrisker.[335] Den sektorövergripande dimensionen manifesterar sig i de ökade sammankopplade elementen mellan straffrätt och migrationshantering.[336] Eftersom migranter i allt högre grad förknippas med brottslighet, anammar både området för brottsbekämpning och migrationskontroll kännetecken och metoder från den andras

[328] Dekkers 2019, s. 2.
[329] COM (2015) 185 final av den 28 april 2015.
[330] COM (2016) 205 final av den 26 april 2016, s. 2.
[331] Smith & LeVoy 2020.
[332] Se Kmak 2018 för en analys av utveckling av krimmigration speciellt i Europa och Finland.
[333] Parkin 2013, ss. 2, 7.
[334] Maneri 2011 se Parkin 2013, s. 2.
[335] Maneri 2011 se Parkin 2013, s. 2.
[336] Parkin, 2013, s. 7.

område, vilket bidrar till en starkare säkerhetisering av migration.[337] En aspekt av denna överlappningsprocess är användningen av informationsteknologi utvecklad för migrationskontrollsändamål för brottsbekämpning, och tvärtom.[338]

Europeiska datatillsynsmannen har vid ett flertal tillfällen uttryckt sin oro över denna trend som observerats inom området med frihet, säkerhet och rättvisa och har uppmärksammat tendenser i EU:s beslutsfattande att förknippa migrationshantering med säkerhetsändamål.[339] Detta anses leda till otydliga gränser mellan områdena. Forskare har noterat att dessa otydliga gränser mellan olika databaser har betydande konsekvenser för grundläggande rättigheter, särskilt mot bakgrund av möjligheten att skapa profiler av individer som på förhand identifieras som 'farliga', baserat på ständigt pågående riskbedömning i linje med den så kallade förebyggande brottsbekämpningsmodellen.[340] Fenomenet materialiseras i ökade befogenheter för brottsbekämpande myndigheter till redan existerande databaser, upprättandet av nya databaser samt utökandet av befogenheter hos befintliga aktörer. Interoperabilitet bygger på samma premisser som i den förebyggande brottsbekämpningsstrategin eftersom den effektivt innebär sammanlänkning och utsuddande av gränser mellan migrationshanteringsverktyg och mekanismer utformade för brottsbekämpning. Ett av de underliggande målen med upprättandet av interoperabilitetsmekanismerna är underlättandet och rationaliserandet av åtkomstmöjligheter, för myndigheter som ansvar för att förebygga, förhindra, upptäcka eller utreda terroristbrott samt annan grov brottslighet, till sådana informationssystem inom EU som inte uteslutande har inrättats för dessa syften.[341] Däremot förändrar interoperabiliteten inte den åtkomsträtt som avses i den rättsliga grunden för vart och ett av de europeiska informationssystemen.[342] Den nya interoperabilitetsmekanismen medför dock en väsentlig förändring i ändamålsbegränsningen och villkoren för tillgång till uppgifterna som finns i de olika databaserna jämfört med tidigare, vilket analyseras mer djupgående i kapitel 6.1.

[337] Dekkers 2019, s. 2. Se också Kmak 2018, s. 4.
[338] Dekkers 2019, s. 2.
[339] EDPS 2018 (b), skäl 20.
[340] Mitsilegas 2017, ss. 16–19.
[341] Förordning 2019/817 och 2019/818, skäl 25.
[342] Om användningen av ESP fastställs i förordning 2019/817 och 2019/818, artikel 7(1).

5.2 Den silobaserade strategin

Traditionellt har kravet på ändamålsbegränsning delvis uppfyllts genom att data har separerats och lagrats i egna databaser, s.k. silon. Uppdelningen har krävt att behöriga myndigheter konsulterar varje databas skilt för sig och således har denna tekniska begränsning inneburit en tydlig bromsande funktion innan åtkomst beviljats. Redan vid antagandet av den nya Europolförordningen år 2017 skedde ett skifte i hur man tidigare behandlat ändamålsbegränsning och fokus förflyttades från de åtskilda databaserna till de enskilda databehandlingsprocesserna. Skiftet innebar inget isolerat initiativ utan snarare ett första steg som banat väg för ett förnyat framtida genomförande av ändamålsbegränsning inom området med frihet, säkerhet och rättvisa, bland annat för förverkligandet av interoperabilitet.[343] Själva idén bakom de interoperabla databasernas arkitektur bygger på att överge det tidigare silobaserade tankesättet till förmån för en centraliserad åtkomst till uppgifter där varje system opererar genom ett nätverk av sammanlänkade databaser bestående av en central databas på EU-nivå i Strasbourg och nationella databaser i varje deltagande medlemsstat.[344]

Enligt Coudert uppfyller den silobaserade strategin tre huvudsakliga mål vilka tillsammans starkt bidrar till upprätthållandet av ändamålsbegränsning.[345] Genom uppdelningen av data i silon förverkligas kraven på datakvalitet och förutsebarhet samt den viktiga funktionen som skyddsåtgärd mot profilering. Kravet på datakvalitet avser att begränsa omfattningen av den data som samlas in och bearbetas.[346] Detta går hand i hand med ändamålsbegränsningens krav på att avgränsa ändamålen både vid insamlingen av uppgifter samt vid deras senare behandling. Den traditionella implementeringen av ändamålsbegränsning på databasnivå gör det möjligt att från början specificera syftet och legitimiteten för databaserna och den behandling som kan utföras vilket medför en mer överskådlig bedömningsprocess.[347] I fråga om förutsebarhet vid behandling av data fungerar målet som en garanti mot godtycklighet genom att de registrerade kan förutse följderna av behandlingen och anpassa sitt beteende därefter.[348] Varje databas agerar då

[343] Coudert 2017, s. 315.
[344] Vavoula 2020, s. 230.
[345] Coudert 2017, s. 316.
[346] Coudert 2017, s. 316.
[347] Coudert 2017, s. 317.
[348] Coudert 2017, s. 317.

som en tydlig kontext vid ändamålsavvägningen. Att flytta denna bedömning till nivån för varje enskild databehandling gör bedömningen mindre transparent.[349] Slutligen innebär åtskiljandet av informationen i fördefinierade databaser möjlighet till större kontroll över länkningen av data vilket hindrar skapandet av omfattande profiler.[350]

Genom att i framtiden binda dessa begränsningar till själva databehandlingsprocessen frångås därmed en viktig form av ändamålsbegränsning som det silobaserade systemet tidigare erbjudit behandlingen av personuppgifter. De nya databehandlingsoperationer som införts i EU:s ramverk för interoperabilitet undergräver principen om ändamålsbegränsning och suddar ut gränserna mellan databaser utformade för olika syften, såsom gränskontroll och brottsbekämpning. En intressant aspekt är att för tio år sedan skulle införandet av den informationsarkitektur som nu håller på att byggas ha varit politiskt, juridiskt och tekniskt sett otänkbar. I ett kommissionsmeddelande från år 2010 fastställs följande:

> Ändamålbegränsning är en mycket viktigt inslag i de flesta av de instrument som omfattas av meddelandet. Ett enda övergripande informationssystem som fyller flera funktioner skulle ge det effektivaste informationsutbytet. Att skapa ett sådant system skulle dock innebära en grov och orättmätig begränsning av individens rätt till integritet och skydd för sina personuppgifter och skapa enorma problem när det gäller utveckling och drift. I praktiken har politiken inom området med frihet, säkerhet och rättvisa utvecklats stegvis, vilket har lett till en rad informationssystem och instrument av olika omfattning och med varierande räckvidd och syfte. Den uppdelade informationshanteringsstruktur som har växt fram de senaste decennierna är mer lämpad att skydda medborgarnas rätt till integritet än något centraliserat alternativ.[351]

Meddelandet framför att den silobaserade informationshanteringsstruktur som varit i användning fram tills nyligen har varit lämpligare för att skydda individers integritet i förhållande till ett centraliserat alternativ. Argumenten som framförts vid antagandet av interoperabilitetsförordningarna är precis det motsatta – snarare än att erkänna värdet i separata, tydligt definierade system, har betoningen övergått till en mer generaliserad användning av tillgängliga uppgifter, och ett fokus på att fixera en enda digital identitet till individerna.[352] Europeiska datatillsynsmannen har uttryckt att interoperabiliteten

[349] Coudert 2017, s. 317.
[350] Coudert 2017, s. 317–318.
[351] Meddelande från kommissionen till Europaparlamentet och rådet, ”Översikt av informationshanteringen inom området med frihet, säkerhet och rättvisa”, COM (2010) 385 final av den 20 juli 2010, ss. 3–4.
[352] Jones 2019, s. 16.

består av mer än summan av sina komponenter då de i slutändan bidrar till att upprätta en omfattande centraliserad databas, särskilt ett centralt biometriskt register över tredjelandsmedborgare, och att en sådan central databas – i motsats till decentraliserade databaser – underförstått ökar risken för missbruk och önskemål om att använda systemet utöver de syften som det ursprungligen var avsett för.[353] Det står klart att de tekniska lösningarna tidigare har medfört en tydlig begränsande effekt på systemens användning, och i och med deras bortfall behövs nu materiella begränsningar. Om de skyddsåtgärder som fastställts genom den silobaserade metoden istället ersätts av reglering vid de olika förfarandena, som genomförs av personuppgiftsansvariga, bör enligt Coudert starkare övervakningsåtgärder utformas.[354] Att inte balansera åtgärderna på detta sätt riskerar annars att ge för mycket spelrum åt de personuppgiftsansvariga.

5.3 Big data och automatiserade system

Den snabba utvecklingen av organiserad brottslighet ökar påtryckningen hos brottsbekämpande myndigheter att hålla jämna steg med kriminella organisationer. Tonvikt har lagts vid utvecklandet av det föregripande och förebyggande arbetet samt informationsutbyte i rätt tid.[355] Hanteringen av flerdimensionella hot mot EU:s inre säkerhet inkluderar information som bygger på underrättelsedata och samarbete mellan brottsbekämpande enheter och gränsförvaltningen.[356] Framstegen som gjorts inom big data-teknologin har tillfört brottsbekämpande aktörer med allt effektivare verktyg.[357] I en era av big data blir frågan huruvida information från olika källor är kopplad för att skapa enskilda profiler en fråga om juridiska begränsningar snarare än tekniska, eftersom de senare gradvis förlorar sin relevans.[358] Risken för diskriminerande profilering blir aktuell i detta sammanhang.[359] Medan uppgifter i databaserna kan användas för riskbedömning

[353] EDPS 2018 (b), skäl 28.
[354] Coudert 2017, s. 323.
[355] Enligt ny hotbedömning ökar den organiserade brottsligheten snabbt i Europa. Enligt statistik mellan åren 2012-2017 har antalet kriminella grupper ökat från 3 600 till över 5 000, vilket innebär en ökning på nästan 40 procent. Preliminära uppgifter visar att utvecklingen fortsätter i samma riktning. Polisens hemsida, tillgänglig på: https://www.poliisi.fi/sv/uutiskaruselli/1/0/okat_hot_av_den_organiserade_brottsligheten_i_europa_nya_internationella_kriminella_gang_har_utvidgat_sin_verksamhet_till_finland_79453.
[356] Tomaszycki 2018, s. 204.
[357] Mycket förenklat kan big data (även kallad stordata) beskrivas som stora datamängder som kan användas på olika innovativa sätt för att upptäcka nya mönster i uppgifterna. Se t.ex. ICO 2017 samt Panneerselvam & Liu & Hill 2015, s. 3.
[358] Quintel 2018, s. 12.
[359] Se FRA 2017 (b), s. 43–44.

eller profilering, som i sig inte är förbjuden eller utgör en kränkning av grundläggande rättigheter,[360] är diskriminerande profilering inte tillåten.[361] Risken för att detta äger rum ökar när databaser är interoperabla, då flera datakategorier, som avslöjar känslig information som etnicitet, hälsa, sexuell läggning och religiösa övertygelser, kan tillgås samtidigt för profileringsändamål.[362] Detta kan i sin tur väcka känslor av minskat förtroende för polis- och gränsförvaltningsmyndigheter. De förutsättningar som denna typ av teknologi kräver för att leverera resultat har ansetts stå i strid med de grundläggande principer som ändamålsbegränsning bygger på.[363]För optimal funktion krävs ett fritt informationsflöde, samt att data kan sammankopplas. Lagring av data i tekniskt åtskilda databaser, styrda av specifika regler, begränsar sådant handlande. En anpassning mot big data och profilering innebär således ett steg från den silobaserade strategin där data samlas i slutna system.

Utvecklingen av effektivare metoder för datoriserat informationsutbyte har i allt högre grad lett till upprättandet av mer strukturerade former av informationsnätverk inom ett brett spektrum av EU:s rättsområden och har idag blivit normen för informationsinsamling.[364] De storskaliga databaserna inom området med frihet, säkerhet och rättvisa bygger på datoriserade system för insamling, utbyte och analys av uppgifter från människor som korsar EU:s yttre gränser.[365] Digitaliseringen leder även till automatisering av processer.[366] Ett av huvuddragen i de automatiserade administrativa systemen är deras förmåga att innesluta administrativt beslutsfattande.[367] Dessa enheter är inte strikt tekniska och inte heller enbart mänskligt styrda utan sociotekniska i den mening att de förknippar sociala (mänskliga) och tekniska (maskinella) element på ett

[360] FRA 2018 (d), s. 17. I polisdirektivet artikel 3(4) fastställs profilering innebära "varje form av automatiserad behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga aspekter rörande denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar".
[361] Polisdirektivet artikel 11(3). När profilering görs i enlighet med lagen är den en legitim undersökningsteknik. För att vara laglig måste profileringen bl.a. baseras på objektiva och rimliga motiveringar och följa de grundläggande rättigheterna, såsom rätten till icke-diskriminering och dataskydd. Se FRA 2018 (d), s. 23.
[362] FRA 2017 (b), s. 43–44.
[363] ICO 2017, s. 21.
[364] Galli 2019, s. 2.
[365] Jeandesboz 2016, s. 292.
[366] Hanke & Vitiello 2019, s. 5.
[367] Curtin 2020, s. 234.

flertal sätt.[368] Vi har förflyttat oss från en tid där automatiserade system endast har hjälpt människor att applicera regler i individuella fall till att närma oss en utsuddning av gränser mellan enbart stödjande funktioner och faktiskt beslutsfattande i dessa system, speciellt med hjälp av artificiell intelligens.[369] Automationens och interoperabilitetens synergi syns tydligt inom gränsförvaltningen, där EU under de senaste åren har föreslagit och antagit olika mekanismer för att upprätta ett integrerat smart gränshanteringssystem.[370] Antagandet av det nya informationssystemet ETIAS bygger t.ex. på individuell automatisk riskbedömning. Likaså ökar det nya informationssystemet EES automatiseringen av gränskontroller. Även om det administrativa beslutsfattandet inte fullständigt ersätts av modern teknologi eller helt och hållet saknar mänsklig intervention har centrala delar av den traditionella förvaltningen automatiserats vilket har en inverkan på individers förtroende för offentliga institutioner.[371] Under den automatiska teknologins era sker delning av data genom koppling av separata databaser så att räckvidden ökar väsentligt. Den expansiva användningen av teknologi och den växande automatiseringen av administrativt beslutsfattande medför utan tvekan radikala förändringar i förvaltningen som är svår att koppla till tidigare processuella förfaranden och rättigheter.[372]

5.4 EU:s integrerade förvaltning – ett flertal sammankopplade aktörer

Ändamålet för vilket data samlas in och behandlas under är avgörande för att koppla uppgifter till ett särskilt förfarande, antingen administrativt eller kriminellt, till vilket en uppsättning garantier för den registrerade är kopplade och därmed har allvarliga konsekvenser för individers rättigheter.[373] Det uppstår en paradox i det faktum att samtidigt som individers handlingar blir allt transparentare för stater har dessa personer allt svårare att förstå vilka statliga organisationer eller aktörer som innehar vilket slags information om dem.[374] Upprepade referenser till informationsglapp och blinda fläckar från lagstiftares sida har väckt frågan ifall vi nått ett panoptikon,[375] där myndigheterna

[368] Jeandesboz 2016, s. 292.
[369] Curtin 2020, s. 237.
[370] COM (2016) 205 final av den 26 april 2016. Se även Hanke & Vitiello 2019, s. 14–15.
[371] Curtin 2020, s. 234.
[372] Curtin 2020 s. 234. Se avhandlingens kapitel 6.2 om de registrerades rättigheter.
[373] Galli 2019, s. 12.
[374] Curtin 2018, s. 847.
[375] I sitt verk Övervakning och straff undersökte filosofen Michel Foucault uppfinningen av Panopticon, skapad av filosofen Jeremy Bentham. Panoptikon utgjorde en cirkelformad fängelsebyggnad där den övervakande befann sig inuti ett torn i centrum av fängelset och kunde se allting som pågick i de

ska kunna se alla grupper av tredjelandsmedborgare med koppling till EU genom en digital katalog.[376] Curtin menar att denna asymmetri inte orsakas av sekretess i den klassiska meningen, vilket innebär avsiktligt döljande av information, utan snarare sekretess som härrör sig från en asymmetri i transparens.[377] Maktasymmetri uppstår när en part i ett förhållande är i en starkare position i relation till den andra, medan informationsasymmetri uppstår då en part har mer information än en annan.[378] I ett interoperabilitetssammanhang blir båda begreppen aktuella. I EU är det domstolarna – och inte lagstiftarna eller förvaltningen – som spelar en aktiv roll i kontrollen av transparens för individer ur ett legalitets- och rättsstatsperspektiv.[379]

EU:s straffrättsliga samarbete och polissamarbete regleras i avdelning V av FEUF och utgör ett område av delad kompetens mellan EU och medlemsländerna. Artikel 82–86 FEUF fastställer den rättsliga grunden för straffrättsligt samarbete, som drivs av principen om ömsesidigt erkännande av domar och rättsliga beslut.[380] Området med frihet, säkerhet och rättvisa är ett område där olika straffrättsliga system samexisterar, och området förenar således inte i sig de nationella lagstiftningarna. Det finns emellertid inte bara ett system med straffrättsliga regler, i den mening vi vanligtvis tenderar att förstå ett straffrättsligt system.[381] Grunden för polissamarbetet i unionen etableras i artikel 87 FEUF, och artikel 87(1) fastställer att ”unionen ska utveckla ett polissamarbete mellan alla behöriga myndigheter i medlemsstaterna, inbegripet polisen, tullen och andra brottsbekämpande organ som är specialiserade på att förebygga, upptäcka och utreda brott”. Informationsutbytet är en väsentlig faktor i detta samarbete. Formellt sett är samarbetet begränsat till polissamarbete. Traditionellt sett har det funnits en åtskillnad mellan arbete som utförs av nationella underrättelseenheter och polismyndigheter.[382] Brottsbekämpning och underrättelseverksamhet är fortfarande till sin grund utformade och drivna på olika sätt, och innesluter bl.a. olika rättsliga myndigheter och interna

övervakades celler utan att de övervakade fångarna visste om de var övervakade eller inte. De var således ständigt sedda men kunde inte själva se. Se Foucault 1977.

