



JURIDISKA FAKULTETEN
vid Lunds universitet

Lina Persson

Artificiell intelligens – ett hot mot den personliga integriteten?

Om efterlevnaden av enskildas rättigheter föreskrivna i GDPR vid profilering och automatiserat beslutsfattande ur ett integritetsperspektiv

JURM02 Examensarbete

Examensarbete på juristprogrammet
30 högskolepoäng

Handledare: David Dryselius

Termin för examen: Period 1 HT2020

Innehåll

SUMMARY	1
SAMMANFATTNING	3
FÖRORD	5
FÖRKORTNINGAR	6
1 INLEDNING	7
1.1 Bakgrund	7
1.2 Syfte och frågeställningar	9
1.3 Metod, material och forskningsläge	9
1.4 Avgränsningar	14
1.5 Disposition	16
2 ARTIFICIELL INTELLIGENS	17
2.1 Definition av artificiell intelligens	17
2.2 Algoritmer och data	18
2.2.1 Algoritm	18
2.2.2 Big data	19
2.3 Maskininlärning	20
2.4 Artificiell intelligens i vår vardag	21
2.5 Reglering av artificiell intelligens	22
3 PERSONLIG INTEGRITET I INFORMATIONSSAMHÄLLET	25
3.1 Personlig integritet	25
3.2 Grundläggande skyddet för den personliga integriteten	27
3.2.1 Europakonventionen	27
3.2.2 Rättighetsstadgan	28
3.2.3 Regeringsformen	28
3.2.4 Dataskyddsförordningen	29
3.3 Företeelser med allvarlig risk för den personliga integriteten	30

4	PROFILERING OCH AUTOMATISERAT BESLUTSFATTANDE	32
4.1	Profilering	33
4.1.1	Den artificiella intelligensens roll vid profilering	34
4.1.2	Profileringsprocessen	34
4.1.3	Risker och problem	36
4.1.4	Regleringen av profilering i GDPR	40
4.1.4.1	Skyddet av personuppgifter	41
4.1.4.2	Särskilda rättigheter för den enskilde	43
4.1.4.2.1	Rätt till klar och tydlig information	45
4.1.4.2.2	Rätt till rättelse och radering	48
4.1.4.2.3	Rätt att göra invändningar	48
4.2	Automatiserat beslutsfattande	50
4.2.1	Förbud mot automatiserat beslutsfattande	50
4.2.1.1	Beslut utan mänsklig inblandning	51
4.2.1.2	Rättsliga följder eller betydande påverkan	52
4.2.2	Undantag från förbudet	53
4.2.3	Särskilda rättigheter för den enskilde	54
4.2.4	Datautvinning eller algoritmiskt beslutsfattande?	56
5	TEKNIK MÖTER JURIDIK	58
5.1	Problem och utmaningar	58
5.1.1	Algoritmisk bristande transparens	61
5.1.2	Ingripande datainsamling och framställning av personuppgifter	65
5.2	Lösningförslag på problemen	67
5.2.1	Rättsliga verktyg	68
5.2.2	Tekniska verktyg	71
5.2.3	EU-strategin	72
6	DISKUSSION OCH AVSLUTANDE REFLEKTIONER	75
6.1	En faktisk medvetenhet...	76
6.2	... och en praktisk möjlig tillämpning...	78
6.3	... förutsätter men garanterar inte efterlevnaden av enskildas rättigheter föreskrivna i GDPR	81
6.4	Avslutande reflektioner	83
	KÄLL- OCH LITTERATURFÖRTECKNING	85
	RÄTTSFALLSFÖRTECKNING	95

Summary

The technical development in artificial intelligence (AI), machine learning algorithms and data collection has made profiling and automated decision-making possible. Individuals are exposed to AI on a daily basis. Profiling and automated decision-making consist of techniques, including the use of algorithms in order to extract knowledge from large amounts of data.

Profiling is an automated processing of personal data that aims to assess an individual's characteristics, behaviour and personal preferences.

Furthermore, automated decision-making is made by AI systems without human intervention. Automated decision-making can take place with or without profiling.

As a result of profiling and automated decision-making, compliance with the protection of personal integrity in today's digitalised and technology-developed environment is faced with challenges. Problems and consequences seen from an integrity perspective of profiling and automated decision-making are discovered. This essay underlines that lack of algorithmic transparency occurs when AI is involved. Article 12–15 General Data Protection Regulation (GDPR) states that controllers must ensure clear and unambiguous explanations to individuals on how the profiling or automated decision-making process is carried out. Such explanation is impossible when the logic behind the profiling process and the automated decision-making are performed by non-transparent algorithms. The problems of non-transparency are therefore a limited compliance with the regulation in GDPR, which leads to a reduced awareness among individuals about controllers' access to their personal data and their additional rights in the context.

Furthermore, problems arise as a result of intrusive data collection and the creation of new personal data in the profiling process. Extensive personal data collection and processing of data often takes place without the

individual's understanding or knowledge. This occurs on a daily basis when individuals connect to the internet. Without an awareness of the processing of personal data processing, the possibility for individuals to invoke the right to rectification, erasure and restriction provided in Articles 16-18 GDPR is restricted. This issue also risks compliance with individual rights in the GDPR. To summarize, the presented difficulties can lead to invasion of privacy. The right of individuals to self-determination and the right to independently make their own unaffected choices is jeopardized.

The solution to the problems and consequences presented varies. The European Commission has this year presented a strategy on artificial intelligence, which proposes measures and solutions to reduce potential problems resulting from the use of AI. Only time can tell the importance of the European Commission's strategy. However, the strategy emphasizes the importance of the fundamental European values in the future development and use of AI. The protection of the individual, the end consumer of AI applications, is highlighted through the strategy in order to strengthen personal integrity. The solutions have the combination of legal and technical tools in common, both from the European Commission and researchers in the field. Compliance with individuals' rights in AI-controlled profiling and automated decision-making requires practical solutions to actually benefit, especially to strengthen the protection of personal integrity. Solutions such as the integration of individuals' rights and transparency standards into technical systems are practical solution with real benefits.

Sammanfattning

Den tekniska utvecklingen inom artificiell intelligens (AI), maskininlärda algoritmer och datainsamling har möjliggjort den profilerings och det automatiserade beslutsfattandet enskilda dagligen exponeras för. Profilerings och automatiserat beslutsfattande består av en uppsättning tekniker, inklusive användning av algoritmer i syfte att utvinna kunskaper ur stora datamängder. Profilerings är en automatiserad personuppgiftsbehandling som avser att framkalla information om en enskild persons egenskaper, beteende och personliga preferenser. Vidare är automatiserat beslutsfattande beslut som fattas av AI-system utan mänsklig inblandning. Automatiserat beslutsfattande kan ske med eller utan profilerings.

Som ett resultat av profilerings och automatiserat beslutsfattande ställs efterlevnaden av skyddet för den personliga integriteten i samtidens digitaliserade och teknikutvecklade miljö inför utmaningar. Problem och konsekvenser sett ur ett integritetsperspektiv vid profilerings och automatiserat beslutsfattande uppdagas. Redogörelsen visar att bristande algoritmisk transparens uppstår när AI involveras. De algoritmer som används och dess arbetsgång ska enligt dataskyddsförordningen (GDPR) kunna framställas begripligt för den enskilde i enlighet med informationskravet i artiklarna 12–15 GDPR. Detta är inte möjligt när logiken och förklaringen bakom profileringsprocessen och det automatiserade beslutsfattande utförs av icke-transparenta algoritmer. Problemen av bristande algoritmisk transparens är således en begränsad möjlig efterlevnad av informationskravet, vilket sedermera leder till en minskad medvetenhet hos enskilda om hanteringen av deras personuppgifter samt deras ytterligare rättigheter i sammanhanget.

Vidare uppstår problem till följd av ingripande datainsamling och profileringsprocessens skapande av nya personuppgifter. En omfattande personuppgiftsinsamling och bearbetning av data sker inte sällan utan

enskilde individens förståelse eller vetskap. Detta inträffar exempelvis dagligen vid enskildas uppkoppling till internet. Utan en medvetenhet av personuppgiftshanteringens existens begränsas enskildas möjlighet att åberopa rätten till rättelse, radering och begränsning som föreskrivs i artiklarna 16–18 GDPR. Även denna problematik riskerar efterlevnaden av enskildas rättigheter i GDPR. Sammantaget kan de presenterade problemen verka integritetskränkande för enskilda individen. Enskildas självbestämmanderätt äventyras samt rätten att självständigt företa egna opåverkade val i livet undermineras.

Lösningen på de problem och konsekvenser som presenteras varierar. EU-kommissionen har i år utarbetat en strategi om AI, vilken föreslår åtgärder och lösningar för att minska potentiella problem till följd av AI-användningen. Betydelsen av EU-strategin får framtiden utvisa. Det som strategin framhäver är däremot vikten av att värna och upprätthålla de grundläggande europeiska värdena vid den framtida utvecklingen och användningen av AI. Skyddet för den enskilda individen, slutkonsumenten av AI-applikationer, framhävs genom strategins åtgärdsförslag i syfte att stärka den personliga integriteten. Gemensamt för lösningsåtgärderna från både EU-kommissionen och forskare inom området är en kombination av rättsliga och tekniska verktyg. Efterlevnaden av enskildas rättigheter vid AI utförd profilering och automatiserat beslutsfattande kräver praktiska lösningar för att få faktiskt nytta, särskilt för att stärka skyddet för den personliga integriteten. Lösningar likt integrering av enskildas rättigheter och transparensnormer i tekniska system är en sådan praktisk lösning med faktiskt nytta.

Förord

Med de sista orden som juriststudent i Lund vill jag rikta ett stort tack till min handledare David Dryselius för goda synpunkter under arbetets gång. Vidare vill jag tacka Lund och allt lundatiden erbjudit som gett mig vänner för livet och oförglömliga minnen. Slutligen ett stort varmt tack till min familj och mina vänner för värdefullt stöd genom hela juristutbildningen.

Lina Persson

Lund, januari 2021

Förkortningar

AI	Artificiell intelligens
Artikel 29-gruppen	Article 29 Working Party
EKMR	Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna
EU	Europeiska unionen
EU-strategin	Vitbok om artificiell intelligens - en EU-strategi för spetskompetens och förtroende
FEUF	Fördraget om Europeiska unionens funktionssätt
GDPR	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
Prop.	Proposition
RF	Regeringsformen (1974:152)
Rättighetsstadgan	Europeiska unionens stadga om de grundläggande rättigheterna
SOU	Statens offentliga utredningar
SvJT	Svensk Juristtidning

1 Inledning

1.1 Bakgrund

Har du sökt efter arbetsannonser på internet? Sökt efter recept till kvällens middag? Eller efter sommarens semesterresa? Utan att du bett om det rekommenderar hemsidor lediga tjänster, maträtter och resmål en tid framöver. Baserat på dina sökningar lär företag känna dig och får reda på information om dina livsmål, rädslor och intressen. Förklaringen är profilering med artificiell intelligens (AI).¹

AI kan beskrivas som en samling tekniker som förenar data och algoritmer.² Den ökande tillgången av stora datamängder i kombination med AI möjliggör profilering och automatiserat beslutsfattande, vilket är uppsatsens fokus.³ Profilering är en automatiserad personuppgiftsbehandling som resulterar i mer eller mindre tillförlitliga förutsägelser och bedömningar om en enskild individs egenskaper och framtida beteende.⁴ Profilering möjliggör individspecifiserade rekommendationer likt exemplen ovan.⁵ Vidare kan profilering verka som beslutsunderlag för ett automatiserat beslutfattande, det vill säga ett beslut skapat utan mänsklig inblandning.⁶

Regleringen vid användning av AI omfattas delvis av befintlig EU-lagstiftning som verkar till skydd för de grundläggande fri- och rättigheterna, främst skydd av personuppgifter och personlig integritet. Men hur väl tillämpningen och efterlevnaden av lagstiftningen fungerar när AI används är kontroversiellt. Den grundläggande rättigheten till personlig

¹ Kommissionens meddelande 'Artificiell intelligens för Europa' (2018) s. 1; Benoist 'Collecting Data for the Profiling of Web Users' (2008) s. 170 ff.

² Se vidare förklaring i kapitel 2.

³ Hildebrandt 'Defining Profiling: A New Type of Knowledge?' (2008) s. 17 f.; Haider och Sundin 'Algoritmer: Så påverkar de din vardag' (2016) s. 12.

⁴ Artikel 4.4 GDPR; Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 6 f.

⁵ Frydinger m.fl. (2018) s. 183.

⁶ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 8.

integritet är en av de mest berörda frågorna till följd av digitaliseringen.⁷ Inte sällan kopplas denna diskussion till profilering och automatiserat beslutsfattande.⁸ För att tillvarata digitaliseringens möjligheter och potentialen med AI samt hantera dess risker har EU-kommissionen utarbetat en övergripande digital strategi, en vitbok med namnet *Om artificiell intelligens – En EU-strategi för spetskompetens och förtroende* (EU-strategin).

