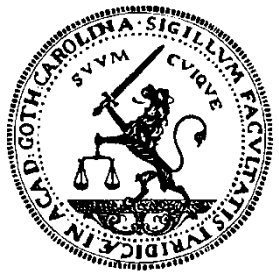

JURIDISKA FAKULTETEN
vid Lunds universitet

Anna Lycke

Biometrisk uppgift – ett hinder för effektiv reglering av biometriska AI-system?

- En utredning av definitionen av biometrisk uppgift enligt gällande EU-rätt och dess betydelse för regleringen av biometriska AI-system

JURM02 Examensarbete

Examensarbete på juristprogrammet
30 högskolepoäng

Handledare: Eduardo Gill-Pedro

Termin för examen: Period 1 VT2022

Innehåll

Summary

This thesis concerns the definition of biometric data in relation to the AI Act as proposed by the European Commission. The examination is conducted with the application of an EU legal method, a legal dogmatic method, and a legal analytical method. The first part consists of a terminological investigation of biometric data as defined in the Data Protection Regulation (DPR). The second part aims to examine how the definition in the DPR affects the regulation of biometric AI systems in the AI Act.

The definition in article 4.14 DPR presents four cumulative requirements that must be assessed when determining whether biometric information can legally classify as biometric data. When examining the meaning of the definition as presented in the DPR, it can be considered as far too narrow. This is mainly a result of the requirement of unique identification of an individual. This is specifically important in regard to the future regulation of biometric AI systems according to the proposal of the European Commission for the new AI Act. Biometric AI systems differ from traditional biometric systems as their area of application usually depends on emotional and behavioral biometric data. However, both behavioral and emotional data tend to lack the ability to uniquely identify individuals. Likewise, the AI systems using them are developed mainly for categorization and inference related purposes. As a result, using an identical copy from the DPR when defining biometric data in the AI Act should not be regarded as a fitting and future proof choice. Both reports and position papers on EU and non-EU level have stated that either replacing or modifying the current definition would be necessary to ensure effective law enforcement for AI. The thesis concludes by stating that this could be done by excluding the requirements related to the identifiable individual.

Sammanfattning

Uppsatsen behandlar den EU-rättsliga definitionen av biometrisk uppgift i förhållande till EU-kommissionens förslag på en kommande AI-förordningen. Utredningen sker med utgångspunkt i en EU-rättslig, rättsdogmatisk och rättsanalytisk metod. Uppsatsen är indelad i två huvuddelar. Den första delen är en terminologisk utredning av dataskyddsförordningens definition av begreppet biometrisk uppgift. Den andra delen syftar till att utreda hur regleringen av biometriska AI-system enligt förslaget till AI-förordningen påverkas av definitionen av biometrisk uppgift.

Definitionen i art. 4.14 dataskyddsförordningen ställer upp fyra kumulativa krav som måste bedömas med hänsyn till den biometriska informationen i det enskilda fallet i syfte att avgöra huruvida informationen i fråga kan klassificeras som biometrisk uppgift. Av uppsatsen utredning framgår att formuleringen av begreppet anses resultera i en alltför insnävad definition som följd av högt ställda krav på unik identifiering av en specifik individ. Detta har särskild betydelse för den framtida regleringen av biometriska AI-system i enlighet med EU-kommissionens förslag till AI-förordningen. Biometriska AI-system skiljer sig från traditionella biometriska system eftersom deras användningsområden till stor del är beroende av biometriska data härstammande från beteendemässiga och emotionella kännetecken. Beteendemässig och emotionell data riskerar dock att sakna förmågan att identifiera individer. Samtidigt utvecklas de AI-system som använder sig av sådan data ofta specifikt i kategoriserings- och uttydningssyften.

Utifrån en analys av begreppets innebörd dras slutsatsen att en exakt kopia av dataskyddslagstiftningens definition av biometrisk uppgift bör därför inte anses som ett passande val för en AI-rättslig kontext. Precis som framgår av rapporter och utredningar av både självständiga organisationer och organisationer på EU-nivå vore det lämpligt att byta ut eller modifiera denna

definition för att säkerställa en effektiv rättstillämpning. Uppsatsen avrundar med att föreslå att detta bör ske genom en exkludering av kravet om unik identifiering.

Förord

Tänk att man äntligen är klar!

Nu har min tid som juriststudent nått sitt slut och det var väl för tur det. Med denna uppsats sätter jag punkt för några år som har kännetecknats av mycket om och men. Nu i maj 2022 kan jag ändå se tillbaka på denna tid som några av de mest lärorika och minnesskapande år hittills.

Jag vill tacka min handledare Eduardo för goda råd och värdefulla synpunkter. Jag vill även tacka mina vänner och familj som har stöttat mig så fint under denna termin.

Lund, maj 2022
Anna

Förkortningar

AI	Artificiell intelligens
AI-förordningen	Förslag till Europaparlamentets och rådets förordning om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter, COM (2021) 206 final
Dataskyddsförordningen	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 upphävandet av direktiv 95/46/EG (allmän dataskyddsförordning)
EKMR	Europeiska konventionen om skydd för de mänskliga rättigheterna
EDPB	Europeiska dataskyddsstyrelsen
EPDS	Europeiska datatillsynsmannen
EU	Europeiska unionen
EU-domstolen	Europeiska unionens domstol
EU-kommissionen	Europeiska kommissionen
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
FEU	Fördraget om Europeiska unionen
FEUF	Fördraget om Europeiska unionens funktionssätt

1. Inledning

1.1 Bakgrund

Användningen av mänskliga egenskaper och beteenden för att identifiera, verifiera och auktorisera individer har ökat i samband med uppkomsten av ny teknik och avancerade system. När egenskaper av denna typ är mätbara faller de in under paraplytermen biometri.[1] Nya tekniker har införts samtidigt som användningsområdena för traditionella biometriska tekniker har breddats.[2] Tidigare dominerades marknaden av system för fingerskanning, ansiktsigenkänning och DNA-analys. Idag kan en individ även identifieras och kategoriseras utifrån kännetecken som tangenttryckning, gest- och signaturdynamik och gångstil.[3]

Som ett resultat av sin naturliga koppling till behandlingen av personuppgifter regleras biometriska system och tekniker ofta av lagstiftning relaterat till integritet och dataskydd.[4] I EU-rätten baseras regleringen av biometriska tekniker och system på huruvida den information de använder sig av anses vara biometriska uppgifter.[5] Begreppets definition och innebörd har dock varit omdiskuterat i doktrin och litteratur.[6]

Biometriska system har även en stark koppling till de moderna användningsområdena för artificiell intelligens (AI).[7] Den 21 april år 2021 presenterade den Europeiska kommissionen (EU-kommissionen) förslag till Europaparlamentets och rådets förordning om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av

[1] Se Wendehorst och Duller (2021) s. 13.
[2] Se COM (2020) 65 final s. 1 ff.
[3] Se Wendehorst och Duller (2021) s. 14.
[4] Se Wendehorst och Duller (2021) s. 23.
[5] Se COM (2020) 65 final s. 22 f.
[6] Jfr bland annat Wendehorst och Duller (2021); Kindt (2018) s. 429 ff.
[7] Se EPRS (2021), avsnitt II f.

vissa unionslagstiftningsakter (AI-förordningen). Målet med förordningen är upprättandet av horisontella regler för utveckling och användning av artificiell intelligens.[8] Av de fyra systemkategorier som förslaget till förordningen behandlar använder sig tre av dem av biometriska uppgifter.[9] Detta rättsliga område kantas dock av svårnavigerade tekniska termer och en interdisciplinär karaktär. Det har lett till oro att vissa biometriska AI-system kan kringgå reglering på EU-nivå.[10] För att undvika kryphål måste definitionen av biometriska uppgifter därför vara passande, framtidssäker och teknisk korrekt.[11]

1.2 Uppsatsens aktualitet

Biometriska teknologier som används i AI-system utgör en signifikant risk för ett flertal grundläggande rättigheter.[12] Det kan röra sig om genomgripande övervakning och spårning av individer, vilket kan resultera i inskränkningar av rätten till privatliv och yttrandefrihet.[13] Ökad kontroll vid allmänna sammankomster kan inverka på mötes- och föreningsrätten genom att ändra sättet grupper och individer kan bedriva sociala och politiska protester.[14] Biometriska AI-system kan även användas för att kategorisera individer, vilket kan resultera i diskriminering och snedvridna beslut i exempelvis utbildnings- och rekryteringsprocesser.[15]

Båda inom och utanför unionen sker ett systematiskt skifte från diskussioner kring etiska AI-ramverk till en rättslig reglering av AI-system.[16] Definitioner skapar och konceptualiserar regulatoriska objekt.[17] I de situationer där

[8] Se motivering till COM (2021) 206 final s. 3.
[9] Se art. 3.34, 3.35 och 3.36 COM (2021) 206 final.
[10] Se Wendehorst och Duller (2021) s. 67; COM (2021) 206 final skäl 6.
[11] Se Wendehorst och Duller (2021) s. 67; Belkadi (2021).
[12] Se ERPS (2021) avsnitt II.
[13] Se Council of Europe Study on Algorithms and Human Rights (2017) s. 12.
[14] Se Council of Europe Study on Algorithms and Human Rights (2017) s. 22 f.
[15] Se COM (2021) 206 final s. 11.
[16] Se ERPS (2021) avsnitt II.
[17] Se Belkadi (2021).

definitionerna behandlar sådant av teknisk natur, såsom vissa typer av data eller tekniska system, sker en översättning av vetenskapliga och tekniska koncept till juridiska termer. Genom denna översättning kolliderar tekniska terminologier med juridiska komponenter och förslag som reflekterar politiska mål. Som ett resultat uppstår inte sällan praktiska konsekvenser för de objekt av teknisk natur som lagstiftaren försöker reglera.[18] Att utreda vad som utgör en biometrisk uppgift blir därför centralt dels ur ett individuellt dataskyddsperspektiv i enlighet med 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 upphävandet av direktiv 95/46/EG (dataskyddsförordningen), dels för att säkerställa transparanta och tillförlitliga AI-system enligt kommande EU-reglering.

Definitionen av biometrisk uppgift i förslaget till AI-förordningen är tagen direkt från EU-rättslig dataskyddslagstiftning utan ytterligare modifikation.[19] Det råder en generell konsensus bland experter att påtvingandet av transparenskrav för aktörer som tillhandahåller AI-system är ett nödvändigt steg för att säkerställa trovärdigheten till artificiell intelligens och går i linje med EU:s grundläggande rättigheter.[20] Dock har EU-kommissionens val att inte justera definitionen av biometriska uppgifter utifrån en mer teknisk synvinkel ifrågasatts.[21] Det är således aktuellt att utreda hur väl regleringen av biometriska AI-system kan komma att fungera i praktiken utifrån vilken typ av information som enligt EU-rätt kan definieras som biometriska uppgifter.

[18] Se Belkadi (2021).
[19] Se skäl 7 COM (2021) 206 final.
[20] Jfr Rodrigues m.fl. (2019), s. 5; The European Consumer Organisation (2021), ’Regulating AI to Protect the Consumer’, Position Paper on the AI Act s. 20; Svenskt Näringsliv (2021), ’Comments on AI Act proposal’ s. 5.
[21] Se Bisztray m.fl. (2021) s. 8; Kindt (2020) s. 65 f.

1.3 Syfte och frågeställning

Uppsatsens övergripande syfte är att utreda hur den EU-rättsliga definitionen av biometrisk uppgift kan påverka regleringen av biometriska AI-system i enlighet med förslaget till den kommande AI-förordningen.

Uppsatsens syfte är därmed tvådelat. Dels kommer definitionen av biometrisk uppgift utredas och tolkas utifrån de krav som ställs upp i dataskyddslagstiftning. Dels syftar uppsatsen till att undersöka och förklara de potentiella konsekvenser som definitionen av biometrisk uppgift kan resultera i för biometriska AI-system utifrån regleringen och definitionerna av dessa i den kommande AI-förordningen.

De frågor som uppsatsen avser att behandla är följande:
- Hur och utifrån vilka rekvisit definieras en biometrisk uppgift enligt gällande EU-rätt?
- Vilken betydelse tillmäts definitionen av biometrisk uppgift i förhållande till de biometriska AI-system som definieras i den kommande AI-förordningen?
- Hur lämplig är användningen av en definition av biometrisk uppgift baserad på dataskyddslagstiftning i en AI-rättslig kontext?
- Bör den EU-rättsliga definitionen av biometrisk uppgift modifieras eller ersättas i en kommande AI-förordningen?

1.4 Avgränsningar

Biometri har länge använts inom fysiologi och definieras enligt traditionell mening som vetenskapliga mätningar av den mänskliga kroppen.[22] Denna uppsats kommer dock endast fokusera på begreppets nutida och teknocentriska innebörd, vilket innefattar mätningar för automatisk igenkänning och kategorisering av personer genom tekniska medel.[23]

Uppsatsen utgörs till stor del av en terminologisk utredning av begreppet biometrisk uppgift. Det innebär att strängheten i bestämmelserna för behandling av biometriska uppgifter inte kommer vara föremål för utredningen i större utsträckning än nödvändigt för att besvara uppsatsens frågeställningar. Följaktligen kommer uppsatsen inte utreda övriga bestämmelser kopplat till förslaget till AI-förordningen eller dataskyddsförordningen. Därmed kommer många andra aktuella rättsliga frågor relaterat till AI således att exkluderas från uppsatsens omfång. Biometriska uppgifter regleras inte heller av någon exklusiv lagstiftning på unionsnivå.[24] Uppsatsen avgränsas därmed ytterligare till de definitioner som framgår av EU-rättslig dataskyddslagstiftning och av internationella standarder. Uppsatsen kommer främst hänvisa till och utgå ifrån definitionen i art. 4.14 dataskyddsförordningen. Som kommer redogöras för i kapitel 2 återfinns definitioner av biometrisk uppgift även i två andra EU-rättsliga dataskyddslagstiftningar. Eftersom dessa dock är identiska med definitionen i dataskyddsförordningen kommer uppsatsen i de flesta fall enbart referera till art. 4.14 i den sistnämnda EU-rättsakten.

Rättsakternas sanktionssystem är vidare endast föremål för granskning på en översiktlig nivå och i den utsträckning som är relevant för diskussion kring terminologiska frågor. Det föreligger en viss brist på relevanta domar från EU-domstolen relaterat till definitionen av biometrisk uppgift och övriga

[22] Se Rommetveit (2016) s.1.
[23] Se Rommetveit (2016) s.1.
[24] Se EPRS (2021) s. 22.

dataskyddsregler gällande artificiell intelligens.[25] Visserligen förekommer biometri som paraplyterm i ett flertal rättsfall från olika områden inom EU-rätten. Det är dock inte möjligt eller relevant att göra en heltäckande utredning av alla de domar som behandlar biometrisk information, vilket innebär en begränsning till de domar som direkt kan kopplas till uppsatsens frågeställningar.

1.5 Terminologi och val av översättning

Biometrisk uppgift v. Biometrisk data

Uppsatsen är av ren EU-rättslig karaktär och behandlar inte nationell svensk rätt. Valet att skriva om biometriska begrepp på svenska innebär dock att vissa godtyckliga val av översättning måste förklaras och tydliggöras. I svensk nationell rätt och doktrin används det svenska begreppet ”biometrisk data” synonymt med det EU-rättsliga begreppet ”biometrisk uppgift”. Det är två separata men förväxlingsbara begrepp.[26] EU har dock valt att översätta den engelska termen ”*biometric data*” till ”biometrisk uppgift” i sina svenska dokument.[27] Här refererar engelskans ”*biometric data”* och svenskans ”biometriska uppgift” till samma begrepp. Uppsatsen kommer utgå från de svenska översättningarna som de framgår av EU-rättsliga källor och enbart använda biometrisk uppgift som översättning av *biometric data*. När det svenska begreppet biometrisk data används är det inte synonymt med biometrisk uppgift utan refererar istället till generell biometrisk information.

IKT

Informations- och kommunikationsteknik. Inbegriper alla de fysiska och immateriella verktyg som kan generera, skicka, ta emot, behandla eller representera data i elektronisk form.

[25] Se FRA (2021) s. 65.
[26] Jfr exempelvis Mot. 2021/22:4360, Maria Malmer Stenergard m.fl. (M), med anledning av prop. 2021/22:81: Anpassning av svensk rätt till EU:s nya in- och utresesystem, s. 2.
[27] Se exempelvis svenska översättningen av art. 4.14 dataskyddsförordningens och art. 3.33 COM (2021) 65 final.

1.6 Metod och material

Centralt för uppsatsen är tolkningen av EU-rättsliga källor mot bakgrund av deras ändamål och syfte. Med hänsyn därtill tillämpas huvudsakligen en EU-rättslig metod.[28] Uppsatsens syfte är delvis att beskriva och systematisera gällande rätt. En kompletterande utgångspunkt för den deskriptiva delen av uppsatsen är därför en rättsdogmatisk metod.[29] Den rättsdogmatiska metoden kännetecknas av användandet av ett begränsat antal källor.[30] Enligt Sandgren ska lag och prejudikat även inbegripa EU-rättsligt material.[31]

Mot bakgrund av metodvalen kommer materialet bestå av de allmänt accepterade rättskällorna, såsom praxis, lagstiftning och relevant doktrin av främst EU-rättslig karaktär.[32] EU-rätten tillämpar ett hierarkiskt system där primärrätten har företräde framför övriga kategorier av rättskällor. Det är de grundläggande fördragen som utgör primärrätten. De består av fördraget om Europeiska unionen (FEU), fördraget om Europeiska unionens funktionssätt (FEUF) samt EU:s stadga om de grundläggande rättigheterna (EU-stadgan).[33]

Sekundärrätten faller in under primärrätten och består huvudsakligen av bindande rättsakter i form av förordningar, direktiv och beslut. I sekundärrätten inbegrips även icke-bindande (*soft law*) rättsakter såsom rekommendationer, ingresser och förslag. Dessa instrument har fått ökad betydelse inom somliga områden men det föreligger fortfarande viss osäkerhet kring deras rättskällevärde. De två högst rangordnade källorna kompletteras av praxis och andra EU-rättsliga källor.[34]

[28] Se Hettne och Otken Eriksson (2011) s. 36.
[29] Se Sandgren (2015) s. 43.
[30] Se Sandgren (2015) s. 43.
[31] Se Sandgren (2015) s. 46.
[32] Se Hettne och Otken Eriksson (2011) s. 40.
[33] Se Hettne och Otken Eriksson (2011) s. 41 f.
[34] Se Hettne och Otken Eriksson (2011) s. 47.