[376] Vavoula 2020, s. 230.
[377] Curtin 2018, s. 847.
[378] Lynskey 2014, s. 592.
[379] Curtin 2018, s. 848.
[380] FEUF 82(1).
[381] Suominen 2014, s. 11.
[382] Dessa enheter har huvudsakligen styrts av olika ändamål i sitt arbete. Medan polismyndigheters fokus kretsat kring information för åtalsprövningsändamål har fokusen hos underrättelseenheter varit på förutsebarhet och riskbaserad analys. Se Derencinovic och Getos 2007 samt Galli 2019, s. 11.

organisationssätt.[383] Medan bägge myndigheter eftersträvar att nå säkerhet i sin vidaste bemärkelse, regleras deras verksamhet på olika sätt.

Ett centralt element i den europeiska säkerhetsagendan är att EU har anammat en paradigmatisk förändring mot förebyggande säkerhet, där säkerhetsunionen i huvudsak betraktas som en union av förebyggande rättvisa.[384] Enligt Mitsilegas finns det tre huvudsakliga skiften inom paradigmen för förebyggande brottsbekämpning: (1) en övergång från en utredning av handlingar som har ägt rum till betoning på misstankar; (2) en övergång från riktade åtgärder till generaliserad övervakning; (3) en tidsmässig förskjutning från det förflutna till framtiden.[385] Denna förebyggande brottsbekämpning syftar till att förhindra potentiella hot snarare än att straffa tidigare handlingar, och på detta sätt införs ett system som baseras på skapandet av misstänkta individer genom pågående riskbedömning.[386] De medel som idag står till förfogande för att förebygga och utreda grov brottslighet har medfört att gränserna mellan kompetensområden gradvis suddats ut. Samma typ av data kan vara av betydelse för aktörer både inom brottsbekämpaningssektorn och nationella underrättelsetjänster, och att dra en skarp linje mellan dessa enheter kan därför bli artificiellt.[387] Med underrättelseverksamhet avses offentliga myndigheters verksamhet för att skaffa, producera och analysera information för att identifiera potentiella hot mot staten och dess befolkning.[388] Brottsbekämpande myndigheters roll i det straffrättsliga systemet bestäms av reglering i processuell straffrätt, särskilt regler om bevisföring. Till skillnad från brottsbekämpningsåtgärder är underrättelseåtgärder utformade för att skydda nationell säkerhet. Medan bevis i straffrättsliga förfaranden måste överensstämma med ett antal begränsningar för att kunna tas upp till domstol, behöver information som samlas in av underrättelsetjänster inte uppnå samma kriterier.[389] Det finns i dagens läge heller ingen korrekt definition som skulle urskilja mellan grundläggande begrepp som ’information’ och

[383] Derencinovic och Getos 2007, s. 96.
[384] Mitsilegas 2017, s. 6.
[385] Mitsilegas 2017, s. 6.
[386] Carrera & Mitsilegas 2017, s. 6.
[387] Colonna 2012, s. 2–10.
[388] RP 199/2017, s. 5.
[389] Derencinovic & Getos 2007, s. 81.

’underrättelsedata’.[390] Det faktum att det i flera länder inte görs något åtskiljande mellan vilken typ av information som faller inom de två olika kategorierna eller vilka aktörer som har tillgång till vilka uppgifter bidrar till ytterligare oklarhet.[391] Fram till ikraftträdandet av lagen om civil underrättelseinhämtning avseende datatrafik (582/2019) och lagen om militär underrättelseverksamhet (590/2019) samt införandet av 5 a kap. i polislagen (872/2011) fanns det i Finland inga lagstadgade befogenheter om civil- och militär underrättelseinhämtning,[392] och nationella säkerhetsmyndigheter genomförde underrättelsearbete inom de ramar som krävts för utförandet av lagstadgade uppgifter.[393] De nya befogenheterna till civil underrättelseinhämtning används endast av skyddspolisen och grunden för skyddspolisens inhämtande av information utgörs i fortsättningen förutom av att förhindra och avslöja brott också av nationell säkerhet.[394] I och med den nya underrättelselagstiftningen blir den finska skyddspolisen en säkerhets- och civilunderrättelsetjänst.

Eftersom underrättelsearbete inte enbart utgör en del av nationell säkerhet utan också en del av EU:s interna säkerhet och i dessa situationer faller innanför unionens regleringsområde ter sig detta problematiskt. Fördelningen av kompetenser mellan behöriga myndigheter skiljer sig också markant åt i de olika medlemsländerna, då detta är upp till var och en stat att reglera.[395] Brottsbekämpande verksamhet kopplas således till informationens användningsändamål, bestående av förebyggande, utredning, upptäckt eller lagförande av allvarliga brott och terrorism, vilket blir den huvudsakliga

[390] Cocq 2017, s. 364. UNDOC har i sin manual definierat information som kunskap i en mer rå form, medan underrätelsedata utgörs av uppgifter som bearbetats och analyserats av behöriga myndigheter för att uppnå ökat värde. Se UNODC 2010, s. 1 och UNDOC 2011, s. 1.
[391] Galli 2019, s. 9.
[392] I RP 199/2017, s. 6–7 fastställer: “Det finns två olika former av underrättelseverksamhet: civil och militär underrättelseinhämtning. Med civil underrättelseinhämtning avses i begreppets vida bemärkelse underrättelsein- hämtning som utförs av en civil myndighet i syfte att producera information till stöd för den operativa verksamheten och den högsta statsledningens beslutsfattande när det gäller andra frågor än sådana som hänför sig till det militära försvaret. (Se Riktlinjer för en finsk underrättelselagstiftning, betänkande av arbetsgruppen för en informationsanskaffningslag, försvarsministeriet, 2015, s. 6.)“ samt att “Underrättelseinhämtning som utförs av en lagövervakningsmyndighet i syfte att skaffa sådan information om brottslingar, brott och de förhållanden där ett brott har begåtts som är av betydelse för att ett brott ska kunna förhindras, avslöjas eller utredas kallas kriminalunderrättelseinhämtning. Underrättelseinhämtning som utövas i syfte att upptäcka, identifiera, förstå och avvärja hot som riktas mot statens inre eller yttre säkerhet kallas säkerhetsunderrättelseinhämtning.“
[393] RP 199/2017, s. 6.
[394] Inrikesministeriets hemsida, tillgänglig på: https://intermin.fi/sv/polisvasendet/civil-underrattelse. Eftersom de militära underrättelsemål som försvarsmakten bedriver i regel inte åtnjuter samma nivå av skydd för grundläggande rättigheter som civila underrättelsemål har dessa separerats i sin egen enhet.
[395] Cocq 2017, s. 354.

gemensamma nämnaren för myndigheternas mandat, inte till vilken kategori av organ som utbyter informationen. Med tanke på den nya rollen som underrättelseverksamhet spelar i upprätthållandet av den allmänna ordningen är en av de frågor som står på spel förhållandet, som ännu inte definierats, mellan underrättelsetjänster och rättsväsendet.[396] Avseende objektiva kriteriet för åtkomstvillkor är det nödvändigt med en åtskillnad mellan brottsutrednings- och underrättelsetjänster i relation till den kriminella verksamhetens natur. I polisdirektivet fastställs som nämnt inte en sådan åtskillnad. Avsaknaden av en tydlig avgränsning kan få följder för individers rättigheter i fråga om brister i en acceptabel nivå av rättslig kontroll. En stor skillnad mellan aktörernas informationsanvändning utgörs av att underrättelseinformation ofta klassas som sekretessbelagd.[397] Igen skiljer sig situationen åt mellan medlemsländerna. I enlighet med rättsstatsprincipen måste underrättelseverksamhetens riktighet garanteras genom effektiv och fungerande kontroll, särskilt genom extern övervakning av tillsynsmyndigheter. I synnerhet är myndighets- och politisk kontroll av underrättelseaktiviteter, såväl som individens tillgång till information om underrättelseåtgärder mot sig själva, mycket viktiga utgångspunkter för grundläggande rättigheter. Detta skapar social legitimitet för åtgärderna. I vissa länder genomgår underrättelseåtgärder som används i anslutning till brottsbekämpning en *ex ante* utvärdering i domstol, i andra inte, vilket påverkar datasubjektens rättigheter.[398] I Finland ska domstolen fatta beslut om användning av civil underrättelseinhämtning.[399] Frågor om vem som har tillgång till vilket slags information och under vems tillsyn återspeglas således i de organisatoriska och administrativa strukturer som uppfyller medlemsstaternas egna konstitutionella eller rättsliga system. När interoperabilitet enbart presenteras som ett tekniskt sätt att ansluta befintliga nätverk, vilket inte kräver ytterligare anpassning, deltar lagstiftarna inte i diskussioner om behöriga myndigheterna eller vad som är att beakta som ett allvarligt brott på EU-nivå – element som varit omstridda inom unionen.[400]

Ett utmärkande drag för EU är dess ”sammansatta” eller ”integrerade förvaltning” (jämför engelskans *composite administration*) vilket innefattar informationsutbyte mellan

[396] Galli 2019, s. 18.
[397] Cocq 2017, s. 371.
[398] Jasserand-Breeman 2019, s. 21.
[399] Se § 7 i lag om civil underrättelseinhämtning avseende datatrafik (582/2019).
[400] Jämför Galli 2016, s. 467 och 468.

offentliga myndigheter på olika nivåer.[401] Ett kännetecken hos den integrerade förvaltningen är dess fragmenterade struktur,[402] bestående av nationella förvaltningar och deras ömsesidiga interaktioner. Detta gör EU beroende av andra, främst av sina medlemsländer, för information.[403] Den integrerade förvaltningen omfattar olika administrativa organ både på EU- och nationell nivå, vilket medför att informationen som utbyts ofta blir systematiskt osynlig eftersom den delas och används på olika nivåer och rättsområden.[404] Inom förvaltningen på EU-nivå antas inte direkt beslut avseende individer utan detta skikt tenderar snarare att fungera som ett slags mellanhand för olika nationella förvaltningar och informationen de behandlar.

Redan i Haagprogrammet från år 2004 lades stark tonvikt vid informationsutbytet mellan EU-byråer och interoperabilitet mellan databaser,[405] särskilt i samband med migrationshantering. De senaste årens utveckling av informationsnätverk har gått hand i hand med en ökning i antalet av och befogenheter hos EU-byråer, som t.ex. Europol, Frontex och eu-LISA, och även en intensifiering i deras åtkomstmöjligheter till data lagrad i EU:s databaser. Dessa organ är en del av den integrerade förvaltningen och utgör rättsligt oberoende enheter vilka är skilda från EU:s institutioner och inrättade för specifika uppgifter i enlighet med EU:s lagstiftning.[406] Genom mekanismer för informell styrning i informationsdelning kan byråerna verka under diskretion. Med tanke på den ökande ’agentifieringen’ inom området finns det därför ett ytterligare lager av komplexitet i informationsdelningen.[407] Det läggs tonvikt på nationell nivå, där EU:s nätverk är tänkta att fungera enbart som informationskällor. De lokala myndigheterna är följaktligen de som använder den information som förvärvats eller delats på överstatlig nivå men agerar i allmänhet på nationell nivå.

Denna nya form av integration ger EU-byråer nya roller och befogenheter. Europol har utvecklats från att bara vara en informationsbank till en alltmer proaktiv aktör och har haft en växande inverkan i synnerhet på utbyte och analys av information. De två

[401] Schneider 2017, s. 81.
[402] Hofmann & Rowe & Türk 2011, s. 908.
[403] Curtin 2018, s. 849.
[404] Curtin 2018, s. 848.
[405] Boehm 2011, s. 7.
[406] Reichel 2014, s. 886.
[407] För utvecklingen av kompetenser för byråer inom området med frihet, säkerhet och rättvisa se Kaunert & Leonard & Occhipinti 2016, ss. 273–284.

interoperabilitetsförordningarna underlättar informationsdelningen kopplad till brottsbekämpning mellan EU:s informationssystem och Europols databaser. Även Frontex befogenheter har gynnats av interoperabiliteten. Innan hade byrån inte tillgång till VIS, Eurodac och ECRIS-TCN, men förordningarna utvidgar tillgången till alla EU:s informationssystem för statistiska uppgifter och riskbedömningsändamål.[408] Även eu-LISA, som har placerats i en styrande position för interoperabiliteten redan innan förordningen formellt antogs, har fått ett utökat mandat. Medan dess uppgifter är klädda som rent tekniska, har eu-LISA långtgående kompetenser inklusive databehandling, operationella uppgifter och övervakning av datakvalitet i EU:s interoperabla databaser.

Det existerar alltså inte bara flera horisontella interaktioner mellan myndigheter från olika medlemsstater utan även flera vertikala interaktioner mellan nationella myndigheter och EU-organ. EU:s säkerhetsbefogenheter utövas av ett brett spektrum av institutioner och ett växande antal byråer och administrativa organ.[409] Intelligensnätverk inom området med frihet, säkerhet och rättvisa består av olika typer av EU-aktörer. Ballaschk har urskilt mellan två nivåer av nätverk: vertikala nätverk som skapats genom formella rättsliga arrangemang, bestående av t.ex. EU-byråer och organ och horisontella nätverk vilka karaktäriseras av en viss grad av informalitet och inkluderar t.ex. Prümavtalet och PNR-register.[410] Utöver dessa nätverk existerar även en mellanliggande nivå bestående av databaserna inom området.[411] Det storskaliga informationsutbyte som underlättas och effektiviseras genom interoperabla informationssystem kommer successivt att underlätta omstruktureringen av ansvarsområden inom brottsbekämpningsverksamheten, till exempel mellan säkerhets- och migrationsaktörer.[412] För skyddet av personuppgifter och rätten till privatliv ter sig detta problematiskt. Det som är framträdande med interoperabilitet som ett system för förbindelser mellan olika myndigheter är att det koncentrerar problemet med öppenhet i samband med olika typer av administration i EU.[413] Det kan alltså bli svårt att fastställa på vilken administrativ nivå ett fel inträffar.

[408] Jones 2019, ss. 49–50.
[409] Curtin 2018, s. 855.
[410] Ballaschk 2015, se Curtin 2017, s. 67.
[411] Ballaschk 2015, se Curtin 2017, s. 67.
[412] Galli 2019, ss. 12–13.
[413] Curtin 2018, s. 857.

6 BEARBETNINGEN AV PERSONUPPGIFTER I FÖRORDNING 2019/817 OCH 2019/818 SAMT BEHOVET AV UTÖKADE SKYDDSÅTGÄRDER

6.1 Utvidgade åtkomsträttigheter till CIR och underliggande databaser för brottsbekämpande myndigheter

6.1.1 Åtkomstmöjligheter enligt en tvåstegsmetod

I kapitel V i förordning 2019/817 och 2019/818 anges vilka myndigheter som är berättigade åtkomst till CIR, hur de kan utnyttja dessa åtkomsträttigheter samt mer detaljerade bestämmelser om åtkomst beroende på om syftet bakom åtkomsten utgörs av identifiering eller tillträde till de underliggande databaserna för brottsbekämpande ändamål. Förordningarna fastställer att brottsbekämpande myndigheter kan använda identitetsuppgifter som finns lagrade i den gemensamma databasen CIR för att utföra sökningar i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott,[414] spåra multipla identiteter,[415] samt underlätta och tillåta identitetskontroller inom medlemsstaternas territorium.[416] Då en sökning utförs för något av dessa syften visas träffar i CIR enligt en tvåstegsmetod. Det första steget visar ifall det finns en matchning av data i någon av de kopplade databaserna. Det senare steget kräver att myndigheterna begär full åtkomst till de databaser i vilka en träff genererats.

Brottsbekämpande myndigheters möjlighet att se dessa träffar resulterar i mer information än vad samtliga myndigheter potentiellt har rätt att ta del av inom sitt kompetensområde. Myndigheter som har åtkomst till minst en av de sammankopplade databaserna kan utföra sökningar genom ESP. Sökportalen möjliggör en översikt över all information relaterad till en enskild tredjelandsmedborgare som finns registrerad i de anslutna EU-informationssystemen samt i Europoluppgifter och Interpols system.[417] En sökning i ESP anger i vilken av de olika sammankopplade databaserna informationen finns för de myndigheter som utför sökningen. Även om portalen inte ger tillträde till de tillgängliga uppgifterna och verktyget därför i sig inte är tillräckligt avancerat för att upprätta en mer detaljerad profil om de berörda individerna, medför en träff uppgifter

[414] Förordning 2019/817 och 2019/818, artikel 22.
[415] Förordning 2019/817 och 2019/818, artikel 21.
[416] Förordning 2019/817 och 2019/818, artikel 20.
[417] WP29 2018, s. 4.

som kan kopplas till olika kategorier av information som resor, migration, internationellt skydd, brottsbekämpning och rättsliga förfaranden.[418] Eftersom en träff består av information som relaterar till en identifierbar person innebär även en träff information i form av personlig data.[419] I fallet *Digital Rights Ireland* fastställde EU domstolen att ”huruvida det föreligger ett ingrepp i den grundläggande rätten till respekt för privatlivet har det föga betydelse huruvida de uppgifter som avser privatlivet är av känslig art eller huruvida de berörda har fått utstå eventuella olägenheter på grund av ingreppet”.[420] WP29 har betonat det faktum att tillgången till uppgifterna är begränsad i sig inte innebär en skyddsåtgärd.[421] Följaktligen utgör även behandlingen av sådana träffar ett ingrepp i de grundläggande rättigheter som skyddas genom artiklarna 7 och 8 i stadgan och måste överensstämma med regleringen i stadgans artikel 52(1) speciellt i fråga om nödvändighet och proportionalitet.