Den befintliga dataskyddslagstiftningen (GDPR) stadgar att en individ har rätt att inte bli utsatt för ett beslut som enbart utgörs av en automatiserad personuppgiftsbehandling, inklusive profilering, om beslutet har rättsliga följder eller påverkar den enskilde i betydande grad.⁹ Vidare föreskriver GDPR en rätt för enskilda till information och insyn. Dessa rättigheter föreligger både vid profilering och vid automatiserad behandling av personuppgifter som genererar ett beslut.¹⁰ Rättigheterna vid användandet av personuppgifter för profilering och automatiserat beslutsfattande är kontroversiella. Diskussioner, kritik och frågor uppkommer när ämnet berörs. Vilken förklaring och förståelse för den automatiserade beslutsprocessen ska individen ha rätt till när beslut bygger på individens profilering? Äventyras efterlevnaden av GDPR:s bestämmelser när mänsklig kraft ersätts med teknisk komplex AI? Är GDPR utformad med en övertro på individernas förståelse för vad de går med på?¹¹

Digitaliseringen och utvecklingen av autonoma teknologier skapar nya möjligheter, men väcker också nya problem.¹² I takt med en ökad användning av AI växer behovet av förståelse för de negativa

⁷ Vitbok om artificiell intelligens (2020) s. 11 f.

⁸ Hildebrandt 'Defining Profiling: A New Type of Knowledge?' (2008) s. 29 f.

⁹ Artikel 22.1 GDPR.

¹⁰ Artiklarna 13.2 f och 14.2 g GDPR.

¹¹ Larsson 'Artificiell intelligens som normativ samhällsutmaning: partiskhet, ansvar och transparens' (2019) s. 363; Larsson m.fl. 'HÅLLBAR AI: Inventering av kunskapsläget för etiska, sociala och rättsliga utmaningar med artificiell intelligens' (2019) s. 23; Wachter m.fl. 'Why a right to explanation of automated decision-making does not exist in the general data protection regulation' (2017) s. 76 ff.

¹² Vitbok om artificiell intelligens (2020) s. 1 och 11 f.

konsekvenserna med AI samt vilka rättsliga och etiska ramverk, principer eller komplement som behövs.¹³ Det är således viktigt att undersöka de juridiska aspekterna av profilering och automatiserat beslutsfattande när AI ersätter den mänskliga kraften.

1.2 Syfte och frågeställningar

Syftet med uppsatsen är att ur ett integritetsperspektiv granska om GDPR:s reglering av profilering och automatiserat beslutsfattande är ändamålsenlig till skydd för enskilda individen med beaktande av AI:s påverkan samt vilka problem som riskerar uppkomma till följd av detta.

För att uppnå uppsatsens syfte avser avhandlingen att besvara följande frågeställningar:

1. Vilka risker och problem uppstår när profilering och automatiserat beslutsfattande utförs av AI?
2. Kan dataskyddslagstiftningen hantera riskerna och problemen eller krävs det kompletterande lösningar och, om jakande svar – vilka? Vad betyder EU-strategin i sammanhanget?
3. Hur påverkar de belysta riskerna och problemen efterlevnaden av enskildas integritetsskyddande rättigheter i GDPR?

1.3 Metod, material och forskningsläge

Uppsatsens redogörelse av gällande rätt genomförs med en traditionell rättsdogmatisk metod samt en EU-rättslig metod. Den rättsdogmatiska metoden används för att analysera, utvärdera eller rekonstruera en rättsregel utifrån tolkning och tillämpning av de allmänt accepterade rättskällorna.¹⁴

¹³ Larsson 'Artificiell intelligens som normativ samhällsutmaning: partiskhet, ansvar och transparens' (2019) s. 340.

¹⁴ Kleineman 'Rättsdogmatisk metod' (2018) s. 21.

Beskrivningen av den rättsdogmatiska metoden bygger emellertid på en förenklad bild av vilket material som tillhör kategorin rättskälla. Det föreligger delade om vilka källor som räknas som rättskällor i svensk rätt. Dahlman, professor och forskare inom juridik, menar att en rättskälla är en källa som innehar en rättslig status grundad på en regel i befintlig rättsordning.¹⁵ En enhetlig uppfattning föreligger om att lagar, lagförarbeten och rättspraxis är rättskällor.¹⁶ Sverige är medlem i EU varpå EU-rättens rättskällor inkluderas i de svenska rättskällorna. EU-rättens rättskällor innefattar EU-fördraget, EU-förordningar, EU-direktiv samt praxis från EU-domstolen.¹⁷

Men det finns också källor vars status är oklara och omdiskuterade, däribland den rättsvetenskapliga doktrinen.¹⁸ Dahlman menar att rättsvetenskaplig doktrin i regel inte är en rättskälla.¹⁹ I motsats till Dahlman menar Kleineman, professor i civilrätt, att den rättsdogmatiskt orienterade litteraturen tillhör de allmänt accepterade rättskällorna.²⁰ Den rättsdogmatiska metoden innebär vissa ställningstaganden, eftersom delade meningar av metodens innebörd föreligger. Jag finner en betydelse i Dahlmans ställningstagande men har valt att vid sidan om lagstiftningen, lagförarbetena och praxis söka svaren i den rättsvetenskapliga litteraturen inom ramen för den rättsdogmatiska metodens syfte: att ta reda på innehållet i gällande rätt. Den doktrin som används för att fastställa gällande rätt är främst forskning av Frydinger, Edvardsson, Olstedt Carlström och Beyer som upptas i boken *GDPR: juridik, organisation och säkerhet enligt dataskyddsförordningen* samt verket *Dataskyddsförordningen (GDPR) m.m.: en kommentar* av Öman, som bl.a. medverkat i Datalagskommittén, Integritetsutredningen och i arbetet av personuppgiftslagen.²¹

¹⁵ Dahlman 'Begreppet rättskälla' (2019) s. 61.

¹⁶ Dahlman 'Begreppet rättskälla' (2019) s. 57; Kleineman 'Rättsdogmatisk metod' (2018) s. 21.

¹⁷ Dahlman 'Begreppet rättskälla' (2019) s. 70.

¹⁸ Dahlman 'Begreppet rättskälla' (2019) s. 59.

¹⁹ Dahlman 'Begreppet rättskälla' (2019) s. 70 f.

²⁰ Kleineman 'Rättsdogmatisk metod' (2018) s. 21.

²¹ Öman, *Dataskyddsförordningen en kommentar* (uppdaterad 29 februari 2020, JUNO) se under rubrik "Författarpresentation".

Den rättsdogmatiska metoden riskerar emellertid att begränsa den fria argumentationen, varför jag valt att inte uteslutande använda den. Jareborg, professor inom straffrätt, menar dock att den rättsdogmatiska metoden inte hindrar ett vidgat perspektiv bortom gällande rätt. Det är enligt Jareborg legitimt för rättsdogmatiken att finna ideala och bättre lösningar utanför gällande rätt och bortom de accepterade rättskällorna.²² Även Sandgren, professor är civilrätt, har en bredare syn på vad den rättsdogmatiska metoden innebär. Han menar att rättsvetenskapen accepterar en mer fri argumentation, i vilken rättskällevärdet kan förenas med värderingar, forskning och extern specialkunskap.²³

I uppsatsen har jag använt den rättsdogmatiska metoden vid fastställande av gällande rätt och analysen av rättsreglerna hänförliga till profilering och automatiserat beslutsfattande. De nämnda rättsreglerna återfinns företrädesvis i EU-rättslig lagstiftning, mer specifikt i GDPR, varför en EU-rättslig metod även använts för att tolka lagens terminologi i enlighet med den EU-rättsliga betydelsen.²⁴

Den EU-rättsliga metodens särskiljande drag är den stora betydelse som tillskrivs EU-domstolens praxis, särskilt vad gäller förståelsen för de grundläggande rättigheterna och tolkning av de materiella EU-rättsliga reglerna.²⁵ Inte sällan tar EU-domstolen lagstiftarens uppgift och blir det pådrivande organet för utvecklingen av EU-lagstiftningen.²⁶

Dataskyddsförordningen är från 2018, vilket gör att praxis från EU-domstolen är begränsad. Det material som använts för att tolka GDPR:s innehåll är främst doktrin, förordningens beaktandesatser och material från EU-organ. Beaktandesatser, s.k. skäl, följer EU-rättslig lagstiftning enligt

²² Jareborg 'Rättsdogmatik som vetenskap' (2004) s. 4.

²³ Sandgren 'Är rättsdogmatiken dogmatisk?' (2005) s. 651 f.

²⁴ Hettne och Otken Eriksson (2011) s. 21; Reichel (2018) s. 109 ff.

²⁵ Reichel 'EU-rättslig metod' (2018) s. 115.

²⁶ Reichel 'EU-rättslig metod' (2018) s. 115 och s. 131.

artikel 296 i Fördraget om Europeiska unionens funktionssätt (FEUF). Artikel 296 FEUF föreskriver en motiveringsskyldighet, vilket betyder en skyldighet att ange skäl till varför den EU-rättsligt bindande rättsakten utarbetats. Skälen är enbart en formföreskrift men kan ge vägledning för hur efterföljande artiklar ska tolkas.²⁷

Material från EU-organ klassas som *soft law* och består av icke-bindande dokument vilka innehåller riktlinjer, förklaringar och tolkningar av unionens rättsregler. Trots dess icke-bindande karaktär har dokumenten en normerande och betydelsefull verkan.²⁸ I uppsatsen använder jag främst dokument utarbetade av Article 29 Working Party (Artikel 29-gruppen) som bestod av företrädare för EU-kommissionen och representanter för EU-medlemsstaternas tillsynsmyndigheter. Artikel 29-gruppen ersattes av den Europeiska dataskyddsstyrelsen när GDPR trädde i kraft. Europeiska dataskyddsstyrelsen har accepterat riktlinjerna som utarbetats av Artikel 29-gruppen.²⁹

Framställningens redogörelse för innehållet i gällande rätt *de lege lata* leder i sin tur till en diskussion *de lege ferenda*. Detta görs genom att en kritisk rättsdogmatisk undersökning präglar diskussionen. Den kritiskt rättsdogmatiska metoden innebär att jag upptar en från gällande rätt fristående och mer långtgående argumentation för att påvisa ett otillfredsställande rättsläge som bör förändras. Uppsatsen innehåller lösningsförslag på de brister som framkommit i uppsatsens undersökande del. Komplettering i form av en kritisk rättsdogmatisk metod, till den mer traditionella rättsdogmatiken, resulterar i att uppsatsens diskussion anlägger mer än en beskrivning av gällande rätt.³⁰ Det material som uppdragar problemen är statistik från EU-kommissionen och EU-kommissionens vitbok om AI. Vitböcker har på senare tid givits en starkare ställning bland

²⁷ Hettne och Otken Eriksson (2011) s. 85 och s. 93 f.

²⁸ Reichel 'EU-rättslig metod' (2018) s. 127 f.

²⁹ Öman, *Dataskyddsförordningen en kommentar* (uppdaterad 29 februari 2020, JUNO) se under rubrik "EU-rättsligt källmaterial".

³⁰ Kleineman 'Rättsdogmatisk metod' (2018) s. 40.

EU:s rättskällor.³¹ Vidare är det material som möjliggör argumentationen och föreslår lösningar dokument utarbetade i Microsofts regi av framstående personer inom området, EU-strategin samt i tvärvetenskapligt material som presenteras nedan.

Framställningen syftar till att undersöka interaktionen mellan teknik och juridik, varför tvärdisciplinär forskning använts för att möjliggöra uppfyllandet av uppsatsens syfte. Tvärvetenskapligt angreppssätt har använts för att finna lösningar om hur gällande rättsregler bör efterlevas på ett förnuftigt och samhällsfrämjande vis.³² Gräns, professor i rättsvetenskap, menar att lösningsförslag uppkomma ur forskning inom enbart ett slutet rättssystem vid undersökning genom den traditionella rättsdogmatiska metoden sällan är tillräckliga. Undersökning och problemlösning av rätten som ett från samhället oberoende system riskerar irrationella konsekvenser sett ur andra perspektiv.³³ Gräns menar således att rättsdogmatisk forskning gynnas av ett tvärvetenskapligt angreppssätt. Rätten avser att verka för samhällets fördel, varför en tvärvetenskaplig metod främjar juridikens kontakt med den verklighet som den i detta fall avser att verka i: det digitaliserade och teknikpräglade samhället.³⁴

Mängden material som finns att tillgå är relativt begränsat med anledning av att ämnet är förhållandevis nytt. Det material som framställningen baseras på är främst internationellt och tvärvetenskapligt. Juridisk och datorvetenskaplig forskning av Hildebrandt och Gutwirth som resulterat i antologin *Profiling the European Citizen: Cross-Disciplinary Perspectives* är särskilt betydelsefull. Hildebrandt och Gutwirth upptar juridisk reglering av profilering och automatiserat beslutsfattande i en datorvetenskaplig forskning som framställs ur i ett samhälleligt perspektiv. Burrells artikel *How the machine 'thinks': Understanding opacity in machine learning algorithms* samt Pasquales litteratur *The Black Box Society – The secret*

³¹ Reichel 'EU-rättslig metod' (2018) s. 128.