Materialet i uppsatsen hämtas från nästan samtliga kategorier i den EU-rättsliga källhierarkien. Det inkluderar primärrätt, EU-stadgan, allmänna rättsprinciper, förarbeten, doktrin och rättspraxis.[35] Dock är utgångspunkten sekundärrätten bestående av gällande och kommande förordningar i form av dataskyddsförordningen och AI-förordningen. All funnen rättspraxis som kan anknytas till tolkningen av relevanta koncept och begrepp kommer att utredas och analyseras. Det föreligger dock en brist på relevant rättspraxis på området, vilket har begränsat materialtillgången till en viss grad.

I uppsatsen avses även att redogöra för internationella tekniska standarder och terminologi. Det sker i syftet att komplettera de rättsliga källorna och underlätta för en analys av till stor del teknisk karaktär. Även litteratur som berör teknik kommer användas för att bistå i vägledningen kring tekniska processer och begrepp. Övriga källor består bland annat av expertkommentarer, vitböcker, rapporter och vetenskapliga artiklar. En central källa är dessutom en studie upprättad på begäran av Europaparlamentet om biometriska tekniker.[36]

Uppsatsen kommer att kompletteras med användandet av en rättsanalytisk metod. Metoden möjliggör en mer informell analys av konsekvenserna av definitionen av biometrisk uppgift eftersom argumentationen uppfattas i avsaknad av ett rätt svar.[37] Genom att använda en rättsanalytisk metod kan kommissionens lagförslag och uttalanden kritiskt granskas i uppsatsens analysdelar. Den rättsanalytiska metoden blir därför ett viktigt verktyg i syftet att analysera det juridiska materialet och rättskällorna i förhållande till icke-juridiskt material. Eftersom uppsatsen till viss del avser granska en kommande rättsakt blir en argumentation enligt *de lege ferenda* relevant.[38]

[35] Se Hettne och Otken Eriksson (2011) s. 40.
[36] Se Wendehorst och Duller (2021).
[37] Se Sandgren (2015) s. 46.
[38] Se Hellern, Jan (1975), ’Argumentation de lege ferenda’, Svensk Juristtidning, s.4, https://svjt.se/svjt/1975/401, besökt 2022-03-29.

Som ett resultat av den EU-rättsliga kontexten kommer uppsatsen således anta en EU-rättslig infallsvinkel. Detta kompletteras med ett tekniskt perspektiv, vilket motiveras med att uppsatsen genomsyras av en till stor del informationsteknologisk karaktär. Det tekniska perspektivet används för att kontextualisera rättsområdet och ge läsaren en bättre förståelse för det ämne uppsatsen behandlar.

1.7 Disposition

Kapitel 2 syftar till att ge läsaren en grundläggande förståelse för användningen av biometriska teknologier och begrepp. Här följer en utredning av uppkomsten av biometrisk uppgift, dess historiska kontext och introduktion i EU-rätten. Det följande kapitel 3 består av en terminologisk utredning av definitionen av biometrisk uppgift i dataskyddsförordningen. Kapitlet avslutas med en delanalys där resultatet av utredningen analyseras.

I kapitel 4 sker en redogörelse för förslaget till den kommande AI-förordningen, dess reglering av biometriska AI-system och systemens användning på grundval av biometriska uppgifter. Kapitlet karaktäriseras av ett starkare analytiskt perspektiv än tidigare kapitel. Inledningsvis presenteras förslaget till den kommande förordningen som syftar till att reglera AI inom unionen. Det följs av en redogörelse av de biometriska AI-system som enligt förordningen använder sig av biometriska uppgifter. Sedan utreds konsekvenserna av begreppsdefinitionen av biometrisk uppgift i relation till de behandlade systemen. Kapitlet avslutas med ytterligare en delanalys. I denna sista analys bedöms lämpligheten av den nuvarande definitionen av biometrisk uppgift i förhållande till biometriska AI-system och övrig dataskyddslagstiftning på EU-rättslig nivå. Vidare undersöks huruvida definitionen är tillräcklig eller om modifikationer bör ske med hänvisning till grundläggande rättigheter, förordningens syfte och allmänna rättsprinciper. Uppsatsen avslutas med ett kapitel om avslutande reflektioner där definitionen av biometrisk data diskuteras ytterligare.

2 EU-rättslig utveckling av biometri och tekniska utgångspunkter

2.1 Historisk och juridisk bakgrund till biometriska begrepp

Termen ”biometri” härstammar från grekiskans *bios* (liv) och *metron* (mätningar)[39] och har historiskt associerats med den statistiska analysen av generell biologisk information.[40] Biometri är därför en allomfattande term relaterat till bearbetningen av biologiska mätvärden med hjälp av statistiska metoder. I stora drag kan det förstås som en vetenskaplig studie om kroppens mått och proportioner.[41] Termen består av ett flertal separata discipliner och insnävningar, vilket inkluderar automatiserad teknik för analys av mänskliga egenskaper i bland annat igenkännings- och kategoriseringssyfte.[42] Genom avläsning av unika kroppsliga kännetecken som exempelvis röst, ögonbotten och fingeravtryck, kan en dator kontrollera eller bekräfta en individs identitet.[43]

Utifrån en juridisk kontext kopplas denna moderna teknocentriska tolkning av biometri främst till frågor om integritet och dataskydd.[44] Inom ramen för informationssäkerhet introducerades begreppet runt år 1980 i syfte att ersätta den dåvarande benämningen ”automatisk personlig identifiering” som använts under tidigare årtionden.[45] Biometri utifrån denna tolkning består av en mängd relaterade begrepp som tillsammans, och i förhållande till varandra,

[39] Se Ashok m.fl. (2010) s. 2402.
[40] Se ISO/IEC TR 24741:2018 avsnitt ”Introduction”.
[41] Se Ashok m.fl. (2010) s. 2402.
[42] ISO/IEC TR 24741:2018 avsnitt 4.1.
[43] Se Wendehorst och Duller (2021) s. 34.
[44] Se Wendehorst och Duller (2021) s. 23.
[45] Se ISO/IEC TR 24741:2018 avsnitt ”Introduction”.

utgör hela den datoriserade process som används för att kontrollera och identifiera människors identiteter. Eftersom biometri även i en rättslig kontext härrör från en naturvetenskaplig bakgrund är det viktigt att beskriva de terminologiska skillnaderna mellan de biometriska begreppen för att i senare skede kunna förstå hur de praktiskt omsätts ur ett juridiskt perspektiv.[46]

Senare delavsnitt redogör utförligt för den EU-rättsliga definitionen av det juridiska begreppet biometrisk uppgift. För att kunna utreda vad definitionen av en biometrisk uppgift innebär bör termen dock inledningsvis särskiljas och förstås separat från närbesläktade begrepp.[47] Relevant dataskyddslagstiftning inkluderar inte definitioner av samtliga centrala begrepp som behövs för att förstå bakgrunden till uppkomsten av biometrisk uppgift som en juridisk konstruktion.[48] Istället hänvisar både rättsliga och tekniska experter ofta till utomstående internationella standarder för att fylla ut kunskapsluckor vid tolkning av olika biometriska data.[49] En vanlig utgångspunkt för definitioner av biometriska begrepp ur ett tekniskt perspektiv är samlingen säkerhetsstandarder utgivna av standardiseringsorganisationerna ISO och IEC (ISO/IEC).[50] Det ska dock betonas att varken dataskyddsförordningen eller övriga rättsakter på unionsnivå direkt hänvisar till utomstående standarder i tolkningssyfte gällande deras bestämmelser.[51]

[46] Se Jasserand (2015) s. 3.
[47] Se Jasserand (2015) s. 3 f.
[48] Se avsaknad av biometriska begrepp med undantag för biometrisk uppgift i dataskyddsförordningen och Europaparlamentets och rådet 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.
[49] Se Jasserand (2016) s. 4 som refererar till Garante (2014), Annex A to the Garante's Order Concerning Biometrics.
[50] Jfr Wiewiórowski (2020) s. 2; Jasserand (2015) s. 5; Gorodnichy (2016) s. 3 ff.
[51] Se Bisztray m.fl. (2021) s. 2.

2.2 Tekniska definitioner av biometriska begrepp

Enligt ISO/IEC beskrivs *biometriska egenskaper* som alla de särskiljande mänskliga kännetecken som går att läsa av i mätbara enheter. De är antingen oföränderliga och stabila biologiska kännetecken, eller föränderliga och beteendebaserade kännetecken.[52] Finger- och ansiktsavtryck, struktur av iris eller handvener, gångstil, handskriven signaturdynamik och unika mönster på näthinnans blodkärl, är alla exempel på biometriska egenskaper hos en individ.[53] Ett *biometriskt prov* definieras som en analog eller digital representation av biometriska egenskaper innan de genomgår en biometrisk extraktion. Exempelvis kan ett lagrat fotografi av ett fingeravtryck utgöra ett biometriskt prov.[54]

Biometrisk teknologi används för att inhämta, lagra och bearbeta biometrisk information och egenskaper om individer.[55] De biometriska egenskaperna genomgår en förvandling till digitala bitar som kan användas för framtida jämförelser. Teknologier och operationer som kategoriseras som biometriska tekniker förlitar sig således på teknisk bearbetning av data relaterat till fysiska, fysiologiska eller beteendeaspekter av den mänskliga kroppen.[56] Den tekniska bearbetningen syftar därmed till att identifiera, verifiera eller kategorisera individer utifrån deras unika biometriska egenskaper.[57]

Ett *biometriskt system* utvecklas för en stor mängd vitt skilda syften som ofta kopplas till tillämpningen av biometrisk igenkänningsteknologi.[58] Ett biometriskt system kan därutöver användas i syfte att kategorisera egenskaper

[52] ISO/IEC 2382-37:2022 avsnitt. 3.1, 37.01.02.
[53] ISO/IEC 2382-37:2022 avsnitt. 3.1, 37.01.02; ISO/IEC 2382-37:2017 avsnitt 3.1.2.
[54] ISO/IEC 2382-37:2022 avsnitt. 3.3, 37.03.21. Termen ’prov’ är här en översättning av engelskans *’sample’* som kommer till uttryck i dokumentet.
[55] ISO/IEC TR 24741:2018 avsnitt. 4.1: som även hänvisar till ISO/IEC 2382-37:2017.
[56] ISO/IEC TR 24741:2018 avsnitt 4.1 och avsnitt 6.
[57] Se Wiewiórowski (2020) s. 8; EPRS (2021) s. 20.
[58] Se Artikel 29 – Arbetsgruppen för dataskydd (2003) s 4; ISO/IEC 2382-37:2022 avsnitt 3.2, 37.02.03.

från samma typ av kroppslig källa, vilket även kan ske när egenskapen inte kan kopplas till en specifik individ.[59] Termen biometrisk *igenkänning* omfattar både identifiering och verifiering.[60] *Biometrisk identifikation* söker efter attribut tillhörande en specifik individ i en databas där biometriska egenskaper lagras.[61] Det skiljer sig följaktligen från *biometrisk verifiering*, som syftar till att bekräfta ett biometriskt identifieringsanspråk genom att jämföra biometriska egenskaper med varandra.[62] En *kategorisering av biometriska egenskaper* samlar in och systematiserar egenskaper utifrån deras kroppsliga källa, oberoende av huruvida det kan kopplas till en specifik individ eller inte. [63] Exempel på biometriska tekniker som biometriska system använder sig av kan således vara näthinneskanning, fingeravtrycksskanning eller hjärtfrekvenssensorer. Från definitionen utesluts analys av beteenden som kan kontrolleras av den mänskliga viljan till en högre grad, vilket bland annat inkluderar sökhistorik, shoppingmönster eller innehållet i skriftliga konversationer.[64]

Tillskillnad från rena tekniska begrepp, som exempelvis *biometrisk egenskap*, härstammar *biometrisk uppgift* från både en teknisk och juridisk kontext. Begreppet som det används inom EU-rätten anses dock vara av ren juridisk karaktär.[65] Termen biometrisk uppgift har använts inom naturvetenskapen innan det adopterades av lagstiftare som ett rättsligt koncept. När begreppet introducerades i EU-rätten modifierades dess innebörd för att kunna användas som underlag för biometrisk reglering i en rättslig kontext.[66] En teknisk definition av biometrisk uppgift enligt internationella standarder *kräver* inte en koppling till en specifik person[67], samtidigt som samma koppling har central betydelse för begreppets juridiska motsvarighet.[68] Den tekniska

[59] ISO/IEC TR 24741:2018 avsnitt 4.2.
[60] ISO/IEC 2382-37:2022 avsnitt. 3.1, 37.01.03.
[61] ISO/IEC 2382-37:2022 avsnitt. 3.8, 37.08.02.
[62] ISO/IEC 2382-37:2022 avsnitt. 3.8, 37.08.03.
[63] ISO/IEC TR 24741:2018 avsnitt 4.2.
[64] Se Wiewiórowski (2020) s. 12.
[65] Se Jasserand (2016) s. 7 f.
[66] Se Jasserand (2015) s. 13 ff.
[67] ISO/IEC 2382-37:2017, avsnitt 3.3.6.
[68] Se Jasserand (2016) s. 7.

definitionen av biometrisk uppgift omfattar biometriska egenskaper och prov när de behandlas i syfte att omvandlas till format som kan användas för biometriska tekniker[69]. Den juridiska definitionen kommer utredas detaljerat i kommande kapitel.

Trots att ett flertal av EU:s institutioner och organ har använt begrepp relaterade till biometri synonymt med varandra bör dessa inte förväxlas.[70] I juridiska rapporter och artiklar har ”biometri” ofta använts för att beskriva samtliga termer med koppling till begreppet, vilket förutom biometriska uppgifter bland annat inkluderar biometriska egenskaper, biometriska tekniker och biometriska system.[71] De tekniska skillnaderna är dock både ett faktum och av stor vikt för att kunna bedöma vad som faller in under EU-rättens tillämpningsområde för biometri.[72] Att EU själv har förväxlat begreppen kan tolkas som att det har förelegat en viss terminologisk oenhetlighet på unionsnivå.[73]

2.3 Biometriska uppgifters utveckling på EU-nivå

Innan millennieskiftet var en koppling mellan biometriska uppgifter och dataskyddsregler inte aktuellt för diskussion på EU-nivå.[74] Tidiga EU-rättsliga dokument gällande dataskydd, inkluderat Europaparlamentets och rådet 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 (dataskyddsdirektivet) och Europarådets konvention 108 av den 28 januari 1981 om skydd för enskilda vid automatisk

[69] ISO/IEC 2382-37:2022 avsnitt 3.3. 37.03.06.
[70] Se Jasserand (2015) s. 3.
[71] Se Jasserand (2015), s.3 – dock notera att ”biometri” här är en översättning från engelskans ”*biometrics*”. Det är oklart om den svenska översättningen på samma sätt har använts som en synonym för övriga biometriska begrepp.
[72] Se Jasserand (2015) s. 3.
[73] Se Jasserand (2015) s. 9 f.
[74] Se Jasserand (2015) s. 8.

databehandling av personuppgifter (Konvention 108), innehöll inga bestämmelser om biometriska uppgifter.[75]

Under tidigt 2000-tal började användningen av biometriska uppgifter inom unionen öka som följd av nya krav och teknologisk utveckling.[76] Medlemsstaterna förpliktigades att lagra ansiktsbilder och fingeravtryck i pass och andra resedokument genom art. 2.1 i Rådets förordning (EG) nr 2252/2004 av den 13 december 2004 om standarder för säkerhetsdetaljer och biometriska kännetecken i pass och resehandlingar som utfärdas av medlemsstaterna. Under samma tidsperiod upprättade unionen databaser i syfte att samla in biometrisk data tillhörande asyl- eller visumsökande individer från länder utanför EU-regionen.[77] Parallellt med initiativen på EU-nivå började privata och offentliga aktörer använda biometriska uppgifter för att effektivisera kontroll och övervakning.[78] Det hade således blivit vanligare att samla in och använda biometriska uppgifter. Frågor gällande deras potentiella status som skyddsvärda uppgifter diskuterades dock fortfarande i relativt liten utsträckning på unionsnivå.[79]

Först år 2003 adresserades kopplingen mellan biometriska uppgifter och dataskyddsregler genom att Arbetsgruppen för dataskydd (arbetsgruppen) publicerade ett arbetsdokument om biometriska metoder (WP80).[80] Arbetsgruppen var ett rådgivande organ som publicerade ett flertal förslag och riktlinjer för personuppgiftsskydd fram tills att det senare skulle komma att ersättas av den europeiska dataskyddsstyrelsen (EDPB) genom art. 68 i dataskyddsförordningen.[81] WP80 var en direkt konsekvens av händelserna

[75] Se Zaborska (2019) s. 99; Jfr även avsaknad av begreppet biometrisk uppgift i både dataskyddsdirektivet och Konvention 108.
[76] Se Jasserand (2016) s. 6.
[77] Se Förslag till rådets förordning om ändring av förordning (EG) nr 1683/95 om en enhetlig utformning av visumhandlingar, Förslag till rådets förordning om ändring av förordning (EG) nr 1030/2002 om en enhetlig utformning av uppehållstillstånd för medborgare i tredjeland, s. 2 och 7.
[78] Se Kindt (2020) s. 62.
[79] Se Kindt (2020) s. 62.
[80] Se Artikel 29 – Arbetsgruppen för dataskydd (2003) s. 3 ff.
[81] Se även art. 94.2 dataskyddsförordningen som stadgar *”[…] Hänvisningar till arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, som inrättades genom artikel 29 i direktiv 95/46/EG, ska anses sim hänvisningar till*

som utspelade sig 11 september 2001 och en av de åtgärder som medlemsstaterna begärde kommissionen vidta i syfte att förbättra dokumentsäkerheten.[82] I dokumentet bedömer den aktuella arbetsgruppen huruvida dataskyddsdirektivet bör kunna tillämpas på biometriska uppgifter.[83] Arbetsgruppen stadgar att de flesta typer av biometriska uppgifter kan indikera behandling av personuppgifter i enlighet med dataskyddsdirektivet. Direktivets dataskyddsrättsliga principer bör därför respekteras vid utveckling av biometriska system.[84] WP80 innehåller dock ingen definition av biometrisk uppgift utan en begreppsförklaring presenteras formellt för första gången på EU-rättslig nivå i samband med införandet av dataskyddsreformen år 2018.[85]

Europeiska dataskyddsstyrelsen, som inrättas genom denna förordning."; Skäl 139 dataskyddsförordningen.

[82] Se Artikel 29 – Arbetsgruppen för dataskydd (2003), s. 2.

[83] Se Artikel 29 – Arbetsgruppen för dataskydd (2003), s. 8 f.

[84] Se Artikel 29 – Arbetsgruppen för dataskydd (2003), s. 11.

[85] Se följande kapitel.