Med andra ord är myndigheters tillgång till ESP inte begränsad till deras specifika kompetens eller uppgift, medan denna specifika kompetens eller uppgift tidigare har begränsat deras tillgång till de enskilda databaserna.[422] Detta har tydliga negativa följder för skyddet av individers grundläggande rättigheter. Information som hämtas via sökportalen fastställer ifall en individs uppgifter ingår i en databas, till exempel Eurodac. Denna kunskap om tillgängliga uppgifter i databasen ger då myndigheten en ledtråd om att en individ tagit sig in i EU på ett otillåtet sätt och/eller ansökt om asyl.[423] En träff resulterar i avslöjande av information genom vilken vissa slutsatser direkt kan dras om en registrerad, vilket i sin tur kan påverka myndigheters handlande och partiskhet.[424] Detta kan ses som ett funktionskryp.[425] Detta innebär dessutom en utvidgning av syftet med de bakomliggande databaserna. Datatillsynsmannen har framhävt att även om de underliggande systemen i CIR har reviderats för att hjälpa myndigheter vid gränshantering och brottsbekämpning, har vart och ett av systemen i grund och botten

[418] WP29 2018, s. 4.
[419] EDPS 2018 (b), skäl 58.
[420] Förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*, p. 33.
[421] WP29 2018, s. 21.
[422] Meijers Committee 2018, ss. 1–6.
[423] FRA 2017 (b), s. 55.
[424] FRA 2017 (b), s. 55.
[425] EU-domstolens har i sin rättspraxis ställt krav på att nationell lagstiftning erbjuder objektiva kriterier för att avgränsa behöriga nationella myndigheters tillgång till uppgifterna och deras senare användning. Domstolen lyfter bl.a. fram kravet på att uppgifter är underkastad förhandskontroll av en domstol eller en oberoende myndighet. Se närmare analysen av domstolens praxis i avhandlingens kapitel 3.3.2.

upprättats för ett mycket specifikt syfte.[426] WP29 har uttryckt att behöriga användares tillgång till information bör begränsas strikt till de situationer där dessa myndigheter skulle ha rätt att få tillgång till alla underliggande uppgifter, eller att träffar enbart skulle visas med avseende på de underliggande databaser som dessa utsedda myndigheter har direkt tillgång till.[427] Samma åsikt har yttrats av Europeiska unionens byrå för grundläggande rättigheter (FRA), som fastställt att tillgång till information om träffar bryter mot principen om ändamålsbegränsning som återspeglas i artikel 8(2) i stadgan, artikel 5(1)(b) i GDPR och artikel 4 (1)(b) i polisdirektivet.[428] Detta förhållningssätt går dock fullständigt emot kommissionens visioner om att säkerställa snabb och friktionsfri åtkomst till databaserna, som i själva verket är ett av de huvudsakliga målen med interoperabilitetsförordningarna.[429]

För att minimera ingreppen i individers grundläggande rättigheter i form av obehörig åtkomst och risk för missbruk bör vissa trösklar och skyddsåtgärder kvarhållas innan full åtkomst tillåts. Avsaknaden av sådana mekanismer kan annars leda till rutinåtkomst och funktionskryp för brottsbekämpande myndigheter och representerar därmed en allvarlig överträdelse av principen om ändamålsbegränsning. Innan ikraftträdandet av interoperabilitetsförordningarna styrdes samtliga bakomliggande databaser i CIR av tydliga kumulativa krav som fungerade som skyddsåtgärder före beviljandet av åtkomsträtt: tillgången måste vara nödvändig för förebyggande, upptäckt eller utredning av terroristbrott eller andra allvarliga brott; tillgången måste vara nödvändig i ett specifikt fall; det bör finnas rimliga skäl att anta att tillgången väsentligen kommer att bidra till förebyggande, upptäckt eller utredning av ett aktuellt brott.[430] Dessutom har åtkomst förutsatt att en oberoende myndighet verifierar att de ovanstående villkoren är uppfyllda innan beviljande.[431] Åtkomstmekanismen i CIR återspeglar delvis villkoren och i enlighet med artikel 22(1) i interoperabilitetsförordningarna får de utsedda myndigheterna endast konsultera CIR ”om det i ett specifikt fall finns rimliga skäl att anta att en sökning i EU-

[426] EDPS 2018 (b), skäl 33.
[427] WP29 2018, ss. 13–14.
[428] FRA 2018 (b), s. 19.
[429] Förordning 2019/817 och 2019/818, artikel 6(1).
[430] EDPS 2018 (b), skäl 60.
[431] Reglerna var dock annorlunda vid utförandet av gränskontrollsrelaterade aktiviteter, vilket möjliggjorde åtkomst till EU-system för identifieringsändamål. Aktiviteter som utförts i samband med gränskontroller och migrationshantering motiverade tillgång till de flesta systemen, utan specifika begränsningar. Se Carrera & Marco & Cortinovis & Ngo Chun 2019, s. 18, fn. 23.

informationssystem kommer att bidra till att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott". Det finns dock ingen tidigare verifiering av en oberoende myndighet som skulle övervaka om dessa villkor är uppfyllda i det första steget, vilket EU-domstolen ställt krav på i sin praxis.[432] Det tredje elementet, rimliga skäl att anta att tillgången väsentligen kommer att bidra till förebyggande, upptäckt eller utredning av ett aktuellt brott, beror främst på misstanken att personen faller under den kategori personer som omfattas av systemet, till exempel asylsökande i Eurodac eller visumfria resenärer i ETIAS. Med hänsyn till ETIAS, EES och Eurodac är brottsbekämpande myndigheter också skyldiga att först konsultera andra system med närmare relevans för brottsbekämpning, bl.a. nationella databaser, Europol-data, uppgifter som är tillgängliga enligt i Prümavtalet och VIS.[433] Tillgång till EES kräver konsultation av nationella fingeravtrycksdatabaser samt de automatiserade fingeravtrycksidentifieringssystemen i andra medlemsstater som är tillgängliga genom Prümavtalet, baserat på beslut 2008/615/RIF.[434] Det föreslagna ETIAS förutsätter förhandskonsultation av alla relevanta nationella databaser samt Europoluppgifter. När det gäller Eurodac, som innehåller särskilt känsliga uppgifter, är kraven som strängast.[435]

Utformningen av detta 'kaskadsystem' har fungerat som en ytterligare säkerhetsåtgärd i informationssystemen. I förordningarna om interoperabilitet har den obligatoriska konsultationen av andra databaser dock avskaffats. Kommissionen har motiverat beslutet i sin konsekvensbedömning med att denna funktion varit för tidskrävande, och att kaskadsystemet, det vill säga skyldigheten för förhandsverifiering och förhandskonsultation, skapar en betydande mängd administrativ börda som resulterar i förseningar och missade möjligheter att ta del av nödvändig information.[436] En annan aspekt är att kaskadsystemet kräver att brottsbekämpande myndighet avslutar sin förfrågning när informationen de behöver återfinns i ett system, men kommissionen anser att detta inte betyder att nästa system i ordning inte också kunde innehålla värdefull

[432] Förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*, p. 62 samt förenade målen C-203/15 och C-698/15, *Tele2 Sverige*, p. 120. EU-domstolens yttrande 1/15, p. 202.
[433] EDPS 2018 (b), skäl 60.
[434] Rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet. EUT 2008/L 210/1–11.
[435] FRA 2018 (b), s. 30.
[436] Kommissionens konsekvensbedömning SWD/2017/0473 final av den 12.12.2017, s. 25.

information för brottsbekämpande ändamål.[437] Detta uttalande är direkt motstridigt med kravet på ändamålsbegränsning. Det upprättade systemet kommer att förenkla myndigheters tillgång till databaser på två sätt genom att: (1) avskaffa kaskadsystemet och (2) tillhandahålla medlemsstaternas brottsbekämpande myndigheter och Europol information, utan några kontrollkrav, i vilka EU-databaser uppgifter om en viss person kan hittas. Det kan inte anses befogat att avlägsna skyddsåtgärder som införts för att försvara grundläggande rättigheter, främst i syfte att påskynda förfaranden.[438] Om det finns ett behov av att förbättra förfaranden bör detta inte göras på bekostnad av skyddsåtgärder. Att ersätta kaskadsystemet med denna nya mekanism innebär också att uppgifter om alla personer betraktas som lika känsliga och därmed att uppgifter om personer i en sårbar situation, som personer som söker internationellt skydd, inte kräver ökade skyddsåtgärder.[439] Ett tydligt exempel utgörs av åtkomstkontrollen i Eurodac, där brottsbekämpande myndigheter i enlighet med systemets reglering först måste konsultera andra system innan de kan begära tillgång till Eurodac. Medlemsstaterna måste först kontrollera fingeravtryck i databaser som är tillgängliga enligt nationell lagstiftning, under Prümavtalet och i tillämpningsbara fall VIS.[440] Information om asylsökande utgör särskilt känslig information och berör en grupp människor som är särskilt utsatta för kränkningar av grundläggande rättigheter.[441] Man har således velat säkerställa att uppgifter om asylsökande endast konsulteras som en sista utväg. Detta innebär att personuppgifter som inte samlats in för brottsutredningar endast bör få användas till brottsbekämpande ändamål, om den information som är nödvändig för att bekämpa grov brottslighet och terrorism inte finns i databaser som är mer direkt kopplade till brottsutredningar, i enlighet med proportionalitetsprincipen och principen om ändamålsbegränsning.[442]

6.1.2 Identifikation som en ny åtkomstgrund

Ett ytterligare syfte med CIR är bekämpningen av identitetsbedrägeri. I enlighet med skäl 38 i interoperabilitetsförordningarna är en förutsättning för detta att ”kunna utföra en

[437] SWD/2017/0473 final av den 12.12.2017, s. 43.
[438] EDPS 2018 (b), skäl 62.
[439] FRA 2018 (b), s. 33.
[440] Eurodacförordningen 603/2013, artikel 20(1).
[441] FRA 2017 (b), s. 28.
[442] FRA 2017 (b), s. 28.

tillräckligt tillförlitlig verifiering av identiteten på de personer vars uppgifter lagras i olika system". Kampen mot identitetsbedrägeri utgör i sig ett legitimt mål av allmänt intresse. En tillförlitlig verifiering av identiteter är dock inte ett mål för interoperabilitet i sig, listat i artikel 2(1) i förordningarna, utan enbart ett verktyg för att uppnå målen med interoperabilitet i förordningarnas artikel 2(2).[443] Målet med brottsbekämpande myndigheters tillgång till EU:s databaser är att bekämpa terrorism och annan allvarlig brottslighet. I interoperabilitetssammanhanget motsvaras detta av att bidra till en hög säkerhetsnivå inom området med frihet, säkerhet och rättvisa i unionen i förordningarnas artikel 2(1)(c). I detta avseende är brottsbekämpande myndigheters tillgång till CIR för att fastställa vilka system som lagrar information om en person endast motiverad i den utsträckning som är nödvändig för att uppnå målet att bekämpa terrorism och annan allvarlig brottslighet.[444]

Upprättandet av en databas med information om miljontals tredjelandsmedborgare, inklusive deras biometriska uppgifter, verkar mycket påträngande med tanke på grundläggande rättigheter. Eftersom denna nya databehandling som syftar till att korrekt identifiera personer utgör en inskränkning måste de följaktligen uppfylla de nödvändighets- och proportionalitetstest som stadgan förutsätter.[445] De problem som avses åtgärdas måste beskrivas tillräckligt tydligt och åtföljas av bevis. Europeiska datatillsynsmannen har noterat att kommissionens konsekvensbedömning är bristfällig i detta syfte och varken förklarar eller uppskattar omfattningen av identitetsbedrägeri.[446] En tydligare problembeskrivning, grundad på bevis, har således saknats.[447] Utan ytterligare indikationer på förekomsten av identitetsbedrägeri är det svårt att säkerställa att de vidtagna åtgärderna är lämplig och proportionerliga med tanke på de nya inskränkningar åtgärderna utgör.[448]

Även polismyndigheters åtkomst till CIR i identifieringssyfte utgör en utvidgning av de faktiska omständigheterna som rättfärdigar polismyndigheternas tillgång till uppgifter

[443] FRA 2018 (b), s. 26.
[444] FRA 2018 (b), s. 31. Se förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*, p. 59 och p. 61 och förenade målen C-203/15 och C-698/15, *Tele2 Sverige*, p. 102.
[445] EDPS 2018 (b), skäl 35.
[446] EDPS 2018 (b), skäl 36.
[447] Europaparlamentet 2019, ss. 1–2.
[448] EDPS 2018 (b), skäl 36.

som finns i databaserna.[449] Artikel 20 i förordningarna introducerar möjligheten för medlemsländernas polismyndigheter att använda CIR enbart för att identifiera en person, med beaktande av vissa omständigheter.[450] Faktum är att interoperabilitet kommer att låsa upp den tidigare begränsade tillgången till EU:s databaser för poliskontrollsändamål inom Schengenområdet. Med inrättandet av det gränskontrollfria Schengenområdet förlorade nationella poliser och gränsmyndigheter tillgången till dessa uppgifter, eftersom de endast tilläts utföra platskontroller av osystematisk karaktär.[451] Endast sökningar av data i SIS tilläts tidigare för att utföra sådana aktiviteter.[452] WP29 har betonat sin oro när det gäller skapandet av åtkomsträttigheter till EU-omfattande databaser med den enda motiveringen att denna databas är tillgänglig och att sådan tillgång skulle vara av mervärde, i detta fall för polismyndigheter.[453] Dessutom har arbetsgruppen velat understryka att framställandet av förfrågningar till CIR i syfte att identifiera en person kan leda till ett mycket stort antal åtkomster med tanke på volymen av identitetskontroller ledda av polismyndigheter.[454] Det bör tilläggas att man genom att reglera de omständigheter för brottsbekämpande myndigheters åtkomst till CIR för att verifiera om identitetsinformation finns i en av databaserna inte kan motivera den betydande minskningen av tillsynen och avlägsnandet av skyddsåtgärder som diskuterats ovan i avsnitt 6.1.1.[455]

Rutinåtkomst för poliskontroll skulle innebära ett ytterligare brott mot ändamålsbegränsning och ett oproportionerligt intrång i integriteten för till exempel resenärer som har gått med på att deras uppgifter behandlas för visum och förväntar sig att deras uppgifter samlas in och behandlas för detta ändamål.[456] Denna åtkomst ska baseras på nationell lagstiftning,[457] och utföras i syfte att bidra till att bekämpa olaglig

[449] Förordning 2019/817 och 2019/818, artikel 20.
[450] Artikel 20(1) fastställer att sökningar i CIR får ske under följande omständigheter: "Om en polismyndighet inte kan identifiera en person på grund av att det saknas en resehandling eller en annan trovärdig handling som styrker personens identitet; Om det föreligger tvivel om de identitetsuppgifter som lämnats av en person; Om det föreligger tvivel om äktheten i den resehandling eller en annan trovärdig handling som lämnats av en person; Om det föreligger tvivel om identiteten på innehavaren av en resehandling eller en annan trovärdig handling; Om en person inte kan eller vägrar att samarbeta."
[451] Carrera & Marco & Cortinovis & Ngo Chun 2019, s. 20.
[452] Carrera & Marco & Cortinovis & Ngo Chun 2019, s. 20.
[453] WP29 2018, s. 11.
[454] WP29 2018, s. 11.
[455] FRA 2018 (a), s. 31.
[456] EDPS 2018 (b), skäl 62.
[457] Förordning 2019/817 och 2019/818 artikel 20(5)–(6).

invandring samt en hög säkerhetsnivå.[458] EU:s datatillsynsman har uttryckt att syftena att bekämpa oregelbunden migration och bidra till en hög säkerhetsnivå inom ramen för artikel 20 är för breda och inte uppfyller kraven på att vara strikt begränsade och exakt definierade, enligt vad som krävs av EU-domstolen.[459] I nationella lagstiftningsåtgärder ska de exakta syftena med identifieringen anges och de behöriga polismyndigheterna ska utses, samt förfaranden, villkor och kriterier för sådana kontroller fastställas.[460] Det åläggs alltså genom bestämmelsen på medlemsstaterna en skyldighet att åtminstone införa vissa regler på nationell nivå. Detta ger emellertid medlemsstaterna en bred prövningsmarginal som inte är förenlig med EU-domstolens praxis. Domstolen fastställde i målet *Digital Rights Ireland* att det i datalagringsdirektivet under prövning

> inte föreskrivs några tydliga och precisa regler som reglerar räckvidden av ingreppet i de grundläggande rättigheter som är stadfästa i artiklarna 7 och 8 i stadgan. Domstolen konstaterar således att direktivet innebär ett ingrepp i dessa rättigheter som i unionens rättsordning är långtgående och synnerligen allvarligt, utan att ingreppet är noggrant avgränsat genom bestämmelser som gör det möjligt att säkerställa att det verkligen är begränsat till vad som är strängt nödvändigt.[461]

Angående kriteriet för nödvändighet har domstolen i *Huber* klargjort att skyddsnivån för individens rättigheter med avseende på behandling av personuppgifter måste vara lika i alla medlemsstater.[462] Domstolens uttalande angående datalagringsdirektivets avgränsning kan anses ännu mer vägande för EU:s lagstiftare när de antar en förordning som per definition inte är begränsad till de resultat som ska uppnås men är bindande i sin helhet och direkt tillämpliga i alla medlemsstater i enlighet med artikel 288 FEUF.[463] WP29 har uttryckt starka tvivel om att sådana ytterligare åtkomsträttigheter som beviljats polismyndigheter skulle uppfylla kravet på specifika regler, anpassade till den stora mängd uppgifter som berörs, och anser att dessa krav i fråga om vad som bör förutses i de nationella åtgärderna för att bevilja polismyndigheterna tillträde till CIR inte är tillräckligt precisa för att uppfylla domstolens ovannämnda krav.[464]

[458] Förordning 2019/817 och 2019/818 artikel 2(1)(b)–(c).
[459] EDPS 2018 (b), skäl 41. Se även förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*, p. 61.
[460] Förordning 2019/817 och 2019/818, artikel 20(5).
[461] Förenade målen C-293/12 och C-594/12, *Digital Rights Ireland*, p. 65.
[462] Domstolens dom av den 16 december 2008, *Huber*, mål C-524/06, ECLI:EU:C:2008:724, p. 52.
[463] FRA 2018 (b), s. 27.
[464] WP29 2018, s. 11.