³² Gräns 'Allmänt om användningen av andra vetenskaper inom juridiken' (2018) s. 438.

³³ Gräns 'Allmänt om användningen av andra vetenskaper inom juridiken' (2018) s. 437.

³⁴ Gräns 'Allmänt om användningen av andra vetenskaper inom juridiken' (2018) s. 438.

Algorithms That Control Money and Information har bl.a. använts vid uppsatsens utredning av den transparensproblematik som föreligger i samband med användning av AI. Svenskt material som jag använt är främst utredningar av Larsson. Larsson är jurist, docent i teknik och social förändring samt forskare inom transparensfrågor kring tillämpad AI. Hans publikation om *Artificiell intelligens som normativ samhällsutmaning: partiskhet, ansvar och transparens* är av betydelse för uppsatsens diskussion.

I uppsatsen anlägger jag ett integritetsperspektiv i syfte att framställningens hållning och diskussion ska genomsyras av de grundläggande värdena om rätten till personlig integritet. Det material som integritetsperspektivet bygger på är enskilda individens grundläggande fri- och rättigheter med fokus på de rättsregler som skyddar den personliga integriteten. Vidare är material likt antologin *Integritet* av Almqvist och Linder samt Integritetskommitténs betänkande *Hur står det till med den personliga integriteten?* (SOU 2016:41) betydelsefullt när rätten till integritet diskuteras i kontexten av nutidens digitaliserade informationssamhälle. Integritetskommittén har uttalat att det saknas forskning om digitaliseringens påverkan på den personliga integriteten. Kommittén uppmärksammade att forskning bör företas för att höja kunskapsnivån i syfte att finna lösningar på tekniska och legala utmaningar.³⁵

1.4 Avgränsningar

Uppsatsens uppställda frågeställningar och det anlagda integritetsperspektivet definierar uppsatsens omfång. För att avgränsa uppsatsen i enlighet med integritetsperspektivet har urvalet av relevanta artiklar gjorts med fokus på enskildas rättigheter, vilka återfinns i kapitel III GDPR. Framställningen berör således inte den personuppgiftsansvarige och personuppgiftsbiträdets allmänna skyldigheter samt deras skyldighet att

³⁵ SOU 2017:52 s. 26.

företa konsekvensbedömningar, som regleras i kapitel IV GDPR. Avgränsningen inkluderar konsekvensbedömningen i artikel 35 GDPR, vilken i och för sig skulle kunna tillföra en relevant aspekt för ämnet, särskilt vid diskussion av algoritmisk transparens men som inte är nödvändigt för besvarandet av uppsatsens frågeställningar.

Vidare upptas laglighetsgrunderna i artikel 6 GDPR endast översiktligt. Samtycke som laglighetsgrund i artikel 6.1 a stärker enskildas självbestämmanderätt samt utgör skydd för enskildas integritet.³⁶ Värdet som skapas av samtyckesbestämmelsen faller inom ramen för uppsatsen och förekommer i framställningen, särskilt vid diskussion om enskilda individens självbestämmanderätt. Däremot sker analys av lagregelns utformning endast i den mån det är relevant för uppsatsen, en djupgående undersökning lämnas således utanför utredningen.

Framställningen är en rättsutredning, varför jag endast kommer göra en översiktlig datavetenskaplig undersökning av AI. Förklaringar av tekniska metoder och system vid profilering och automatiserat beslutsfattande är således begränsade. Framställningen anlägger ett integritetsperspektiv varför profileringen som åsyftas fokuserar på individuell profilering och utelämnar gruppprofilering. Den datorvetenskapliga forskningen upptar återkommande risken för samhälls- eller grupp-bias i autonoma och algoritmiska system, vilket kan få diskriminerande konsekvenser.³⁷ Med hänsyn till fokus på den personliga integriteten och konsekvenser i form av bristande transparens utelämnas diskrimineringsdiskursen i denna utredning.

³⁶ Frydinger m.fl. (2018) s. 35 f.

³⁷ Se bl.a. Mittelstadt m.fl. 'The ethics of algorithms: Mapping the debate' (2016) och Burrell 'How the machine 'thinks': Understanding opacity in machine learning algorithms' (2016).

1.5 Disposition

Uppsatsen är indelad i sex kapitel, där denna inledning utgör det första. Kapitel två redogör grundläggande för den teknik som är väsentlig för profilering och automatiserat beslutsfattande. AI och datainsamling beskrivs, dess praktiska betydelse framhävs och en önskad reglering av AI belyses.

Kapitel tre ger stöd åt uppsatsens integritetsperspektiv. Begreppet personlig integritet utreds och en redogörelse av det lagstadgade grundläggande skyddet och bakomliggande skyddsintresset för den personliga integriteten belyses.

Kapitel fyra undersöker profilering och automatiserat beslutsfattande utifrån regleringen i GDPR och AI:s roll i sammanhanget. Redogörelsen belyser riskerna och konsekvenserna hänförliga till profilering och automatiserat beslutsfattande, vilket till viss del bevarar uppsatsens första frågeställning. I enlighet med integritetsperspektivet undersöks främst enskildas rättigheter i GDPR vid profilering och automatiserat beslutsfattande. Diskussion om möjligheten att efterleva dessa integritetsskyddande rättigheter upptas i sammanhanget, vilket delvis besvarar uppsatsens tredje frågeställning.

Kapitel fem undersöker mötet mellan teknik och juridik. Problem och utmaningar kopplade till profilering och automatiserat beslutsfattande med involvering av AI belyses. Lösnings- och åtgärdsförslag av framstående personer inom området presenteras, inkluderat EU-strategin. Genomgående diskuteras efterlevnaden av enskildes integritetsskyddande rättigheter. I kapitel fem besvaras således samtliga av uppsatsens frågeställningar utifrån forskning och utifrån diskussion mot bakgrund av vad redogörelsen utrett.

Avslutande kapitel sex knyter ihop uppsatsen genom djupare diskussioner och avslutande reflektioner av uppsatsens grundläggande syfte och frågeställningar utifrån det valda integritetsperspektivet.

2 Artificiell intelligens

AI är ett område inom datorvetenskapen där målet är att utveckla datorprogram eller robotar som efterliknar mänsklig intelligens. Syftet med AI är att efterlikna de kognitiva funktionerna av människans hjärna som förmågan att lära sig av erfarenheter, förstå naturligt språk, lösa problem utifrån varierade omständigheter samt tänka och resonera självständigt.³⁸ AI med mänskligt tänkande benämns som *artificiell generell intelligens* och är en hypotetisk och outvecklad variant av AI. Framställningen avser inte att undersöka framtidens mål utan undersökningen kommer utgå från nutida varianter av AI.³⁹

I litteraturen och forskningen används AI som ett paraplybegrepp för forskningsområden, vilka gemensamt handlar om datorsystem som uppvisar ett intelligent beteende. Maskininlärning, djupinlärning, naturlig språkinlärning, röstigenkänning, neutrala nätverk och robotik är alla fält inom AI.⁴⁰ I detta kapitel följer en redovisning av den teknik som möjliggör och utför profilering och automatiserat beslutsfattande.

2.1 Definition av artificiell intelligens

Det finns ingen vedertagen definition av AI och begreppet har kritiserats för att vara en svag akronym.⁴¹ EU-kommissionen påtalar vikten av att definiera AI på ett flexibelt och anpassningsbart sätt med tanke på den teknologiska utvecklingen men samtidigt definiera AI tillräckligt precist för att upprätthålla rättssäkerheten.⁴² Mot bakgrund av detta anför EU-

³⁸ Turban, Aronson och Ting-Peng (2005) s. 540 f.

³⁹ Larsson 'Artificiell intelligens som normativ samhällsutmaning: partiskhet, ansvar och transparens' (2019) s. 340; Lundqvist 'Artificiell Intelligens – rättsordning och rättstillämpning' (2020) s. 384 och fotnot 7.

⁴⁰ Larsson 'Artificiell intelligens som normativ samhällsutmaning: partiskhet, ansvar och transparens' (2019) s. 340.

⁴¹ Jordan 'Artificial Intelligence – The Revolution Hasn't Happened yet' (2019) s. 5.

⁴² Vitbok om artificiell intelligens (2020) s. 18.

kommissionen en välavvägd definition som även uppsatsen avser att utgå ifrån. EU-kommissionens definition av begreppet AI är följande:

”Artificiell intelligens avser system som uppvisar intelligent beteende genom att analysera sin miljö och vidta åtgärder – med viss grad av självständighet – för att uppnå särskilda mål. AI-baserade system kan vara helt programvarubaserade och fungera i den virtuella världen (till exempel röstassistenter, bildanalysprogram, sökmotorer, tal- och ansiktigenkänningssystem), eller inbäddas i maskinvaruenheter (till exempel avancerade robotar, självkörande bilar, drönare eller tillämpningar för sakernas internet).”⁴³

2.2 Algoritmer och data

De främsta beståndsdelarna i AI är *algoritmer* och *data*.⁴⁴ Algoritmer är ingen ny företeelse utan har funnits och haft betydelse även i den analoga världen men i dagens informationssamhälle med ett digitalt överflöd av data har algoritmer fått en explosionsartad betydelse. Data är materialet som algoritmer tekniskt behandlar.⁴⁵

2.2.1 Algoritm

En algoritm innehåller systematiska, otvetydiga och precisa instruktioner på programspråk som avser att lösa en uppgift. En algoritm får utgångspunkter genom indata, vilket är värden som tillförs algoritmen. Algoritmen hanterar indata utifrån givna instruktioner och genererar i sin tur utdata, vilket är värden som producerats av algoritmen och som ofta benämns resultatet.⁴⁶

⁴³ Kommissionens meddelande 'Artificiell intelligens för Europa' (2018) s. 1 f.; Vitbok om artificiell intelligens (2020) s. 18 och fotnot 46.

⁴⁴ Vitbok om artificiell intelligens (2020) s. 2 och s. 18.

⁴⁵ Haider och Sundin 'Algoritmer: Så påverkar de din vardag' (2016) s. 4 och s. 12.

⁴⁶ Janlert (2015) s. 89.

Arbetsprocessen hos algoritmen förutsätter ingen förståelse av data eller konsekvensbedömning av resultatet.⁴⁷ Inte sällan liknas en algoritm med ett matlagingsrecept. Ett recept utgörs av instruktioner som steg för steg beskriver hur ingredienserna ska föras samman och hanteras för att det ska resultera i en middag. Receptet, likaså algoritmen, är instruktioner vilka är valda för att uppnå ett önskat resultat.⁴⁸

En sökning med en sökmotor resulterar i regel i hundratusentals träffar. När vi söker efter lediga arbetstjänster, semesterresor eller middagsrecept är det algoritmer som styr träffarna – träffarna som vi sedermera bearbetar och agerar utefter. Mänsklig hantering av all data är i princip omöjlig i dagens digitaliserade miljö, varför algoritmer som sorterar och prioriterar data har blivit viktigare i takt med digitaliseringen. Sorteringen och prioriteringen av data och information resulterar i att nätverkstjänster skapar rangordning av webbsidor och rekommenderar den enskilde om exempelvis kvällens middagsrecept.⁴⁹

2.2.2 Big data

Data behövs för att algoritmer ska kunna applicera sina instruktioner och generera ett resultat. Vår värld har utvecklats till att bestå av mängder av digitala redskap, exempelvis datorer och smarttelefoner. Ur digitala redskap skapas data som framställs i olika former – bild, ljud och text. *Big data* är ett felaktigt definierat begrepp om vi endast talar om data i stora volymer. Big data består dels av stora digitalt lagrade datamängder, dels av tekniker för att extrahera information gömd inuti den lagrade data. Big data är således olika system som brukar och sammanställer stora mängder data till begriplig information.⁵⁰

⁴⁷ Seipel (2004) s. 42 f.

⁴⁸ Haider och Sundin 'Algoritmer: Så påverkar de din vardag' (2016) s. 6.

⁴⁹ Haider och Sundin 'Algoritmer: Så påverkar de din vardag' (2016) s. 7.

⁵⁰ Mohanty 'Big Data: An Introduction' (2015) s. 1 ff.