3 Biometrisk uppgift i dataskyddslagstiftning

3.1 Dataskyddsförordningens definition av biometrisk uppgift

Skyddet av fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter harmoniserades tidigare genom dataskyddsdirektivet.[86] I syfte att anpassa skyddet till samtiden och den tekniska utvecklingen introducerades dataskyddsförordningen den 25 maj 2018.[87] Förordningen har ett extraterritoriellt tillämpningsområde och reglerar hur personuppgifter får behandlas av offentliga och privata aktörer.[88]

Dataskyddsförordningen skyddar således personuppgifter. Samtliga personuppgifter skyddas av de allmänna reglerna om dataskydd som framgår av förordningen.[89] Det innebär att en behandling av personuppgifter dels måste följa de grundläggande principerna.[90] Dels behöver behandlingen av personuppgifterna ha stöd i en rättslig grund.[91]

I samband med ikraftträdandet av dataskyddsförordningen presenteras en definition av biometrisk uppgift för första gången på EU-nivå.[92] Art. 4.14 dataskyddsförordningen definierar en biometrisk uppgift som följer:

[86] Se art. 1.1 dataskyddsdirektivet.
[87] Se skäl 5 och 6 dataskyddsförordningen.
[88] Se art. 3.1 dataskyddsförordningen.
[89] Se art. 5 och 6 dataskyddsförordningen.
[90] Se art. 5 dataskyddsförordningen.
[91] Se art. 6.1 dataskyddsförordningen.
[92] Se Kindt (2020) s. 63 f.

”[…] ***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 fingeravtrycksuppgifter*”.

Samma definition återfinns i 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 (LED-direktivet).[93] LED-direktivet introducerades samtidigt som dataskyddsförordningen i syfte att reglera behandlingen av personuppgifter när detta sker av behöriga myndigheter vid brottsbekämpning, brottsmålshantering eller straffverkställighet.[94]

All biometrisk information som kan anses vara personuppgifter omfattas av allmänna dataskyddsregler.[95] Ur ett EU-rättsligt perspektiv är frågan om huruvida biometrisk information definieras som biometriska uppgifter betydelsefull av främst två specifika anledningar. För det första tilldelas biometrisk uppgifter ett mer omfattande behandlingsskydd än annan biometrisk data.[96] Enligt dataskyddsförordningen anses biometriska uppgifter tillhöra en särskild kategori av personuppgifter och är enligt art. 9.1 förbjudna att behandla.[97] Enligt EU-kommissionen motiveras det speciella behandlingsförbudet av det faktum att personuppgifter som till sin natur är känsliga med hänsyn till grundläggande rättigheter och friheter bör åtnjuta särskilt skydd.[98] Kategorisering av biometriska uppgifter som känsliga personuppgifter var ett resultat av Europaparlamentets inblandning vid

[93] Se art. 3.13 LED-direktivet.
[94] Se skäl 4,7 och 9 LED-direktivet.
[95] Se art. 5 dataskyddsförordningen om principer för behandling av personuppgifter och art. 6 dataskyddsförordningen om laglig behandling av personuppgifter.
[96] Se exempelvis redogörelsen för övriga biometriska begrepp i avsnitt 3.1.
[97] Se undantag till huvudregeln i art. 9.2 dataskyddsförordningen.
[98] Se skäl 51 dataskyddsförordningen.

omröstningen av dataskyddsförordningen.[99] I kommissionens framlagda förslag till dataskyddsförordningen var biometriska uppgifter ursprungligen endast att anses som genetisk data.[100] Vid omröstningen av förslaget beslutade Europaparlamentets att lägga till biometriska uppgifter i listan över särskilda och känsliga personuppgifter vid uppfyllande av kravet att de används för att ”entydigt identifiera” en individ.[101]

För det andra är definitionen i art. 4.14 dataskyddsförordningen central för tillämpningen av andra gällande och framtida EU-rättsakter. Som kommer diskuteras närmare i kapitel 4 sker regleringen av AI-system i det nuvarande förslaget till den kommande AI-förordningen på grundval av deras användning av biometriska uppgifter som de definieras i dataskyddslagstiftning.[102] Det är därför viktigt att utreda och precisera definitionen av biometrisk uppgift i art. 4.14 dataskyddslagstiftningen även för tillämpning av bestämmelser inom andra rättsområden på EU-nivå.

För att data ska klassificeras som en biometrisk uppgift krävs det utifrån definitionen i art. 414 dataskyddsförordningen att det (1) rör sig om en personuppgift som (2) genomgått särskild teknisk behandling och (3) rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken, samt slutligen (4) används i identifikationssyfte.[103] I kommande avsnitt följer en övergripande redogörelse av respektive rekvisit.

[99] Se ändringen i art. 9.1 Europaparlamentets lagstiftningsresolution av den 12 mars 2014 om förslaget till Europaparlamentets och rådets förordning för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning) (COM (2012) 0011 – C7-0025/2012 – 2012/0011(COD)).
[100] Se Jasserand (2016) s. 19.
[101] Se Jasserand (2016) s. 19 f.; art. 9.1 dataskyddsförordningen.
[102] Se art. 3.34, 3.35, 3.36 och 3.37 COM (2021) 206 final.
[103] Se art. 4.14 dataskyddsförordningen.

3.2 Rekvisit för klassificering som biometrisk uppgift i enlighet med art. 4.14 dataskyddsförordningen

3.2.1 Personuppgift

Det första rekvisitet för att data ska utgöra en biometrisk uppgift är att det också tar formen av en personuppgift som det definieras i dataskyddsförordningen.[104] Innan dataskyddsförordningen trädde ikraft år 2018 baserades den EU-rättsliga regleringen av personuppgifter på definitionen i dataskyddsdirektivet.[105] Definitionen skulle vidare tolkas i ljuset av art. 1 dataskyddsdirektivet. I art. 4.1 dataskyddsdirektivet valde EU-kommissionen att brett definiera personuppgifter som följer:

” […] varje upplysning som avser en identifierad eller identifierbar fysisk person (den registrerade). En identifierbar person är en person som direkt eller indirekt, framför allt genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet”.

Dataskyddsförordningen behåller en nästintill identisk kopia av definitionen av personuppgift i dataskyddsdirektivet men speglar i större grad den teknologiska utvecklingen genom att introducera ett bredare tillämpningsområde.[106] Enligt dataskyddsförordningen lyder definitionen av personuppgift i art. 4.1 som följer:

” […] ***varje upplysning*** *som* ***avser*** *en* ***identifierad eller identifierbar*** *fysisk person (nedan kallad en registrerad), varvid en identifierbar* ***fysisk person*** *är en person som direkt eller indirekt kan identifieras särskilt med hänvisning*

[104] Se definition av biometrisk uppgift i ovanstående avsnitt 3.1.
[105] Se art. 2(a) dataskyddsdirektivet; art. 1 dataskyddsdirektivet.
[106] Se exempelvis skäl 6, 7 och 9 dataskyddsförordningen.

till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet".

Av art. 4.1 dataskyddsförordningen kan utläsas att EU-kommissionen fastställer kriterier utifrån fyra beståndsdelar av definition för att information ska kunna anses vara personuppgifter. Kriterierna anses utgöras av (i) varje upplysning, (ii) som avser, (iii) en identifierad eller identifierbar, samt (iv) fysisk person.[107] Samma lista av kriterier framgår även av EU-rättslig doktrin gällande personuppgifter.[108]

Kriterium (i) ska tolkas brett och innebär att informationen kan vara av både objektiv och subjektiv karaktär.[109] Informationen är inte heller begränsad till ett specifikt format utan alla former av data kan innehålla personuppgifter.[110] Det inkluderar bland annat numeriska data, videofilmer, ljud och fotografier.[111] Enligt kriterium (ii) måste information *avse* en individ.[112] Bestämmelsen innebär att informationen inte nödvändigtvis måste säkerställa en persons direkta identitet genom exempelvis namn eller personnummer. Det räcker att information hjälper till att avslöja detaljer om individen eller att behandlingen av informationen påverkar individen i någon utsträckning.[113]

Kriterium (iii) syftar till att informationen måste kunna identifiera en specifik individ, antingen självständigt eller i kombination med annan information.[114] Slutligen innebär kriterium (iv) att endast information om fysiska personer kan klassificeras som personuppgifter. Information som berör en juridisk

[107] Se art 4.1 dataskyddsförordning; Richie (2020).
[108] Se Artikel 29 – Arbetsgruppen för skydd av personuppgifter (2007) s. 6; Se även Europeiska kommissionen, 'What is considered personal data under the EU GDPR?', <https://gdpr.eu/eu-gdpr-personal-data/>, besökt 2022-04-05.
[109] Se Purtova (2018) s. 48; Se även C-434/16 *Nowak* p. 34.
[110] Se Richie (2020); Purtova (2018) s. 48.
[111] Se Richie (2020; Purtova (2018) s. 50 f.
[112] Se art. 4.1 dataskyddsförordningen; Richie (2020).
[113] Se Richie (2020); Purtova (2018) s. 53 f.
[114] Se Richie (2020); Purtova (2018) s. 4

person kan därför inte omfattas av dataskyddsförordningens personuppgiftsskydd. Personuppgifter kan inte heller bestå av information som tillhör en avliden fysisk person.[115]

3.2.2 Erhållits genom en särskild teknisk behandling

Efter det första kravet kopplat till definitionen av personuppgift följer krav (2) om att den biometriska uppgiften måste vara ett resultat av en särskild teknisk behandling.[116] Termen ”särskild teknisk behandling” härrör från ett förslag från Europarådets tillsatta kommitté rörande bioetik (kommittén).[117] Förslaget gällde revisionen av Konvention 108 och kommittén diskuterade den dåvarande definitionen av biometrisk uppgift som i detta skede inte inkluderade kravet på att vara produkten av en teknisk behandling.[118] Kommittén menade att EU-kommissionens dåvarande förslag på definitionen av biometrisk uppgift skulle riskera att resultera i att en för stor mängd data omfattades av begreppet. Kommittén betonade att många biometriska egenskaper endast genomgår vanlig behandling, exempelvis utbyte av videor och publicering av fotografier, vilket inte borde anses kräva särskild lagstiftning.[119]

De EU-rättsliga lagstiftarna specificerar inte vad särskild teknisk behandling konkret innebär.[120] Huruvida kravet specifikt syftar till en teknisk behandling av ett biometriskt system bekräftas inte av lagtexten, även om det är troligt att bestämmelsen är menad att tolkas på detta sätt.[121] Utifrån övrig litteratur

[115] Se skäl 27 dataskyddsförordningen.
[116] Se art. 4.14 dataskyddsförordningen.
[117] Jfr Kindt (2018) s. 531.
[118] Se Kindt (2018) s. 531; COM (2012) 11 final art. 4.11 där den dåvarande definitionen lydde: *”alla uppgifter som rör en enskild persons fysiska, fysiologiska eller beteendemässiga kännetecken och som gör det möjligt att identifiera honom eller henne individuellt, såsom ansiktsbilder eller fingeravtrycksuppgifter*”.
[119] Se Kindt (2018) s. 531 f.
[120] *En definition av ”särskild teknisk behandling” saknas i dataskyddsförordningen*; Jfr Bisztray (2021) s. 4.
[121] Se Kindt (2018) s. 531.

och kommentarer kan det tolkas som att den tekniska behandlingen speciellt betonar vikten av IKT-resurser kopplade till lämplig mjukvara.[122] I sina artiklar redogör Bisztray m.fl. och Jasserand för hur en teknisk behandling av biometriska uppgifter i praktiken genomförs.[123] Som nämnt i tidigare kapitel kategoriseras de biometriska tekniker som systemen använder sig av traditionellt utifrån syftena igenkänning, identifiering och kategorisering.[124]

I ett *biometriskt igenkänningssystem*, som innefattar de biometriska teknikerna identifiering och verifiering, utförs operationer vanligtvis i två faser där varje fas innefattar ett flertal steg.[125] I den första fasen *registrering* sker en insamling och lagring av biometriska egenskaper. Nästa steg är en överföring av den biometriska egenskapen till ett bildformat.[126] Det sparade resultatet i bildformat är ett biometriskt prov som systemet sedan i fas två *igenkänning* behandlar och lagrar.[127] Att provet behandlas innebär att den genom en algoritm extraheras, reduceras och transformeras till en matematisk representation av den ursprungliga biometriska egenskapen. Den matematiska representationen lagras i en biometrisk mall som används för framtida jämförelser när en individ ska identifieras eller verifieras.[128] Skäl 51 i dataskyddsförordningen utesluter explicit ansiktsbilder och fingeravtryck som endast lagrats. Det innebär att en särskild teknisk behandling inleds först vid extraktionssteget. En biometrisk uppgift exkluderar således biometriska prov och utgörs istället av den slutgiltiga produkten som lagras i en biometrisk mall.[129]

I ett biometriskt kategoriseringssystem är faserna istället *träning* och *klassificering*. De grundas oftast på maskininlärningsalgoritmer och klassificering kan ta formen av antingen binär klassificering eller

[122] Se Zabroska (2019) s. 101.
[123] Se Jasserand (2016) s. 9 f.; Bisztray m.fl. (2021) s. 3 ff.
[124] Se avsnitt 2.2.
[125] Se Bisztray m.fl. (2021) s. 4.
[126] *Exempelvis ett fingeravtryck sparas som en fingeravtrycksbild,* se hur detta exempel används i art. 4.14 dataskyddsförordningen.
[127] Se Jasserand (2016) s. 9 f.
[128] Se Jasserand (2016) s. 10.
[129] Se Bisztray m.fl. (2021) s. 3.

multiklassad klassificering. I det förstnämnda delas den biometriska informationen upp i högst två samlingar, exempelvis man/kvinna. I det sistnämnda delas informationen istället upp i fler än två datasamlingar, exempelvis ålder, hårfärg eller klädstil. En multiklassad verifiering är vanligt i videoövervakningssyften där drag behöver bestämmas utifrån enbart en bild.[130] I klassificeringsfasen samlas först den biometrisk egenskapen in. I likhet med igenkänningssystemets fas 1 skapas ett biometriskt prov utifrån en digital bildrepresentation av egenskapen.[131] Slutligen används det biometriska provet för att skapa en form av biometrisk mall som bedöms av tränade maskininlärningsklassificerare och delas in i kategorier.[132]

3.2.3 Rör fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken

För att information ska omfattas av definitionen i art. 4.14 dataskyddsförordningen krävs att den biometriska uppgiften härrörs från antingen ett fysisk, fysiologisk eller beteendemässigt kännetecken.[133] Fysiska och fysiologiska kännetecken är närbesläktade. Medan den förstnämnda syftar till kroppen själv, relateras fysiologi till kroppens funktioner.[134] I kontexten av biometriska egenskaper bör begreppen dock kunna användas synonymt med varandra.[135] Fysiska egenskaper är antingen morfologiska eller anatomiska. Morfologiska egenskaper är alla kroppsliga yttre kännetecken, medan anatomiska egenskaper syftar till den interna kroppsstrukturen.[136] Fysiska och fysiologiska egenskaper inkluderar irismönster, fingeravtryck, ögonfärg, ansiktsbilder och så vidare.[137]

---

[130] Se Bisztray (2021) s. 3.
[131] Se Bisztray (2021) s. 4.
[132] Se Bisztray (2021) s. 4.
[133] Se art. 4.14 dataskyddsförordningen.
[134] Se W, Kenneth och Wills, Michael (2018), 'Differences Between "Physical" & "Physiological', Sciencing, <https://sciencing.com/differences-between-physical-physiological-8774303.html>, besökt 2022-04-08.
[135] Se exempelvis EPRS (2021) s.6; Jain m.fl. (2004) s. 4 ff.; Arbetsgruppen för skydd av personuppgifter (2012) s. 4.
[136] Se Zaborska (2019) s. 101.
[137] Se Zaborska (2019) s. 101.

Det ges ingen förklaring till vad en beteendemässig egenskap definieras som i dataskyddsförordningen. Biometriska uppgifter kopplade till beteendemässiga egenskaper beskriv i övrig litteratur som dynamiska och inbegriper båda fysiska och kognitiva beteenden.[138] En bedömning av varje enskilt fall krävs för att avgöra huruvida en egenskap klassificeras som beteendemässig eller ej.[139] Beteendemässiga biometriska egenskaper exemplifieras dock ofta som gångstil, röstmönster, samt unika tangentbordsmönster.[140]

3.2.4 Möjliggör eller bekräftar unik identifiering av en fysisk person

Det sista rekvisitet (4) för biometrisk uppgift kräver att informationen möjliggör eller bekräftar unik identifieringen av en fysisk person.[141] Kravet kan vid ett första intryck framstå som en upprepning av krav (iii) för definition av personuppgift enligt art. 4.1 dataskyddsförordningen.[142] Det föreligger dock en betydande skillnad som framgår av formuleringarna ”möjliggör eller bekräftar” samt ”unik identifiering” i art. 4.14 dataskyddsförordningen. Att behöva unikt identifiera en person anses ställa upp högre krav än rekvisit (iii) om att avse en identifierbar person, vilket även kommer diskuteras närmare i avsnitt 3.3.

Enligt internationella standarder innebär en identifiering i en biometrisk kontext att en jämförelse sker av biometriska prov med lagrade mallar innehållandes biometriska uppgifter i databaser.[143] Genom en s.k. en-till-många process i en biometrisk kontext behöver identifieringen inte säkerställa

[138] Se Krausová (2018) s. 164; Wendehorst och Duller (2021) s. 14.
[139] Jfr EPRS (2021), s. 21; Dantcheva m.fl. (2015) s. 1 f.
[140] Se Wendehorst och Duller (2021, s. 14 s. 21.
[141] Se avsnitt 3.1.
[142] Se avsnitt 3.2.1 och formulering i art. 4.1 dataskyddsförordning.
[143] ISO/IEC 2382-37:2022, avsnitt. 3.8, 37.08.02; Jfr även avsnitt 3.2.2 om särskild teknisk behandling.

en individs identitet.[144] Istället syftar identifieringen till att para ihop den sparade data med det biometriska provet.[145]

Biometrisk identifiering ska inte förväxlas med biometrisk verifieringen. Den senare termen inbegriper den process för att verifiera en individs påstådda identitet, vilken tillskillnad från identifiering är en en-till-en process.[146] En verifiering kan exempelvis vara ansiktsupplåsning i en specifik telefon där systemet jämför ett ansikte i realtid med en enda lagrad bild.[147]

3.2.5 Sammanfattning av biometrisk uppgift i EU-rättslig kontext och de uppställda kraven för klassificiering.

Biometri är en paraplyterm och innefattar många olika former av biometrisk information i en modern teknocentrisk kontext.[148] Om den biometriska informationen i fråga uppfyller kravet på status som personuppgift enligt art. 4.1 dataskyddsförordningen omfattas den av de generella skyldigheterna som framkommer av dataskyddsförordningen.[149] Om den biometriska informationen dessutom klassificeras som en biometrisk uppgift enligt art. 4.14 dataskyddsförordningen erhåller den även status känslig personuppgift enligt art. 9.1 och omfattas av ett allmänt behandlingsförbud.