Lagstiftarna har varit mån om att understryka att interoperabilitetsförordningarna formellt sett inte ändrar på tidigare beviljade åtkomsträttigheter enligt den rättsliga grunden i varje enskild databas som ingår i systemet.[465] Ändringarna som införts genom de nya reglerna bör emellertid inte underskattas, eftersom de drastiskt kommer att modifiera sätten på vilka uppgifter om tredjelandsmedborgare kommer att användas för ett brett spektrum av förfaranden. Interoperabilitet kommer i själva verket att utvidga användningen av sådan information, särskilt genom att införa nya åtkomstmöjligheter samt möjligheter att behandla tredjelandsmedborgares uppgifter i de olika systemen, för att bekämpa identitetsbedrägerier och underlätta identitetskontroller samt rationalisera åtkomstmöjligheter för brottsbekämpande myndigheter och fäster således nya syften och betydelser till uppgifternas behandling.[466] Samtidigt som dessa expanderande åtgärder antagits, är den parallellt pågående minskningen av skyddsåtgärder, bl.a. genom avlägsnandet av kaskadsystemet och det tidigare silobaserade systemet, svår att motivera. Den ändamålsbegränsning som nu avlägsnas har fungerat som en tydlig skyddsåtgärd för individers personuppgifter. Centraliseringen av data ökar riskerna för olaglig tillgång och användning av de registrerades uppgifter och kräver därför en ökad säkerhetsnivå, särskilt för känsliga uppgifter som biometrisk data.[467] Upprätthållandet av starka rättsliga och tekniska skyddsåtgärder är därmed avgörande för tryggande av de registrerades grundläggande rättigheter. I och med det pågående skiftet i synen på ändamålsbegränsning som presenterats i avhandlingen blir de registrerades egen vetskap om behandlingen av personuppgifter därför viktig. En central faktor utgörs här av tillgång till information för att de registrerade ska kunna kontrollera hur egna personuppgifter behandlas och används.

6.2 De registrerades rättigheter

6.2.1 Asymmetri för EU:s digitala medborgare

En viktig aspekt av den införda regleringen är den asymmetriska maktbalans den ger upphov till i förhållandet mellan de registrerade och registeransvariga. Medan interoperabilitetsramen möjliggör expanderade åtkomstmöjligheter till interoperabla

[465] Se bl.a. SWD/2017/0473 final av den 12.12.2017 och Europaparlamentet 2019.
[466] Carrera & Marco & Cortinovis & Ngo Chun 2019, s. 17.
[467] Se mål C-291/12, *Schwarz*, p. 61–62.

uppgifter för brottsbekämpande myndigheter, har dessa åtgärder inte kompletterats med utökade åtkomsträttigheter för de registrerade digitala medborgarna.[468] En bredare och snabbare åtkomst för myndigheter motsvaras för de registrerade av en försvårad och fragmenterad åtkomst till information, bl.a. om tillgängliga rättsmedel.[469] Graden av komplexitet och fragmentering kommer att bero på olika normativa system för informationsdelning, samarbete mellan byråer och samarbetsavtal med tredjeländer.[470] Dataskyddsregleringen och dess inneboende principer, däribland ändamålsbegränsning, fokuserar i hög grad på kontroll av den lagliga insamlingen av data. Eftersom både den positiva effekten och skadan av databehandlingen beror på de ändamål och metoder som personuppgifterna används på, är ett alternativt sätt att närma sig detta problem en förskjutning av fokus till regleringen av uppgifternas användning och effekt på individen.

Då kriterierna för dataskyddets tillämplighet uppfylls, faller alla levande fysiska personer under EU:s jurisdiktion inom ramen för dataskyddsregleringen och får status som digitala EU-medborgare.[471] Detta inkluderar inte bara unionsmedborgare utan också tredje-landsmedborgare, inklusive asylsökande och migranter. En kränkning av de registrerades grundläggande rättigheter riskerar att uppstå i och med de förändringar interoperabilitetsåtgärderna medför, och den svaga position som de registrerade försätts i genom sammankopplingen av de olika informationssystemen. Dels eftersom databaserna opererar i bakgrunden av olika regelverk och utanför direkt offentlig granskning, dels eftersom de registrerade individerna kan ha svårt att förstå hur användningen av den data som lagras i de olika systemen påverkar beslutsfattande.[472] De registrerade är inte alltid heller medvetna om att deras data kan användas för flera olika syften. Äganderätten till personuppgifter och huruvida förekomsten av en sådan rättighet påverkar de registrerades kontrollmöjligheter har uppmärksammats i denna kontext. Viljan att behandla personuppgifter och data som egendom kan kopplas till det starka skydd som traditionellt förknippas med äganderätt. Det bör framhållas att den vardagliga användningen av begreppet äganderätt skiljer sig mycket från dess juridiska sakrättsliga definition. För närvarande finns det inte någon enighet kring en materiell äganderätt över data, även fast

[468] Carrera 2020.
[469] Groenendijk 2020.
[470] Catanzariti 2020.
[471] Se avhandlingens kapitel 3.2.1.
[472] Nygård 2020.

omfattningen av datainsamling har ökat avsevärt.[473] Användning av termen äganderätt till data medför i själva verket betydande utmaningar och kan vara olämplig eftersom data inte besitter samma egenskaper som vanlig egendom. Av dessa skäl saknas också en rättslig grund för idén om ägandet av personuppgifter. Även om äganderätten i teorin kunde erbjuda de registrerade ett starkare skydd för sina personuppgifter är sådana fall osannolika i praktiken då tredjelandsmedborgare är skyldiga att lämna över sina uppgifter till behöriga myndigheter och erbjuds inga andra alternativ ifall de vill ta sig in i EU.[474] Därmed tillför en potentiell äganderätt inte tredjelandsmedborgare något eftersom de inte besitter några kommersiella eller juridiska befogenheter gentemot medlemsstater och EU-organ i detta avseende.[475] I GDPR definieras således inte heller äganderätt uttryckligen som ett eget begrepp.

Vid redogörelsen för syftet med GDPR etableras i skäl 7 att ”fysiska personer bör ha kontroll över sina egna personuppgifter”. Som konsekvens erkänner GDPR olika nivåer av kontrollrättigheter. Dessa återfinns också i polisdirektivet, om än i en omarbetad version. Rättigheterna är fördelade över tre olika avsnitt: (1) information och tillgång till uppgifter, (2) rättelse och radering och (3) invändningar och automatiserat individuellt beslutsfattande. Rättigheterna kräver inte nödvändigtvis att individerna har kontroll över data på samma sätt som de har kontroll över egendom. Snarare har individer rätt att kontrollera att uppgifter om dem endast används på rättvisa och rimliga sätt. Rättigheterna tillskrivs de registrerade i egenskap av fysiska personer och begränsar delvis de rättigheter att behandla data som de personuppgiftsansvariga besitter. Dessutom hjälper ett rättighetsbaserat tillvägagångssätt att säkerställa åtminstone ett minimikrav på jämlikhet, vilket i sin tur underlättar behovet att tillse att datahanteringen är rättvis.[476] Interoperabilitet kan betraktas som ett icke-hierarkiskt ramverk där personuppgifts-ansvariga och tredjeparter kan använda data för flera men begränsade ändamål, och de registrerade kan möta detta genom kontroll av utvalda bitar av data.[477] En icke-äganderätt kunde även anses utgöra en garanti för individer eftersom deras data då kunde tolkas som en inneboende del av deras personlighetsrättigheter och det därför inte skulle vara

[473] Hoeren 2014, s. 751.
[474] Catanzariti 2020.
[475] Catanzariti 2020.
[476] Catanzariti 2020.
[477] Catanzariti 2020.

nödvändigt med en äganderätt för att säkerställa ett bättre rättsligt skydd.[478]

6.2.2 Rätt till information och tillgång till uppgifter

Den registrerade bör ha möjlighet att utöva sin rätt till information om ändamålet med databehandlingen, som utgör en viktig källa till kontroll. Att säkerställa rätten till information när data samlas in och lagras i interoperabla databaser kan vara en utmaning med tanke på de många syften som existerar för uppgifternas användning, samtidigt som informationen är en förutsättning för att den registrerade ska få åtkomst till andra kontrollmekanismer, som rätten till tillgång, rättelse och radering av felaktiga uppgifter.[479] Information utgör även en princip för god förvaltning, som i enlighet med artikel 41(2) i stadgan omfattar individens rätt att få tillgång till sina handlingar. Artikel 47 i interoperabilitetsförordningarna fastställer att myndigheter som samlar in personuppgifter är skyldiga att tillhandahålla de registrerade information om denna behandling. I databaserna regleras dock inte rätten till information då redan lagrade data ges åtkomst för sekundära syften, med undantag för Eurodac.[480] Även om EU:s dataskyddslagstiftning inte förser registrerade med en rätt till information när myndigheter konsulterar redan lagrade uppgifter, kan vissa skyldigheter härledas från rätten till god förvaltning, till exempel när ett beslut om en tredjelandsmedborgares framtid baseras på information som behandlas i databaserna.[481]

Enligt tidigare undersökningar utförda av FRA saknar individer tillräcklig kunskap om dataskyddsbrott och tillgängliga rättsmedel.[482] Dessutom kan vissa grupper av registrerade tredjelandsmedborgare, som migranter i en oregelbunden situation, ha en begränsad förmåga att absorbera och förstå den givna informationen, speciellt vad gäller dataskyddsfrågor.[483] Detta gäller särskilt när det aktuella informationssystemet tjänar ett flertal syften och processer. I FRA:s undersökningar noterades också en motstridighet mellan skyldigheten att informera de registrerade och hur de informeras i praktiken.[484] Detta framkallar frågor kring hur kvaliteten på informationen påverkar förfaranden och

[478] Catanzariti 2020.
[479] Nygård 2020.
[480] FRA 2018 (a), s. 39.
[481] FRA 2018 (a), s. 39.
[482] Se FRA 2010, FRA 2012, FRA 2017 (a).
[483] Se FRA 2010, FRA 2012, FRA 2017 (a).
[484] Se FRA 2010, FRA 2012, FRA 2017 (a).

förtroendet för systemet som helhet. Ringaktning av informationsskyldigheten kan ha faktiska konsekvenser för medlemsstaterna, bl.a. kan det medföra att beslut som fattats ogiltigförklaras. Hovrätten i Paris upphävde år 2014 ett beslut om överföring av en asylsökande till Spanien av polisen i Paris eftersom den asylsökande inte informerades om väsentliga skyddsåtgärder, såsom användningen av hans fingeravtryck, eller uppgifter om registeransvariga och mottagarna av data.[485]

Innan en behandling av personuppgifter äger rum bör den registrerade informeras, i enlighet med GDPR artikel 13 och 14, bl.a. om ändamålen för uppgifternas behandling, vilka kategorier av personuppgifter som behandlas, om den registeransvariges identitet, om mottagarna av personuppgifterna och om datalagringsperiodens omfattning. Denna skyldighet beror inte på en begäran från den registrerade utan den registeransvarige måste proaktivt följa skyldigheten, oavsett om den registrerade visar intresse för detta eller inte.[486] Rätten till tillgång till egna uppgifter erkänns uttryckligen i GDPR artikel 15 och anges också som ett element i den grundläggande rätten till skydd av personuppgifter i artikel 8(2) i stadgan,[487] och utgör en nyckelaspekt i den europeiska dataskyddslagstiftningen.[488] Artikel 15 ger individen möjlighet att begära en kopia av sina lagrade personuppgifter samt annan kompletterande information. Detta hjälper individer att förstå hur och varför en personuppgiftsansvarig använder sig av deras data och möjliggör kontroll av att detta görs på ett lagligt sätt. En individ har bara rätt till sina egna personuppgifter och inte till information som rör andra personer, såvida inte informationen också handlar om dem.[489] I enlighet med artikel 15 ska även ”förekomsten av rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifterna eller begränsningar av behandling av personuppgifter som rör den registrerade eller att invända mot sådan behandling”, ”rätten att inge klagomål till en tillsynsmyndighet”, samt ”om personuppgifterna inte samlas in från den registrerade, all tillgänglig information om varifrån dessa uppgifter kommer” erhållas.

[485] Dom av franska Administrative Court of Appeal, Nr. 14PA00421, av den 31 juli 2014. Se FRA 2018 (a), s. 29.
[486] FRA 2018 (c), s. 207.
[487] I artikel 8(2) fastställs att ”var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem”.
[488] Se domstolens dom av den 17 juli 2014, *YS m.fl.*, förenade målen C-141/12 och C-372/12, ECLI:EU:C:2014:2081.
[489] Se domstolens dom av den 7 maj 2009, *Rijkeboer*, mål C-553/07, ECLI:EU:C:2009:293.

Dessutom bör en registeransvarig tillhandahålla den registrerade information om "förekomsten av automatiserade beslutsfattande, inklusive profilering [...] och åtminstone i dessa fall meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade".[490] Den automatiserade processen som skapa länkar i syfte att upptäcka multipla identiteter utgör automatiserat beslutsfattande i den mening som avses i dataskyddsregleringen. Dataskyddsreglerna ger traditionellt sett individer en hög skyddsnivå under sådana omständigheter med tanke på bristen på mänsklig ingripande. Till exempel föreskriver GDPR artikel 22 och artikel 11 i polisdirektivet att en registrerad har rätt att inte bli föremål för ett beslut, som enbart bygger på automatiserad behandling och som har rättsliga effekter för honom eller henne eller på liknande sätt påverkar honom eller henne betydligt utan något mänsklig ingripande. Enligt WP29 krävs inte att den registrerade proaktivt söker invändning mot ett sådant beslut.[491] Det är dock mycket tveksamt om det kan anses vara ett allmänt förbud eller snarare utgör en individuell rättighet av *opt out*-karaktär.[492] I enlighet med GDPR artikel 22(2) kan emellertid automatiserade beslut med rättsliga effekter eller som väsentligt påverkar individer vara acceptabla om det är nödvändigt för att ingå eller utföra ett kontrakt mellan den registeransvarige och den registrerade eller om den registrerade gav uttryckligt samtycke. Enligt artikeln är automatiserat beslutsfattande också acceptabelt om det är tillåtet enligt lag och om den registrerades rättigheter, friheter och berättigade intressen skyddas på lämpligt sätt.

Som konstaterats tidigare i avhandlingens kapitel 5.3 angående automatiserade processer i informationssystem kan algoritmiska beslut visa sig svåra att både förklara och förstå. Visserligen ger dataskyddsförordningen rätt till förklaring av algoritmer, men detta innebär bara en *ex ante* förklaring snarare än en *ex post* motivering.[493] I praktiken skulle en efterhandsförklaring innebära att en registrerad skulle informeras om logiken och de enskilda omständigheterna som påverkat utfallet i deras specifika beslut, de uppgifter eller funktioner som beaktades i hennes specifika fall och deras vikt eller

[490] GDPR, artikel 13(2)(f).
[491] WP29 2017, s. 19.
[492] Se Suksi 2019, s. 292 och fn. 48. Det går att identifiera väldigt olika tillvägagångssätt i nationella lagar som implementerar artikel 22 i GDPR. Se Malgieri 2019, s. 5–6. Finland verkar uppfatta artikel 22 som ett förbud, medan flera andra medlemsstater inte gör det. Trots att man i Finland uppfattar det som ett förbud, använder myndigheterna sig fortfarande av automatiserat beslutsfattande. Se även Suksi 2018, s. 334–335.
[493] Wachter & Mittelstadt & Floridi 2017, ss. 82–83.

klassificeringsgrunder vid beslutet.[494] Regleringen i GDPR utgör inte en grund för individer att hävda denna typ av förklaring. Uppenbarligen löser detta inte problemet med asymmetri i information till nackdel för den registrerade. Allmänna villkor för utövandet av den registrerades rättigheter fastställs i GDPR artikel 12 och syftar till att minska den administrativa bördan genom att kräva att den registrerades begäran följs upp utan onödigt dröjsmål och att information ska göras tillgänglig på ett kortfattat, begripligt och lättillgängligt sätt.[495] En vägran att tillmötesgå den registrerades begäran ska motiveras och baseras på en lagenlig grund.[496] Utöver detta ska den personuppgiftsansvarige underrätta den registrerade ”om möjligheten att framföra klagomål till tillsynsmyndigheten och att använda andra rättsmedel”.[497]

6.2.3 Rätt till rättelse och radering

Den registrerade har i enlighet med artikel 16 GDPR rätt att begära att inexakta och felaktiga uppgifter rörande henne själv rättas av den personuppgiftsansvarige. Även bristfälliga personuppgifter ska kunna kompletteras. I vissa situationer har en registrerad rätt att kräva att den personuppgiftsansvarige raderar personuppgifter.[498] Rätten att få sina personuppgifter raderade föreligger dock inte då behandlingen ”grundar sig på unionsrätten eller lagstiftningen i en medlemsstat”.[499] Det bör framhävas att nationella myndigheter och experter fäster en stor grad av trovärdighet vid biometriska data, samt att bearbetningen av sådana uppgifter är tekniskt komplex och att detta gör det svårt för berörda personer att bestrida fel och ännu svårare att bevisa att en biometrisk matchning genererats felaktigt.[500] Detta faktum bör ses i ljuset av att EU:s informationssystem har fastställts innehålla en betydande mängd felaktiga alfanumeriska data. Utvärderingar av kommissionen, Europeiska datatillsynsmannen och expertgruppen om informations-system samt FRA:s forskning har understrukit problem med datatillförlitlighet i bl.a. SIS och VIS.[501]

[494] Wachter & Mittelstadt & Floridi 2017, s. 78.
[495] Polisdirektivet, artikel 12.
[496] GDPR, artikel 12(4). Grunderna för vägran regleras i GDPR artikel 23(1)(a)–(f).
[497] GDPR, artikel 12.
[498] GDPR, artikel 17.
[499] GDPR, artikel 17(3)(b).
[500] FRA 2018 (a), s. 16.
[501] FRA 2018 (a), s. 82.