Det är viktigt att skilja mellan begreppen *data* och *information*. Liebenau och Backhouse definierar data som symbolisk företrädare som avser att representera människor, objekt, händelser och begrepp. Information är istället resultatet av modellering, formatering, organisering eller konvertering av data på ett vis som ökar förståelsen för mottagaren. Information är således data ordnad och sorterad på ett meningsfullt sätt.⁵¹

2.3 Maskininlärning

Maskininlärning, ett delområde inom AI, är en metod som syftar till att utveckla datorsystem till att *lära*. Även om maskininlärning funnits länge har dess betydelse ökat sen digitaliseringen möjliggjort hantering av stora mängder datamaterial.⁵² Maskininlärningsmetoder kan förbättra mjukvara genom att utifrån en stor mängd data träna algoritmer att uppnå ett planerat mål. Maskininlärningsalgoritmer kan upptäcka mönster och lära sig att göra förutsägelser genom att bearbeta data och upplevelser snarare än att handla efter uttryckliga programmeringsinstruktioner. Algoritmer kan lära sig under tiden de används och förbättra sin effektivitet över tid i takt med att algoritmen lagrar data. Genom maskininlärning kan AI-system självständigt registrera sin omgivning och yttre miljö och agera därefter. Det ska dock framhållas att även om systemen kan uppfatta sin omgivning självständigt, är det människan som begränsar systemet och programmerar målen som maskininlärda AI-system avser att utföra.⁵³

Maskininlärning har vidare bidragit till s.k. *djupinlärning*. Djupinlärning är en typ av maskininlärning som bearbetar en större mängd data och kräver mindre mänsklig programmering. Resultaten som uppkommer via

⁵¹ Liebenau och Backhouse (1990) s. 2; Canhoto och Backhouse 'General Description of the Process of Behavioural Profiling' (2008) s. 48.

⁵² Franklin 'History, motivations, and core themes' (2014) s. 26 ff.

⁵³ Vitbok om artificiell intelligens (2020) s. 18; McKinsey Analytics 'An executive's guide to AI' (2018) s. 1.

djupinlärningsmetoder är ofta mer precisa resultat än via traditionella maskininlärningsmetoder.⁵⁴

Självkörande bilar, medicinsk diagnostik, personliga produktrekommendationer och prisjusteringar i realtid för internetkunder är exempel på områden där maskininläring och djupinläring används.⁵⁵ Av intresse för denna uppsats är den maskininläring som används för profilering och automatiserat beslutsfattande.⁵⁶

2.4 Artificiell intelligens i vår vardag

De senaste framstegen inom AI har uppkommit genom att maskininläring har tillämpats på stora processade datamängder, Big data.⁵⁷ Framstegen har vidare resulterat i den profilering och det automatiserade beslutsfattandet vi medvetet eller omedvetet dagligen kommer i kontakt med.⁵⁸

AI utgör en del av vår vardag. När vi exempelvis översätter språk på nätet, använder sökmotorer på internet, blockerar skräppost i mejlen, köper internetrekommenderade produkter eller lyssnar på låtar våra telefoner rekommenderat använder vi AI-lösningar.⁵⁹ Vidare skapar vi användargenererad data, vilket är digitala spår som vi enskilda användare efterlämnar vid exempelvis användning av nätets sökmotorer.⁶⁰ Vår förmåga att överblicka och kontrollera hur data som är användargenererad hanteras och sprids vidare är liten. Det kan till synes verka som inte allt för problematiskt för den enskilde, åtminstone inte vid varje enskilt tillfälle. Det problematiska uppstår när stora mängder data från olika källor sammanställs

⁵⁴ McKinsey Analytics 'An executive's guide to AI' (2018) s. 6.

⁵⁵ Alpaydin (2020) s. 4 ff.; Vitbok om artificiell intelligens (2020) s. 18.

⁵⁶ Hildebrandt 'Defining Profiling: A New Type of Knowledge?' (2008) s. 17 f.

⁵⁷ Franklin 'History, motivations, and core themes' (2014) s. 26 ff.

⁵⁸ Hildebrandt 'Defining Profiling: A New Type of Knowledge?' (2008) s. 17 f.

⁵⁹ Kommissionens meddelande 'Artificiell intelligens för Europa' (2018) s. 1 f.

⁶⁰ Haider och Sundin 'Algoritmer: Så påverkar de din vardag' (2016) s. 12; Mohanty 'Big Data: An Introduction' (2015) s. 5.

med AI och bildar individspecifiserade mönster och samband av den enskilde.⁶¹

Konsekvenserna av AI är både positiva och negativa. AI är en utveckling som genererar positiva resultat för enskilda, företag och samhället i stort. Företagen effektiviserar sina organisationer genom att automatisera verksamhetsområden med hjälp av AI. Vidare hjälper AI oss att behandla och fastställa sjukdomar, minska dödligheten vid trafikolyckor och bekämpa klimatförändringar.⁶² Dock riskerar AI också att medföra nackdelar i form av integritetsintrång hos enskilda, minskat skydd av personuppgifter, förstärkande av samhällelig bias och ökad informationsasymmetri mellan enskilda och datainnehavare.⁶³

Rättsliga utmaningar följer i takt med att AI alltmer används och integreras i vår vardag. Beslut som tidigare var fattat enbart av mänsklig kraft genereras nu genom algoritmiskt beslutsfattande. Vidare kvarstår skyddet av enskildas grundläggande fri- och rättigheter oavsett hur beslutet tillkommit.⁶⁴

Förhållandet mellan rätten och AI, mer specifikt hur lagstadgade bestämmelser kring profilering och automatiserat beslutsfattande samspelar med den tekniska utvecklingen, avser de kommande kapitlen undersöka.

Dessförinnan följer en kort redogörelse av reglering av AI.

2.5 Reglering av artificiell intelligens

”Sverige behöver utveckla regler, standarder, normer och etiska principer i syfte att vägleda etisk och hållbar AI och användning av AI.”⁶⁵ Det föreskrev regeringen 2018 i artikeln *Nationell inriktning för artificiell*

⁶¹ Haider och Sundin 'Algoritmer: Så påverkar de din vardag' (2016) s. 14 f.

⁶² Kommissionens meddelande 'Artificiell intelligens för Europa' (2018) s. 1 f.; Larsson 'Artificiell intelligens som normativ samhällsutmaning: partiskhet, ansvar och transparens' (2019) s. 339 ff.

⁶³ Vitbok om artificiell intelligens (2020) s. 11 f.; Larsson 'Artificiell intelligens som normativ samhällsutmaning: partiskhet, ansvar och transparens' (2019) s. 342.

⁶⁴ Vitbok om artificiell intelligens (2020) s. 12.

⁶⁵ Regeringskansliet 'Nationell inriktning för artificiell intelligens' (2018) s. 10.

intelligens. Regeringen menar att utvecklingen av AI behöver vägledas med ändamålsenliga ramverk för att infria nyttan med AI. Ramverken ska balansera grundläggande behov av integritetsskydd, tillit, samhällsskydd samt möjliggöra tillgång till data och tillvarata potentialen med AI.⁶⁶

EU-kommissionen har konstaterat att EU behöver, för att stärka sin globala konkurrenskraft och tillvarata teknologiskiftet, agera efter en solid EU-strategi.⁶⁷ Den data-agila ekonomin kommer förändra och påverka hela världen. För en framgångsrik och ledande digital omställning krävs riktlinjer och ramar för att garantera en tillförlitlig teknik. Det krävs vidare att företagen innehar kunskap och har möjligheten att tillgå de rätta verktygen för att digitalisera.⁶⁸ Med anledning av detta utarbetade EU-kommissionen en AI-strategi, som betonar vikten av att EU och dess medlemsländer främjar utvecklingen av AI och hanterar medföljande utmaningarna i ljuset av de grundläggande europeiska värderingarna.⁶⁹

EU-strategin presenterar tanken av ett framtida AI-regelverk. Ett regelverk som avser att skapa en gemensam europeisk ram i syfte att öka enskilda individers förtroende.⁷⁰ Regelverket ska verka för att minimera riskerna med AI, särskilt de risker som äventyrar de grundläggande rättigheterna och enskildas skydd för den personliga integriteten.⁷¹ EU-kommissionen betonar vidare vikten av en effektiv kontroll av efterlevnad av befintlig EU-lagstiftning och nationell lagstiftning. AI:s viktigaste egenskaper riskerar nämligen en korrekt tillämpning den befintliga lagstiftningen. Det kan således vara nödvändigt att anpassa eller förtydliga den befintliga lagstiftningen för att inte hamna efter framtidens användning av AI eller riskera att inskränka den personliga integriteten längs vägen.⁷² Med denna insikt avser kommande redogörelse att undersöka och kontrollera

⁶⁶ Regeringskansliet 'Nationell inriktning för artificiell intelligens' (2018) s. 10.

⁶⁷ Bakardjieva Engelbrekt, Michalski, Oxelheim (2020) s. 7.

⁶⁸ Kommissionens meddelande 'Att forma EU:s digitala framtid' (2020) s. 15.

⁶⁹ Vitbok om artificiell intelligens (2020) s. 1 och s. 10; Bakardjieva Engelbrekt, Michalski, Oxelheim (2020) s. 7 f.

⁷⁰ Vitbok om artificiell intelligens (2020) s. 10

⁷¹ Vitbok om artificiell intelligens (2020) s. 12 och s. 15

⁷² Vitbok om artificiell intelligens (2020) s. 15.

efterlevnaden av GDPR, särskilt de rättigheter som skyddar den personliga integriteten. I linje med detta följer dessförinnan en utblick över den personliga integriteten i informationssamhället.

3 Personlig integritet i informationsamhället

Vad betyder det för den personliga integriteten när allt som kan digitaliseras också digitaliseras och när situationer där AI kan användas också förefaller att just användas?⁷³

Allt större mängd av information om enskilda individer lagras. Informationen samkörs och analyseras genom tekniskt effektiva metoder. Den personliga integriteten riskeras att inskränkas när staten utövar övervakning eller när företag följer våra konsumtionsbeteenden. Till detta kommer vår egen roll i sammanhanget där vi frivilligt lägger ut våra privatliv på sociala medier och bidrar till att bli synliggjorda på nätet. Frågan är om vi avskaffar den personliga integriteten och suddar ut gränsen mellan privatliv och offentlighet på egen hand. Oavsett om vi vill det lämnar vi digitala spår efter oss.⁷⁴ Det är svårt för enskilda att nyttja nätet utan att generera data åt olika tjänster.⁷⁵ Riskerna påvisar att det finns anledning att belysa personlig integritet i samtidens digitaliserade samhälle, vilket följande avsnitt avser att undersöka.

3.1 Personlig integritet

Vad enskilda betraktar som integritetskränkande varierar över tid, präglas av samtiden och utgörs av en subjektiv känsla. Tidigare Justitiekanslern Skarhed anför som ett exempel på detta ett överklagande av Länsstyrelsens beslut om kameraövervakning på Stortorget i Malmö. Beslutet överklagades till Högsta förvaltningsdomstolen med grunden att kameraövervakningen utgjorde integritetsintrång för den enskilda individen. Högsta domstolen

⁷³ Gröning 'Inledning' (2014) s. 7 f.

⁷⁴ Gröning 'Inledning' (2014) s. 7 f.

⁷⁵ Haider och Sundin 'Algoritmer: Så påverkar de din vardag' (2016) s. 15.

förbjöd kameraövervakning på torget. Fallet upprörde och uppmärksammades i media. Skarhed noterade att enskilda individer inte var upprörda på grund av att de var övervakande utan tvärt om, att det inte var tillåtet att bli övervakade. Exemplet illustrerar hur tiderna och samhället förändrar vad som anses integritetskränkande.⁷⁶ Hur samtidens informationssamhälle påverkar synen på enskildas integritet har undersökts av Integritetskommittén, vilket presenteras nedan.

Regeringen tillsatte 2016 Integritetskommittén med uppdrag att utifrån enskildas perspektiv utreda och analysera den personliga integriteten vid ökad användning av informationsteknik. Kartläggningen utmynnade i delbetänkandet *Hur står det till med den personliga integriteten?* (SOU 2016:41). Regeringen framhöll i en tidigare utredning att det inte föreligger en vedertagen accepterad definition av begreppet *personlig integritet*.⁷⁷ Integritetskommittén ansåg att det likt tidigare utredningar inte är meningsfullt att precis definiera och avgränsa begreppet. Kommittén argumenterade för att en legitim definition inte är möjlig med anledning av att rätten till en personlig sfär inte är absolut. Rätten till en personlig sfär varierar över tid och är beroende av situationen. Kommittén har i sin beskrivning av begreppet utgått från att enskilda har rätt till privata tankar och kommunikation med andra. Vidare har kommittén tagit hänsyn till att enskilda har rätt att bestämma vilken personlig information som ska tilldelas vem och hur informationen får användas i olika sammanhang, särskilt vid digital informationsinsamling.⁷⁸

I överensstämmelse med förarbeten utelämnas en precis definition av begreppet personlig integritet med fördel i denna uppsats. Framställningen samstämmer istället med Integritetskommitténs beskrivning av den personliga integriteten.

⁷⁶ Skarhed 'JK och den personliga integriteten' (2014) s. 10 f.

⁷⁷ Prop. 2009/10:80 s. 175.

⁷⁸ SOU 2016:41 s. 39 f.

3.2 Grundläggande skyddet för den personliga integriteten

Rätten till personlig integritet skyddas i ett antal svenska lagar, konventioner och EU-direktiv. Följande framställning berör de mest relevanta regleringarna till skydd för den personliga integriteten.