Genom ikraftträdandet av dataskyddsförordningen introducerades för första gången en definition av biometrisk uppgift på EU-rättslig nivå. Förordningen skapade därmed en ny rättslig kategori av biometriska uppgifter som kan kvalificeras som biometriska personuppgifter.[150] Tillskillnad från tidigare tolkningar av biometrisk uppgift enligt teknisk och interdisciplinär karaktär

[144] Se Wendehorst och Duller (2021) s. 20.
[145] Se Jasserand (2016) s. 12.
[146] Se Wendehorst och Duller (2021) s. 20; Jasserand (2016) s. 12.
[147] Jfr Wendehorst och Duller (2021) s. 13.
[148] Se avsnitt 2.1.
[149] Se art. 5 och art 6 dataskyddsförordningen.
[150] Se Jasserand (2016) s. 22.

kan definitionen i art. 4.14 dataskyddsförordningen anses vara ett rent juridiskt begrepp.[151]

Enligt dataskyddsförordningen definieras biometrisk uppgift som en personuppgift som uppstått genom särskild teknisk behandling och rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person.[152] Som diskuterat i detta kapitel ställer begreppsformuleringen upp fyra kumulativa krav måste uppfyllas för att biometrisk data ska anses vara en biometrisk uppgift. I kommande avsnitt följer en analys av kraven som syftar till att precisera vilken slags biometrisk information som utifrån definitionen i art. 4.14. dataskyddsförordningen kan klassificeras som biometrisk uppgift.

3.3 Delanalys I

Personuppgift

Biometriska uppgifter är ur ett EU-rättsligt perspektiv en underkategori till personuppgifter.[153] Det bör därför ske en bedömning om huruvida biometrisk data klassificeras som en personuppgift innan övriga rekvisit för biometrisk uppgift utreds. Formuleringen i art. 4.1 dataskyddsförordningen innebär en bred tolkning av termen personuppgift, vilket bekräftas av praxis från EU-domstolen.[154] I tidiga EU-rättsliga dokument gällande biometri uttrycks dock på att biometrisk data inte nödvändigtvis måste klassificeras som personuppgifter. Det var Arbetsgruppen för dataskydd och skydd av personuppgifter publicerade arbetsdokument om biometri från år 2003 och 2012 som menade att de flesta former av biometriska data är att anse som personuppgifter.[155] Uttalandena indikerar att det föreligger undantag till en

[151] Se avsnitt 2.2.
[152] Se art 4.14 dataskyddsförordningen.
[153] Se art. 4.14 dataskyddsförordningen.
[154] C-434/16 *Nowak,* p. 34.
[155] Se Artikel 29 – Arbetsgruppen för dataskydd (2003) s. 12; Arbetsgruppen för skydd av personuppgifter (2012) s. 7.

påstående huvudregeln om att biometriska uppgifter alltid är en subkategori till personuppgifter.

Utifrån vägledningen och definitionen i det då gällande dataskyddsdirektivet presenterar arbetsgruppen exempel på vad som bör kunna anses som personuppgifter.[156] Däribland inkluderas biometriska egenskaper såsom fingeravtryck, venmönster, handskrivna namnteckningar, unika talmönster, och även DNA-uppgifter.[157] Exemplen består av både fysiska och beteendemässiga kännetecken. Arbetsgruppens uttalanden om att biometriska uppgifter inte alltid måste vara personuppgifter kan då tolkas som att denna mängd undantag borde vara relativt få. En utredning av förhållandet mellan biometrisk data och personuppgifter bör därför göras för att kunna fastställa dessa indikerade undantag. Definitionen av personuppgift i art. 4.1 dataskyddsförordningens ställer upp fyra rekvisit som är förankrade i varandra.[158]

Inledningsvis kan slutsatsen dras att rekvisit (i) om att det ska handla om en upplysning samt rekvisit (iv) om kravet på att informationen härrör från en fysisk person, båda bör kunna anses uppfyllda utan att det krävs en särskilt djupgående analys. Som diskuterat i avsnitt 3.2.1 ska rekvisit (i) tolkas brett och inkluderar alla format av data. Gällande rekvisit (iv) är biometrisk uppgift till sin natur information som härrör från en fysisk person.[159] Arbetsgruppen noterar även att en biometrisk uppgift visserligen kan ändras eller raderas men den biometriska egenskap som uppgiften extraherats från förblir oföränderlig, vilket stärker kopplingen till en fysisk person.[160] Kvar återstår således rekvisit (ii) som ställer upp krav på att informationen måste *avse* en individ, samt rekvisit (iii) om dess förmåga att *identifiera* en specifik individ.

[156] Se Artikel 29-arbetsgrupp för skydd av personuppgifter (2012) s. 8.
[157] Se Artikel 29-arbetsgrupp för skydd av personuppgifter (2012) s. 8.
[158] Se avsnitt 3.2.1.
[159] Se avsnitt 3.2.1.
[160] Se Artikel 29-arbetsgrupp för skydd av personuppgifter (2012) s. 2.

(ii) *avse* en individ

Troligtvis bör det i praktiken vara svårt att argumentera för att biometriska data inte hade kunnat nå upp till kravet på att *avse* en individ, vilket även gäller efter att den genomgått teknisk behandling. Biometrisk data oavsett modifikation anses vara så pass nära kopplad till en individ att det skulle kräva mycket för att kunna motivera att informationen inte skulle kunna påverka denna i någon grad.[161] Arbetsgruppen diskuterar även begreppet närmare i sitt yttrande från 2012 om utveckling i biometrisk teknik.[162] Där uttrycks att biometriska uppgifter alltid har en naturlig och direkt koppling till en individ.[163] Det innebär att den biometriska uppgiften bör påverka individen i åtminstone någon utsträckning oavsett vilken kategori av kännetecken uppgiften härstammar ifrån.

(iii) Identifierad eller identifierbar

Enligt uttalanden från Arbetsgruppen för skydd av personuppgifter innebär krav (iii) att en individ ska kunna ”särskiljas” från en grupp.[164] Det innebär att kravet på identifiering i detta sammanhang är relativt lågt eftersom det inte krävs ett bekräftande eller säkerställande av en persons unika identitet. [165] Att rekvisit (iii) även anger att personen i fråga ska vara identifierad eller identifierbar resulterar i ett ännu lägre ställt krav. Identifierbar innebär att individen inte måste vara identifierad för tillfället men tekniskt sett kan identifieras om informationen kombineras med annan fristående information.[166] I denna kontext behöver den biometriska informationen inte på egen hand vara tillräcklig för identifiering, vilket skiljer sig från kravet på unik identifiering i art. 4.14 dataskyddsförordningen.[167]

[161] Jfr avsnitt 3.2.1 om krav (3) på att individen ska vara identifierbar eller identifierad.
[162] Artikel 29-arbetsgrupp för skydd av personuppgifter (2012).
[163] Se Artikel 29-arbetsgrupp för skydd av personuppgifter (2012) s. 2.
[164] Se Artikel 29 – Arbetsgruppen för skydd av personuppgifter (2007) s. 12.
[165] Se Artikel 29 – Arbetsgruppen för skydd av personuppgifter (2007) s. 12 f.; Jasserand (2016), s. 8.
[166] Se Jasserand (2016) s. 9.
[167] Se redogörelse för detta i kommande avsnitt 3.2.4.

För att anses uppfylla kravet på identifiering räcker det därmed att den biometriska uppgiften kan särskilja en person från en grupp, antingen självständigt eller i kombination med andra uppgifter. Biometriska egenskaper definieras som alla de särskiljande mänskliga kännetecken som går att läsa av i mätbara enheter.[168] Definitionen tyder på en naturlig koppling till mänskliga attribut, vilket bör anses kunna resultera i ett automatiskt uppfyllande av kraven på personuppgift.[169] En biometrisk uppgift härstammar i sin tur alltid från en biometrisk egenskap.[170] Det är genom processen av särskild teknisk behandling som egenskapen extraheras och omvandlas till en biometrisk uppgift.[171] Om det i teorin finns vissa biometriska uppgifter som inte anses vara personuppgifter kan slutsatsen dras att dessa undantagsfall uppstår när den tekniska behandlingen innebär ett anonymiserande av egenskapen till den grad att dess förmåga att identifiera en fysisk person försvinner.[172] Detta bör inte vara fallet med biometriska uppgifter i ett biometriskt igenkänningssystem eftersom det grundläggande syftet med processen är att identifiera. Den biometriska uppgiften förlorar därmed aldrig information som behövs för identifiering. Även Arbetsgruppen för skydd av personuppgifter för uppgiftsskydd har publicerat ett dokument där det framkommer att biometrisk uppgift anses vara personuppgifter på grundval att de kan användas för att identifiera en specifik individ.[173]

I ett biometriskt kategoriseringssystem innehåller dock de biometriska mallarna inte alltid tillräckligt med information för att identifiera en individ. Det styrks av ett yttrande av Arbetsgruppens som stadgar att en biometrisk mall skapad från en ansiktsbild innehåller personuppgifter om den används för verifiering eller identifiering.[174] Om den biometriska mallen dock enbart används i ett kategoriseringssystem med minimal information, exempelvis

[168] ISO/IEC 2382-37:2022, avsnitt 3.1, 37.01.02; Se även avsnitt 2.2.
[169] *Dvs. är en upplysning som avser en identifierad eller identifierbar fysisk person*, se avsnitt. 3.2.1.
[170] Se avsnitt 2.2 och 3.2.2.
[171] Se avsnitt 3.2.2.
[172] Se avsnitt 3.2.1 om krav (2) på identifierad eller identifierbar person.
[173] Se Artikel 29 – Arbetsgruppen för skydd av personuppgifter (2007) s. 8.
[174] WP192 Opinion 02/12 (2012) s 4.

indelning utifrån kön, kan det inte klassificeras som personlig data.[175] Den biometriska data som genomgått teknisk behandling i ett kategoriseringssystem bör därför kunna riskera att inte definieras en personuppgift. Det innebär att informationen inte heller skulle gå att klassificera som en biometrisk uppgift enligt art. 4.14 dataskyddsförordningen.

Kravet på särskild teknisk behandling

De tekniska aspekterna av kravformuleringen i art. 4.14 dataskyddsförordningen framkommer av kravet på särskild teknisk behandling. Kravet bör indikera att ingen rå biometrisk information kan definieras som en biometrisk uppgift utan att först ha genomgått en teknisk process.[176] Alla biometriska prov, det vill säga analoga eller digitala representationer av biometriska egenskaper, får därför rättslig status som biometrisk uppgift först när teknisk behandling av dessa inleds.[177] I praktiken innebär kravet att enbart lagring och bibehållandet av biometrisk data rättsligt sett inte omfattas av definitionen i art. 4.14 dataskyddsförordningen.[178]

Denna restriktiva tolkning av biometrisk uppgift framgår även av skälen till dataskyddsförordningen. Där stadgas att behandling av foton systematiskt inte är att anses vara biometriska uppgifter om de inte bearbetats tekniskt i syfte att åstadkomma identifiering av fysisk person.[179] Om fotot i fråga hade genomgått en process som kräver teknisk behandling hade detta dock kunnat ändras. Om den tekniska behandlingen av fotot hade inneburit att den biometriska egenskapen kunde ligga till grund för analys av ett ansiktsuttryck hade den kunnat kategoriseras som en biometrisk uppgift.[180]

---

[175] WP192 Opinion 02/12 (2012) s 4.
[176] Jfr exempelvis Jasserand (2016) s. 9.
[177] Se avsnitt 3.2.2.
[178] Se avsnitt 3.2.2; Kindt (2018) s. 537.
[179] Se skäl 51 dataskyddsförordningen.
[180] Se skäl 51 dataskyddsförordningen; Nine Engineering (2021), 'GDPR and biometrics: an overview', <https://www.nineengineering.com/post/gdpr-and-biometrics-an-overview>, besökt 2022-03-28.

Det har betonats att biometrisk information oavsett teknisk behandling kan ses som prerekvisit för biometrisk identifiering.[181] Det har resulterat i argument för att ett uteslutande från rättslig reglering av kategorin bestående av obehandlad lagrad biometrisk data utgör en risk mot datasubjektens fundamentala rättigheter och friheter.[182] Exkluderingen av fristående lagring och insamling av biometriska egenskaper i definitionen för biometrisk uppgift skiljer sig från ISO standards.[183] Riskerna med biometriska egenskaper som enbart lagras i databaser har diskuterats av både EU-domstolen och Europadomstolen. Samtliga rättsfall som diskuteras i nedanstående stycke belyser riskerna med lagring av biometrisk information och de potentiella konsekvenserna detta kan resultera i gällande fundamentala rättigheter enligt EU-stadgan och EKMR.

Av Europadomstolens praxis framgår att bibehållandet av fingeravtryck anses vara en inskränkning i rätten till respekt till privatliv enligt artikel 7 EKMR.[184] Europadomstolen betonar även att skyddet av personuppgifter speciellt är av fundamental betydelse för rätten till privatliv när informationen i fråga genomgår automatisk behandling och används i brottsbekämpningssyften.[185]

Riskerna med lagring av biometrisk information och biometriska prov har även adresserats av EU-domstolen i *Willems* och *Schwarz.*[186] I båda fallen var kontexten att individer motsatte sig lagring av sin biometriska data i syfte att få ett e-Pass eller identitetskort utfärdat i enlighet med Rådets förordning (EG) nr 2252/2004 av den 13 december 2004 om standarder för säkerhetsdetaljer och biometriska kännetecken i pass och resehandlingar som utfärdas av medlemsstaterna (Rådets förordning (EG) nr 2252/2004).[187] I

[181] Se Kindt (2018) s. 530.
[182] Se Kindt (2018) s. 530 f.
[183] Se ISO/IEC TR 24741:2018, avsnitt 3.3 37.03.06 - där biometrisk uppgift även inkluderar biometriska prov.
[184] Europadomstolen i mål nr 30562/04 och 30566/04 S. and Marper v. The United Kingdom p. 85.
[185] Europadomstolen i mål nr 19522/09 M.K. v. France p. 35.
[186] Förenade målen C-446/12 och C-449/12 *Willems,* p. 46; C-291/12 *Schwarz,* p. 30.
[187] Se art 1.2 Rådets förordning (EG) nr 2252/2004; Förenade målen C-446/12 och C-449/12 *Willems,* p.2; C-291/12 *Schwarz* p. 2.

Willems grundade sig dessutom motsättningen i oron att uppgifterna kunde återanvändas i andra syften och att de lagrades i otillförlitliga databaser.[188]

Rör fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken

Krav (3) i art. 4.14 dataskyddsförordningen om koppling till fysiska, fysiologiska eller beteendemässiga kännetecken, tillåter en omfattande inkludering av mänskliga egenskaper.[189] Enligt Bisztray används biometriska egenskaper av biologisk karaktär oftast i igenkänningssyfte, medan de av beteendemässig karaktär är bäst lämpade för klassificering av individer.[190] Båda typer av egenskaper kan dock ofta användas i samtliga tre kategorier. Exempelvis kan ett fingeravtryck identifiera och verifiera en person eftersom det har ett unikt mönster. Samtidigt kan fingeravtryckets storlek, form och färg kategorisera utifrån kön eller hudfärg.[191]

Uppgifter som endast relateras till, men inte direkt rör, en persons fysiska fysiologisk eller beteendemässiga egenskaper bör däremot inte anses vara biometriska uppgifter utifrån definitionen i art. 4.14 dataskyddsförordningen. Det innebär att ren s.k. emotionell data inte uppnår kraven för definitionen av biometrisk uppgift.[192] Emotionell data kan bland annat bestå av ansiktsuttryck och andra känslouttryck.[193]

Möjliggörande eller bekräftande av unik identifiering

I relation till biometriska uppgifter kan två specifika frågeställningar utläsas av krav (4) om unik identifiering.[194] Den första frågeställningen berör det omfång som ”identifiering” har i denna kontext och hur det kan tolkas utifrån det faktum att lagstiftarna valt att inkludera både termen ”möjliggör” och

[188] C-446/12 och C-449/12 *Willem,* p. 18.
[189] Se Jasserand (2016) s. 12.
[190] Se Bisztray m.fl. (2021) s. 5.
[191] Se Bisztray m.fl. (2021) s. 5.
[192] Se McStay (2020) s. 4.
[193] Se McStay (2020) s. 2.
[194] Se art. 4.14. dataskyddsförordningen.

”bekräftar”.[195] Enligt Jasserand betonar expertutlåtanden och litteratur inom det moderna tillämpningsområdet för biometri en relativt insnävad definition av det fristående begreppet ”identifiering” i biometriska kontexter.[196] Innebörden syftar vanligtvis enbart till biometrisk identifikation som det redogörs för i avsnitt 3.2.4. I förhållande till definitionen av biometrisk uppgift i enlighet med art. 4.14 dataskyddsförordningen har det dock argumenterats för att även biometrisk verifiering bör inkluderas i termen ”unik identifiering”.[197] Anledningen till detta är att definitionen uppger både ”möjliggörande” och ”bekräftande” som potentiella metoder för unik identifiering. Att *möjliggöra* anses representera biometrisk traditionell biometrisk identifikation medan att *bekräfta* identifiering anses representera biometrisk verifiering.[198]

Den andra frågeställningen relateras till strängheten och innebörden av ”unik identifiering”.[199] Med att identifieringen, som enligt ovanstående stycke bör inbegripa både verifiering och identifiering, måste vara unik menas att en individs biometriska kännetecken bör överensstämma med den tidigare lagrade biometriska uppgiften.[200] Som nämnt i avsnitt 3.2.4 är kravet för unik identifiering högre ställt än det identifieringskrav för personuppgift som det framgår av art. 4.1 dataskyddsförordningen. En unik identifiering för biometrisk uppgift i enlighet med art. 4.14 dataskyddsförordningen anses dessutom allmänt vara den allra högsta nivån av identifiering.[201]

Formuleringen av krav (4) kan resultera i att vissa biometriska system lyckas kringgå dataskyddsrättslig regleringen. Detta hade kunnat vara fallet om systemen använder biometriska data som saknar förmågan att unikt identifiera en individ. Detta bör främst vara fallet i de situationer där den biometriska informationen används i kategoriseringssyfte. Som redogörs för

[195] Se formulering i art. 4.14. dataskyddsförordningen.
[196] Se Jasserand (2016) s. 13.
[197] Se avsnitt 3.2.4.
[198] Se Jasserand (2016) s. 13.
[199] Se formulering i art. 4.14. dataskyddsförordningen.
[200] Se Jasserand (2016) s. 15.
[201] Se Jasserand (2016) s. 14.

i avsnitt 2.2 delas syftena för biometrisk teknologi upp i de tre huvudkategorierna identifiering, verifiering och kategorisering.[202] Ett *möjliggörande* eller *bekräftande* av unik identitet omfattar som nämnt enbart identifierings- och verifieringssyften. Kategorisering av individer omnämns därmed inte av formuleringen i art. 4.14 dataskyddsförordningen.[203] Om ett biometriskt system som huvudsakligen utvecklats i syfte att kategorisera individer ska anses använda sig av biometriska uppgifter måste informationen således även kunna användas för att identifiera eller verifiera en individ. Om detta inte är fallet anses inte den biometriska informationen klassificeras som biometrisk uppgift enligt EU-rätt.[204] Det innebär att den biometriska informationen visserligen kan vara personuppgifter som genomgått särskild teknisk behandling och rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken, men ändå inte omfattas av definitionen i art. 4.14 dataskyddsförordningen.