Artikel 48 i interoperabilitetsförordningarna reglerar rätten till åtkomst, rättelse, radering och begränsning av behandlingen av personuppgifter som lagras i MID. Enligt artikeln gäller dessa bestämmelser inte fel i identitetsdata lagrade i CIR som härrör sig från de underliggande IT-systemen. I enlighet med artikel 40 förblir den registeransvarige för uppgifterna i CIR den myndighet i medlemsstaterna som är registeransvarig för uppgifterna i respektive system, vilket innebär ett stort antal myndigheter. I praktiken kommer ett fel som upptäcks i MID att baseras på felaktiga uppgifter i CIR.[502] Korrigeringen enligt artikel 48, som endast tar upp fel som härrör sig från MID och inte de som ingår i CIR, verkar därmed olämplig och främjar ett mycket fragmenterat sätt att utöva rätten till korrigering och radering, vilket kan anses ineffektivt för individen.[503]

I enlighet med artikel 48(7) ska de ansvariga myndigheterna i fall av oenighet ”anta ett administrativt beslut med en skriftlig förklaring till den berörda personen om varför den inte är beredd att rätta eller radera uppgifter som rör honom eller henne”. Detta beslut ska i enlighet med artikel 48(8) ”ge den berörda personen information om möjligheten att invända mot det beslut som fattats [...] och, i tillämpliga fall, information om hur talan kan väckas vid eller klagomål inges till behöriga myndigheter eller domstolar samt möjligheterna till bistånd, även från tillsynsmyndigheterna”. En webbportal med information om de rättigheter och förfaranden som avses i förordningarnas artikel 47 och 48 stadgas om i artikel 49. Webbportalen fungerar som ett verktyg för att övervinna praktiska hinder som hämmar korrigering och innebär i detta avseende ett steg i rätt riktning för att ge de registrerade en effektivare möjlighet att utöva sina rättigheter. Problemet som kvarstår är hur individer blir medvetna om den behandling som utlöser dessa rättigheter i artikel 47 och 48.

6.2.4 Begränsade rättigheter enligt polisdirektivet och tillgång till ett effektivt rättsmedel

De ovannämnda kontrollrättigheterna är föremål för ett antal begränsningar inom polisdirektivets tillämpningsområde eftersom fullt åtnjutande av dessa rättigheter skulle innebära en begränsning av den brottsbekämpande verksamhetens effektivitet.[504] Rätten

[502] FRA 2018 (b), s. 50.
[503] FRA 2018 (b), s. 50.
[504] de Hert & Papakonstantinou 2016, s. 12.

till information, tillgång samt rättelse erkänns i polisdirektivets reglering men de uttrycks på ett sätt som möjliggör den grad av flexibilitet som krävs för deras behandling.[505] Enligt polisdirektivets artikel 15 kan medlemsstaterna begränsa rätten till tillgång så länge åtgärden är nödvändig och proportionell och utförs för specifika orsaker, t.ex. tjänar till att undvika att hindra rättsliga och kriminella förfaranden, skydda andras rättigheter och friheter eller skydda nationell eller allmän säkerhet. Enligt artikel 15 kan den registrerades begäran om tillgång till data eller korrigering och radering av uppgifter avslås av samma skäl, under förutsättning att de informeras om vägran utan onödigt dröjsmål, görs medvetna om sin rätt att lämna in ett klagomål mot beslutet och ges skälen till vägran om inte detta skulle undergräva ett av ovannämnda syften. De rättsliga mekanismer som reglerar de bakomliggande databaserna speglar också rätten till åtkomst, korrigering och radering, med vissa begränsningar som gäller för databasen SIS.[506] Dessa mer specifika bestämmelser ger medlemsstaterna en viss uppskattningsmarginal, t.ex. när det gäller förfaranden att tillåta den registrerade att utöva sina rättigheter och om begränsningarna för dessa rättigheter.[507] Trots införandet av polisdirektivet kvarstår således ett lapptäcke av bestämmelser om rätten till tillgång i brottsbekämpningssektorn. Europadomstolen har emellertid i sin rättspraxis belyst vikten av tillgång till ens personuppgifter som en väsentlig del av åtnjutandet av rätten till privatliv, och betonat vikten av effektiva processuella regler i fall av datalagringsåtgärder, bl.a. som en del av att säkerställa den lagliga behandlingen av data av brottsbekämpande myndigheter.[508] Dessutom har domstolen i enlighet med artikel 13 i Europakonventionen uppmärksammat vikten av effektiva rättsmedel och åtminstone en möjlighet till oberoende övervakning och granskning.[509] Europadomstolen har konstaterat överträdelser av artikel 8 i Europakonventionen i flera fall där den sökande inte har kunnat ifrågasätta riktigheten av information som förvaras i hemliga register.[510]

Om den registrerades utövande av rättigheter och kontroll genom tillsynsmyndigheter föreskrivs exklusivt i artikel 17 i polisdirektivet och artikeln har inte någon motsvarighet

[505] de Hert & Papakonstantinou 2016, s. 12.
[506] FRA 2018 (a), s. 99.
[507] Dimitrova & de Hert 2018, ss. 121–122.
[508] Europadomstolens dom av den 18 oktober 2011 i mål *Khelili mot Schweiz*, 16188/07.
[509] Europadomstolens dom av den 6 juni 2006 i mål *Segerstedt-Wiberg m.fl. mot Sverige*, 62332/00 och dom av den 16 februari 2000 i mål *Amann mot Schweiz*, 27798/95.
[510] Europadomstolens dom i mål *Rotaru mot Rumänien*.

i GDPR. Detta fungerar som en indirekt metod för den registrerade att fortfarande erhålla önskad information, då tillsynsmyndigheten måste utföra alla nödvändiga kontroller och granskningar av behandlingen av uppgifterna, och informera den registrerade om resultatet därav.[511] I Finland utgörs denna myndighet av dataombudsmannen. Genom reformen av den finska underrättelselagstiftningen inrättades även nya former av kontroll av underrättelseverksamheten. Lagen om övervakning av underrättelseverksamheten (121/2019) fastställer i 2 § parlamentarisk kontroll genom underrättelsetillsynsutskottet samt laglighetskontroll genom underrättelsetillsynsombudsmannen i anslutning till dataombudsmannens byrå. Offentliga myndigheters verksamhet bör kunna övervakas och individer måste ha en faktisk möjlighet att kontrollera sin information enligt lag. Det bör framhållas att inte alla medborgare förlitar sig på polisens verksamhet utan förbehåll. En smidig hantering av ärenden vid kontrollmyndigheter såsom dataombudsmannen är då av stor vikt. I HFD målet 2018:162 hade A lämnat in en begäran till datatillsynsmannen om att kontrollera lagenligheten av de uppgifter gällande A som ingick i polisens register, i vilka ”A inte hade rätt till insyn enligt 44 § i lagen om behandling av personuppgifter i polisens verksamhet”.[512] Datatillsynsmannen tolkade gällande lagstiftning som att begäran om en inspektion bör göras personligen vid polisstationen. Då en sådan begäran om inspektion av polisregistret redan i princip indikerar att sökande antar oklarheter i polisens verksamhet, är lagtolkningen oroväckande då det i sådana fall skulle vara möjligt att ändra informationen innan datatillsynsmannen ens börjar behandla begäran om kontroll.[513] Kärnan i målet utgjordes av huruvida datatillsynsmannen hade handlat rätt i att inte ta A:s begäran till behandling utan istället rådgiva A att framföra en begäran om rätt till insyn personligen på plats på polisstation och därefter meddela att behandlingen av ärendet avslutats. Därefter följde en debatt om huruvida detta var ett förvaltningsbeslut som borde ha kunnat överklagas.

Tillvägagångssättet för att skapa en rätt till indirekt utövande av de registrerades rättigheter i artikel 17 verkar vara inspirerat av de relativt nya domarna från Europadomstolen i målen *Roman Zakharov mot Ryssland*[514] och *Szabò och Vissy mot*

[511] Marquenie 2017, s. 332.
[512] Högsta förvaltningsdomstolens (HFD) avgörande HFD 2018:162.
[513] Effis yttrande till riksdagens förvaltningsutskott gällande Dataombudsmannens byrås verksamhets-berättelse 2018.
[514] Europadomstolens dom av den 4 december 2015 i mål *Roman Zakharov mot Ryssland*, 47143/06.

Ungern[515] gällande underrättelseverksamhet.[516] Europadomstolen krävde korrekt och oberoende övervakning av hemlig underrättelseverksamhet och en obligatoriska anmälan till den övervakade så snart en sådan anmälan inte längre kunde äventyra syftet med en övervakningsåtgärd. Detta är speciellt viktigt då informerandet kopplas till andra viktiga rättigheter som åtkomsträttigheter och rätt att korrigera felaktiga uppgifter. I målet *Schrems* ställde EU-domstolen krav på de nationella tillsynsmyndigheternas möjlighet att genomföra oberoende utredningar.[517] Detta är av vikt särskilt när den behöriga myndigheten utfärdat ett neutralt svar till den registrerade som sedan står inför en situation där hen inte vet vilka personuppgifter som erhållits om honom eller henne, än mindre huruvida de är korrekta och behandlas lagligen.[518] Det har emellertid ifrågasatts ifall indirekt tillgång till uppgifter uppfyller de viktigaste syftena bakom rätten till tillgång, t.ex. huruvida tillsynsmyndigheten alltid är i stånd att upptäcka fel och se till att de korrigeras.[519] Om tillsynsmyndigheten inte kan uppfylla detta behov uppstår frågan huruvida en registrerad ska kunna driva sitt ärende vid domstol om denne inte har tillgång till sina uppgifter och eventuellt inte vet om tillsynsmyndigheten har korrigerat felen.[520] Ett annat problem är att den information som tillsynsmyndigheten kan avslöja måste godkännas av brottsbekämpande- och eventuellt andra myndigheter, vilket utmanar kravet på att tillsynsmyndigheterna ska vara oberoende.[521] För att tillsynen ska vara effektiv måste tillsynsmyndigheterna få tillräcklig och korrekt information från myndigheterna. Situationen är utmanande eftersom speciellt underrättelseinformation till stor del är hemlig och tillsynsmyndigheterna inte har tillgång till andra informationskällor än myndigheterna under tillsyn.

Artikel 47 i stadgan kräver ett effektivt rättsmedel och en rättvis rättegång vid en oberoende och opartisk domstol som är inrättad genom lag. Artikel 47 inför en hög standard för rättsligt skydd eftersom den inte anser att ett effektivt rättsmedel från ett icke-rättsligt organ är tillräckligt för att fylla kravet. Möjligheten att lämna ett administrativt klagomål inför en tillsynsmyndighet i enlighet med artikel 77 i GDPR och

[515] Europadomstolens dom av den 12 januari 2016 i mål *Szabó och Vissy mot Ungern*, 37138/14.
[516] Sajfert & Quintel 2018, s. 14.
[517] Mål C-362/14, *Schrems*, p. 99.
[518] Sajfert & Quintel 2018, s. 7.
[519] Dimitrova & de Hert 2018, s. 123.
[520] Dimitrova & de Hert 2018, s. 123.
[521] Polisdirektivet, artikel 42.

artikel 52 i polisdirektivet anses inte vara ett effektivt rättsmedel enligt artikeln.[522] GDPR artikel 78–79 och polisdirektivet artikel 53–54 innehåller rätten till ett effektivt rättsmedel mot beslut som fattats av tillsynsmyndigheter, den registeransvarige eller personuppgiftsbiträde i enlighet med artikel 47 i stadgan. EU-domstolen har också i målet *El Hassani* fastslagit att för att kraven för tillämpningen av artikel 47 i EU-stadgan ska vara uppfyllda räcker det att nationella myndigheter tillämpar EU-lagstiftning, till exempel viseringskodexen, gentemot individer.[523] Domen bekräftar rätten till ett effektivt rättsligt skydd för tredjelandsmedborgare.

6.2.5 Sammanfattning och framtida åtgärder

Behovet av öppenhet och standardisering av tillämpliga regler är av avgörande betydelse för förekomsten av effektiva rättsmedel i interoperabilitetsförordningarna. I nuläget är situationen bristfälligt reglerad. Såväl de registrerade som dataskyddsmyndigheter, nationella myndigheter och EU-organ står inför en mycket komplex och fragmenterad rättslig struktur när interoperabilitetsmekanismerna väl står klara för användning. Detta förorsakas bl.a. av flera ändringar i befintliga regelverk, introducerandet av nya databaser och den förhållandevis nya tillämpningen av dataskyddsförordningen och polisdirektivet.[524] Det råder en generell brist på kunskap om hur dessa regler fungerar tillsammans och bör genomföras i praktiken. Bristande transparens och reglernas komplexitet blir särskilt påtaglig inom området för brottsbekämpande verksamhet, där uppgifterna kan bli föremål för brottmålsförfaranden.[525]

Registrerade vars personuppgifter samlas in under ett GDPR-ändamål har specifika rättigheter som kopplas till denna process och då deras uppgifter används vidare i ett brottsbekämpande sammanhang, kan de inte utnyttja samma skyddsåtgärder.[526] Polisdirektivet ålägger inte medlemsstaterna att i sin nationella lagstiftning införa en skyldighet att informera individer om bearbetningen och därmed inte heller om sekundär behandling av personuppgifter. I polisdirektivets artikel 13 åläggs enbart ett krav på att

[522] Samma sak gäller i Finland där förvaltningsklagan och klagomål till JO och JK inte betraktas som rättsmedel i och med att avgörandena inte kan ändra på det ursprungliga beslutet.
[523] Se domstolens dom av den 13 december 2017, *El Hassani*, mål C‑403/16, ECLI:EU:C:2017:960.
[524] Brouwer 2020.
[525] Brouwer 2020.
[526] Jasserand-Breeman 2019, s. 127.

göra specifik information tillgänglig för individer. Problematiken kring rätten till information för de registrerade kan sammanfattas i följande punkter: (1) skyldigheten att informera individer fokuserar på det ögonblick då personuppgifter samlas in och lagras, inte på tillfället när uppgifterna senare används för att informera myndigheter i sitt beslutsfattande, tex. vid brottsbekämpande myndigheters sekundära åtkomst till uppgifter; (2) de registrerade har ofta mer angelägna prioriteringar eller är helt enkelt inte medveten om vikten som lagrade personuppgifter kan ha för framtida beslut som påverkar dem; (3) information som lämnas om syftet med att bearbeta biometriska data förblir teknisk och svår att förstå för den registrerade; (4) i en interoperabel miljö innebär mångfalden av brottsbekämpande myndigheter som behandlar personuppgifter, de olika informationssystem som de arbetar med och därmed tillämpningen av flera rättsliga regelverk för dataskydd ytterligare problem för den registrerade, då det faktum att rätten ska utövas mot en registeransvarig i en miljö av många sammankopplade aktörer kan göra det svårt för den registrerade att få en grundlig översikt över sina data.

Meijers kommitté har ifrågasatt hur dessa rättigheter i verkligheten kommer säkerställas under interoperabilitetsförordningarna då det enligt nuvarande praxis redan har bevisats vara svårt för individer som konfronteras med storskaliga databaser, att hävda dessa rättigheter.[527] Bristen på standardiserade regler för maskininlärning eller användningen av algoritmer är också problematiskt för skyddet av dataskyddsstandarder, både vad gäller individers tillgångsrättigheter och övervakning hos dataskyddsmyndigheter och domstolar. Det kommer att vara svårt att bedöma lagenligheten och riktigheten i de insamlade uppgifterna. Interoperabiliteten kommer att leda till mer komplexitet snarare än förenkling, både gäller dataskydd och dess övervakning. Avsaknaden av öppenhet och försvårade möjligheter till ansvarsutkrävande å ena sidan och brister i effektiva rättsmedel å andra sidan förvärras av den kombination av opacitet och uppgiftsmaximering som interoperabilitet försöker uppnå.[528] Den centrala frågan är fortfarande hur man kan göra insamlingen av information, dess användning och interoperabel delning av data transparent. Curtin hävdar att trots att EU:s informationsutbyte och verktyg djupt påverkar människors integritet, är det mycket lite som berörda individer faktiskt kan göra

[527] Meijers Committee 2018, s. 6.
[528] Curtin 2017, s. 71.

för att utmana dessa processer.[529] Detta skapar väsentliga rättsliga utmaningar, eftersom de drabbade individerna lämnas för att navigera ensamma i ett landskap präglat av betydande rättslig osäkerhet.[530]

Kort sagt kommer den centraliserande logiken som driver interoperabiliteten med en fragmenterad logik för rättvisa för individer. Om målet är att erbjuda bättre skydd för de registrerade kan ett fokus på öppenhet och tydliga databehandlingsbegränsningar för registeransvariga lämpa sig bättre och erbjuda ett starkare skydd för registrerade, eftersom en sådan reglering alltid skulle gälla, medan de registrerades kontrollrättigheter till stor grad aktualiseras enbart när de aktivt åberopas av registrerade.[531] Det sker för tillfället en utvidgning av EU:s kompetens inom informationsutbyte som emellertid inte kompenseras av en tillräckligt omfattande ram för att skydda rätten till ett effektiv rättsmedel. Som en del av lösningen på behovet att ta itu med denna asymmetri har utformningen och utvecklandet av ett interoperabelt rättsligt paradigm lyfts fram, med utgångspunkten att frångå även silorna för rättsmedel och den fragmentering av dataskydd som uppstår till följd av regleringen i de olika EU-databaserna.[532] På detta sätt skulle större enhällighet eftersträvas.

En annan åtgärd som bör prioriteras är förbättrandet av de nationella dataskyddsmyndigheternas övervakningsroll och funktioner för att effektivt uppfylla nuvarande och framtida tillsynsbehov. Det nätverk interoperabilitet skapar, genom länkar mellan system, identiteter och syften, olika registeransvariga och ett flertal tillämpliga nationella lagar kommer att öka bördan av tillsynsmyndigheternas övervakningsuppgifter. För att säkerställa både individuella rättigheter och riktigheten i uppgifternas behandling är det viktigt att korrekt implementering av lagar övervakas effektivt, och att EU och nationella dataskyddsmyndigheter har tillräckliga befogenheter, kunskap och personal.[533] Vissa aspekter regleras i detalj på EU-nivå och införs uppifrån, andra är emellertid mer benägna att skapa synliga åtskillnader eftersom de överlåts till medlemsstaternas lagstiftning. I den totala budget på 425 miljoner euro som beräknats för

[529] Curtin 2017, s. 72.
[530] Mitsilegas 2020.
[531] Leiser och Custers 2019, s. 14.
[532] Carrera 2020.
[533] Se Guerra 2020 och Brouwer 2020.

de första nio åren av intreoperabilitetsarbetet,[534] har i budgeten inga öronmärkta medel planerats för de nationella dataskyddsmyndigheterna trots de nya uppgifter och den ökade arbetsbörda interoperabilitetsramen medför.[535] I artikel 51(4) i interoperabilitets-förordningarna föreskrivs enbart att medlemsstaterna ska se till att deras tillsynsmyndigheter har tillräckliga resurser och expertis för att fullgöra de nya uppgifter som förordningarna anförtror dem. I ljuset av de omfattande förändringar interoperabiliteten medför, och med beaktande av att liknande teknik antagligen är här för att stanna, är de nya uppgifterna tillsynsmyndigheterna påförs något som måste tas på allvar och åtgärdas på lämpligt sätt.