3.2.1 Europakonventionen

Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR) stadgar i artikel 8 att ”Var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens”. Bestämmelsen föreskriver skyddet för den personliga integriteten och har av Europadomstolen getts en vid tolkning. Skyddet omfattar information om den enskilda, enskildas personliga utveckling och individers relationer till andra enskilda.⁷⁹

Europadomstolens praxis visar att staten har en negativ och positiv förpliktelse vad gäller upprätthållandet av skyddet. Den negativa förpliktelsen är att staten ska avstå från att göra intrång i enskildas privat- och familjeliv medan den positiva förpliktelsen innebär att staten ska skydda enskilda från integritetsintrång från andra enskilda.⁸⁰ Den svenska regeringen ansåg att Sveriges trovärdighet, som en fördragsslutande part, skulle öka om skyddet för den personliga integriteten grundlagsfästes i svensk rätt. Detta resulterade i den nuvarande lydelsen av 2 kap. 6 § 2 st. regeringsformen (RF).⁸¹

Sverige är vad gäller personuppgiftsskydd folkrättsligt bunden av Europarådets dataskyddskonvention om skydd för enskilda vid automatisk

⁷⁹ SOU 2016:41 s. 151 f

⁸⁰ SOU 2016:41 s. 152; Se t.ex. Airey mot Irland, X och Y mot Nederländerna och Eliza Söderman mot Sverige.

⁸¹ Prop. 2009/10:80 s. 176.

databehandling av personuppgifter, CETS nr 108. Bestämmelserna i dataskyddskonventionen utvecklar och värnar om det grundläggande skyddet för den personliga integriteten som stadgas i artikel 8 EKMR.⁸²

3.2.2 Rättighetsstadgan

År 2000 presenterade EU den Europeiska unionens stadga om de grundläggande rättigheterna (rättighetsstadgan). Rättighetsstadgan föreskriver skydd för den personliga integriteten i ett antal artiklar. Artikel 3 stadgar att var och en har rätt till fysisk och mental integritet. Enligt artikel 7 har enskilda rätt till respekt för sitt privatliv och enligt artikel 8 gäller en rätt till skydd av personuppgifter om den enskilde. Uppgifterna ska hanteras lagenligt, för bestämda ändamål och efter den enskildes samtycke. Den enskilde innehar också rätt att få tillgång och rättelse av de insamlade uppgifterna. Rättighetsstadgan återspeglar medlemsstaternas synsätt avseende de grundläggande fri- och rättigheterna och skyddet av den personliga integriteten genom syftar bestämmelserna i stadgan.⁸³

3.2.3 Regeringsformen

2 kap. 6 § 2 st. RF stadgar följande:

”[...] är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.”

Bestämmelsen infördes i RF genom 2010 års grundlagsändringar.

Grundlagsutredningen betonade vikten av ett stärkt skydd för enskilda mot

⁸² Förslag till Rådets beslut om skydd för enskilda vid automatisk databehandling av personuppgifter (2018) s. 1; Jermsten *Regeringsformen, kommentar till 2 kap. 6 §* (uppdaterad 1 januari 2019, JUNO) se under rubrik 3.1.

⁸³ SOU 2016:41 s. 152; Se artiklarna 3, 7 och 8 rättighetsstadgan.

intrång i fri- och rättigheterna från det allmännas sida.⁸⁴ Regeringen framhöll i utredningen att enskildas självbestämmanderätt är grundläggande i en demokrati och bör på grundlagsnivå stärkas. Respekten till individers rätt att bestämma det allmännas tillgång till personlig information framhölls genom lagändringen.⁸⁵ Integritetskommittén framlagda förslag om stärkt skydd för den personliga integriteten resulterade i 2 kap. 6 § 2 st. RF.⁸⁶ Regeringen instämde med kommittén om att syftet bakom integritetsskyddet bör vara att skydda information om enskildas personliga förhållanden.⁸⁷

Bestämmelsen 2 kap. 6 § 2 st. RF tillämpas inte vid åtgärder som enskild företar mot annan enskild, utan enbart när åtgärder vidtas av det allmänna.⁸⁸ Det innebär dock inte att bestämmelsen är betydelselös i ett sådant sammanhang. Att skyddet för den personliga integriteten grundlagförts visar ett betydande värde, oberoende av omständigheterna i en specifik händelse.⁸⁹

3.2.4 Dataskyddsförordningen

GDPR är den centrala regleringen inom EU vad gäller dataskydd. Efter flera års förhandlingar mellan EU:s medlemsstater antogs GDPR i april 2016 och började tillämpas i maj 2018. I samband med det upphävdes EU:s dataskyddsdirektiv (95/46/EG), den svenska implementeringen av dataskyddsdirektivet som var personuppgiftslagen (1998:204) och EU:s personuppgiftsförordning (1998:1191).⁹⁰ GDPR syftar till att ”skydda

⁸⁴ Prop. 2009/10:80 s. 1; Isberg och Eliason *Grundlagarna* (uppdaterad 1 januari 2019, JUNO) se under rubrik ”2 kap. Grundläggande fri- och rättigheter”, avsnitt ”Regleringens huvuddrag”.

⁸⁵ Prop. 2009/10:80 s. 176.

⁸⁶ Isberg och Eliason *Grundlagarna* (uppdaterad 1 januari 2019, JUNO) se under rubrik ”2 kap. Grundläggande fri- och rättigheter”, avsnitt ”Regleringens huvuddrag”.

⁸⁷ Prop. 2009/10:80 s. 177.

⁸⁸ Prop. 2009/10:80 s. 250.

⁸⁹ Prop. 2009/10:80 s. 176 ff.; Isberg och Eliason *Grundlagarna* (uppdaterad 1 januari 2019, JUNO) se under rubrik ”2 kap. Grundläggande fri- och rättigheter”, avsnitt ”regleringens huvuddrag”.

⁹⁰ Öman, *Dataskyddsförordningen en kommentar* (uppdaterad 29 februari 2020, JUNO) se under rubrik ”Inledning”, avsnitt ”Kort historik”.

enskildas grundläggande fri- och rättigheter, särskilt deras rätt till skydd av personuppgifter”.⁹¹ GDPR stadgar vidare bestämmelser om det fria flödet av personuppgifter inom Europeiska unionen.⁹²

Ursprunget till reglering av dataskydd inom Europa är att dataskydd betraktas som en mänsklig rättighet. Ur Europadomstolens praxis kan det exempelvis utläsas att artikel 8 EKMR varit tillämplig vid behandling av personuppgifter.⁹³ Skäl 1 GDPR stadgar även att enskildas skydd vid behandling av deras personuppgifter är en sådan grundläggande rättighet som följer av artikel 8 rättighetsstadgan.

Sammantaget stadgar de grundläggande rättigheterna i regleringarna ovan skydd för den personliga integriteten. Med skydd för den personliga integriteten menas särskilt skydd av information om enskildas personliga förhållanden och respekt för privatliv. Vidare har praxis visat att de grundläggande rättigheterna till skydd för den personliga integriteten har tillämpats vid personuppgiftsbehandling. Det är intressant för den kommande redogörelsen att vara medveten om det fundamentala skyddet för den personliga integriteten, vilket även råder vid personuppgiftsbehandling.

3.3 Företeelser med allvarlig risk för den personliga integriteten

Integritetskommittén presenterade i sin utredning faktiska och potentiella integritetsrisker som vi utsätts för av modern teknik. Kommittén uttalade att vårt moderna informationssamhälle medför en oöverskådlig förståelse för hur våra uppgifter hanteras och sprids. Ur ett individperspektiv presenterade kommittén företeelser som är kopplade till risker för den personliga

⁹¹ Artikel 1.2 GDPR.

⁹² Artiklarna 1.1 och 1.3 GDPR.

⁹³ Öman, *Dataskyddsförordningen en kommentar* (uppdaterad 29 februari 2020, JUNO) se under rubrik ”Inledning”, avsnitt ”Kort historik”.

integriteten och klassificerade dessa utifrån tre nivåer: viss risk, påtaglig risk och allvarlig risk.⁹⁴

Integritetskommitténs undersökning visar att allvarliga risker för personlig integritetskränkning utgörs av en större informationsinsamling om enskilda. Kommittén listade företeelser som utgör allvarlig risk för den personliga integriteten. I listan exemplifieras företeelser på konsumentområdet och Big data.⁹⁵ Företeelser på konsumentområdet åsyftar främst datainsamling om våra konsumtionsbeteenden. Denna insamling används främst till profilering, individanpassad marknadsföring och individanpassade sökresultat (skapandet av s.k. filterbubblor).⁹⁶

Integritetskommittén sammanfattar sin uppfattning av den personliga integritetens ställning i den digitaliserade miljön enligt följande. Antalet aktörer som använder personuppgifter ökar, likaså ökar användningsområdet för de insamlade personuppgifterna. Myndigheter och företag har genom personuppgiftsinsamling möjlighet att skapa en alltmer fullständig profil av en enskild person. I takt med ökad teknisk informationshantering minskar möjligheten för enskilda att överblicka och begränsa aktörers användning av deras personliga information. Som ett resultat av detta menar Integritetskommittén att enskilda successivt utsätts för försämringar av den personliga integriteten.⁹⁷

För uppsatsens del är det intressant hur GDPR hanterar dessa problem. Funderingar uppkommer kring om GDPR kan hantera digitaliseringen och stärka skyddet för den personliga integriteten eller om den tekniska utvecklingen försvårar efterlevnaden av regelverket. Detta avser de kommande kapitlen att undersöka.

⁹⁴ SOU 2016:41 s. 27 f., s. 135 och s. 148.

⁹⁵ SOU 2016:41 s. 30 f. och s. 86.

⁹⁶ SOU 2016:41 s. 62 och s. 86.

⁹⁷ SOU 2016:41 s. 33.

4 Profilering och automatiserat beslutsfattande

Som framgått ovan är en betydande del av skyddet för den personliga integriteten i dagens digitaliserade värld skyddet av enskildas personuppgifter. Profilering och automatiserat beslutsfattande behandlar och processar enskildas personuppgifter. Detta har expanderat inom ett flertal sektorer. Bank- och finanssektorn, hälso- och sjukvården, marknadsföring- och reklambranschen använder exempelvis profilering som verktyg för bl.a. individanpassade rekommendationer och automatiserat beslutsfattande.⁹⁸

Den tekniska utvecklingen som möjliggjort hantering av stora datamängder samt expansionen av AI som underlättat skapandet av profiler och automatiserade beslut medför både för- och nackdelar. Hanteringen av personuppgifter sker till största del genom mer eller mindre automatiska behandlingar. GDPR innehåller bestämmelser i syfte att hantera de negativa följder som profilering och automatiserat beslutsfattande riskerar orsaka, vilket framförallt är intrång i den personliga integriteten.⁹⁹

Kommande avsnitt redogör för profilering och automatiserat beslutsfattande utifrån regleringen i GDPR med beaktan av AI:s involvering och teknikens påverkan. I anknytning till detta anförs diskussion om efterlevnaden av enskildas integritetsskyddande rättigheter.

⁹⁸ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 5 f.

⁹⁹ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 5 f.

4.1 Profilering

Profilering definieras i artikel 4.4 GDPR enligt följande:

”*profilering*: varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar”

Öman konkretiserar definitionen ovan och menar att profilering kan beskrivas som en automatiserad behandling av personuppgifter som sker i syfte att bedöma en enskild persons egenskaper.¹⁰⁰ Vidare anser Artikel 29-gruppen att följande tre rekvisit måste vara uppfyllda för att det ska anses vara profilering i enlighet med artikel 4.4:

- Det är en *automatisk behandling*
- Behandlingen avser *personuppgifter*¹⁰¹, och
- Syftet med profileringen är att *bedöma den enskilda personens personliga egenskaper*.¹⁰²

Öman menar att det inte är fråga om profilering om processen består av både en automatiserad och icke-automatiserad behandling av personuppgifterna. Han uppmärksammar emellertid att detta har diskuterats av Artikel 29-gruppen i dess utformade riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt GDPR.¹⁰³ Artikel 29-gruppen belyser att artikel 4.4 inte är utformad med skrivelsen ”enbart”¹⁰⁴

¹⁰⁰ Öman, *Dataskyddsförordningen en kommentar* (uppdaterad 29 februari 2020, JUNO) kommentaren till 4.4 GDPR.

¹⁰¹ Se definition och förklaring av *personuppgifter* i avsnitt 4.1.4.1.

¹⁰² Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 6 f.

¹⁰³ Öman, *Dataskyddsförordningen en kommentar* (uppdaterad 29 februari 2020, JUNO) kommentaren till 4.4 GDPR.