Problematiken med kravet på unik i identifiering för ett kategoriseringssystem härrör från den typ av biometriska egenskaper som används i kategoriseringen. För att kunna fastställa eller bekräfta en individs identitet behöver den biometriska informationen i de flesta härstamma från fysiska eller fysiologiska kännetecken.[205] Kategoriseringssystem brukar istället använda sig av emotionella eller beteendemässiga data.[206] Emotionell data riskerar dels att inte kunna användas i igenkänningssyfte, dels att inte direkt röra fysiska, fysiologiska eller beteendemässiga kännetecken.[207]

Det är dock ett faktum att så kallade *soft traits*, ofta av beteendemässig karaktär och bäst lämpad för kategoriseringssyften, i många fall kan tänkas

[202] Detta bekräftas även på EU-nivå, Se exempelvis Wendehorst och Duller (2021) s. 20 f – där nämns även en potentiell fjärde kategori i form av ”uttydning”, vilket dock främst blir aktuellt vid användning av speciella AI-system och kommer diskuteras i uppsatsens senare avsnitt 4.3.2.1.
[203] Se art. 4.14 dataskyddsförordningen.
[204] Se art. 4.14 dataskyddsförordningen.
[205] Se Wendehorst och Duller (2021) s.21.
[206] Se Wendehorst och Duller (2021) s.21; Bisztray m.fl (2021) s. 5.
[207] Se analys i sista stycket under avsnittets del gällande kravet på ” *Rör fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken”.*

möjliggöra även identifiering eller verifiering. Sättet att använda en datormus är exempelvis en beteendemässig egenskap men bör i vissa fall också vara en tillräcklig unik egenskap för att kunna kopplas till en specifik individ. I dessa situationer kan den beteendemässiga egenskapen ligga till grund för biometrisk uppgift. Med beaktande av materialet ovan bör det dock finnas situationer där även beteendemässiga egenskaper för kategoriseringssyfte inte kan visa på en tillräckligt stark koppling till en individ efter teknisk behandling. Denna data riskerar då att inte nå upp till kravet för biometriska uppgift.

3.3.1 Slutsatser av Delanalys I

Sammantaget kan slutsatsen dras att dataskyddsförordningen ger en tvetydlig definition av biometrisk uppgift. Det kan dels argumenteras för att formuleringen i art. 4.14 dataskyddsförordningen utgör en relativt bred definition av vad som klassificeras som biometrisk uppgift. En bred definition av begreppet skulle vidare innebära att EU-kommissionen tar hänsyn till det faktum att nya biometriska tekniker konstant utvecklas och släpps ut på marknaden. Dels kan det motsatsvis argumenteras för att definitionen i art. 4.14 dataskyddsförordningen är snäv och utesluter mycket relevant biometrisk information från dess omfång.

Utifrån de kriterier som har analyserats kan vissa antaganden göras gällande definitionen av biometrisk uppgift. För det första bör en majoritet av biometrisk information kunna klassificeras som personuppgifter. Det mest omdiskuterade hindret mot detta hade varit kravet på identifierad eller identifierbar individ. Eftersom kravet dock är ställt mycket lågt bör det inte föreligga några hinder i relation till biometriska kännetecken av fysisk eller fysiologisk karaktär. Även obehandlade beteendemässiga kännetecken bör nå upp till det lågt ställda kravet. Om de beteendemässiga kännetecknа istället används i ett kategoriseringssystem kan de i vissa fall tänkas anonymiseras till den grad att de förlorar förmågan att identifiera en individ. Detta gäller

speciellt om den beteendemässiga biometrisk informationen är av minimal karaktär.

Utifrån kravet på särskild teknisk behandling utesluts all rå biometrisk information, vilket utifrån en teknisk bemärkelse hade inneburit att inga lagrade biometriska prov kan klassificeras som biometriska uppgifter. Eftersom biometriska uppgifter måste härstamma från fysiska, fysiologiska eller beteendemässiga kännetecken bör även all emotionell biometrisk data exkluderas. Det kan dock argumenteras för att viss emotionell data kan falla in under en beteendemässiga beteckning. Detta har inte exemplifierats på EU-nivå, vilket innebär att det blir svårt att precisera vilken data som hade kunnat omfattas. Slutligen stärker kravet på unik identifiering att ren emotionell data bör vara exkluderad från definitionen i art 4.14 dataskyddsförordningen. Det är dock oklart om framtida system och tekniker kan möjliggöra identifiering även genom denna typ av data. Eftersom kravet på unik identifiering är högt ställt riskerar även beteendemässig data att inte falla in under definitionen av biometrisk uppgift. Det gäller specifikt i kategoriseringssystem som inte utvecklats för igenkänningssyften. En bedömning i varje enskilt fall bör göras för att avgöra huruvida den biometriska informationen har en tillräckligt stark koppling till en specifik individ.

Den biometriska information som kan tänkas ligga till grund för biometrisk uppgift bör således främst härstamma från fysiska och fysiologiska kännetecken. Fingeravtryck, ansiktsbilder, irismönster och andra särskiljande drag som genomgått teknisk behandling bör med största sannolikhet alltid kunna anses vara biometriska uppgifter. Svårare blir att avgöra huruvida beteendemässig biometrisk information, såsom viss signaturdynamik eller talmönster, kan omfattas av definitionen. Ansiktsuttryck och annan ren emotionell information bör utifrån en terminologisk utredning uteslutas. Det ska dock nämnas att exemplen av biometrisk uppgift som getts av EU-organ inte alltid överensstämmer med den tillsynes insnävade definition som EU-kommissionen beslutat om i sin dataskyddslagstiftning.

Kritiken som formulerats mot definitionen av biometrisk uppgift i art 4.14 dataskyddsförordningen har i stor utsträckning berört det faktum att definitionen inte tar hänsyn till den precisa tekniska terminologi som använts i tidigare biometriska kontexter och internationella standarder. Detta gäller de tekniska definitionernas avsaknad av kravet på särskild teknisk behandling och en lägre satt ribba för identifiering. Experter menar att den juridiska definition som framgår av lagtexten inte reflekterar tekniska förfaranden och processer. De betonar vidare vikten av att använda korrekt teknisk terminologi i syfte att förstå biometriska uppgifter i en rättslig kontext.[208]

[208] Se Jasserand (2016) s. 13.

4 Förslaget till en kommande AI-reglering på EU-nivå

4.1 Bakgrund till förslaget om AI-förordningen

I syfte att adressera utmaningarna med de ökade användningsområdena för AI presenterade EU-kommissionen förslaget till en ny förordningen om regleringen av artificiell intelligens den 21 april 2021.[209] Artificiell intelligens är en paraplyterm för de teknologier som kombinerar data, algoritmer och datorkraft.[210] Enligt EU:s tillsatta högnivåexpertgrupp för artificiell intelligens (expertgruppen[211]) kännetecknas AI dels av förmågan att uppvisa intelligent beteende genom analys av omgivningen, dels av förmågan att ta beslut med viss grad av autonomi.[212]

Förordningen som uteslutande behandlar AI är den första av sitt slag och upprättar horisontella regler för både utveckling och användning av AI-system i enlighet med unionens värden.[213] Genom en riskbaserad metod önskar EU-kommissionen dels främja AI-innovation inom unionen, dels adressera de större orosmomenten som maskinlärning ger upphov till.[214]

Motiveringen till förslaget anger fyra specifika mål med den kommande AI-förordningen.[215] Det första målet syftar till att säkerställa att AI-system som

[209] Se motivering till COM (2021) 206 final s. 1.
[210] Se COM (2020) 65 final s. 2.
[211] Se COM (2020) 65 final s. 8; Se även motivering till COM (2021) 206 final s. 8 - ”*Expertgruppen består av 52 välkända expert från olika sektorer som har i uppgift att ge kommissionen råd om genomförandet av deras AI-strategi”.*
[212] Se FRA (2021) s. 19.
[213] Se skäl 1 och 5 till COM (2021) 206 final.
[214] Se skäl 14 till COM (2021) 206 final.
[215] Se motivering till COM (2021) 206 final s. 3.

distribueras och används inom unionen är säkra och förenliga med befintlig lagstiftning om de grundläggande rättigheterna och EU:s värden.[216] Vidare syftar det andra målen till att säkerställa rättssäkerhet samt att förbättra och effektivisera kontroll av befintlig lagstiftning tillämplig på AI. Mål tre och fyra betonar vikten av att säkerställa innovation och främja utvecklingen av AI inom den inre marknaden.[217] Den rättsliga grunden för förslaget är art. 114 i FEUF, som ställer upp krav på att åtgärder ska säkerställa upprättandet av den inre marknaden och dess funktioner.[218]

AI-förordningen ska begränsas till de minimikrav som är nödvändiga för att hantera de risker och problem som AI förknippas med. I samband med detta uttrycker EU-kommissionen att syftet med förordningen är att undvika oproportionerliga begränsningar av den tekniska utvecklingen inom unionen.[219] Förordningen varken ersätter eller påverkar andra närbesläktade regleringar, såsom den allmänna dataskyddsförordningen, utan syftar istället till att verka som *lex specialis* och komplettera dessa.[220]

4.1.1 Risk för grundläggande rättigheter i samband med användning av AI

Ramverket för grundläggande rättigheter utgör den normativa grunden och riktningen för design, utveckling och distribueringen av AI-verktyg och system.[221] Vidare är EU-stadgan utgångspunkten för regleringen av AI på EU-nivå gällande de grundläggande rättigheterna.[222] Utvecklare och leverantörer av AI är föremål för EU-rättslig lagstiftning om grundläggande rättigheter såsom dataskydd, rätten till privatliv och skydd mot diskriminering. Deras AI-drivna verksamheter måste därutöver även beakta

[216] Se motivering till COM (2021) 206 final s. 3.
[217] Se motivering till COM (2021) 206 final s. 3.
[218] Se motivering till COM (2021) 206 final s. 6.
[219] Se motivering till COM (2021) 206 final s. 3.
[220] Se Veale och Zuiderveen Borgesius (2021) s. 101; Motivering till COM (2021) 65 final s.4.
[221] Jfr Smuha m.fl. (2021) s. 6 f.
[222] Jfr FRA (2021) s. 47.

lagstiftning relaterat till områden som konsumentskydd, produktansvar och produktsäkerhet.[223]

I skälen till AI-förordningen stadgas att omfattningen av de negativa effekterna som förordningen har på grundläggande rättigheter bland annat inkluderar rätten till människans värdighet, respekt för privat- och familjeliv, organisations- och yttrandefrihet, informationsfrihet samt rätten till ett effektivt rättsmedel och till en opartisk domstol.[224] I vitboken om EU:s strategier för AI från år 2020 hänvisar EU-kommissionen till Europarådets utredning om artificiell intelligens i förhållande till EKMR i syfte att ytterligare exemplifiera vilka grundläggande rättigheter som kan påverkas av AI-system.[225] Dessa inkluderar, men är inte begränsade till, rätten till rättvis rättegång och korrekt förfarande, icke-diskriminering, yttrandefrihet, mötes- och föreningsfrihet, privat- och familjeliv samt skydd av personuppgifter.[226]

4.1.2 Riskbaserad metod

För att uppnå en balanserad och proportionerlig reglering baseras AI-förordningen på en riskbaserad metod.[227] Introduktionen av en riskbaserad metod motiverades med viljan att säkerställa att de bindande rättsreglerna är proportionerliga och effektiva. EU-kommissionen uttrycker att metoden kan användas för att anpassa förordningens bestämmelser till intensiteten och omfattningen av de risker som AI-systemen kan generera.[228]

Enligt den riskbaserade metoden förbjuds viss AI och olika krav ställs på AI-system på grundval av den kategori de tillhör.[229] Risknivåerna som tillämpas

[223] Se COM (2020) 65 final s. 10.
[224] Se skäl 28 COM (2021) 206 final.
[225] Se COM (2020) 65 final s. 10.
[226] Se COM (2020) 65 final s. 10.
[227] Se motivering till COM (2021) 206 final s. 8; Skäl 14 COM (2021) 206 final.
[228] Se skäl 14 COM (2021) 206 final.
[229] Se exempelvis skäl 14 COM (2021) 206 final.

på AI kan delas in i följande fyra kategorier: (1) Oacceptabel risk, (2) Hög risk, (3) Begränsad risk, (4) Minimal risk.[230]

(1) Oacceptabel risk

Enligt en studie av EU-kommissionen var det ett kontroversiellt beslut att inkludera en kategori som helt förbjuder vissa användningsområden av AI.[231] Högnivåexpertgruppen om AI beskrev ett starkt motstånd och påtryckningar från industrin, vilket resulterade i att expertgruppen uteslöt termer som ”*non-negotiable*” och ”*red-lines*” från deras rekommendationer.[232] I EU-kommissionens förslag introduceras dock ändå en kategori av AI-system och metoder som är helt förbjudna.[233] Beslutet grundas i och motiveras av att en mindre samling användningsområden av AI innebär en garanterad kränkning av grundläggande rättigheter.[234]

(2) Hög risk

AI-system som anses utgöra hög risk är en central del av förslaget till den kommande AI-förordningen.[235] Högrisksystem anses riskera ha en negativ effekt på individers säkerhet och de fundamentala rättigheter som återfinns i EU-stadgan.[236] Begreppet hög risk som det används i AI-förordningen är dock relativt vagt definierat.[237] Av art. 6 i AI-förordningen framgår ett antal klassificeringsregler och riktlinjer för hur aktörer kan avgöra huruvida deras AI-system anses falla in under någon av de två underkategorierna av högrisksystem. Den ena kategorin består av de AI-system som explicit framgår av bilaga III till förordningen (Bilaga III).[238] Den andra kategorin

[230] Se motivering till COM (2021) 206 final s. 13.
[231] Final Report (2021) s. 98.
[232] Veale och Zuiderveen Borgesius (2021) s. 98.
[233] Förbudet framgår av art. 5 COM (2021) 206 final.
[234] Se Europeiska kommissionen (2021), ‘New rules for Artificial Intelligence – Questions and Answers’, Bryssel 2021-04-21 s. 1 f.
[235] Se EPRS (2021) s. 62.
[236] Se skäl 28 COM (2021) 206 final.
[237] Se exempelvis Lukianet (2021).
[238] Se art. 6.2 COM (2021) 206 final.

baseras på tillämpningen av gällande EU-rättsregler om produktansvar.[239] AI-system som faller inom ramen för högriskbeteckningen måste följa de krav som ställs upp i Kapitel II i förslaget till förordningen. Kraven relateras till teknisk dokumentation, inrättning av riskhanteringssystem, arkivering, data och dataförvaltning, transparens, mänsklig insyn och cybersäkerhet.[240] En mer detaljerad redogörelse av dessa krav faller dock utanför uppsatsens omfång.

(3) Begränsad risk

De AI-system som anses utgöra begränsad risk är föremål för transparenskrav vid vissa användningsområden. Användarna ska vara medvetna om deras interaktioner med systemet.[241] Nyttan med kravet på transparens har dock ifrågasatts med hänvisning till att det överlappar med gällande dataskyddsregler.[242] I dataskyddsförordningen finns redan uppställda krav på att behandlingen av personuppgifter måste vara transparent i förhållande till profilering och automatiskt beslutsfattande.[243]

(4) Minimal risk

Den sista kategorin innehåller alla de AI-system som inte omfattas av övriga tre kategorier. AI-förordningen innehåller inga kravbestämmelser för system med minimal risk. Likaså faller en majoritet av AI-system in under denna kategori och kan distribueras och användas fritt utan att behöva ta hänsyn till EU-rättsliga krav i enlighet med förslaget till AI-förordningen.[244]

[239] Se art. 6.1 (a) och (b) COM (2021) 206 final; Lukianets (2021).
[240] Se art. 8 ff. COM (2021) 206 final.
[241] Se art. 52 COM (2021) 206 final.
[242] Se Edwards (2022), 'The EU AI Act: a summary of its significance and scope' s. 14 f.
[243] Se art. 13.2 (f) dataskyddsförordningen.
[244] Se EPRS (2021) s. 62. Jfr avsaknad av bestämmelser för AI-system med minimal risk i förhållande till motivering till COM (2021) 206 final s. 13.

4.2 Kritik mot biometrisk uppgift i AI-rättslig kontext på EU-nivå

I skälen till AI-förordningen stadgas att begreppet biometrisk uppgift ska tolkas i överensstämmelse med definitionen i art. 4.14 dataskyddsförordningen och art. 3.13 LED-direktivet.[245] Valet att återanvända en exakt kopia av dataskyddslagstiftningens definitioner har adresserats av både experter och EU-organ. I en publicerad studie på efterfrågan av en kommitté bestående av medlemmar av Europaparlamentet[246] framgår att innebörden av biometrisk uppgift i dataskyddsförordningen är otydlig. Kommittén menar att detta riskerar att resultera i tolkningssvårigheter för definitionerna av systemen som regleras av AI-förordningen.[247] Studien betonar att biometrisk uppgift bör granskas kritiskt i förhållande till de konsekvenser som begreppstolkningen kan resultera i för termer såsom biometrisk kategorisering och känsloigenkänning.[248]

Även europeiska datatillsynsmannen (EDPS) menar att definitionen av biometrisk uppgift och dess tillämpning i en dataskyddsrättslig kontext behöver förtydligas. De uttrycker även att definitionen inte täcker alla problemområden som presenteras i litteratur och lagtexter.[249] Det finns således en uttalad oro att vissa AI-system använder data relaterat till människokroppen som enligt dataskyddsförordningens och AI-förordningens bemärkelse inte är att anses vara biometriska uppgifter.[250] Kritik mot den nuvarande definitionen har även uttrycks av unionens medlemsstater. I en

[245] Se skäl 7 COM (2021) 206 final; Av skälet framgår att kravet även ska tolkas i enlighet med samma definition av biometrisk uppgift i art. 3.18 Europaparlamentets och rådet 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.
[246] *Panel for the Future of Science and Technology (STOA).*
[247] Se EPRS (2021) avsnitt IV.
[248] Se EPRS (2021) avsnitt IV.
[249] Se EPRS (2021) avsnitt IV.
[250] Se EPRS (2021) s. 53.

kommentar till AI-förordningen av det slovenska EU-ordförandeskapet föreslås ett uteslutande av kravet på ”möjliggör eller bekräftar identifiering” i syfte att bättre adressera problematiska tillämpningsområden av biometrisk uppgift i förhållande till AI-system.[251]

4.3 Biometriska AI-system

AI-förordningen är inte begränsad till reglering av biometriska AI-system som använder sig av biometriska uppgifter. I art. 1(a) framkommer att förordningen fastställer harmoniserade regler för utsläpp, distribution och användning av samtliga AI-system i unionen.