[534] COM (2017) 794 final av den 12 December 2017, Explanatory Memorandum.
[535] Groenendijk 2020.

7 AVSLUTNING

Det står klart att interoperabiliteten mellan EU:s storskaliga informationssystem inom området med frihet, säkerhet och rättvisa som upprättats genom antagandet av förordning 2019/817 och 2019/818 inte är begränsad till tekniska åtgärder för att komplettera befintliga och framtida informationssystem med ytterligare korsmatchningsfunktioner. I själva verket syftar ramverket till att bygga en ny systemarkitektur genom upprättandet av nya sammankopplade storskaliga databaser samt ytterligare centraliserade system. I takt med informationssamhällets framskridande och utvecklingen av mer avancerad teknologi blir de möjligheter som digitalt lagrade personuppgifter kan medföra allt viktigare, speciellt i brottsbekämpningssyfte. Den höga tillförlitlighet som kopplas till individers biometriska uppgifter gör denna information framförallt attraktiv för brottsbekämpande myndigheter. I detta avseende blir det viktigt med åtkomstmöjligheter för brottsbekämpande myndigheter till de databaser där personuppgifter lagras. Hittills har nationella brottsbekämpande organ haft möjlighet att utnyttja interoperabiliteten hos de nationella systemen, med varierande nivåer av interoperabilitet, men en smidig åtkomst till systemen på EU-nivå ska nu förbättra säkerheten i hela unionen.

Skyddet av personlig integritet som dataskyddslagstiftningen eftersträvar å ena sidan och effektiv brottsbekämpning å andra sidan framställs många gånger som en motsättning mellan två värderingar som båda behöver balanseras och inskränkas för att nå en jämvikt i samhället. Det uppstår därmed en polarisering mellan det enskilda och det kollektiva intresset. Dataskyddsrättigheterna och den personliga integriteten de ämnar skydda har en stark koppling till rättsstatsprincipen och ett välfungerande demokratiskt samhälle vilket står i strid med massövervakning av individer. En för långtgående övervakning kan resultera i att samhällets institutionella tillit riskerar att försvagas medan en avsaknad av tillräckligt skydd mot allvarlig brottslighet och terrorism kan leda till en liknande tillitsförlust. Då övervakningen av individers mobilitet blir normen inom EU uppstår frågan ifall interoperabilitetens tillämpningsområde kommer att utvidgas ytterligare till att inkludera även EU-medborgare i framtiden? Eftersom planer på sådana åtgärder redan har yttrats verkar ett sådant antagande inte så avlägset.

I GDPR fastställs reglerna för sekundär behandling av personuppgifter som samlas in för ett GDPR-syfte, medan polisdirektivet innehåller regler för sekundär behandling av

personuppgifter som samlas in och vidare behandlas för ett brottsbekämpande syfte. Analysen i avhandlingen visar att tolkningen av ändamålsbegränsning skiljer sig åt påtagligt mellan dessa regelverk. Som fastslagits i kapitel 4.3 tilldelas ändmålsbegränsningen en osäkrare roll i polisdirektivets reglering med möjlighet att använda uppgifter även för icke-kompatibla ändamål inom brottsbekämpande verksamhet, så länge åtgärderna respekterar kravet på nödvändighet och proportionalitet. Denna uppdelning av dataskyddsregler har också motiverat granskningen av vilken påverkan som skiljaktigheterna mellan regelverken kan ha för det skydd som beviljas registrerade individer. I avhandlingen undersöktes om den efterföljande användningen av GDPR-uppgifter utgör en första bearbetning eller en sekundär bearbetning enligt polisdirektivet. Genom att analysera frågan hur ändamålsbegränsningen i dataskyddsförordningen och polisdirektivet förhåller sig till behandling av personuppgifter som samlats in under ett icke brottsbekämpande sammanhang men senare överförs till behandling i ett brottsbekämpande sammanhang dras slutsatsen att problemet förblir oreglerat på EU-nivå. Avsaknaden av uttryckliga regler i frågan och det faktum att polisdirektivet utgör ett minimidirektiv som ska implementeras i nationell lagstiftning lämnar således över problemet till medlemsstaterna själva med risk för skiljaktigheter mellan lagstiftning. Om syftet med databehandlingen och den grupp myndigheter som har tillgång till uppgifter definieras mycket allmänt, kommer ändamålsbegränsning som sådan inte att erbjuda något skydd för de berörda personerna. I praktiken kan det bli svårt för individer och dataskyddsmyndigheter att verkställa eller verifiera att denna princip faktiskt efterlevs. Dessa faktorer har tillsammans lett till en urvattning av principen normativa innehåll vilket också innebär en försämring av individens dataskydd om det inte ersätts med andra alternativa skyddsåtgärder.

Det har föreslagits att vi måste förändra vår syn på ändamålsbegränsning och förflytta oss från ett traditionellt fokus på begränsningen av dataflöden till ett nytt fokus på reglering av metoder för delning av data och dess användning. Detta representerar mer ett tillvägagångssätt i linje med skyldigheten för inbyggt dataskydd och dataskydd som standard i artikel 25 i allmänna dataskyddsförordningen. Med tanke på ändamålsbegränsningens ställning som en komponent i den grundläggande rätten till dataskydd som uttryckligen hänvisar till ändamålsbegränsning som ett av dess grundläggande element och EU-domstolens erkännande av principen som en del av det

väsentliga innehållet i den grundläggande rätten till skydd för personuppgifter blir en långtgående förändring svår att motivera. EU-domstolen har dock ännu inte fastställt vad som utgör en kränkning av det väsentliga innehållet inom ramen för rätten till dataskydd. Med beaktande av EU-domstolens tidigare prövning av det väsentliga innehållet i en av stadgans rättigheter och domstolens resonemang i *Digital Rights Ireland*, där det väsentliga innehållet i skyddet av privatlivet och personuppgifter inte ansågs kränkas, kan man utifrån de likartade omständigheterna dra slutsatsen att interoperabilitetsramverkets reglering sannolikt inte står i strid med dataskyddets väsentliga innehåll trots dess allvarliga ingrepp i dataskyddet. Detta talar fortfarande emot uppfattningen att principen enbart skulle utgöra icke-bindande rätt i form av *soft law,* enligt vilken ändamålsbegränsning endast skulle behöva behandlas som en riktlinje för databehandling, vilket skulle möjliggöra avvikande från principen när den anses oläglig för personuppgiftsansvariga.

Skiftet till interoperabla databaser innebär i verkligheten en form av nya åtkomstmöjligheter för brottsbekämpande myndigheter inom EU. Tvåstegsmetoden som ger myndigheter åtkomst till uppgifterna i databasen CIR samt den nya möjligheten att använda uppgifterna för identifikationsändamål i enlighet med artikel 20 i förordningarna innebär en faktisk utökning av brottsbekämpande myndigheters befogenheter. Dessa åtgärder innebär allvarliga begränsningar av individens grundläggande rättigheter, inte minst för deras dataskydd vilket också har varit det centrala temat under granskning i denna avhandling, och kräver således noggrann övervägning, efterföljande av dataskyddsreglering och uppfyllandet av specifika skyddsåtgärder som utvecklats i Europadomstolens och EU-domstolens praxis.

Ändamålsbegränsning utgör en av dataskyddets hörnstenar och innebär en väsentlig skyddsåtgärd för missbruk av personuppgifter. Principen har förverkligats på olika sätt, t.ex. med olika funktioner för åtskillnad av uppgifter i de enskilda databaserna. Bland annat genom utnyttjandet av ett silobaserat tillvägagångssätt har man tidigare eftersträvat en decentraliserad informationshanteringsstruktur inom området med frihet, säkerhet och rättvisa. Även upprättandet av en kaskadmekanism med olika krav på obligatorisk konsultation av andra databaser samt förhandskontroll kopplad till sekundär åtkomst till databaserna har bidragit till att säkerställa att efterlevnaden av ändamålsbegränsningen

och domstolens praxis garanterats inom området. Ändringar i EU:s säkerhetslandskap och en förskjutning mot en allt mer förebyggande brottsbekämpningsstrategi och sammanlänkningen mellan brottslighet och migration har dock stått i strid med de grundläggande värderingar ändamålsbegränsning bygger på. De ändringar som interoperabilitetsförordningarna medför förenklar således myndigheters sekundära tillgång till databaser genom att: (1) avskaffa kaskadsystemet; (2) tillhandahålla medlemsstaternas brottsbekämpande myndigheter och Europol information, utan några kontrollkrav, i vilka EU-databaser uppgifter om en viss person kan hittas. Det kan inte anses befogat att avlägsna skyddsåtgärder som införts för att försvara grundläggande rättigheter, främst i syfte att påskynda förfaranden, speciellt då det är fråga om känslig information.

Även om begränsningarna föreskrivs i lag och kan antas uppfylla mål av allmänt intresse som erkänns av unionen och behovet av att skydda andras rättigheter och friheter i enlighet med stadgans artikel 52(1) återstår kraven på nödvändighet och proportionalitet. Varje inskränkning i principen om ändamålsbegränsning bör likaså uppfylla villkoren formulerade i artikel 52(1) i stadgan. Kommissionens konsekvensbedömning i fråga om åtgärdernas nödvändighet och proportionalitet saknar en tydlig problemdefinition och bevisföring för sina motiv, vilket är av stor betydelse för att kunna avgöra om åtgärderna är proportionella och nödvändiga på förhand. Det faller därmed på EU-domstolens ansvar att i sista hand tolka principerna om nödvändighet och proportionalitet för att säkerställa skyddet av de registrerade. För att bedöma om interoperabilitetsramen ger tillräckliga skyddsåtgärder för registrerade vars personuppgifter kan återanvändas för brottsbekämpande syften, har i avhandlingen de minimikrav som domstolen uppställt i praxis, speciellt med beaktandet av domstolarnas avgöranden i ärenden beträffande brottsbekämpande myndigheters behandling av personuppgifter, sammanställts och analyserats och sedan jämförts mot bestämmelserna i interoperabilitetsförordningarna. Eftersom EU-domstolen tydligt skiljer mellan frågan om datalagring och åtkomst i sin rättspraxis, har arbetets analys fokuserat på domstolens slutsatser kring den senare aspekten. EU-domstolen har varit tydlig med att understryka risken för stigmatisering i koppling till brottsbekämpning och ser ett känsligt problem i att uppgifter som ursprungligen samlats in för andra ändamål senare används för brottsbekämpningsändamål. Centraliseringen av data ökar risker för olaglig tillgång och

användning av de registrerades uppgifter och kräver därför en ökad säkerhetsnivå, särskilt för känsliga uppgifter som biometrisk data. Mot bakgrund av EU-domstolens och Europadomstolens praxis som analyserats i denna avhandling verkar kraven på ett strikt nödvändighets- och proportionalitetstest inte uppfyllas. Speciellt domstolens avgöranden i målen *Digital Rights Ireland* och *Tele2 Sverige* har utstakat tydliga ramar för de krav som behöver uppfyllas för att brottsbekämpande myndigheters behandling av personuppgifter ska anses vara befogad och i enlighet med etablerade dataskyddsprinciper. Domstolen har yttrat ett krav på att det ska finnas en skälig misstanke om delaktighet i terroristbrott eller allvarlig brottslighet och att åtkomsten till uppgifterna måste vara explicit begränsad till ändamålet att bekämpa grov brottslighet. Därtill inkluderar kraven tydliga och exakta regler för begränsningarnas omfattning, oberoende tillsyn och den registrerades tillgång till information. I nuläget möjliggör förordningarna och tillämpningen av polisdirektivet i de olika medlemsstaterna risk för skiljande reglering.

Interoperabiliteten innebär en komplicerad konstellation ur ett juridiskt perspektiv, inte bara på grund av dess direkt inskränkande inverkan på individers dataskydd utan också i och med komplexiteten i de många olika rättsliga ramar och mekanismer som skapar respektive databas och beviljar befogenheter till EU-organ och nationella myndigheter. Centraliseringen av personuppgifter har implikationer för dragandet av gränser mellan traditionell brottsbekämpning och underrättelsetjänster, och påverkar vidare omfördelningen av kompetensområden och uppgifter inom den brottsbekämpande verksamheten, säkerhets- och migrationsaktörer inkluderat. Genom att slå samman databaser upprättade för migrationssyften med system som också lagrar information om brottslingar blir det svårare att bevisa om myndigheter har behandlat personuppgifter för ett specifikt syfte. Den ökade roll som underrättelsetjänster spelar i brottsbekämpningsrelaterade frågor visar att separationen av dessa från övriga brottsbekämpande organ avseende tillämpningen av direktiv 2016/680 är svår att förklara och kan vara skadligt för den konsekventa efterlevnaden av de registrerades rättigheter, speciellt behovet av ett effektivt rättsskydd. Fragmenteringen återspeglar emellertid utvecklingen av medlemsstaternas polissamarbete och EUROPOL som specialområden, vilket kan göra potentiell framtida harmonisering utmanande och arbetsdryg.

Medan interoperabilitetsramen möjliggör expanderade åtkomstmöjligheter till brottsbekämpande myndigheter, har dessa åtgärder inte kompletterats med utökade åtkomsträttigheter för de registrerade digitala medborgarna. Individer besitter en rätt att kontrollera att uppgifter om dem endast används på rättvisa och rimliga sätt. Rättigheterna tillskrivs de registrerade i egenskap av fysiska personer och begränsar delvis de rättigheter att behandla data som den personuppgiftsansvarige besitter. EU:s integrerade förvaltning av detta område och dess flertal aktörer bidrar dock till ytterligare transparensproblem och kan inverka negativt på individens möjlighet att använda dessa skyddsåtgärder. Om existensen och användningen av en individs uppgifter i olika databaser förblir okänd eftersom uppgifterna erhålls av icke synliga aktörer kommer formella regler för öppenhet eller tillgång inte att hjälpa den drabbade individen. Rättigheter är till lite hjälp när de möter information eller aktörer som i stort sett är okända. Det kan alltså bli svårt att fastställa på vilken administrativ nivå ett fel görs. Det blir också svårt för allmänheten eller för institutioner som inte är involverade i de interoperabla nätverken att kräva tillgång till uppgifterna och behandlingen av deras data.

I nuläget är situationen bristfälligt reglerad. Såväl de registrerade som dataskyddsmyndigheter, nationella myndigheter och EU-organ står inför en mycket komplex och fragmenterad rättslig struktur. Med tanke på effektiviteten i de antagna förordningarna och EU:s storskaliga databaser, inklusive brottsbekämpande myndigheters åtkomstmöjligheter, är behovet av öppenhet och standardisering av tillämpliga regler av avgörande betydelse. Med beaktande av den senaste tidens utveckling är interoperabilitet, om än i en mer utvecklad framtida form där de grundrättighetsstridiga ingripandena som presenterats i avhandlingen åtgärdats, troligen här för att stanna. Vi kan mycket väl ha nått en punkt utan återvändo. En balanserande utveckling blir då strävan mot en enhetligare reglering av registrerades kontrollrättigheter och mer transparens, samt förbättrandet av de nationella dataskyddsmyndigheternas övervakningsroll och funktioner för att effektivt uppfylla nuvarande och framtida tillsynsbehov, och för att motarbeta den nu rådande asymmetrin i förhållandet mellan registeransvariga och registrerade.

KÄLLFÖRTECKNING

MONOGRAFIER OCH ARTIKLAR

Boehm, Franziska, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level.* Berlin-Heidelberg: Springer, 2011.

Brkan, Maja, 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors'. *Maastricht Journal of European and Comparative Law*, Vol. 23, Nr. 5/2016, s. 812–841.

Brouwer, Evelien, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System.* Leiden-Boston: Martinus Nijhoff Publishers, 2008.

Brouwer, Evelien, *International cooperation and the exchange of personal data: Safeguarding trust and fundamental rights* i Carrera, Sergio & Mitsilegas, Valsamis (red.): *Constitutionalising the Security Union. Effectiveness, Rule of Law and Rights in Countering Terrorism and Crime*. Bryssel: Centre for European Policy Studies, 2017.

Brouwer, Evelien, *Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation* i Besselink, L.F.M. & Prechal, S. & Pennings, F. (red.): *The Eclipse of the Legality Principle in the European Union*. The Netherlands: Kluwer Law International, 2011.

Bygrave, Lee A., *Data privacy law: an international perspective.* Oxford: Oxford University Press, 2014.

Carrera, Sergio & Stefan, Marco & Cortinovis, Roberto & Luk, Ngo Chun, 'When mobility is not a choice. Problematising asylum seekers' secondary movements and their criminalisation in the EU'. *CEPS Papers in Liberty and Security in Europe*, Nr. 11/2019, s. 1–40.

Carrera, Sergio & Mitsilegas, Valsamis, *Constitutionalising the Security Union* i Carrera, Sergio & Mitsilegas, Valsamis (red.): *Constitutionalising the Security Union. Effectiveness, Rule of Law and Rights in Countering Terrorism and Crime.* Bryssel: Centre for European Policy Studies, 2017.

Caruana, M., 'The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement'. *International Review of Law, Computers & Technology*, Vol. 33, Nr. 3/2019, s. 249–270.

Cocq, Céline C., 'Information' and 'intelligence': The current divergences between national legal systems and the need for common (European) notions'. *New Journal of European Criminal Law*, Vol. 8, Nr. 3/2017, s. 352–373.

Colonna, Liane, 'The new EU proposal to regulate data protection in the law enforcement sector: raises the bar but not high enough'. *IRI Promemoria*, Nr. 2/2012, s. 1–10.

Coudert, Fanny, 'The Europol Regulation and Purpose Limitation: From the Silo Based Approach to What Exactly'. *European Data Protection Law Review*, Vol. 3, Nr. 3/2017, s. 313–324.

Craig, Paul & de Búrca, Gráinne, *EU Law: Text, Cases, and Materials.* UK: Oxford University Press, 2015.

Curtin, Deirdre, ‘Second order secrecy and Europe’s legality mosaics’. *West European Politics*, Vol. 41, Nr. 4/2018, s. 846-868.