¹⁰⁴ Jmf artikel 22 GDPR.

automatiserad behandling utan med orden ”varje form av automatisk behandling”. Utifrån det menar Artikel 29-gruppen att profilering måste omfatta automatiserad behandling men att mänsklig inblandning inte med nödvändighet innebär att profilering i lagens mening är uteslutet.¹⁰⁵

4.1.1 Den artificiella intelligensens roll vid profilering

Hildebrandt och Gutwirth menar att profileringens bakomliggande teknik innefattande AI är en av de viktigaste teknikerna för att skapa ordning i oredan som uppstår på grund av all data som produceras.¹⁰⁶

Profilering sker i en mängd olika sammanhang. Hildebrandt uttalar att sammanhangens gemensamma nämnare är att termen profilering refererar till en uppsättning tekniker som oftast delar en gemensam egenskap, vilket är *användningen av algoritmer för att utvinna kunskap ur stora datamängder*.¹⁰⁷

4.1.2 Profileringsprocessen

Profilering kan delas in i tre steg. Första steget är insamling av data. Andra steget är automatiserad analys av denna data för att upptäcka korrelationer. Tredje steget är applicering av dessa korrelationer på en enskild person, i syfte att möjliggöra förutsägelser och bedöma den enskildas egenskaper och framtida beteende.¹⁰⁸

Automatiserad profilering är resultatet av ”data mining” som på svenska kallas datautvinning.¹⁰⁹ Det som sker vid datautvinning är att stora

¹⁰⁵ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 7.

¹⁰⁶ Hildebrandt och Gutwirth ’General Introduction and Overview’ (2008) s. 1.

¹⁰⁷ Hildebrandt ’Defining Profiling: A New Type of Knowledge?’ (2008) s. 17.

¹⁰⁸ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 7.

¹⁰⁹ Definition från Nationalencyklopedin ’data mining’.

datamängder bryts ner med algoritmer i syfte att hitta samband mellan data. Verktygen för processen utgörs av beräkningseffektiva algoritmer inom maskininlärning, vilka är skapade inom ramen för artificiell intelligens. De korrelationer som genererats vid datautvinningen representerar sannolikheter för liknande utfall i framtiden. Profileringen anger inte grunder eller orsaker till korrelationerna, utan resulterar enbart i mer eller mindre tillförlitliga förutsägelser baserat på tidigare information. Förutsägelser avser slutligen att användas som bedömnings- eller beslutsunderlag gentemot enskilda individer.¹¹⁰

Algoritmer utgör kärnan i den automatiserade profileringsprocessen och har två viktiga roller för datautvinning. För det första kan algoritmer kontrollera profileringsprocessen och på så vis avgöra hur profileringen sker. För det andra kan algoritmer genom matematiska processer identifiera trender, relationer och preferenser ur datamängden. Utveckling och användning av allt mer avancerade algoritmer resulterar också i att profileringsprocessen kan skapa effektivare profiler än vad enbart mänsklig kraft kan framställa.¹¹¹

För att belysa profilering ur ett otekniskt och mer lättbegripligt vis kan profilering förklaras genom ett icke-automatiserat förfarande: mänskligt tänkande. Profilering kan beskrivas som en form av kategorisering, vilket alla människor rutinmässigt använder. Vi lever efter vår egen, omgivningens och samhällets generaliseringar och givna stereotyper utan att reflektera över det. Vi gör förutsägelser om situationer och andra människor baserat på fördomar, vilka är skapade av bland annat våra erfarenheter. Hur denna icke-automatiserade profilering uppkommer, med andra ord hur processen i människans hjärna skapar förutsägelser baserat på tidigare erfarenheter och fördomar är mycket svårt att förklara.¹¹² Den tanken av profileringsprocessen är intressant att ha i åtanke när problematiken kring profilering och automatiserat beslutsfattande vidare diskuteras.

¹¹⁰ Hildebrandt 'Defining Profiling: A New Type of Knowledge?' (2008) s. 18.

¹¹¹ Anrig, Browne och Gasson 'The Role of Algorithms in Profiling' (2008) s. 65.

¹¹² Hildebrandt 'Defining Profiling: A New Type of Knowledge?' (2008) s. 24.

4.1.3 Risker och problem

Profilering innebär att utifrån personlig information om en enskild bedöma dennes egenskaper, intressen eller beteendemönster i syfte att placera individen i en kategori. Genom att kategorisera enskilda individer möjliggörs bedömningar och förutsägelser om en person.¹¹³

Profilering och automatiserat beslutsfattande skapar en rad fördelar. Framförallt är det ett resurssparande och effektivt tillvägagångsätt för organisationer och företag. Som nämnts ovan används profileringsprocessen inom många kommersiella områden. Skräddarsydda personliga rekommendationer och erbjudande är exempel på resultat av profileringsprocessen. Dessa utgör effektiva medel för reklam- och marknadsföringsbranschen. Banker och försäkringsbolag drar även nytta av profileringens fördelar genom att resurseffektivt fatta automatiserade beslut avseende den registrerades möjlighet till lån och försäkringspremier. Vidare nyttjar utbildnings-, hälso- och sjukvårdssektorerna fördelarna med profilering. Fördelarna som uppkommer genom profilering och automatiserat beslutsfattande följer dock inte utan nackdelar och risker.¹¹⁴

Genom profilering och automatiserat beslutsfattande riskeras enskildas fri- och rättigheter att inskränkas, särskilt rätten till personlig integritet. Konsekvenserna varierar givetvis men profileringens kategorisering av enskilda individer riskerar att diskriminera, bevara stereotyper, leda till social segregation samt begränsa personen i fråga till information som är baserad på dennes preferenser. Processerna kan vara ogenomsådliga, leda till felaktiga förutsägelser och enskilda riskeras att profileras utan deras vetskap eller förståelse.¹¹⁵ Av intresse i sammanhanget är särskilt

¹¹³ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 7.

¹¹⁴ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 5; Frydinger m.fl. (2018) s. 183.

¹¹⁵ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 5 f.

konsekvenserna av personalisering och riktade rekommendationer, vilket genereras av profilering och automatiserat beslutsfattande.

En variant av profilering är s.k. *personalisering*. Personalisering är personlig profilering på individnivå som används av företag och organisationer för att individanpassa och skräddarsy deras tjänster, produkter eller webbsidor. Den utvecklade informations- och kommunikationstekniken har möjliggjort personalisering av tjänster, vilket särskilt implementeras inom e-handeln.¹¹⁶ Personalisering resulterar främst i individualiserad marknadsföring samt personliga tjänst- och produktrekommendationer.¹¹⁷

Personalisering utgörs av en komplex informationsteknik styrd av *ambient intelligens*. Ambient intelligens är ett tillstånd när informationstekniken integreras i vår vardagliga miljö och skapar en miljö i realtid som reagerar på och anpassar sig till närvaron av personer. Det sker exempelvis när en internethemsida anpassar sig efter mottagarens preferenser för att på så sätt individualisera tjänsten efter användaren. För att möjliggöra fulländade nätverkstjänster som reagerar efter en miljö skapas personalisering dels på information om den specifika mottagaren, dels på information från tredje part om mottagaren och andra användare. Informationen från tredje part kan utgöras av demografiska data, statistiska profiler och användarinformation från andra företag. Användbar information inom personalisering omfattar mer än enbart profilering utifrån en enskild individs personuppgifter. Värdet av personuppgifterna uppkommer när de analyseras i sin kontext och tillsammans med övrig information och data. Personalisering kan anses gå utöver den profilering som framställning ovan tagit upp. Vid personalisering

¹¹⁶ Hildebrandt 'Defining Profiling: A New Type of Knowledge?' (2008) s. 23 f.; van der Hof och Prins 'Personalisation and its Influence on Identities, Behaviour and Social Values' (2008) s. 111 ff.

¹¹⁷ van der Hof och Prins 'Personalisation and its Influence on Identities, Behaviour and Social Values' (2008) s. 113 ff.

blir informationen om en användare således mer fullständig och avslöjande än vad den hade blivit om informationen analyserats fristående.¹¹⁸

Konsekvenserna av personalisering är relaterade till profileringens risker. Skydd för den personliga integriteten och skyddet av personuppgifter är den främsta utmaningen med personalisering och profileringprocessen. Företag och organisationer utnyttjar informationstekniken och använder personalisering som ett kraftfullt instrument. Företag kan utläsa vem en individ är, vad den behöver samt dess framtida handlingsmönster. Vidare kan företag konstruera ”identiteter” baserat på personens klassificering och beteendemönster. Personalisering resulterar sedermera i att personen ifråga erbjuds rekommendationer och individanpassade förslag, vilka är baserat på dennes klassificering och givna ”identitet”.¹¹⁹

Studier har visat att de flesta individer inte uppfattar att de blir föremål för personalisering eller åtminstone inte förstår tekniken bakom processen, vilket riskerar att enskildas grundläggande rättigheter inte åberopas.¹²⁰ Rekommendationer som ges en internetanvändare är nogga utvalda utifrån mottagarens preferenser och information från och om tredje part. En människas rätt till frihet innefattande att utan påtryckning göra egna val i livet, exempelvis självständigt välja produkter, tjänster och nyheter, riskerar att undergrävas på grund av personalisering. Vidare ges enskilda inte samma möjlighet att lära och skapa nya beteenden, vilket uppkommer genom hantering av oförutsedda och nya situationer, när individer endast matas med utvald och ”anpassad” information.¹²¹

¹¹⁸ van der Hof och Prins 'Personalisation and its Influence on Identities, Behaviour and Social Values' (2008) s. 111 ff.; Hildebrandt 'Defining Profiling: A New Type of Knowledge?' (2008) s. 23.

¹¹⁹ van der Hof och Prins 'Personalisation and its Influence on Identities, Behaviour and Social Values' (2008) s. 113 ff.

¹²⁰ van der Hof och Prins 'Personalisation and its Influence on Identities, Behaviour and Social Values' (2008) s. 115 f.

¹²¹ van der Hof och Prins 'Personalisation and its Influence on Identities, Behaviour and Social Values' (2008) s. 121 och s. 126; Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 5 f.

En ytterligare konsekvens av profilering, särskilt personalisering, är transparens och kontroll av processen. Profileringsprocessen och bakomliggande algoritmer är privatägda och huruvida de fullt ut är föremål för allmänhetens granskning kan diskuteras. Vid företagets användning av personalisering förekommer det dolda instrument för att spåra och upptäcka information om deras användare. En negativ konsekvens av detta är att användarna inte alltid är medvetna om att deras information samlas in och sammanställs till personliga profiler.¹²²

Ett känt exempel från år 2012 är när matvarukedjan Target i USA drog den konkreta slutsatsen att en tonårskvinna var gravid baserat på hennes köpbeteende. Targets profilering utgjordes av AI som baserades på algoritmer och stora mängder data. Data innefattande personuppgifter om kvinnan samt data om Targets resterande kunder och deras konsumtionsbeteende. AI-systemet undersökte de ändrade köpvanorna som kvinnan uppvisade och jämförde det med hennes tidigare köpbeteende samt ändrade köpvanor hos övriga kunder. Resultatet, att förutspå hennes framtida behov, möjliggjorde Targets personliga produktrekommendationer. Kvinnan bodde hemma varpå hennes pappa fick syn på reklamen och ställde sig frågande. Profileringen upplevdes med stor sannolikhet integritetskränkande för kvinnan. Target är inte det enda företaget som använder enskildas personliga information för att profilera sina existerande och potentiella kunder.¹²³

Sammantaget riskerar profilering, särskilt personalisering, att styra och kontrollera tillgången av den information som tillkommer medborgarna i samhället. Genom att personalisering av tjänster minimerar och styr människans fria val, delvis utan individen förståelse, äventyras enskildas grundläggande fri- och rättigheter.

¹²² van der Hof och Prins 'Personalisation and its Influence on Identities, Behaviour and Social Values' (2008) s. 116 f.

¹²³ Duhigg 'How Companies Learn Your Secrets' (uppdaterad 16 februari 2012); SOU 2016:41 s. 351.

4.1.4 Regleringen av profilering i GDPR

Informationstekniken har de senaste årtiondena utvecklats i en rasande takt och inget tyder på att den kommer att minska i framtiden. Frydinger m.fl. menar behandling av stora mängder personuppgifter är nästa steg i utvecklingen, vilket medför fördelar och risker. Risk för intrång i enskildas integritet vid behandling av personuppgifter och risk för att enskilda därför inte tillåter att deras personuppgifter behandlas. GDPR utarbetades med dessa risker i åtanke. GDPR avser att främja den datadrivna ekonomin genom att skapa tillit hos enskilda vid behandlingen av deras personuppgifter.¹²⁴ Två grundläggande syften i regelverket som båda uttrycks i artikel 1 GDPR är dels att *skydda fysiska personer med avseende på behandlingen av personuppgifter*, dels möjliggöra *det fria flödet av personuppgifter inom unionen*.

Skäl 1 GDPR hänvisar till det som Frydinger m.fl. menar utgör kärnan i regelverket, vilket är den grundläggande rättigheten till skydd av personuppgifter som anges i artikel 8.1 rättighetsstadgan. Vidare anger skäl 4 en viktig norm, nämligen att behandlingen av personuppgifter ”bör utformas så att den tjänar människor”. Skäl 4 skyddar individens integritet vid behandling av deras personuppgifter.¹²⁵ Men skäl 4 anger också att:

”rätten till skydd av personuppgifter inte är absolut; den måste förstås utifrån sin uppgift i samhället och vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen.”.

Frydinger m.fl. påtalar att det är viktigt att förstå, tolka och tillämpa GDPR:s artiklar i enlighet med grundsatsen i skäl 4. De menar att lagreglerna i GDPR oftast endast blir begripliga om de läses i ljuset av skäl 4. Vid svåra tillämpningssituationer måste myndigheter och domstolar

¹²⁴ Frydinger m.fl. (2018) s. 15 ff.