Ett AI-system definieras som ” […] *programvara som utvecklats med en eller flera av de tekniker och metoder som förtecknas i bilaga 1 och som, för en viss uppsättning människodefinierade mål, kan generera utdata såsom innehåll, förutsägelser, rekommendationer eller beslut som påverkar de miljöer som de samverkar med”.*[252]

Som framgår av definitionen ovan är AI-förordningen tillämpbar på allmänna AI-system som nyttjar olika tekniker och medel vid användning och behandling av data.[253] Förordningen delar in AI-system i fyra underkategorier: allmänna AI-system[254], AI-system för känsloigenkänning[255], AI-system för biometrisk kategorisering[256] och slutligen AI-system för biometrisk fjärridentifiering.[257] Bortsett från kategorin av allmänna AI-system sker reglering av övriga tre kategorier på

[251] Se Slovenian Presidency (2021) s. 36.
[252] Art. 3.1 COM (2021) 206 final.
[253] Jfr EPRS (2021) s. 2.
[254] Art. 3.1 COM (2021) 206 final.
[255] Art. 3.34 COM (2021) 206 final.
[256] Art. 3.35 COM (2021) 206 final.
[257] Art. 3.36 COM (2021) 206 final.

grundval av deras koppling till biometriska uppgifter.[258] För dessa biometriska AI-system är användning av biometrisk data i form av biometriska uppgifter således ett *sine qua non*-rekvisit för att vara föremål för den specifika reglering reserverad åt systemen definierade i art. 3.34-36 AI-förordningen.[259] Regleringen av biometriska AI-system utgör därför en central del av förordningens omfång.

I kontexten för biometrisk igenkänning och kategorisering skiljer sig AI-system från traditionella biometriska system främst genom en effektivisering av funktioner.[260] Genom olika maskininlärningsområden som djupinlärning (*deep learning*) och datorseende algoritmer *(computer vision algorithms*), kan datorer och system i högre utsträckning än innan samla in och behandla uppgifter. Algoritmerna underlättar extraktionen av kännetecken från större datasamlingar och djupinlärning är den dominanta metoden för identifiering och analys av dessa.[261] Resultatet blir bland annat ofta både en snabbare och mer träffsäker identifiering av individer, vilket främjar uppkomsten av biometriska system i realtid.[262] I kommande avsnitt utreds de tre olika kategorierna av biometriska AI-systemen och deras användning av biometriska uppgifter.

4.3.1 Biometriska fjärridentifieringssystem

Ett biometriskt fjärridentifieringssystem är ett AI-system som definieras utifrån två kriterier.[263] Dels måste det användas i syfte att identifiera en individ på distans genom jämförelse av deras biometriska data med de biometriska uppgifterna i en referensdatabas. Dels måste användaren av AI-

[258] Se EPRS (2021) s. 1 - *i texten nämns ”biometrics” vilket författaren tolkar används synonymt med ”biometriska uppgifter i denna kontext*” (se även avsnitt 2.2 där förekomsten av förväxling diskuteras).
[259] Se Czarnocki (2021) s. 2.
[260] Se Madiega och Mildebrath (2021) s. 2.
[261] Se Madiega och Mildebrath (2021) s. 2 - d*et hänvisar speciellt till ansiktsigenkänning men kan tillämpas på alla kännetecken.*
[262] Se Madiega och Mildebrath (2021) s.3.
[263] Se art. 3.35 COM (2021) 65 final.

systemet vara omedvetandes om huruvida individen i fråga kommer vara närvarande och kan identifieras.[264] Av formuleringen i Bilaga III till AI-förordningen framgår även explicit att regleringen för biometriska fjärridentifieringssystem avser användning i både identifierings- och kategoriseringssyfte.[265] I de dokumenterade förekomsterna av systemen i Europa har alla tagit formen av ansiktsigenkänning i realtid (*live facial recognition*).[266]

Ett biometriskt fjärridentifieringssystem delas in i två undergrupper som framgår av art. 3.36 och 3.37 AI-förordningen. I art. 3.36 beskrivs hur ett system för fjärridentifiering kan ske i realtid. Det innebär att insamlingen, jämförelsen och identifieringen av biometriska uppgifter sker utan betydande dröjsmål. Identifiering av individen sker därför genom direktupptagningar, eller näst intill direktupptagningar, av material i exempelvis videoformat.[267]

I brottsbekämpningssyfte anses användningen av biometrisk fjärridentifikation i realtid vara särskilt inskränkande på individers grundläggande rättigheter. I skälen till AI-förordningen motiverar kommissionen detta med att användningen av systemen kan skapa en känsla av konstant övervakning och indirekt avskräcka utövandet av rättigheter som mötes- och föreningsfrihet.[268] Realtidssystem kategoriseras därför som oacceptabel risk och förbjuds enligt 5.1(d) förutom i undantagsfall som framgår av bestämmelsen.[269] Undantagsfallen berör situationer där biometrisk fjärridentifiering är absolut nödvändigt för förhindring och bekämpning av ett urval brott. Samtidigt måste de faktorer som framgår av art. 5.2 AI-förordningen alltid tas i beaktning vid användning av systemen.[270] Biometrisk fjärridentifiering i realtid är även ett exempel på högrisksystem enligt Bilaga III.[271] Detta kan framstå som förvirrande eftersom det redan

[264] Se art. 3.35 COM (2021) 65 final.
[265] Se Bilaga III p.1.
[266] Se Ragazzi m.fl. (2021) s. 44.
[267] Se skäl 8 COM (2021) 206 final.
[268] Se skäl 18 COM (2021) 206 final.
[269] Se skäl 19 COM (2021) 206 final; art. 5.1(d) COM (2021) 206 final.
[270] Se art. 5.1(d) COM (2021) 206 final.
[271] Bilaga III p. 1(a).

omfattas av förbudet i art. 5.1(d) AI-förordningen för oacceptabla system. Att begreppet tillhör två olika risknivåer förklaras med att risknivåerna i AI-förordningen inte är ömsesidigt uteslutande.[272] Det innebär att biometriska fjärridentifieringssystem i realtid som uppfyller något av undantagen i art. 5.1(d) visserligen inte är strikt förbjudna men deras status som hög risk återstår och hänsyn måste ta till de krav som ställs på dessa.[273] Enligt skälen till AI-förordningen bör vissa fjärridentifieringssystem i realtid inte omfattas alls. Detta gäller när den biometriska identifieringen sker live på internet, exempelvis vid livestreaming av video.[274]

Ett system för biometrisk fjärridentifiering kan även ske i efterhand som framgår av art. 3.37 AI-förordningen. Motsatsvis till art. 3.36 innebär det att identifieringen med användning av biometriska uppgifter sker efter att tidsramen för ”utan betydande dröjsmål” passerat.[275] Efterhandssystem använder således biometriska uppgifter som redan är insamlade och genomför en identifiering av individen med betydande dröjsmål.[276] Enligt Bilaga III till AI-förordningen klassificeras biometriska fjärridentifieringssystem i efterhand som AI-system med hög risk.[277]

Infångandet av biometriska uppgifter av ett fjärridentifieringssystem sker som utgångspunkt i offentliga miljöer. Detta har kopplats till diskussionen kring huruvida rätten till privatliv och skyddet av personuppgifter bör respekteras i samma utsträckning som om systemet användes i mer privata miljöer.[278] Enligt praxis ska EKMR även anses ge skydd åt information som till sin natur inte är privat.[279] Samma principer kan utläsas av EU-domstolens uttalanden.[280]

[272] Se Wendehorst och Duller (2021) s. 63.
[273] Se Wendehorst och Duller (2021) s. 63.
[274] Se skäl 9 COM (2021) 206 final; Veale och Zuiderveen Borgesius (2021) s. 101.
[275] Se art. 3.37 COM (2021) 206 final; Skäl 8 COM (2021) 206 final.
[276] Se skäl 8 COM (2021) 206 final.
[277] Bilaga III p. 1(a).
[278] Se Ragazzi m.fl. (2021) s. 48.
[279] Se Peck v. The United Kingdom, nr 44647/98, ECHR 2003.
[280] Se Ragazzi m.fl. (2021) s. 48.

4.3.1.1 Fjärridentifieringssystem i relation till traditionella igenkänningssystem

I Bilaga III stadgas att biometriska fjärridentifieringssystem alltid kvalificeras som hög risk oberoende av den kontext de används i.[281] Av bestämmelsen i bilagan framgår att alla varianter av fjärridentifieringssystem kan användas i både verifierings- och identifieringssyfte.[282] Det överensstämmer med tolkningen av biometrisk identifiering i enlighet med dataskyddsförordningen.[283] Formuleringen i Bilaga III indikerar dock att AI-system för biometrisk identifiering som inte sker i samband med fjärridentifiering ej räknas som högrisk. Traditionella biometriska AI-system för identifiering och verifieringen omfattas inte av några specifika krav i förordningen. Istället indikerar EU-kommissionen att dessa vanliga AI-igenkänningssystem indirekt skyddas genom behandlingsförbudet som ställs upp i art. 9.1 dataskyddsförordningen.[284]

4.3.2 Biometriska AI-känsloigenkänningssystem

AI-system för känsloigenkänning definieras i art. 3.34 AI-förordningen som system för att uttyda eller identifiera fysiska personers känslor eller avsikter på grundval av deras biometriska uppgifter. Känsloigenkänning klassificeras som ett interdisciplinärt område som utgörs av en kombination av psykologi, kognitionsvetenskap och datavetenskap.[285] System som använder sig av känsloigenkänning kan exempelvis extrahera och identifiera någon av de grundläggande känslorna: ilska, glädje, rädsla, överraskning, avsmak och sorg.[286] Användningsområdena sträcker sig även till att samla in och

[281] Bilaga III p. 1(a).
[282] Se formulering i bilaga III p.1.
[283] Se avsnitt 3.2.4.
[284] Se skäl 8 COM (2021) 206 final.
[285] Se Czarnocki (2021) s. 1.
[286] Se Czarnocki (2021) s. 1 f.

klassificera information som härstammar från mätning av galvaniska hudreaktioner[287], hjärnvågsaktivitet, hudtemperatur och andra okonventionella datatyper.[288]

Biometriska AI-system för känsloigenkänning anses utgöra en begränsad risk enligt art. 52.2 AI-förordningen och omfattas därför som utgångspunkt endast av transparenskrav. System i denna kategori kan dock också klassificeras som hög risk i enlighet med Bilaga III om de används av brottsbekämpande myndigheter, vilket kan ske genom tillämpningen av lögndetektorer eller liknande verktyg.[289] Om systemen används i utbildnings- eller rekryteringssyfte kan de i vissa fall också klassificeras som hög risk i enlighet med art. 6.3 och art. 6.4 i Bilaga III. Både EDPS och EDPB har dock gemensamt kritiserat valet att inte förbjuda alla former av känsloigenkänningssystem och kategorisera dessa som oacceptabel risk.[290] Riskerna med AI-system för känsloigenkänning kan främst kopplas till integritets- och dataskyddsrättsliga grunder såsom risken att få sin information avslöjad eller sina känslor kategoriserade utifrån profilering.[291]

Syftet med ett känsloigenkänningssystem är som indikerat uppfångandet av en individs känslostämning.[292] Detta sker främst genom undersökning av ansiktsuttryck och teknologin beroende av maskininlärningselement. [293] Systemen kan som nämnt även använda sig av mer okonventionella mänskliga attribut, såsom hudreaktioner och blodtryck.[294] Med uppfångandet av en individs avsikter menas tolkningen av ett emotionellt tillstånd som en manifestation av en avsikt. Det kan exemplifieras med att ett känslouttryck

[287] *Galvanisk hudreaktion: ”förändring av det elektriska motståndet i huden i samband med känslomässiga reaktioner och vid vissa andra tillstånd”*, definition tagen från Karolinska institutet, tillgänglig: < https://mesh.kib.ki.se/term/D005712/galvanic-skin-response>
[288] Se Czarnocki (2021) s. 1 f.
[289] Bilaga III, p. 6(b).
[290] Se EDPB-EDPS: Joint Opinion 5/2021 s. 12 p. 35.
[291] Se Czarnocki (2021) s. 2.
[292] Se EPRS (2021) s. 20.
[293] Se EPRS (2021) s. 20 - *där det framgår att exempelvis även tonläge och kroppsrörelser är relativt vanligt förekommande*.
[294] Se Access Now (2021) s. 7.

som ångest hade kunnat kopplas till avsikter relaterat till våldsamma eller oförutsägbara handlingar.[295]

I likhet med övriga biometriska AI-system som definieras i AI-förordningen måste användningen ske på grundval av biometriska uppgifter.[296] Ett känsloigenkänningssystem som använder sig av annan biometrisk data kopplat till människokroppen omfattas därför inte av transparenskraven i art. 52.2.[297] De kan dock fortfarande anses utgöra hög risk om de uppfyller kraven i Bilaga III, eftersom dessa bestämmelser är tillämpbara på alla AI-system.[298] För att det biometriska AI-systemet för känsloigenkänning ska omfattas av definitionen i art. 3.34 AI-förordningen och vara föremål för transparenskrav behöver den biometriska informationen som behandlas uppfylla kraven för biometrisk uppgift som ställs upp i art. 4.14 dataskyddsförordningen. Enligt studien upprättad på begäran av Europaparlamentet om biometriska tekniker indikerar definitionen i art. 3.34 att en individs känslor och avsikter kan framgå av biometriska uppgifter.[299] Dock betonar studien att framkomsten av känslor och avsikter endast kan ske om biometrisk uppgift tolkas brett.[300]

Systemen har inte heller alltid kapaciteten att möjliggöra identifiering eller verifiering av individen, vilket även hör samman med kravet på särskild teknisk behandling.[301] AI-system utvecklas inte för allmänna syfte, så kallade *general-purpose systems,* utan utvecklas istället nästan uteslutande med ett specifikt syfte i åtanke.[302] Även om biometrisk igenkänning kan utgöra en del av ett känsloigenkänningssystem är det inte en nödvändig funktion eftersom vare sig identifiering eller verifiering av en individ krävs för att uttyda eller identifiera känslor och avsikter. Samtidigt är inte inkluderingen av känsloigenkänning heller nödvändig för ett traditionellt AI-igenkänningssystem, inkluderat både identifiering och verifiering. Detta

[295] Se EPRS (2021) s. 20.
[296] Se formulering i art. 3.34 COM (2021) 206 final.
[297] Jfr Czarnocki (2021) s. 1.
[298] Se avsnitt 4.1.2.
[299] Se EPRS (2021) avsnitt V.
[300] Se EPRS (2021) avsnitt V.
[301] Se Czarnocki (2021) s. 2.
[302] Jfr Czarnocki (2021) s. 2.

eftersom känslor inte är en essentiell komponent som behövs för att fastställa en individs identitet.[303]

Ett känsloigenkänningssystem som inte specifikt avser behandla data i identifierings- eller verifieringssyfte använder således ofta mindre detaljerad information än vad som behövs för att unikt identifiera en person.[304] Exempel kan vara ett system för att avläsa ansiktsuttryck som installeras i en affär för att uttyda konsumenters känslor och dra slutsatser om köpvanor. Detta system kan undkomma klassificering i enlighet med art. 3.34 AI-förordningen eftersom informationen som behandlas inte kan användas för att bekräfta eller fastställa en specifik konsuments identitet.[305]

Som redogjort för i tidigare avsnitt kan underlag för igenkänningssystem bestå av information såsom hjärtslag, galvaniska hudreaktioner och gångstil. Ingen av dessa informationstyper kan i praktiken användas för att unikt identifiera en individ.[306] Problematiken med identifieringskravet för biometrisk uppgift bekräftas även av EU-rättsliga organ, som framhåller att innebörden av en bred tolkning av biometrisk uppgift i denna kontext skulle innebära att definitionen utesluter kravet på unik identifiering av en individ.[307] De flesta känsloigenkänningssystem bör därför inte kunna användas för att unikt identifiera en individ, samtidigt som ett traditionellt igenkänningssystem inte kan användas för att uttyda känslor eller avsikter.

Den biometriska informationen måste utöver resterande krav även relateras till fysiska, fysiologiska eller beteendemässiga kännetecken hos en individ.[308] Vanliga igenkänningssystem använder ofta rena fysiska eller fysiologiska egenskaper för att identifiera individer, såsom DNA eller fingeravtryck.[309] Av dessa egenskaper framgår dock varken känslor eller avsikter. För ett

[303] Se Czernocki (2021) s. 2.
[304] Se The European Consumer Organisation (2021) s. 9; Se även avsnitt 3.2.4.
[305] Se The European Consumer Organisation (2021) s. 9.
[306] Se Access Now (2021) s. 7.
[307] Se EPRS (2021) avsnitt V.
[308] Art. 4.14 dataskyddsförordningen; Se även avsnitt 3.2.3.
[309] Se Wendehorst och Duller (2021) s. 13.

biometriskt känsloigenkänningssystem innebär detta att de biometriska uppgifter som systemet använder istället ofta behöver härstamma från biometriska egenskaper relaterat till emotionell data.[310] Emotionell data anses utifrån en terminologisk tolkning av biometrisk uppgift som huvudregel inte inkluderas i begreppsdefinitionen.[311] Ur ett tekniskt perspektiv finns dock undantag i form av vissa instanser där emotionell data kan visa på en stark koppling till fysiska eller beteendemässiga attribut. Som nämnt i delanalys I är detta en bedömning som bör göras i varje enskilt fall.[312]

I praktiken hade kravet på behandling av biometriska uppgifter i enlighet med dataskyddslagstiftning riskerat att en majoritet av AI-baserade känsloigenkänningssystem faller utanför definitionen i art. 3.34 AI-förordningen. De blir därmed inte heller föremål för de transparenskrav som framgår av art. 52.2 AI-förordningen.[313] Enligt utredningsrapporter av AI-förordningen innebär beroendet av biometriska uppgifter ett potentiellt hinder för att säkerställa en helomfattande och framtidssäker EU-rättslig reglering av biometriska känsloigenkänningssystem.[314]

4.3.2.1 Uttydning som syfte med biometriska tekniker

Definitionen i art. 3.34 AI-förordningen av AI-system för känsloigenkänning anger explicit två syften. Det biometriska AI-systemet kan syfta till att antingen identifiera eller uttyda fysiska personers känslor eller avsikter. Inkluderingen av begreppet ”uttyda” indikerar tillägget av ett nytt syfte med biometriska system utifrån ett EU-rättsligt perspektiv.[315]

[310] Jfr exempelvis Czarnocki (2021), s. 2 f.
[311] Se avsnitt 3.2.3.
[312] Se avsnitt 3.3.
[313] Se Czarnocki (2021), s. 1; Art. 52 COM (2021) 206 final.
[314] Jfr Access Now (2021) s. 6 f.
[315] Se EPRS (2021) s. 20.