Curtin, Deirdre, *Security of the interstice and interoperable data sharing: A first cut* i Carrera, Sergio & Mitsilegas, Valsamis (red.): *Constitutionalising the Security Union. Effectiveness, Rule of Law and Rights in Countering Terrorism and Crime*. Bryssel: Centre for European Policy Studies, 2017.

Curtin, Deirdre, *The EU Automated State Disassembled* i Fisher, Elizabeth & King, Jeff & Young, Alison (red.): *The Foundations and Future of Public Law: Essays in Honour of Paul Craig*. UK: Oxford University Press, 2020.

de Busser, Els & Vermeulen, Gert, *Towards a Coherent EU Policy on Outgoing Data Transfers for Use in Criminal Matters? The Adequacy Requirement and the Framework Decision on Data Protection in Criminal Matters. A Transatlantic Exercise in Adequacy* i Cools, M. & De Ruyver, B. & Easton, M. & Pauwels, L. & Ponsaers, P. & Vande, W.G. (red.): *EU and International Crime Control*, Antwerpen–Apeldoorn–Portland: Maklu, 2010.

de Hert, Paul & Gutwirth, Serge, ‘Interoperability of police databases within the EU: An accountable political choice?’. *International Review of Law, Computers & Technology*, Vol. 20, Nr. 1-2/2006: s. 21–35.

de Hert, Paul & Papakonstantinou, Vagelis, ‘The new police and criminal justice data protection directive’. *New journal of European criminal law*, Vol. 7, Nr. 1/2016, s. 7–19.

de Vries, Karin, *Right to Respect for Private and Family Life* i van Dijk, Pieter & van Hoof, Fried & van Arjen, Rijn & Zwaak, Leo (red.): *Theory and practice of the European Convention on Human Rights.* Cambridge: Intersentia Publishers, 2018.

Dekkers, Tim, ‘Technology driven crimmigration? Function creep and mission creep in Dutch migration control.’ *Journal of Ethnic and Migration Studies*, Vol. 46, Nr. 9/2019, s. 1849–1864.

Derencinovic, Davor & Getos, Anna-Maria, ‘Cooperation of law enforcement and intelligence agencies in prevention and suppression of terrorism’. *Revue internationale de droit penal*, Vol. 78, Nr. 1-2/2007, s. 79–112.

Dimitrova, Diana & de Hert, Paul, *The Right of Access Under the Police Directive: Small Steps Forward* i Medina, M. & Mitrakas, A. & Rannenberg, K. & Schweighofer, E. & Tsouroulas, N. (red.): *Privacy Technologies and Policy*. Schweiz: Springer, 2018.

Focault, Michel, *Discipline and Punish. The Birth of the Prison.* New York: Vintage Books, 1997.

Galli, Francesca, ‘Digital Rights Ireland as an opportunity to foster a desirable approximation of data retention provision’. *Maastricht Journal of European and Comparative Law*, Vol. 23, Nr. 3/2016, s. 460–477.

Galli, Francesca, ‘Interoperable Law Enforcement. Cooperation Challenges in the EU Area of Freedom, Security and Justice’. *Robert Schuman Centre for Advanced Studies Research Paper, Nr. 15/2019.*

Harris, David & O'Boyle, Michael & Bates, Ed & Buckley, Carla, *Harris, O'Boyle, and Warbrick: Law of the European Convention on Human Rights.* UK: Oxford University Press, 2014.

Hanke, Philip & Vitiello, Daniela, *High-Tech Migration Control in the EU and Beyond: The Legal Challenges of “Enhanced Interoperability*” i Lazzerini, Elena &

Carpanelli, Nicole (red.): *Use and Misuse of New Technologies: Contemporary Challenges in International and European Law*. Schweiz: Springer, 2019.
Herlin-Karnell, Ester, 'The domination of security and the promise of justice: on justification and proportionality in Europe's 'Area of Freedom, Security and Justice''. *Transnational Legal Theory*, Vol. 8, Nr. 1/2017, s. 79–102.
Hijman, H, *The European Union as a constitutional guardian of internet privacy and data protection.* Amsterdam: University of Amsterdam, 2016.
Hoeren, Thomas, 'Big Data and the Ownership in Data: Recent Developments in Europe'. *European Intellectual Property Review,* Vol. 36, Nr. 12/2014.
Hofmann, Herwig C. H. & Rowe, Gerard C. & Türk, Alexander H, *Administrative Law and Policy of the European Union.* UK: Oxford University Press, 2011.
Jaskulowski, K, 'The securitisation of migration: Its limits and consequences'. *International Political Science Review*, Vol. *40, Nr.* 5/2019, s. 710–720.
Jasserand-Breeman, C, *Reprocessing of biometric data for law enforcement purposes: Individuals' safeguards caught at the Interface between the GDPR and the 'Police' directive?* Groningen: University of Groningen, 2019.
Jeandesboz, Julien, 'Smartening border security in the European Union: An associational inquiry'. *Security Dialogue*, Vol. 47, Nr. 4/2016, s. 292–309.
Kaunert, Christian & Leonard, Sarah & Occhipinti, John, *Introduction: Agency Governance in the European Union's Area of Freedom i Security and Justice* i Kaunert, Christian & Leonard, Sarah & Occhipinti, John (red): *Justice and Home Affairs Agencies in the European Union*. UK: Routledge, 2016.
Kędzior, Magdalena, 'GDPR and beyond—a year of changes in the data protection landscape of the European Union'. *ERA Forum*, Nr. 19/2019, s. 505–509.
Kmak, Magdalena, 'Crimmigration and Othering in the Finnish Law and Practice of Immigration Detention'. *No Foundations: An Interdisciplinary Journal of Law and Justice*, Vol. 15, 1/2018, s. 1–22.
Leiser, M. R. & Custers, B. H. M., 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680'. *European Data Protection Law Review*, Vol. 5, Nr. 3/2019, s. 367–378.
Lenaerts, Koen, 'Limits on Limitations: The Essence of Fundamental Rights in the EU'. *German Law Journal*, Vol. 20, Nr. 6/2019, s. 779–793.
Liu, Nancy Y., *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics.* Abingdon: Routledge, 2011.
Lynskey, Orla, 'Deconstructing Data Protection: The Added-Value of a Right to Data Protection in the EU Legal Order'. *International and Comparative Law Quarterly*, Vol. 63, Nr. 3/2014, s. 569–598.
Malgieri, Gianclaudio, 'Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations'. *Computer Law & Security Review*, Vol. 35, Nr. 5/2019, s. 1–26.
Marquenie, Thomas, 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework'. *Computer Law & Security Review*, Vol. 33, Nr. 3/2017, s. 324–340.
Mifsud Bonnici, J. P., 'Exploring the non-absolute nature of the right to data protection'. *International Review of Law, Computers & Technology*, Vol. 28, Nr. 2/2014, s. 131–143.
Mitsilegas, Valsamis, *The Security Union as a paradigm of preventive justice: Challenges for citizenship, fundamental rights and the rule of law* i Carrera,

Sergio & Mitsilegas, Valsamis (red.): *Constitutionalising the Security Union. Effectiveness, Rule of Law and Rights in Countering Terrorism and Crime*. Bryssel: Centre for European Policy Studies, 2017.

Muller, Benjamin J., *Security, Risk and the Biometric State: Governing Borders and Bodies.* Abingdon: Routledge, 2010.

Mäkinen, Jenna, *The background and nature of data within EU data protection law with reference to new technology* i Korpisaari Päivi (red): *Oikeus, tieto ja viesti: Viestintäoikeuden vuosikirja 2015*. Helsingfors: Helsingin yliopiston oikeustieteellinen tiedekunta, 2016.

Panneerselvam, John & Liu, Lu & Hill, Richard, *An Introduction to Big Data* i Babak, Akhgar & Saathoff, Gregory B. & Arabnia, Hamid R. & Hill, Richard & Staniforth, Andrew & Bayerl, Petra Saskia (red.): *Application of Big Data for National Security*. UK: Elsevier Inc., 2015.

Parkin, Joanna, 'The Criminalisation of Migration in Europe. A State-of-the-Art of the Academic Literature and Research'. *CEPS Paper in liberty and security in Europe*, Nr. 61/2013.

Pech, Laurent, 'The Rule of Law as a Constitutional Principle of the European Union'. *Jean Monnet Working Paper, Nr. 4/2009*.

Peczenik, Aleksander, 'Om den förvaltningsrättsliga forskningen och rättsdogmatiken'. *Förvaltningsrättslig Tidskrift*, häfte 2, 1990, s. 41–52.

Porcedda, Maria G., 'Law Enforcement in the Clouds: Is the EU Data Protection Legal Framework up to the Task?' i Gutwirth, S. & Leenes, R. & de Hert, P. & Poullet, Y. (red.): *European Data Protection: In Good Health?* Dordrecht: Springer, 2012.

Purtova, Nadezhda, 'Between the GDPR and the Police Directive: Navigating Through the Maze of Information Sharing in Public-Private Partnerships'. *International Data Privacy Law*, Vol. 8, Nr. 1/2018 (a), s. 52–68.

Purtova, Nadezhda, 'The law of everything. Broad concept of personal data and future of EU data protection law'. *Law, Innovation and Technology*, Vol. 10, Nr. 1/2018 (b), s. 40–81.

Quintel, Teresa, 'Connecting personal data of Third Country Nationals - Interoperability of EU databases in the light of the CJEU's case law on data retention'. *University of Luxembourg Law Working Paper Series,* Nr. 2/2018.

Reichel, Jane, 'Communicating with the European Composite Administration'. *German Law Journal*, Vol. 15, Nr. 5/2014, s. 883–906.

Ritleng, Dominique,'Lärdomar av EU-domstolens parallella domar i målen Åkerberg Fransson och Melloni'. *SvJT* 2014, s. 36–70.

Sajfert, Juraj & Quintel, Teresa, 'Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities'. *Edward Elgar Publishing,* 2019, Forthcoming.

Saurugger, Sabine & Terpan, Fabien, *The Court of Justice of the European Union and The Politics of Law.* UK: Palgrave, 2017.

Schneider, Jens-Peter, *Information-exchange and its problems* i Harlow, Carol & Leino, Päivi & della Cananea, Giacinto (red.): *Research Handbook on EU Administrative Law.* UK: Edward Elgar Publishing, 2017.

Suksi, Markku, 'Förvaltningsbeslut genom automatiserat beslutsfattande – statsförfattnings- och förvaltningsrättsliga frågor i en digitaliserad myndighetsmiljö'. *JFT* 2018, s. 329–371.

Suksi, Markku, ’Rättsstatlighet, god förvaltning och ämbetsansvar vid automatiserat beslutsfattande’. *JFT* 2019, s. 267–302.

Suksi, Markku, *Ändamålsbundenhetsprincipen i finsk, nordisk och EU-rätt* i Baumbach, T. & Blume, P. & Gøtze, M. (red.): *Ret på flere felter: Forvaltning, Governance, Retssikkerhed: Festskrift til Carsten Henrichsen*. Köpenhamn: Jurist- og Økonomforbundet, 2015.

Suominen, Annika, ‘What Role for Legal Certainty in Criminal Law Within the Area of Freedom, Security and Justice in the EU’. *Bergen Journal of Criminal Law and Criminal Justice*, Vol. 2, Nr. 1/2014, s. 1–31.

Tomaszycki, Krzysztof, ‘The interoperability of European information systems for border and migration management and for ensuring security’. *Law and Politics*, Vol. 16, Nr. 3/2018, s. 195–211.

van der Ploeg, Irma & Sprenkels, Isolde, *Machine-Readable BodiesBiometrics, Informatization and Surveillance* i Mordini, E. & Green, M. (red.): Identity, Security and Democracy. Nederländerna: IOS Press, 2009.

van der Sloot, Bart, ‘Legal consistency after the General Data Protection Regulation and the Police Directive’. *European Journal of Law and Technology*, Vol. 9, Nr. 3/2018, s. 1–18.

Vavoula, Niovi, *Databases for Non-EU Nationals and the Right to Private Life. Towards a System of Generalised Surveillance of Movement?* i Bignami, Francesca (red.): *EU Law in Populist Times: Crises and Prospects*. UK: Cambridge University Press, 2020.

Vavoula, Niovi, ‘The ‘Puzzle’ of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection’. *European Law Review*, 2019 Forthcoming.

von Grafenstein, Maximilian, *The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation.* Tyskland: Nomos Verlagsgesellschaft mbH, 2018.

Wachter, Sandra & Mittelstadt, Brent & Floridi, Luciano, ‘Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation’. *International Data Privacy Law*, Vol. 7, Nr. 2/2017, s. 76–99.

EU-LAGSTIFTNING

Fördrag

Europeiska unionens stadga om de grundläggande rättigheterna av den 26 oktober 2012/C 326/02. EUT 2012/C 326/391–407.

Fördraget om Europeiska unionen av den 26 oktober 2012/C 326/01. EUT 2012/C 326/13–390 (konsoliderad version).

Fördraget om Europeiska unionens funktionssätt av den 26 oktober 2012/C 326/01. EUT 2012/ C 326/47–390 (konsoliderad version).

Förordningar

Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna

av uppgifter om viseringar för kortare vistelse (VIS-förordningen). EUT 2008/L 218/60–81.
Europaparlamentets och rådets förordning (EG) nr 1986/2006 av den 20 december 2006 om tillträde till andra generationen av Schengens informationssystem (SIS II) för de enheter i medlemsstaterna som ansvarar för att utfärda registreringsbevis för fordon. EUT 2006/L 381/1–3.
Europaparlamentets och rådets förordning (EG) nr 1987/2006 av den 20 december 2006 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II). EUT 2006/L 381/4–23.
Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (omarbetning) EUT 2013/L 180/1–30.
Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 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). EUT 2016/L 119/1–88.
Europaparlamentets och rådets förordning (EU) 2017/2226 av den 30 november 2017 om inrättande av ett in- och utresesystem för registrering av in- och utreseuppgifter och av uppgifter om nekad inresa för tredjelandsmedborgare som passerar medlemsstaternas yttre gränser, om fastställande av villkoren för åtkomst till in- och utresesystemet för brottsbekämpande ändamål och om ändring av konventionen om tillämpning av Schengenavtalet och förordningarna (EG) nr 767/2008 och (EU) nr 1077/2011. EUT 2017/L 327/20–82.
Europaparlamentets och rådets förordning (EU) 2018/1240 av den 12 september 2018 om inrättande av ett EU-system för reseuppgifter och resetillstånd (Etias) och om ändring av förordningarna (EU) nr 1077/2011, (EU) nr 515/2014, (EU) 2016/399, (EU) 2016/1624 och (EU) 2017/2226. EUT 2018/L 236/1–71.
Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG. EUT 2018/L 295/39–98.
Europaparlamentets och rådets förordning (EU) 2019/817 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området gränser och viseringar, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 och (EU) 2018/1861 samt rådets beslut 2004/512/EG och 2008/633/RIF. EUT 2019/L 135/27–84.
Europaparlamentets och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt samarbete, asyl och migration och om

ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816. EUT 2019/L 135/85–135.

Direktiv

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. EGT 1995/L 281/31–50.

Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 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 2016/L 119/89–131.

Beslut

Rådets beslut 2007/533/RIF av den 12 juni 2007 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II). EUT 2007/L 205/63–84.

Rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet. EUT 2008/L 210/1–11.

Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete. EUT 2008/L 350/60-71.

FINSKA FÖRFATTNINGAR

Lagar

Dataskyddslag (1050/2018).
Finlands grundlag (731/1999).
Lag om behandling av personuppgifter inom Försvarsmakten (332/2019).
Lag om behandling av personuppgifter inom Tullen (650/2019).
Lag om behandling av personuppgifter i polisens verksamhet (616/2019).
Lag om behandling av personuppgifter vid Gränsbevakningsväsendet (639/2019).
Lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018).
Lag om civil underrättelseinhämtning avseende datatrafik (582/2019).
Lag om övervakning av underrättelseverksamheten (121/2019).
Polislag (872/2011).
Strafflagen (29/1889).

Regeringens propositioner och andra förarbeten och utlåtanden till lag

Grundlagsutskottets utlåtande 14/2018 till Regeringen proposition 9/2018 med förslag till lagstiftning som kompletterar EU:s allmänna dataskyddsförordning.

Grundlagsutskottets utlåtande 26/2018 till Regeringen proposition 31/2018 med förslag till lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten och till vissa lagar som har samband med den.
Regeringens proposition till riksdagen med förslag till lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten och till vissa lagar som har samband med den (31/2018).
Regeringens proposition till riksdagen med förslag till lagar om ändring av vissa bestämmelser om behandling av personuppgifter inom justitieministeriets förvaltningsområde (2/2020).
Regeringens proposition till riksdagen med förslag till lag om övervakning av underrättelseverksamheten och lag om ändring av 7 § i statstjänstemannalagen (199/2017).
Regeringens proposition till riksdagen med förslag till lagstiftning som kompletterar EU:s allmänna dataskyddsförordning (9/2018).

RÄTTSFALL

EU-domstolens domar och förslag till avgörande

Domstolens dom av den 2 oktober 2018, *Ministerio Fiscal*, mål C-207/16, ECLI:EU:C:2018:788.
Domstolens dom av den 3 september 2008, *Kadi och Al Barkat International Foundation/ rådet och kommissionen*, mål C-402/05 P, ECLI:EU:C:2008:461.
Domstolens dom av den 3 september 2015, *Inuit Tapiriit Kanatami*, mål C-398/13 P, ECLI:EU:C:2015:535.
Domstolens dom av den 4 december 1974, *van Duyn*, mål 41–74, ECLI:EU:C:1974:133.
Domstolens dom av den 6 november 2003, *Lindqvist*, mål C-101/01, ECLI:EU:C:2003:596.
Domstolens dom av den 6 november 2012, *Otis m.fl.*, mål C-199/11, ECLI:EU:C:2012:684.
Domstolens dom av den 6 oktober 2015, *Schrems*, mål C-362/14, EU:C:2015:650.
Domstolens dom av den 7 juni 2012, *Insinööritoimisto InsTiimi*, mål C-615/10, ECLI:EU:C:2012:324.
Domstolens dom av den 7 maj 2009, *Rijkeboer*, mål C-553/07, ECLI:EU:C:2009:293.
Domstolens dom av den 8 april 2014, *Digital Rights Ireland och Seitlinger m.fl.,* förenade målen C-293/12 och C-594/12, ECLI:EU:C:2014:238.
Domstolens dom av den 9 augusti 1993, *Marshall*, mål C-271/91, ECLI:EU:C:1993:335.
Domstolens dom av den 9 november 1995, *Francovich*, mål C-479/93, ECLI:EU:C:1995:372.
Domstolens dom av den 9 november 2010, *Volker und Markus Schecke och Eifert*, förenade målen C-92/09 och C-93/09, ECLI:EU:C:2010:662.
Domstolens dom av den 13 april 2000, *Karlsson m.fl.*, mål C-292/97, EU:C:2000:202.
Domstolens dom av den 13 december 2017, *El Hassani*, mål C-403/16, ECLI:EU:C:2017:960.
Domstolens dom av den 13 juli 1989, *Wachauf*, mål C-5/88, EU:C:1989:321.