¹²⁵ Frydinger m.fl. (2018) s. 29 f.

beakta skäl 4 och eftersträva en lämplig avvägningen i enlighet med proportionalitetsprincipen.¹²⁶

Utöver dessa grundläggande värden genomsyras GDPR av fundamentala principer vilka gäller för all behandling av personuppgifter. Nedan redogörs de relevanta principerna för profilering och automatiserat beslutsfattande.

4.1.4.1 Skyddet av personuppgifter

Definitionen av profilering i artikel 4.4 GDPR föreskriver att profilering ska innefatta behandling av *personuppgifter*. Definitionen av personuppgifter lyder enligt artikel 4.1 GDPR följande:

”*personuppgifter*: 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 till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringssuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet”

Tillämpningen av GDPR är avhängigt att behandlingen avser data som innehåller personuppgifter. Data som inte innehåller personuppgifter faller därför utanför GDPR:s tillämpningsområde. Däremot är definitionen av personuppgifter bred och inkluderar en mängd upplysningar som kan kopplas till en identifierbar fysisk person. En e-postadress innehållande namn och företagsspecificering är till exempel en personuppgift. Vidare kan data utgörande personuppgifter exempelvis vara namn, personnummer, adress, ljudklipp m.m. Personuppgiftsdefinitionen omfattar även indirekta

¹²⁶ Frydinger m.fl. (2018) s. 30 ff.; Jmf. C-131/12 Google Spain mot AEPD och Mario Costeja González.

uppgifter som kräver att upplysningen kombineras med andra uppgifter för att möjliggöra identifiering av en person.¹²⁷

Skäl 30 GDPR anger att fysiska personers närvaro på nätet kan knyta dem till nätidentifierare, genom att personens utrustning lämnar spår i form av exempelvis IP-adresser eller kakor. Dessa spår, i kombination med unika identifierar och kompletterade uppgifter som tas emot av serverna, kan användas för att skapa identiteter och profiler av enskilda fysiska personer.¹²⁸

I fallet *Nowak mot Data Protection Commission* från 2017 uttalar EU-domstolen att ”varje upplysning” i definitionen av personuppgifter ska ges en vidsträckt betydelse. Detta kan innefatta objektiva och subjektiva upplysningar i form av bedömningar, förutsatt att upplysningarna kan knytas till en enskild identifierbar person.¹²⁹ Målet *Nowak mot Data Protection Commission* bekräftar Artikel 29-gruppens ställningstagande att definitionen av personuppgifter ska ges en vid innebörd och kan utgöras av exempelvis en individs identifierbara personlighet över internet.¹³⁰ Här bör tilläggas att *Nowak mot Data Protection Commission* samt Artikel 29-gruppens uttalande tar sikte på definitionen av personuppgifter i dataskyddsdirektivet (95/46/EG). Men detta saknar betydelse i sammanhanget eftersom personuppgiftsdefinitionen i GDPR och dataskyddsdirektivet 95/46/EG nästintill är identiska. Jag anser därför att de bedömningar, förutsägelser och antaganden om en persons beteende och egenskaper som skapas av profileringsprocesserna utgör personuppgifter även enligt GDPR.

Vad skyddas egentligen genom skyddet av personuppgifter? Litteraturen uppmärksammar att skyddet av personuppgifter är lättförklarligare om GDPR förstås som ett skydd för *mänsklig värdighet*. Artikel 4.1 GDPR

¹²⁷ Frydlinger m.fl. (2018) s. 44 f.

¹²⁸ Skäl 30 GDPR.

¹²⁹ C-434/16 *Peter Nowak mot Data Protection Commission* p. 34.

¹³⁰ Artikel 29-gruppen om begreppet personuppgifter (2007) s. 4 och s. 14.

utger definitionen av personuppgifter, vilken stadgar att personuppgifter är ”varje upplysning som avser en identifierad eller identifierbar fysisk person”.¹³¹

Frydinger m.fl. har kopplat samman ”upplysningar” som stadgas i bestämmelsen och människans värdighet genom följande resonemang. Vad andra vet eller inte vet om en enskild individ påverkar dennes möjligheter att leva ett självständigt liv där individen utformar sina egna tankar, värderingar och mål. Valen och vilka mål den enskilde väljer att eftersträva påverkas av vilken information som myndigheter, företag och allmänheten har om den enskilde. Personlig information som andra förfogar över kan utnyttjas för att begränsa personens möjlighet till självbestämmande. Personuppgifter som används i marknadsföringssyfte kan exempelvis användas som manipulation i syfte att locka konsumtion. Myndigheternas och företagens hantering av personuppgifter kan få avgörande inflytande över en enskild individs livsval.¹³²

Sambandet mellan ”upplysningar” som avser enskild, med andra ord personuppgifter, och människans värdighet är således starka enligt Frydinger m.fl. Det som skyddas genom skyddet av personuppgifter är människans rätt till självbestämmande, rätt till att definiera sin egen identitet och möjligheten att leva efter sin självbild. GDPR avser att skydda uppgifter i nära anknytning till dessa skyddsvärden med anledning av att personuppgifter är känsliga ur ett integritetsperspektiv och lätt kränker enskildas värdighet.¹³³

4.1.4.2 Särskilda rättigheter för den enskilde

De skyddsvärden som tagits upp i de två föregående avsnitten är abstrakta. Vilka värden som företag och myndigheter i deras dagliga hantering av personuppgifter ska efterleva kan emellertid besvaras mer konkret.

¹³¹ Frydinger m.fl. (2018) s. 33.

¹³² Frydinger m.fl. (2018) s. 33 f.

¹³³ Frydinger m.fl. (2018) s. 33 f.

Artikel 5 GDPR föreskriver ett antal konkreta grundläggande principer för behandling av personuppgifter. Skäl 72 förtydligar att profilering omfattas av GDPR:s samtliga bestämmelser avseende behandlingen av personuppgifter, där inkluderat de rättsliga grunderna för behandlingen och förordningens principer. Principerna i artikel 5 är utformade efter lämpliga avvägningar mellan de rättigheter som stadgas i skäl 4 samt att alla principer på olika sätt uttrycker skydd för mänsklig värdighet.¹³⁴

Principen om laglighet, korrekthet och öppenhet som återfinns i artikel 5.1 a är särskilt intressant i förhållande till profilering. *Laglighetsprincipen* innebär att personuppgifter endast får behandlas om det föreligger lagstöd. Lagliga grunder anges främst i artikel 6 och är: samtycke, fullgörande av avtal, fullgörande av rättslig förpliktelse, skyddande av intresse som är av grundläggande betydelse för enskild, utförande av uppgift av allmänt intresse eller myndighetsutövning samt intresseavvägning. Samtycke möjliggör enskildas självbestämmanderätt och styr hur omgivningen ska få påverka individens liv. Frydinger m.fl. menar att samtycke utgör huvudregeln för de lagliga grunderna men påpekar även att det därmed inte behöver utgöra den vanligaste lagliga grunden. Enbart ett samtyckeskrav som laglig grund skulle kunna inskränka andra fri- och rättigheter, varför de resterande fem lagliga grunderna för behandling av personuppgifter existerar. De sex laglighetsgrunderna skapar tillsammans en avvägning mellan olika skyddsintressen av att behandla enskildas personuppgifter.¹³⁵

Principen om korrekthet bör förstås i ljuset av enskildas rätt till självbestämmande. Det kan framstå som missvisande att den svenska översättningen är *korrekthet*, jämfört med den engelska termen *fairness*. Skäl 39 i GDPR anger att behandlingen ska vara rättvis. Principen stadgar att personuppgifter inte får inhämtas genom påtryckningar. Vidare ska den

¹³⁴ Frydinger m.fl. (2018) s. 35 f.

¹³⁵ Frydinger m.fl. (2018) s. 35 f.

enskildes förväntningar beaktas korrekt, bland annat genom att tillse den enskilde informationen om behandlingen av dennes personuppgifter.¹³⁶

Principen om öppenhet eller transparens innebär att den enskilde vars personuppgifter behandlas ska informeras om vilka behandlingar som sker med dennes personuppgifter. Principen uttrycks i ett antal olika artiklar, särskilt i de artiklar som föreskriver ett informationskrav till skydd för den enskilde. Dessa artiklar kommer närmare att behandlas i de kommande avsnitten.¹³⁷

Utöver principen om laglighet, korrekthet och öppenhet återfinns i artikel 5 ytterligare ett antal principer som genomsyrar tillämpningen av artiklarna i GDPR. GDPR stärker de registrerades rättigheter samt ålägger personuppgiftsansvariga skyldigheter.¹³⁸ Personuppgiftsansvarig är den som bestämmer över en viss personuppgiftsbehandling.¹³⁹ Vid profilering kan den registrerade åberopa sina rättigheter mot den personuppgiftsansvarige som framställer profilen och mot den personuppgiftsansvarige som fastställt ett automatiserat beslut om den registrerade, även om det inte är samma person. GDPR ger således den registrerade starkare rättigheter genom att ålägga skyldigheter för den personuppgiftsansvarige.¹⁴⁰

4.1.4.2.1 Rätt till klar och tydlig information

Artikel 12 GDPR föreskriver att vid utövandet av den registrerades rättigheter ska det ske en tydlig information och kommunikation mellan den personuppgiftsansvariga och den registrerade. Artikel 12.1 anger att kommunikationen av all den information som avses i artiklarna 13 och 14

¹³⁶ Frydinger m.fl. (2018) s. 36.

¹³⁷ Frydinger m.fl. (2018) s. 37.

¹³⁸ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 16.

¹³⁹ Se artikel 4.7 GDPR; Frydinger m.fl. (2018) s. 51.

¹⁴⁰ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 16.

samt artiklarna 15–22 ska vara ”koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk”.¹⁴¹

Artikel 12 anger *hur* informationen ska tillhandahållas medan artikel 13 och 14 anger *vilken* information som ska tillhandahållas vid insamling av personuppgifter. Artikel 13 är tillämplig när personuppgifter samlats in från den registrerade medan artikel 14 gäller när informationen erhållits från annan än den registrerade. Gemensamt för dessa är att den personuppgiftsansvarige vid personuppgiftsbehandling ska informera om bland annat sin identitet, kontaktuppgifter, ändamål och rättsliga grunden för behandlingen, mottagare av personuppgifterna, lagringstiden, den registrerades rätt till rättelse, radering och rätten att återkalla ett samtycke.¹⁴²

Personuppgiftsbehandlingar sker ofta i marknadsförings- och försäljningssyfte. Behandlingarna är mer eller mindre omfattande, varav de mer omfattande behandlingarna är profilering. De uppgifter som används vid behandlingen varierar. Det kan röra sig om endast namn och adress medan det även kan handla om stora mängder personuppgifter rörande IP-adresser, köphistorik, sökbeteende på webbsidor m.m. Behandlingen av de sistnämnda personuppgifterna sker ofta genom s.k. cookies eller kakor. Som ett resultat av bl.a. artiklarna 5, 6 och 12–14 GDPR dyker rutan ”genom att klicka i ’godkänn’ accepterar du vårt användande av cookies” upp, något användaren måste godkänna eller neka genom ett knapptryck.¹⁴³

Om behandlingen inbegriper beslutsfattande som grundas på profilering måste den personuppgiftsansvarige förtydliga och informera den registrerade om att behandlingen innefattar både profilering och beslutsfattande grundat på profilen som skapats.¹⁴⁴ Skäl 60 GDPR

¹⁴¹ Artikel 12 GDPR; Öman, *Dataskyddsförordningen en kommentar* (uppdaterad 29 februari 2020, JUNO) kommentaren till artikel 12 GDPR.

¹⁴² Öman, *Dataskyddsförordningen en kommentar* (uppdaterad 29 februari 2020, JUNO) kommentaren till artiklarna 12, 13 och 14 GDPR.

¹⁴³ Frydinger m.fl. (2018) s. 179 f. och fotnot 9.

¹⁴⁴ Artiklarna 13.1 c, 13.2 f, 14.1 c och 14.2 GDPR; Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 17.

föreskriver även att den personuppgiftsansvariges skyldigheter enligt öppenhetsprincipen som stadgas i artikel 5.1 a omfattar att informera om förekomsten av profilering samt konsekvenserna av förekommande profilering.¹⁴⁵

Vidare föreskriver artikel 15 GDPR en rätt för den registrerade att få bekräftelse på hur personuppgifterna behandlas eller har använts. Artikeln ger den registrerade rätt att få tillgång till de personuppgifter som legat till grund för profileringen samt vilken typ av övriga uppgifter som använts för att skapa profilen. Artikel 29-gruppen menar även att det föreligger en rätt för den profilerade individen att få reda på vilket segment den placerats i. Den personuppgiftsansvarige ska enligt artikel 15.3 utge allmän information och därutöver ska de uppgifter som används som ingångsvärden för att skapa profilen uppvisas.¹⁴⁶

Slutsatsen i avsnitt 4.1.4.1, att information om en enskild person som uppkommit av profileringsprocess utgör personuppgifter, leder till vidare reflektioner. Informationskravet i artikel 14 GDPR bör enligt mig omfatta även de nya personuppgifterna som skapats ur profileringsprocessen. Personuppgiftsansvarig ska således i enlighet med artikel 14 informera den registrerade om dennes personliga egenskaper som har framkommit, eller skapats, genom profileringsprocessen. Hur väl den personuppgiftsansvarige i praktiken efterlever artikel 14 när profilering skapat personuppgifter kan ifrågasättas. Med stor sannolikhet brister företagets efterlevnad av informationsskyldigheten i detta hänseende, vilket riskerar att undergräva den enskildes rättigheter. Det riskerar särskilt att undergräva möjligheten att utöva följande integritetsskyddande rättigheter.