Som diskuterat i tidigare kapitel indikerar dataskyddsförordningen endast syftena identifiering, verifiering och kategorisering.[316] Det kan dras liknelser till de tekniska definitionerna av biometriska tekniker som också endast inkluderar de tre ovanstående syftena.[317] Att uttyda blir således en fjärde kategori av användningssyften med biometriska tekniker.[318]

Som diskuterat i 4.3.2 räcker inte definitionen av biometrisk uppgift för att reglera system som inte nödvändigtvis kräver unik identifiering av en person. System i uttydningssyfte är av sin natur inte också kopplade till identifieringssyften. Exempelvis används sådana teknologier till lögndetektorer vars syfte är att uttyda känslor och avsikter. Dessa använder sig av fysiska kännetecken såsom blodtryck för att avgöra huruvida en person talar sanning. Informationen som behandlas kan dock inte användas för att identifiera personen i fråga.[319]

4.3.3 Biometriska AI-kategoriseringssystem

I likhet med ett allmänt kategoriseringssystem syftar ett biometrisk AI-kategoriseringssystem till att hänföra fysiska personer till kategorier utifrån kännetecken på grundval av biometriska uppgifter. Det kan inkludera kön, ålder, ögonfärg, tatueringar, sexuell läggning och så vidare.[320] Biometriska AI-system för kategorisering regleras i art. 52.1 AI-förordningen och anses därmed utgöra begränsad risk i likhet med ett känsloigenkänningssystem.

Enligt EDPS belyser korsningen mellan biometrisk information och AI en utveckling där mängden biometriska kategoriseringssystem ökar.[321] Även om identifiering fortsätter vara en viktig beståndsdel av den generella

[316] Se avsnitt 2.2 och 3.3 om kravet på ”*rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken*”.
[317] Se avsnitt 2.2.
[318] Se Wendehorst och Duller (2021) s. 13.
[319] Se definition av biometriskt AI-kategoriseringssystem i art. 3.35 COM (2021) 206 final.
[320] Se definition i art. 3.35 COM (2021) 206 final.
[321] Se EPRS (2021) avsnitt II.

tillämpningen av biometrisk information, är det inte alltid självklart att ett kategoriseringssystem kan användas för identifiering av en individ. AI-system baserade på kategorisering kan i praktiken fungera självständigt från övriga biometriska tekniker. Det är dock oklart i vilken utsträckning detta gäller.[322] I studien på efterfrågan av Europaparlamentet betonas även att den data som behandlas i kategoriseringssyften inte nödvändigtvis måste kunna avse en identifierad eller identifierbar person.[323] Det argumenterar vidare för att detta kan tolkas som att sådan biometrisk information inte kan anses vara personuppgifter enligt EU-rättslig lagstiftning. Det resulterar i sin tur i oklarheter huruvida uppgifterna kan omfattas av definitionen av biometrisk uppgift enligt dataskyddsförordningen och AI-förordningen.[324]

Ett biometriskt AI-system kan kategorisera utifrån biometriska egenskaper som inte möter det höga kravet på unik identifiering uppställt i art. 414 dataskyddsförordningen.[325] Liksom ett AI-känsloigenkänningssystem kan kategorisering ske på grundval av egenskaper såsom galvaniska hudreaktioner, röst och hjärtslag.[326] I ett svar på EU-kommissionens samråd för antagande av AI-förordning framhålls att det dock även är möjligt att kategorisera individer utifrån biometriska uppgifter som uppfyller alla krav i art. 4.14.[327] Ett AI-system hade exempelvis kunnat analysera fotografier för att kategorisera individer utifrån hår- eller ögonfärg.[328] Det finns dock ett flertal kategorier som biometriska uppgifter inte kan ligga till grund för. Dessa framgår av definitionen av ett biometriskt AI-kategoriseringssystem som innehåller följande exempel på kategorier: *”[…] såsom kön, ålder, hårfärg, ögonfärg, tatueringar, etniskt ursprung eller sexuell eller politisk läggning”.* [329]

[322] Se EPRS (2021) avsnitt II.
[323] Se EPRS (2021) avsnitt II.
[324] Se EPRS (2021) avsnitt II f.
[325] Se Access Now (2021) s. 6 f.
[326] Se Access Now (2021) s. 6.
[327] Se Access Now (2021) s. 7.
[328] Se Access Now (2021) s. 7.
[329] Se art. 3.34 COM (2021) 206 final.

Formulering i bestämmelsen ovan kan uppfattas som oklar eftersom kategorier såsom sexuell eller politisk läggning inte bevisligen kan baseras på varken biometriska uppgifter eller övriga biometriska egenskaper. Att utifrån fysiska, fysiologiska eller beteendemässiga kännetecken dra slutsatser om sexuella eller politiska inriktningar anses varken vara korrekt eller etniskt försvarbart.[330] Påståendet om att AI-system kan användas för att uttyda sexuell och politisk läggning har delvis sitt ursprung i Michal Kosinskis teorier om frenologi and fysionomi, som enligt dagens mått anses vara utdaterade, rasistiska och ha starka kopplingar till eugenik.[331] Kosinski publicerade bland annat verket som av utomstående källor benämns som ”*AI Gaydar*”[332]. Det är en bevisat problematisk och vetenskapligt inkorrekt utredning om hur en persons sexuella läggning kan utvinnas och avslöjas av ansiktsbilder.[333] Enligt utredningsrapporten innebär påståendet om att fysiska och fysiologiska kännetecken kan användas i syfte att bedöma en persons politiska preferenser en inskränkning i rätten att tänka fritt och forma självständiga åsikter. Det anses även utgöra en kränkning av den mänskliga värdigheten.[334]

[330] Se Access Now (2021) s. 8.
[331] Se Access Now (2021) s. 8.
[332] Se Burdick, Alan, ’The A.I ”Gaydar” Study and the Real Dangers of Big Data’, 2017-09-15, < https://www.newyorker.com/news/daily-comment/the-ai-gaydar-study-and-the-real-dangers-of-big-data>, besökt 2022-04-05.
[333] Se Access Now (2021) s. 8.
[334] Se Access Now (2021) s. 8 f.

4.4 Delanalys II

AI-förordningens överlappning och anpassningsbarhet med gällande dataskyddslagstiftning och biometriska uppgifter som personuppgifter

I skälen till AI-förordningen uttrycks att tolkningen av biometrisk uppgift bör överensstämma med dataskyddslagstiftningens definition av begreppet. EU-rättsakter såsom dataskyddsförordningen klassificeras även som en central sekundärkälla inom kontexten av AI på EU-nivå.[335] Dataskyddslagstiftning är således ett viktigt instrument för att kontrollera och reglera användning av AI inom unionen. Problematiken relaterat till biometriska AI-systems användning av biometriska uppgifter kan delvis vara ett resultat av att definitioner ursprungligen anpassade för dataskyddslagstiftning inte alltid är effektiva i en AI-rättslig kontext. Som Belkadi förespråkar föreligger en betydelsefull skillnad mellan de två rättsområdena. Ett ramverk för dataskyddslagstiftning utgår ifrån individens fundamentala rättigheter och ett individbaserat fokus genomsyrar dataskyddsförordningens tillämpningsområde. En personuppgift är information som relateras till den identifierbar individen, vilket likväl innebär att de relevanta skyddsobjekten och skyddsintressena ur ett dataskyddsrättsligt perspektiv främst är kopplade till individen.[336]

När artificiell intelligens ska regleras är en snäv inriktning på individen inte optimal. Med hänsyn till de uppmärksammade riskerna med AI-system syftar en AI-reglering på EU-nivå till att skydda allmänhetens intressen. Dessa inkluderar bland annat säkerhetsintressen, hälsa och andra fundamentala rättigheter.[337] Det innebär att skyddet av personuppgifter således endast är en av de beståndsdelar som AI-förordningen adresserar. Tillskillnad från dataskyddsförordningen utgörs det rättsliga subjektet av både grupper och

[335] Jfr FRA (2021) s. 48.
[336] Jfr Belkadi (2021).
[337] Se skäl 5 COM (2021) 206 final.

individer.[338] Rättsligt skydd på EU-nivå för den identifierbara individen och dennes personuppgifter är därför som nämnt endast en av många regulatoriska dimensioner i AI-förordningen. Dataskyddsförordningen syftar till att främst adressera den dimension som berör datasubjektets personuppgifter, medan AI-förordningen har ett mycket bredare skyddsomfång. EU-kommissionens val att kopiera dataförordningens definitioner utan ytterligare modifikationer för tillämpning i en AI-rättsakt kan därför anses problematisk. Genom att kräva en koppling till den identifierbara individen riskerar många användningsområden av AI-system att kringgå reglering. Tillämpningen av biometriska känsloigenkännings- och kategoriseringssystem sker som diskuterat i uppsatsen exempelvis på ett spektrum av individuella och gruppbaserade användningsområden.

EU-kommissionens val att använda en kopia av dataskyddslagstiftningens definition av biometrisk uppgift kan indikera att tillräcklig hänsyn inte tagits till AI:s inverkan på biometriska tekniker. Som Belkadi diskuterar skiljer sig syftena med utveckling av traditionella biometriska system och biometriska AI-system åt. Traditionella biometriska system syftar oftast till att identifiera en specifik individ. Fram tills för några år sedan utgjorde vanliga ansikts- och fingeravtrycksavläsning en överväldigande majoritet av biometriska tekniker.[339] En definition av biometriska uppgifter som data med en stark koppling till individen är i dessa fall effektiv. Detta eftersom systemen syftade till att specifikt identifiera en fysisk person utifrån unika kroppsliga data av fysisk karaktär. Det sker dock nu en övergång till nya biometriska tekniker som använder sig av maskininlärning för att effektivisera och precisera processer. Tillskillnad från traditionella biometriska system utvecklas ett biometrisk AI-system huvudsakligen i syfte att profilera individer genom användning av kategoriserings- och känsloigenkänningstekniker. Användningsområdena för biometriska tekniker har därför i snabb takt breddats.

[338] Jfr bland annat Belkadi (2021); skäl 17, 36-38 och 44 COM (2021) 206 final.
[339] Se Belkadi (2021).

Eftersom biometrisk uppgift är en underkategori till personuppgifter kommer kopplingen till säkerställandet av individers identitet alltid vara närvarande i enlighet med den nuvarande definitionen. Många AI-system riskerar därmed att kringgå reglering eftersom den biometriska data de använder inte visar på en tillräckligt stark koppling till den identifierbara individen. Exempelvis kan emotionell data användas i AI-system för att profilera grupper och individer utan någon som helst koppling till personlig data. Den biometriska informationen är således känslig och privat men anses inte EU-rättsligt utgöra personuppgifter.[340] Den rättsliga kategorin av biometriska uppgifter som biometriska personuppgifter bör därför inte anses vara ett lämpligt val för regleringen och definitionen av biometriska AI-system.

Övriga krav som framgår av art. 4.14 dataskyddsförordning i förhållande till definitionerna av biometriska AI-system

I ovanstående stycken redogörs för hur dataskyddsförordningens definition av biometrisk uppgift kan tänkas vara opassande för regleringen av AI-system eftersom kravet på status som personuppgift innebär ett strikt fokus på individen. Likaså kan övriga krav som framgår av formuleringen i art. 4.14 dataskyddsförordningen tänkas vara problematiska i denna kontext. Särskilt kravet på unik identifiering har bemötts av kritik i både expertuttalanden och övrig doktrin.[341] Att biometrisk uppgift måste möjliggöra eller bekräfta en specifik individs identitet resulterar enligt många i en alltför insnävad definition av begreppet. Bakgrunden till detta är att kravet höjer ribban ytterligare för identifiering av en individ och således förstärker kopplingen till en specifik fysisk person. Kravet speglar de dominerande koncepten som var aktuella under tiden för den första generationens biometriska egenskaper och anses inte ta andra generations egenskaper i beaktning.[342] Exempelvis hade biometriska AI-känsloigenkänningssystem som baseras på kännetecken

[340] Jfr McStay (2020) s. 4.
[341] Se avsnitt 4.2.
[342] Jfr bland annat Wendehorst och Duller (2021) s. 13 ff.

såsom puls, kroppstemperatur, och anonyma ansiktsuttryck i form av leenden och gäspning, uteslutits från definitionen i art. 3.34 AI-förordningen.[343]

Även kravet på särskild teknisk behandling kan i en AI-rättslig kontext framstå som begränsande för en stor del biometriska system. Enligt kravet bör den biometriska informationen ta formen av biometrisk uppgift först vid inledandet av extraktionssteget i den tekniska processen.[344] Som Czernocki betonar är det ur en teknisk synvinkel oklart om samtliga data i biometriska AI-system behöver genomgå en sådan teknisk behandling som avsnitt 3.2.2 redogör för. Detta bör specifikt vara fallet med känsloigenkänningssystem i uttydningssyfte. Biometriska tekniker brukade kännetecknas av de tre syftena verifiering, identifiering och kategorisering. Som ett resultat av den teknologiska utvecklingen har ett fjärde uttydningssyfte blivit allt vanligare. Med hjälp av AI hade systemet kunnat uttyda och utvinna känslouttryck i form av muskelrörelser, ansiktsrynkningar eller tonskillnader i röst. Systemet hade direkt kunnat kategorisera dessa känslouttryck utan att behöva extrahera en hel biometrisk mall. Det är endast vid denna extraktion som systemet utifrån en EU-rättslig tolkning anses tekniskt behandla den biometriska informationen.[345]

Som diskuterat i kapitel 3 bör det tolkas som att den EU-rättsliga definitionen av biometrisk uppgift utesluter ren emotionell data. Kravet på att den biometriska informationen endast kan härstamma från fysiska, fysiologiska och beteendemässiga kännetecken, begränsar kraftigt antalet AI-system som kan omfattas av AI-förordningens definitioner. Särskilt oklart blir denna terminologiska tolkning i förhållande till känsloigenkänningssystem. Som namnet indikerar bör bruket av dessa system till stor del vara beroende av emotionell data. Att uttyda känslor och avsikter kräver oftast avläsning av rena emotionella uttryck. Både känsloigenkänningssystem och kategoriseringssystem använder sig även i allt högre utsträckning av

[343] Jfr Wendehorst och Duller (2021) s. 67.
[344] Se avsnitt 2.2.
[345] Se Czernocki (2021) s. 3.

okonventionella beteendemässiga kännetecken. Som redogjorts för i kapitel 2 och 3 är känsloigenkänningssystem och kategoriseringssystem bäst lämpade att använda sig av beteendemässig data. I och med den tekniska utvecklingen bör det kunna förutses att en ökad användning av okonventionella och otraditionella beteendemässiga biometriska kännetecken kommer ske i både igenkännings-, uttydnings- och kategoriseringssyfte. Av detta kan slutsatsen dras att definition av biometrisk uppgift i art. 4.14 är för snäv för att ge ett heltäckande och framtidssäkert rättsligt skydd åt alla relevanta biometriska AI-system.

Potentiell modifikation och ändring av begreppet biometrisk uppgift för en AI-rättslig kontext

AI-förordningen har ännu inte trätt ikraft och EU-kommissionens nuvarande förslag kan fortfarande vara föremål för omfattande modifikationer. Utifrån uppsatsens utredning och analys av biometrisk uppgift i en AI-rättslig kontext kan antagandet göras att en reglering av artificiell intelligens troligtvis hade kunnat förstärkas om definitionen av begreppet modifierades och särskildes från dataskyddsförordningens motsvarighet. Eftersom definitionen av biometrisk uppgift är bäst lämpad för att skydda rätten till privatliv i enlighet med dataskyddslagstiftning kan det argumenteras för att definitionen bör ändras i syfte att säkerställa en framtidssäker och heltäckande reglering för samtliga berörda rättigheter som den kommande AI-förordningen avser skydda.

Det kan diskuteras huruvida den juridiska termen biometrisk uppgift bör fortsätta vara teknikneutral men utesluta alla krav på teknisk behandling. Som diskuterat i avsnitt 3.3 kan enbart lagring av biometriska prov utgöra risker för fundamentala rättigheter. Samtidigt hade en totalt uteslutande av kravet på särskild teknisk behandling riskerat att resultera i en för bred definition av biometrisk uppgift. Det kan innebära att en oproportionerlig mängd AI-system omfattas av kraven i AI-förordningen, vilket i sin tur kan riskera hämma innovationen inom unionen. Kravet på särskild teknisk behandling

kan således anses nödvändigt för att främja utveckling och distribuering av artificiell intelligens. Utan ett sådant krav hade varje behandling av biometrisk information potentiellt kunnat inbegripas i definitionen[346]

I ett förslag till utkastet av AI-förordningen föreslås ett byte från biometrisk uppgift till biometriskbaserad data i definitionerna av biometriska AI-system.[347] Den nya definitionen har uppgetts kunna förbättra regleringen av biometriska kategoriserings- och känsloigenkänningssystem.[348] Även om det inte framgår explicit av förslaget härstammar den föreslagna ändringen troligtvis från studien upprättad på begäran av Europaparlamentet om biometriska tekniker.[349] Där diskuteras rekommendationer menade att adressera och lösa problemet med vad de anser vara en för insnävad definition av biometrisk uppgift för uppfyllandet av syftet att effektivt reglera förordningens uppräknade AI-system.[350] I studien föreslås tre potentiella lösningar. Den första lösningen hade inneburit en modifikation av definitionen ”biometrisk uppgift” och i syfte att särskilja den från definitionen i art. 4.14 dataskyddsförordningen. Enligt den andra lösningen bör istället definitionerna av känsloigenkänningssystem och kategoriseringssystem ändras för att utesluta hänvisning till en särskild typ av biometrisk uppgift eller information.[351]

Slutligen föreslås i den tredje lösningen att förordningen introducerar en helt ny definition som kan formuleras i stil med ”biometriskbaserad data” (*biometric-based data*). Denna nya formulering kan ersätta biometrisk uppgift i definitionerna av biometriska AI-system. Enligt studien beskrivs biometriskbaserad data i stor utsträckning överensstämma med definitionen av biometrisk uppgift i dataskyddsförordningen. Skillnaden ligger i det faktum att biometriskbaserad data ”*may or may not allow or confirm the*

[346] Jfr Wendehorst och Duller (2021) s. 67.
[347] Se Draft Report (2022) Amendment 64. Översättningen från ”biometric-based data” är godtycklig eftersom rapporten är ny och ingen officiell svensk översättning har getts.
[348] Se Algorithm Watch (2022) s. 2.
[349] Se Wendehorst och Duller (2021) s. 67.
[350] Se Wendehorst och Duller (2021) s. 67.
[351] Se Wendehorst och Duller (2021) s. 67 f.

identification of a natural person". [352] Kravet på unik identifiering stryks därmed. Samtidigt skulle kravet på särskild teknisk behandling kvarstå. Det stämmer bättre överens med den generella tekniska definitionen av begreppet. Studien avslutar med att påstå att det sista alternativet gällande biometriskbaserad data skulle ha minst störande påverkan på andra EU-lagstiftningar, vilket kan antas vara anledningen till att förslaget till rapporten gått på denna linje i sin utredning.