Domstolens dom av den 15 december 2009, *Commission / Finland*, mål C-284/05, ECLI:EU:C:2009:778.
Domstolens dom av den 15 februari 2015, *N.*, mål C-601/15 PPU, ECLI:EU:C:2016:84.
Domstolens dom den 15 juli 1964, *Flaminio Costa mot E.N.E.L.*, mål 6-64, ECLI:EU:C:1964:66.
Domstolens dom av den 16 december 2008, *Huber*, mål C-524/06, ECLI:EU:C:2008:724.
Domstolens dom av den 17 december 1970, *Internationale Handelsgesellschaft*, mål C-11/70, ECLI:EU:C:1970:114.
Domstolens dom av den 17 juli 2014, *YS m.fl.*, förenade målen C-141/12 och C-372/12, ECLI:EU:C:2014:2081.
Domstolens dom av den 17 oktober 2013, *Schwarz*, mål C-291/12, ECLI:EU:C:2013:670.
Domstolens dom av den 20 maj 2003, *Österreichischer Rundfunk m.fl.*, förenade målen C-465/00, C-138/01 och C-139/01, ECLI:EU:C:2003:294.
Domstolens dom av den 21 december 2011, *N.S. m.fl.*, förenade målen C-411/10 och C-493/10, ECLI:EU:C:2011:865.
Domstolens dom av den 21 december 2016, *Tele2 Sverige*, förenade målen C-203/15 och C-698/15, ECLI:EU:C:2016:970.
Domstolens dom av den 26 februari 2013, *Melloni*, mål C‑399/11, ECLI:EU:C:2013:107.
Domstolens dom av den 26 februari 2013, *Åkerberg Fransson*, mål C-617/10, ECLI:EU:C:2013:105.
Domstolens dom av den 29 januari 2008, *Promusicae*, mål C-275/06, ECLI:EU:C:2008:54.
Domstolens yttrande 1/15 av den 26 Juli 2017, ECLI:EU:C:2017:592.
Förslag till avgörande av generaladvokat Sharpston, *Pfleger,* mål C-390/12, EU:C:2013:747.
Pågående mål C-623/17, *Privacy International.*

<u>Europeiska människorättsdomstolen</u>

Dom av den 1 juli 2008 i mål *Liberty m.fl. mot Storbritannien*, 58243/00.
Dom av den 4 december 2008 i mål *S. och Marper mot Storbritannien*, 30562/04 och 30566/04.
Dom av den 4 december 2015 i mål *Roman Zakharov mot Ryssland*, 47143/06.
Dom av den 4 maj 2000 i mål *Rotaru mot Rumänien*, 28341/95.
Dom av den 6 juni 2006 i mål *Segerstedt-Wiberg m.fl. mot Sverige*, 62332/00.
Dom av den 12 januari 2016 i mål *Szabó och Vissy mot Ungern*, 37138/14.
Dom av den 13 november 2012 i mål *M.M. mot Storbritannien*, 24029/07.
Dom av den 16 februari 2000 i mål *Amann mot Schweiz*, 27798/95.
Dom av den 18 april 2013 i *mål M.K. mot Frankrike*, 19522/09.
Dom av den 18 oktober 2011 i mål *Khelili mot Schweiz*, 16188/07.
Dom av den 24 april 1990 i mål *Huvig mot Frankrike*, 11105/84.
Dom av den 25 februari 1997 i mål *Z. mot Finland*, 22009/93.
Dom av den 26 mars 1987 i mål *Leander mot Sverige*, 9248/81.
Dom av den 29 juni 2006 i mål *Weber och Saravia mot Tyskland*, 54934/00.

Högsta förvaltningsdomstolens beslut

Beslut givet av HFD den 30.11.2018/ 5658, Dnr 5873/1/17.

Utländska domar

Frankrike, Administrative Court of Appeal, Nr. 14PA00421, 31 juli 2014.

INTERNATIONELLA ÖVERENSKOMMELSER OCH KONVENTIONER

Den allmänna förklaringen om de mänskliga rättigheterna, 10.12.1948, U.N. Doc. A/RES/217(III).

Europeiska konventionen om skydd för de mänskliga rättigheterna ändrad genom protokoll nr 11 och 14, 4 November 1950.

Internationella konventionen om medborgerliga och politiska rättigheter, New York 16.12.1966, i kraft 23.3.1976, 999 UNTS 171.

Schengenregelverket - Konvention om tillämpning av Schengenavtalet av den 14 juni 1985 mellan regeringarna i Beneluxstaterna, Förbundsrepubliken Tyskland och Franska republiken om gradvis avskaffande av kontroller vid de gemensamma gränserna. EGT 2000/L 239/19–62.

EU-DOKUMENT

Artikel 29-gruppen (WP29)

WP29 2007. *Yttrande 4/2007 om begreppet personuppgifter*, antaget den 20 juni 2007 (WP 136).

WP29 2013. *Yttrande 03/2013 om ändamålsbegränsningar*, antaget den 2 april 2013 (WP 203).

WP29 2014. *Yttrande 1/2014 om tillämpningen av principerna om nödvändighet och proportionalitet samt dataskydd inom brottsbekämpningssektorn*, antaget den 27 februari 2014 (WP 211).

WP29 2017. *Riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679*, antaget den 3 oktober 2017 (WP 251).

WP29 2018. *Opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration*, antaget den 11 april 2018 (WP 266).

Europaparlamentet

Europaparlamentet 2019. Briefing, *Interoperability between EU border and security information systems*, av den 14 juni 2019.

Europeiska dataskyddsstyrelsen (EDPB)

EDPB 2018. *Endorsement 1/2018*, av den 25 maj 2018.

EDPB 2019. *Riktlinjer 4/2019, Inbyggt dataskydd och dataskydd som standard*, av den 13 november 2019.

Europeiska datatillsynsmannen (EDPS)

EDPS 2017 (a). *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, av den 11 april 2017.

EDPS 2017 (b). *Statement on the concept of interoperability in the field of migration, asylum and security,* av den 8 maj 2017. Tillgänglig på: https://edps.europa.eu/sites/edp/files/publication/17-05-08_statement_on_interoperability_en.pdf. Senaste besöksdatum 26.5.2020.

EDPS 2017 (c). *Diskussionsunderlag om interoperabilitet mellan informaionssystem inom området med frihet, säkerhet och rättvisa,* av den 17 november 2017.

EDPS 2018 (a). *EDPS calls for wider debate on the future of information sharing in the EU,* av den 16 oktober 2019. Tillgänglig på: https://edps.europa.eu/press-publications/press-news/press-releases/2018/edps-calls-wider-debate-future-information-sharing_en. Senaste besöksdatum 26.5.2020.

EDPS 2018 (b). *Yttrande 4/2018 om förslagen till två förordningar om inrättande av en ram för interoperabilitet mellan EU:s storskaliga informationssystem*, av den 16 april 2018.

EDPS 2019. *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data,* av den 19 december 2019.

EU:s byrå för grundläggande rättigheter (FRA)

FRA 2010. *Data Protection in the European Union: the role of National Data Protection Authorities* (Strengthening the fundamental rights architecture in the EU II). Luxemburg: Publications Office of the European Union, 2010.

FRA 2012. *Access to justice in cases of discrimination – Steps to further equality.* Luxemburg: Publications Office of the European Union, 2012.

FRA 2016. *Short Thematic Report. National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies*, av den 20 juni 2016.

FRA 2017 (a). *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Volume II: field perspectives and legal update*. Luxemburg: Publications Office of the European Union, 2017.

FRA 2017 (b). *Fundamental rights and the interoperability of EU information systems: borders and security*. Luxemburg: Publications Office of the European Union, 2017.

FRA 2018 (a). *Under watchful eyes: biometrics, EU IT systems and fundamental rights.* Luxemburg: Publications Office of the European Union, 2018.

FRA 2018 (b). *Interoperability and fundamental rights implications: Opinion of the European Union Agency for Fundamental Rights*, av den 11 april 2018.

FRA 2018 (c). *Handbook on European data protection law*. Luxemburg: Publications Office of the European Union, 2018.

FRA 2018 (d). *Preventing unlawful profiling today and in the future: a guide.* Luxemburg: Publications Office of the European Union, 2018.

Kommissionsdokument

Kommissionens beslut om inrättande av en expertgrupp för informationssystem och interoperabilitet, COM (2016) C 257/03 av den 17 juni 2016. EUT 2016/C 257/3–6.

Kommissionens expertgrupp för informationssystem och interoperabilitet, Slutrapport, ST 8434/1/17 REV 1 av den 11 maj 2017, Bryssel.

Kommissionens förslag till Europaparlamentets och rådets förordning om inrättande av en ram för interoperabilitet mellan EU-informationssystem (polissamarbete och rättsligt samarbete, asyl och migration), COM (2017) 794 final av den 12 December 2017, Strasbourg.

Kommissionens *Joint declaration on the EU's legislative priorities for 2018-19*, av den 14 december 2017.

Kommissionens kommunikation, *Shaping Europe's digital future*, av den 19 februari 2020.

Kommissionens konsekvensbedömning SWD/2017/0473 final av den 12.12.2017, Strasbourg.

Meddelande från kommissionen till Europaparlamentet, Europeiska rådet och rådet, *Att genomföra den europeiska säkerhetsagendan mot terrorism och bana väg för en säkerhetsunion*, COM (2016) 230 final av den 20 april 2016, Bryssel.

Meddelande från kommissionen till Europaparlamentet och rådet, *Starkare och smartare informationssystem för gränser och säkerhet*, COM (2016) 205 final av den 26 april 2016, Bryssel.

Meddelande från kommissionen till Europaparlamentet och rådet, *Översikt av informationshanteringen inom området med frihet, säkerhet och rättvisa*, COM (2010) 385 final av den 20 juli 2010, Bryssel.

Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt regionkommittén, *En digital agenda för Europa*, KOM (2010) 245 final av den 19 maj 2010, Bryssel.
Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt regionkommittén, *En europeisk migrationsagenda*, COM (2015) 240 final av den 13 maj 2015, Bryssel.

Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt regionkommittén, *En EU-strategi för data*, COM(2020) 66 final av den 19 februari 2020, Bryssel.

Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt regionkommittén, *Europeiska interoperabilitetsramen – genomförandestrategi*, COM (2017) 134 final av den 23 mars 2017, Bryssel.

Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt regionkommittén, *Europiska Säkerhetsagendan*, COM (2015) 185 final av den 28 april 2015, Strasbourg.

Meijers kommitté

Comments on the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) 12 December 2017, CM1802, COM (2017) 794, antaget den 19 Februari 2018.

ÖVRIGA KÄLLOR

Boehm, Franziska & Cole, Mark D., *Data Retention after the Judgement of the Court of Justice of the European Union*. Rapport gjord på uppdrag av De Gröna/EFA, Europaparlamentet 2014.

Bunyan, Tony, 'The "Point of no return" Interoperability morphs into the creation of a Big Brother centralised EU state database including all existing and future Justice and Home Affairs databases'. *Statewatch Analysis*, Vol. 20, Nr. 7/2018.

Effis Yttrande till riksdagens förvaltningsutskott gällande Dataombudsmannens byrås verksamhetsberättelse 2018.

Europarådet, Resolution 2187: Venedigkommissionens checklista för rättsstatsprincipen (dok. 14387), 2016.

Förklaringar avseende stadgan om de grundläggande rättigheterna, EUT 2007 C 303/02, s. 17–35.

Institute of Electrical and Electronics Engineers (IEEE), Standard Glossary of Software Engineering Terminology Volume 610 of IEEE, 1990.

Jones, Chris, *Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular*

Status. Background document for a legal seminar organised on 14-15 November 2019 in Brussels by PICUM, the Centre for European Policy Studies (CEPS) and European Migration Law.

The Information Commissioner's Office (ICO), *Big data, artificial intelligence, machine learning and data protection*, 2017. Tillgänglig på: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

UNODC, Criminal Intelligence. Manual for Front-Line Law Enforcement, 2010.

UNODC, Criminal Intelligence. Manual for Analysts, 2011.

ELEKTRONISKA KÄLLOR

Brouwer, E. R., 'A Point of No Return in Purpose Limitation? Interoperability and the Blurring of Migration and Crime', Un-Owned Personal Data – Interoperable EU Borders and Transitioning Rights Blog Forum, 2020. Tillgänglig på: http://www.migrationpolicycentre.eu/interoperable-informations-systems-in-the-eu-area-freedom-security-justice/. Senaste besöksdatum 26.5.2020.

Carrera, Sergio, 'Towards interoperable justice. Interoperability and its asymmetry in access rights by EU digital citizens', Un-Owned Personal Data – Interoperable EU Borders and Transitioning Rights Blog Forum, 2020. Tillgänglig på: http://www.migrationpolicycentre.eu/interoperable-informations-systems-in-the-eu-area-freedom-security-justice/. Senaste besöksdatum 26.5.2020.

Catanzariti, Mariavittoria, 'Individuals or 'bare data'? Un-owned Data for Interoperable Borders', Un-Owned Personal Data – Interoperable EU Borders and Transitioning Rights Blog Forum, 2020. Tillgänglig på: http://www.migrationpolicycentre.eu/interoperable-informations-systems-in-the-eu-area-freedom-security-justice/. Senaste besöksdatum 26.5.2020.

Dataombudsmannens byrå, tillgänglig på: https://tietosuoja.fi/sv/vad-ar-en-personuppgift. Senaste besöksdatum 26.5.2020.

eu-LISA hemsida: https://www.eulisa.europa.eu/Newsroom/News/Pages/Gaps-closed-between-information-systems-for-security-borders-and-migration-management.aspx. Senaste besöksdatum 20.5.2020, publicerad 14.5.2019.

Europaparlamentets hemsida (a): https://www.europarl.europa.eu/factsheets/sv/sheet/6/sources-and-scope-of-european-union-law. Senaste besöksdatum 26.5.2020.

Europaparlamentets hemsida (b): https://www.europarl.europa.eu/factsheets/sv/sheet/157/varstvo-osebnih-podatkov. Senaste besöksdatum 26.5.2020.

Europeiska datatillsynsmannens hemsida:

https://edps.europa.eu/press-publications/press-news/press-releases/2018/edps-calls-wider-debate-future-information-sharing_en. Senaste besöksdatum 26.5.2020, publicerad 16.4.2018.

Europeiska rådets hemsida: https://www.consilium.europa.eu/en/press/press-releases/2019/05/14/interoperability- between-eu-information-systems-council-adopts-regulations/. Senaste besöksdatum 26.5.2020, publicerad 14.5.2019.

Finska polisens hemsida: https://www.poliisi.fi/sv/uutiskaruselli/1/0/okat_hot_av_den_organiserade_brottsligheten_i_europa_nya_internationella_kriminella_gang_har_utvidgat_sin_verksamhet_till_finland_79453. Senaste besöksdatum 7.12.2019, publicerad 2.4.2019.

FN:s internationella organisation för migration (IOM) hemsida: https://www.iom.int/key-migration-terms#Irregular-migration. Senaste besöksdatum 20.5.2020.

Groenendijk, Kees, 'Nothing new under the sun? Interoperability of EU justice and home databases', Un-Owned Personal Data – Interoperable EU Borders and Transitioning Rights Blog Forum, 2020. Tillgänglig på: http://www.migrationpolicycentre.eu/interoperable-informations-systems-in-the-eu-area-freedom-security-justice/. Senaste besöksdatum 26.5.2020.

Guerra, Clara, 'Interoperability and refugees from a data protection perspective', Un-Owned Personal Data – Interoperable EU Borders and Transitioning Rights Blog Forum, 2020. Tillgänglig på: http://www.migrationpolicycentre.eu/interoperable-informations-systems-in-the-eu-area-freedom-security-justice/. Senaste besöksdatum 26.5.2020.

Inrikesministeriets hemsida: https://intermin.fi/sv/polisvasendet/civil-underrattelse. Senaste besöksdatum 26.5.2020.

Kommissionens hemsida (a): https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en. Senaste besöksdatum 26.5.2020.

Kommissionens hemsida (b): https://ec.europa.eu/taxation_customs/general-information-customs/customs-security/ics2_en. Senaste besöksdatum 26.5.2020.

Mitsilegas, Valsamis, 'Interoperability as a Rule of Law Challenge', Un-Owned Personal Data – Interoperable EU Borders and Transitioning Rights Blog Forum, 2020. Tillgänglig på: http://www.migrationpolicycentre.eu/interoperable-informations-systems-in-the-eu-area-freedom-security-justice/. Senaste besöksdatum 26.5.2020.

Nygård, Ann-Charlotte, 'EU wide availability of personal data of third country nationals for migration and security purposes – the challenge of ensuring fundamental rights

safeguards', Un-Owned Personal Data – Interoperable EU Borders and Transitioning Rights Blog Forum, 2020. Tillgänglig på: http://www.migrationpolicycentre.eu/interoperable-informations-systems-in-the-eu-area-freedom-security-justice/. Senaste besöksdatum 26.5.2020.

Smith, Alyna & LeVoy, Michele, 'A Point of No Return in Purpose Limitation? Interoperability and the Blurring of Migration and Crime', Un-Owned Personal Data – Interoperable EU Borders and Transitioning Rights Blog Forum, 2020. Tillgänglig på: http://www.migrationpolicycentre.eu/interoperable-informations-systems-in-the-eu-area-freedom-security-justice/. Senaste besöksdatum 26.5.2020.

Statewatch, "Automating the exchange of police data: Council looks to national databases". Tillgänglig på: http://statewatch.org/news/2019/ sep/eu-interop-national.htm. Senaste besöksdatum 6.3.2020, publicerad 9 September 2019.

ILLUSTRATIONER

Figur I, Europeiska kommissionen: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0794&from=ET