[352] Se Wendehorst och Duller (2021) s. 69.

5 Avslutande reflektioner och slutsatser

Konceptet biometrisk uppgift utgör en central del av regleringen och kontrollen av biometriska tekniker och system inom unionen. Det står klart att definitionen av begreppet som tolkat ur ett dataskyddsrättsligt perspektiv även kommer lägga grunden för kontrollen och regleringen av majoriteten av de riskabla AI-systemen enligt den nuvarande utformningen av förslaget till den kommande AI-förordningen. EU-kommissionens val att villkora definitionerna av samtliga biometriska AI-system till deras användning av biometriska uppgifter innebär att den terminologiska tolkningen av begreppet blir avgörande för huruvida systemet omfattas av förordningens bestämmelser. Biometriska uppgifter tilläts därför stor betydelse för regleringen av biometriska AI-system i enlighet med förslaget till den kommande AI-förordningen.

Gällande uppsatsens första frågeställning kan en biometrisk uppgift sammanfattningsvis definieras som produkten av en teknisk process där en biometrisk egenskap har behandlats i syfte att möjliggöra unik identifiering av en specifik individ. Med denna definition utesluts en stor mängd emotionell och beteendemässig biometrisk data som inte når upp till det högt ställda kravet på identifiering. Definitionen har kritiserats eftersom den enbart anses reflektera den första generationens biometriska egenskaper som används i traditionellt identifiering- och verifieringssyfte. I detta avseende får det anses behövligt att se över de formuleringar i definitionen som kräver en koppling till en specifik individ. En mer framtidssäker och teknikneutral definition hade i relation till detta även gynnats av att exkludera kravet på att den biometriska informationen behövde vara en underkategori till personuppgift. För att säkerställa en heltäckande definition och skydd för känsloigenkänning- och kategoriseringssystem hade kravet på unik identifiering behövt uteslutas helt. En särskild teknisk behandling är dock

nödvändigt för att förhindra att definitionen av biometrisk uppgift inte omfattar all behandling av biometrisk data. Ett förtydligande av begreppet på EU-nivå hade dock varit behövligt. Möjligtvis hade detta kunnat ske i form av en handbok utfärdad på EU-nivå. För att inte utesluta vissa känsloigenkänningssystem hade handboken förslagsvis kunnat ta hänsyn till tekniska definitioner från internationella standarder som betonar att även biometriska prov som inte genomgått extraktion kan vara biometriska uppgifter i vissa situationer. Det är dock oklart huruvida en alltför specifik vägledning kan få negativa konsekvenser för säkerställandet av en framtidssäker och teknikneutral reglering.

Med beaktande av uppsatsens material tycks det vara svårt att avgöra exakt hur definitionen av biometrisk uppgift rent tekniskt riskerar att negativt påverka regleringen av AI-förordningens omnämnda biometriska AI-system. Många av de AI-system och biometriska tekniker som diskuteras i förslaget används i praktiken antingen i väldigt liten utsträckning eller inte alls. Exempelvis har känsloigenkänning genom behandling av okonventionella biometriska egenskaper såsom gångstil ännu inte börjat användas inom unionen.[353] Samtidigt ska betonas att formuleringen i AI-förordningen lyder ”ske på grundval av biometriska uppgifter”, vilket kan tänkas vara ett medvetet val i syfte att bredda definitionen eftersom formuleringen inte explicit uttrycker att AI-system ska behandla biometriska uppgifter i traditionell mening. Varken EU-kommissionen eller övriga relevanta EU-organ har dock gett en mer detaljerad redogörelse eller vägledning för hur begreppet ska tolkas. Det blir därför svårt att ta ställning till huruvida ”ske på grundval av” i praktiken skulle skilja sig från att systemet behandlar uppgifterna. Denna oklarhet hade dock troligtvis kunnat undvikas om EU-kommissionen överväger att ersätta biometrisk uppgift med exempelvis biometriskbaserad data i lagtexten. I vilken utsträckning EU i framtiden kommer ta hänsyn till den tekniska karaktär som genomsyrar detta komplexa rättsområde återstår dock att se.

[353] Jfr Ragazzi m.fl. (2021) s. 43.

Käll- och litteraturförteckning

Europeiska unionen

Europeiska kommissionen

Europeiska kommissionen, *Bilagor till Förslag till Europaparlamentets och rådets förordning om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter,* Bryssel den 21.4.2021 COM (2021) 206 final ANNEXES 1 to 9. [cit. COM (2021) 206 final].

Europeiska kommissionen, *Förslag till Europaparlamentets och rådets förordning om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter*, Bryssel den 21.4.2021 COM (2021) 206 final. [cit. COM (2021) 206 final].

Europeiska kommissionen, *Förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning)*, Bryssel den 25.1.2012 COM (2012) 11 final. [cit. COM (2012) 11 final].

Europeiska kommissionen (2021*), New rules for Artificial Intelligence – Questions and Answers*, Bryssel den 21.04.2021.

Europeiska kommissionen, *On Artificial Intelligence – A European approach to excellence and trust, White Paper from the Commission to the European Council*, Bryssel den 19.2.20 COM (2020) 65 final. [cit. COM (2020) 65 final].

Europeiska kommissionen (2021*), Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe*, Final Report (D5). [cit. Final Report (2021)].

Wiewiórowski, Wojciech (2020), *The State of Biometrics: Update from the European Data Protection Supervisor EPDS*. [cit. Wiewiórowski (2020)].

Europaparlamentet

European Parliamentary Research Service (2021), *Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence*, Study by request of Panel for the Future of Science and Technology. [cit. EPRS (2021)].

European Parliament (2022), *Draft Report: On the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts*, COM2021/0206 – C9-0146/2021 – 2021/0106(COD). [cit. Draft Report (2022)].

Europaparlamentets lagstiftningsresolution av den 12 mars 2014 om förslaget till Europaparlamentets och rådets förordning för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning) (COM (2012) 0011 – C7-0025/2012 –2012/0011(COD)).

Madiega, Tambiama och Mildebrath Hendrik (2021), *Regulating facial recognition in the EU, In-depth Analysis, European Parliamentary Research Service*. [cit. Madiega och Mildebrath (2021)].

Ragazzi, Francesco och Mendos Kuskonmaz, Elif och Plájás, Ildikó och Van de Ven, Ruben och Wagner, Ben (2021), *Biometric Behavioural Mass*

Surveillance in EU Member States, Report for the Greens/EFA in the European Parliament. [cit. Ragazzi m.fl. (2021)].

Wendehorst, Christiane och Duller, Yannic (2021), *Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces*, Study requested by the JURI and PETI committees, Policy Department for Citizens' Rights and Constitutional Affairs. [cit. Wendehorst och Duller (2021)].

Europeiska rådet

Council of Europe Study, *Algorithms and Human Rights: Study on the human rights dimensions of automated data processing techniques and possible regulatory implications, DGI (2017),*12, Prepared by the committee of experts on internet intermediaries (MSI-NET). [cit. Council of Europe Study on Algorithms and Human Rights (2017)].

Europarådet, *Konvention 108 av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter*.

Slovenian Presidency, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, 2021/0106 (COD), Bryssel den 29.11.2021.[cit. Slovenian Presidency (2021)].

Övriga EU-rättsliga källor

Artikel 29 – Arbetsgruppen för dataskydd, *Arbetsdokument om biometri,* 12168/02/SV WP80, antaget 2003-08-01. [cit. Artikel 29 – Arbetsgruppen för dataskydd (2003)].

Artikel 29 – Arbetsgruppen för skydd av personuppgifter, *Yttrande 4/2007 om begreppet personuppgifter,* 01248/07/EN WP 136, antaget 2007-06-20. [cit. Artikel 29 – Arbetsgruppen för skydd av personuppgifter (2007)].

Artikel 29 - Arbetsgruppen för skydd av personuppgifter, *Yttrande 3/2012 om utveckling i biometrisk teknik*, *00720/12/EN, WP193*, antaget 2012-04-27. [cit. Arbetsgruppen för skydd av personuppgifter (2012)].

European Data Protection Board, *EDPB-EDPS: Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artifical Intelligence Act)*. [cit. EDPB-EDPS: Joint Opinion 5/2021].

European Union Agency for Fundamental Rights, FRA (2021), *Fundamental Rights Report – 2021*. [cit. FRA (2021)].

The European Consumer Organisation (2021), *Regulating AI to Protect the Consumer*, Position Paper on the AI Act.

Offentligt tryck i nationell rätt

Garante (2014), *Annex A to the Garante's Order Concerning Biometrics*, 2014-11-12.

Mot. 2021/22:4360, Maria Malmer Stenergard m.fl. (M), *med anledning av prop. 2021/22:81: Anpassning av svensk rätt till EU:s nya in- och utresesystem*.

Internationella standarder

ISO/IEC 2382-37:2022 (en) (2022), *Information technology – Vocabulary – Part 37: Biometrics.* [cit. ISO/IEC 2382-37:2022].

ISO/IEC TR 24741:2018 (2018), *Information technology – Biometrics – Overview and application.* [cit. ISO/IEC TR 24741:2018].

ISO/IEC 2382-37:2017, *Information technology – Vocabulary – Part 37: Biometrics.* [ISO/IEC 2382-37:2017].

Litteratur, artiklar, rapporter och dokument

Access Now (2021), *Access Now's submission to the European Commission's adoption consultation on the Artificial Intelligence Act*. [cit. AccessNow (2021)].

Algorithm Watch (2022), *Civil society reacts to EP AI draft report,* Joint Statement by Algorithm Watch and civil society partners. [cit. Algorithm Watch (2022)].

Ashok, Jammi och Shivashankar, Vaka och Mudiraj, P.V.G.S (2010), 'An Overview of Biometrics', *International Journal on Computer Science and Engineering*, Volym 02 nr 07, s. 2402-2408. [cit. Ashok m.fl. (2010)].

Bisztray, Tamas och Gruschka, Nils och Bourlai, Thirimachos och Fritsch, Lothar (2021), 'Emerging biometric modalities and their use: Loopholes in the terminology of the GDPR and resulting privacy risks', *2021 International Conference of the Biometrics Special Interest Group (BIOSIG)*. [cit. Bisztray m.fl. (2021)].

Czarnocki, Jan (2021), ‘Will new definitions of emotion recognition and biometric data hamper the objectives of the proposed AI Act?’, *2021 International Conference of the Biometrics Special Interest Group (BIOSIG)*. [cit. Czarnocki (2021)].

Dantcheva, Antitza och Elia, Petros och Ross, Arun (2015), ’What else does your biometric data reveal? A survey on soft biometrics’, *IEEE Transactions on Information Forensics and Security*, Volym 11 nr 3, s. 441-467. [cit. Dantcheva m.fl. (2015)].

Edwards, Lillian (2022), ‘The EU AI Act: a summary of its significance and scope’, *Ada Lovelace Institute: Expert Opinion*. [cit. Edwards (2022), ‘The EU AI Act: a summary of its significance and scope’].

Gorodnichy, Dimitry (2016), ‘New age glossery of biometric terms for automated border control and video surveillance application’*, Technical Report*, Government of Canada. [cit. Gorodnichy (2016)].

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

Jain, Anil K och Ross, Arun och Prabhakar, Salil (2004), ’An Introduction to Biometric Recognition’, *IEEE Transactions on Circuits and Systems for Video Technology,* Volym 14 nr 1, s. 4-20. [cit. Jain m.fl. (2004)].

Jasserand, Catherine (2015*),* ‘Avoiding Terminological Confusion Between the Notions of ‘Biometrics’ and ‘Biometric Data’: An Investigation Into the Meanings of the Terms From a European Data Protection and a Scientific Perspective’, *International Data Privacy Law,* Volym 6 nr 1*,* s. 63-76. [cit. Jasserand (2015)].

Jasserand, Catherine (2016), ‘Legal Nature of Biometric Data: From ‘Generic’ Personal Data to Sensitive Data: Which Changes Does the New Data Protection Framework Introduce?’, *European Data Protection Law review*, Volym 2 nr 3, s. 63-76 [cit. Jasserand (2016)].

Kindt, Else (2020), ‘A First Attempt at Regulating Biometric Data in the Union’, i: A. Kak (ed.), *Regulating Biometrics. Global Approaches and Urgent Questions*, AINow Institute, New York University, s. 62-69. [cit. Kindt (2020)].

Kindt, Else (2018), ‘Having yes, using no? About the new legal regime for biometric data’, *Computer Law & Security Review,* Volym 34 nr 3, s. 523-538. [cit. Kindt (2018)].

Krausová, Alzbeta (2018), ’Online Behavior Recognition: Can We Consider It Biometric Data under GDPR?’, *Masaryk University Journal of Law and Technology,* Volym 12 nr 2, s. 161-177. [cit. Krausová (2018)].

McStay, Andrew (2020), ‘Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy’, *Big Data & Society,* s. 1-12. [cit. McStay (2020)].

Purtova, Nadezhda (2018), ‘The law of everything. Broad concept of personal data and future of EU data protection law’, *Law, Innovation and Technology,* Volym 10 nr 1, s. 40-81. [cit. Purtova (2018)].

Rodrigues, Rowena och Siemaszko, Konrad och Warso, Zuzanna (2019), ’SIENNA D4:2: Analysis of the legal and human rights requirements for AI and robotics in and outside the EU’, *Version V2.0, Zenodo*. [cit. Rodrigues m.fl. (2019)].

Rommetveit, Kjetil (2016), ’Introducing Biometrics in the European Union: Practice and Imagination’, i Delgado, Ana (red.), *Technoscience and Citizenship: Ethics and Governance in the Digital Society,* 1a uppl., Springer International Publishing. [cit. Rommetveit (2016)].

Sandgren, Claes (2015), *Rättsvetenskap för uppsatsförfattare*, 3e uppl., Nordstedts Juridik, Stockholm. [cit. Sandgren (2015)].

Smuha, Nathalie och Ahmed-Rengers, Emma och Harkens, Adam och Li, Wenlong och MacLaren, James och Piselli, Riccardo och Yeung, Karen (2021), ’How the EU can Acgieve Legally Trustworthy AI: A Response to the European Commission’s Proposal for an Artifical Intelligence Act’. [cit. Smuha m.fl. (2021)].

Svenskt Näringsliv (2021), ’Comments on AI Act proposal’.

The European Consumer Organisation – BEUC10 (2021*), Regulating AI to Protect the Consumer: Position Paper on the AI Act*. [cit. The European Consumer Organisation (2021)].

Veale, Michael och Zuiderveen Borgesius, Frerdrik (2021), ’Demystifying the Draft EU Artifical Intelligence Act: Analysing the good, the bad, and the unclear elements of the proposed approach’*, Computer Law Review International,* Volym 22 nr 4, s. 97-112. [cit. Veale och Zuiderveen Borgesius (2021)].

Zaborska, Sylwia (2019), ‘Legal Regulation of the Protection of Biometric Data under the GDPR’, *Studia luridica Lublinensia,* Volym 28 nr 2*,* s. 97-106. [cit. Zaborska (2019)].

Elektroniska källor

Belkadi, Lydia (2021), ‘The Proposed Artificial Intelligence Act and Biometric Systems: A Peek Into the Conceptual Maze (Part I and II)’, Ku Leuven, <https://www.law.kuleuven.be/citip/blog/the-proposed-artificial-intelligence-act-and-biometric-systems-part-i/>, besökt 2022-03-26. [cit. Belkadi (2021)].

Burdick, Alan (2017), ’The A.I ”Gaydar” Study and the Real Dangers of Big Data’, < https://www.newyorker.com/news/daily-comment/the-ai-gaydar-study-and-the-real-dangers-of-big-data>, besökt 2022-04-05.

Europeiska kommissionen, ‘What is considered personal data under the EU GDPR?’, <https://gdpr.eu/eu-gdpr-personal-data/>, besökt 2022-04-05.

Hellern, Jan (1975), ’Argumentation de lege ferenda’, Svensk Juristtidning, <https://svjt.se/svjt/1975/401>, besökt 2022-04-04.

Koch, Richie (2020), ’What is considered personal data under the EU GDPR?’, GDPR.EU, Proton Technologies AG, <https://gdpr.eu/eu-gdpr-personal-data/>, besökt 2022-04-03. [cit. Richie (2020)].

Lukianets, Nikita (2021), *A (more) visual guide to the proposed EU Artificial Intelligence Act*, EU-kommissionens European AI Alliance, <https://futurium.ec.europa.eu/en/european-ai-alliance/open-discussion/more-visual-guide-proposed-eu-artificial-intelligence-act?language=da>, besökt 2022-04-07. [cit. Lukianets].

Nine Engineering, ‘GDPR and biometrics: an overview’, <https://www.nineengineering.com/post/gdpr-and-biometrics-an-overview>, besökt 2022-03-28.

W, Kenneth och Wills, Michael (2018), ‘Differences Between ”Physical” & “Physiological’, Sciencing, <https://sciencing.com/differences-between-physical-physiological-8774303.html>, besökt 2022-04-08.

Rättsfallsförteckning

EU-domstolen

Europeiska unionens domstol av den 20 december 2017, C-434/16, *Nowak*, ECLI:EU:C:2017:994.

Europeiska unionens domstol av den 16 april 2015, Förenade målen C-446/12 och C-449/12, *Willems,* ECLI:EU:C:2015:238.

Europeiska unionens domstol av den 17 oktober 2013, C-291/12, *Schwarz,* ECLI:EU:C:2013:670.

Europadomstolen

Peck v. The United Kingdom, nr 44647/98, ECHR 2003.

S. and Marper v. The United Kingdom, nr 30562/04 and 30566/04, ECHR 2007.

M.K. v. France, nr 19522/09, ECHR 2013.