¹⁴⁵ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 17.

¹⁴⁶ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 18.

4.1.4.2.2 Rätt till rättelse och radering

Profileringen och dess genererade resultat sker oftast i syfte att göra förutsägelser om enskilda individer. Eftersom det är just förutsägelser ökar risken för fel. Fel kan uppstå genom att ingångsdatan är felaktig, irrelevant eller tagen ur sin kontext. Vidare kan det föreligga fel hos algoritmen som leder till felaktiga korrelationer mellan data, vilket i sin tur kan skapa felaktiga profiler.¹⁴⁷

Rätt till rättelse, radering och begränsning regleras i artiklarna 16, 17 och 18 GDPR. Artikel 16 ger den registrerade rätt till rättelse av felaktiga personuppgifter. Den registrerade har rätt att dels få en felaktig uppgift ersatt med en korrekt uppgift, dels komplettera en ofullständig uppgift. Rätten till rättelse gäller även vid profilering när felaktig information har använts i profileringsprocessen. Enskilda har rätt att ifrågasätta och få rättelse av felaktig information som lett till att enskilda placerats i fel segment eller kategorier och som därav felaktigt förutsäger deras beteende.¹⁴⁸

Rätten till rättelse i artikel 16 och rätten till radering som stadgas i artikel 17 avser dels indata (personuppgifterna som brukades för framställandet av profilen), dels utdata (profilen själv eller informationen om personen som genererats via profileringen).¹⁴⁹

4.1.4.2.3 Rätt att göra invändningar

Artikel 21.1 GDPR föreskriver att den registrerade har rätt att göra invändningar mot personuppgiftsbehandling som grundar sig på artiklarna 6.1 e och 6.1 f. Detta omfattar också profilering som grundas på dessa bestämmelser. Artikel 6.1 e handlar om databehandling som sker i allmänt

¹⁴⁷ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 18.

¹⁴⁸ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 18.

¹⁴⁹ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 18.

intresse eller inom myndighetsutövning medan artikel 6.1 f avser behandling som är nödvändig för personuppgiftsansvarigas ändamål eller tredje parts berättigade intresse. Rätten att invända är således relativt begränsad. För profileringens vidkommande innebär det att den personuppgiftsansvarige måste avbryta¹⁵⁰ profileringsprocessen om den registrerade utövar rätten som föreskrivs i artikel 21.1. Detta gäller dock inte om personuppgiftsansvarige kan påvisa att det föreligger berättigade skäl som väger tyngre än den registrerades rättigheter.¹⁵¹ Den personuppgiftsansvarige ska således överväga hur betydelsefull profileringen är för ändamålet, profileringens konsekvenser för den enskilda individens fri- och rättigheter samt en generell avvägning mellan skilda intressen.¹⁵² Vad som avses med berättigade skäl ges inte närmare definiering i GDPR. Artikel 29-arbetsgruppen förklarar däremot att det kan tänkas föreligga berättigade skäl om profileringen gynnar samhället. Det är således enligt gruppen inte tillräckligt för den personuppgiftsansvarige att åberopa ett affärsintresse.¹⁵³

Artikel 21.2 ger den registrerade en *ovillkorlig* rätt att invända mot personuppgiftsbehandling som används för direkt marknadsföring. Detta omfattar rätten att invända mot profilering som sker i koppling till sådan direkt marknadsföring. Den ovillkorliga rätten innebär att ingen intresseavvägning görs.¹⁵⁴ Som redogjorts ovan resulterar profilering och särskilt personalisering främst i individanpassad marknadsföring, varför denna rättighet är viktig för den enskilda individen i sammanhanget.¹⁵⁵ Artikel 21.3 föreskriver verkan av att åberopa artikel 21.2, vilket är att personuppgifterna inte längre får behandlas för direkt marknadsföring. Skäl

¹⁵⁰ Artikel 18.1 d GDPR.

¹⁵¹ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 19.

¹⁵² Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 19 f.

¹⁵³ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 19.

¹⁵⁴ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 20.

¹⁵⁵ van der Hof och Prins 'Personalisation and its Influence on Identities, Behaviour and Social Values' (2008) s. 113 ff.

70 GDPR anger att nyss nämnda rättighet bör meddelas den enskilde klart och tydligt.¹⁵⁶

4.2 Automatiserat beslutsfattande

Automatiserat beslutsfattande kan äga rum med eller utan profilering.

Likaså kan profilering ske utan att ett automatiserat beslut fattas.

Automatiserat beslutsfattande och profilering kan således vara separata men profilering kan utgöra beslutsunderlag till det beslut som fattas automatiserat, vilket innebär att profilering är en del av det automatiserade beslutet.¹⁵⁷

Ett exempel är om en bank utför profilering av sina kunder i syfte att förutse kundernas betalningsförmåga. I sådana fall har profilering skett. Om bankens AI-system sedermera tar ett automatiserat beslut om kundens rätt till ett beviljat banklån, baserat på profileringen om kundens betalningsförmåga, utgör det ett automatiserat beslutsfattande inkluderat profilering som avses i artikel 22 GDPR.¹⁵⁸ Förbudet mot automatiserat beslutsfattande som föreskrivs i artikel 22 samt den enskildes rättigheter i sammanhanget redogörs i de kommande avsnitten.

4.2.1 Förbud mot automatiserat beslutsfattande

Öman menar att innebörden och användningen av profilering sannolikt har störst betydelse när profilering är en del av ett automatiserat beslutsfattande som regleras i artikel 22.1 GDPR.¹⁵⁹

¹⁵⁶ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 20; Öman, *Dataskyddsförordningen en kommentar* (uppdaterad 29 februari 2020, JUNO) kommentaren till artikel 21 GDPR.

¹⁵⁷ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 8.

¹⁵⁸ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 8 f.

¹⁵⁹ Öman, *Dataskyddsförordningen en kommentar* (uppdaterad 29 februari 2020, JUNO) kommentaren till artikel 4.4 GDPR.

Den registrerades rätt vid automatiserat individuellt beslutsfattande föreskrivs i artikel 22.1:

”Den registrerade ska ha rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne.”

Artikeln stadgar följaktligen ett *förbud* mot beslut skapat genom en automatisk behandling, inkluderat profilering, vilken har rättsliga följder eller betydande påverkar den enskilde. Förbudet gäller oberoende av om den enskilde åberopar sin rätt enligt artikeln.¹⁶⁰

4.2.1.1 Beslut utan mänsklig inblandning

Artikel 22.1 GDPR ger uttryck för att ett automatiserat beslut grundat på personuppgifter som skapats utan mänsklig inblandning kan vara integritetskränkande. Artikeln förbjuder enbart beslut som uppkommit helt utan mänsklig inblandning. Det ska noteras att beslutet inte utgör behandlingen av personuppgifter utan det är hanteringen av personuppgifterna som leder fram till beslutet som är behandlingen i GDPR:s mening.¹⁶¹

För att artikel 22.1 ska vara tillämplig ska både behandlingen och beslutet ske utan mänsklig inblandning.¹⁶² Det inte är möjligt att kringgå artikel 22.1 genom att påstå att fysiska personer involverats i beslutsprocessen. Artikel 29-gruppen menar att om företag rutinmässigt tillämpar automatiskt skapade profiler på enskilda utan att egentligen påverka beslutet är detta fortfarande ett beslut som enbart fattats via automatiserad behandling, d.v.s. utan

¹⁶⁰ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 20 f. och s. 36.

¹⁶¹ Frydinger m.fl. (2018) s. 221.

¹⁶² Frydinger m.fl. (2018) s. 221.

mänsklig inblandning. Den menar också att en korrekt mänsklig inblandning kräver att granskning av beslutet sker meningsfullt, snarare än som en symbolisk gest.¹⁶³

4.2.1.2 Rättsliga följder eller betydande påverkan

För en enskild individ ska åtnjuta rätten att inte bli föremål för automatiskt beslutsfattande krävs det enligt artikel 22.1 GDPR att beslutet har ”rättsliga följder” för den registrerade eller på ”liknande sätt i betydande grad påverkar” individen.

Begreppen ”rättsliga följder” eller ”liknande sätt i betydande grad påverkar” definieras inte i GDPR. För att finna vägledning menar Frydinger m.fl. att det är lämpligt att se till de normativa grunderna i GDPR. Som framställningen tidigare anfört beaktar dessa grundläggande värden mänsklig värdighet och individens rätt att leva ett liv med möjlighet att fatta självständiga beslut utifrån egna värderingar. Frydinger m.fl. utvecklar resonemanget och påtalar att automatiserad behandling av personuppgifter kan kränka mänsklig värdighet, främst på grund av att självbestämmanderätten inskränks. Detta kan medföra rättsliga följder eller annan påverkan för den enskilde. Rättighetsstadgan utgör enligt Frydinger m.fl. lämpliga riktlinjer vid bedömningen av om artikel 22.1 är tillämplig.¹⁶⁴

Skäl 71 GDPR föreskriver att ”automatiserat avslag på en kreditansökan online eller e-rekrytering utan personlig kontakt” kan utgöra betydande följder. I linje med skäl 71 har Artikel 29-gruppen uttalat konkreta riktlinjer. Beslut som har rättsliga följder kräver att beslutet påverkar den enskildes juridiska rättigheter, rättsliga ställning eller den enskildes rättigheter enligt ett avtal. Trots att beslutsprocessen inte har rättsliga följder kan artikel 22.1 vara tillämplig om beslutet skapar tillräckligt betydande följder för den

¹⁶³ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 21 f.

¹⁶⁴ Frydinger m.fl. (2018) s. 221 f.

enskilde. Beslutet ska påverka den enskildes ”omständigheter, beteende eller valmöjlighet” eller att beslutet har ”långvariga konsekvenser”.¹⁶⁵

Artikel 29-gruppen menar att automatiserade beslut om riktad personlig reklam grundad på profilering troligen inte påverkar den enskilda i en sådan ”betydande grad” som krävs för att uppnå förbudet i artikel 22.1 GDPR. Den exemplifierar sitt ställningstagande med uttalandet ”reklam för en typisk modebutik på nätet som grundas på en enkel demografisk profil: ’kvinnor i Bryssel i åldern 25–35 år som sannolikt är intresserade av mode och vissa klädesartiklar’” inte påverkar den enskilde i betydande grad. Vidare menar Artikel 29-gruppen att beroende på omständigheterna kan beslutet dock få betydande följer i den mening som stadgas i artikel 22.1 GDPR. Avgörande faktorer är bland annat hur grundlig profileringsprocessen är, om data avseende den enskilde hämtats på olika webbplatser, den enskilde personens förväntningar, reklamens utformning samt om känslig information om den enskilde använts.¹⁶⁶

4.2.2 Undantag från förbudet

Artikel 22.1 GDPR föreskriver således ett allmänt förbud mot helt automatiserat beslutsfattande med rättsliga eller liknande följder. Artikeln innehåller emellertid också undantag från förbudet.

Undantagen i artikel 22.2 GDPR är följande; a) om beslutet är nödvändigt för ingående eller fullgörande av avtal mellan den registrerade och personuppgiftsansvarige b) om det tillåts enligt unionsrätten eller nationell rätt, eller c) om den registrerade uttryckligen har samtyckt till den automatiserade behandlingen.

¹⁶⁵ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 22 f.

¹⁶⁶ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 23.

En enskild individ kan således bli föremål för helt automatiserat beslutsfattande om någon av ovanstående undantag är tillämpliga. Frydlinger m.fl. refererar till Artikel 29-gruppens exempel avseende vad som kan berättiga undantaget i artikel 22.2 a. Exemplet som följer är ett företag som utlyst en ledig tjänst och som får motta en stor mängd arbetsansökningar. För att möjliggöra sökandet efter lämpliga kandidater bland alla arbetsansökningar kan ett automatiserat beslutsfattande anses nödvändigt. Frydlinger m.fl. uppmärksammar att det automatiserade beslutsfattandet inte tar sikte på slutliga beslutet utan snarare på delbeslutet i processen, det vill säga urvalet av potentiella kandidater.¹⁶⁷ Vad gäller undantaget i artikel 22.2 b föreskriver skäl 71 att övervakning, förebyggande av bedrägerier och skatteundandragande som exempel när lagstiftningen kan tillåta automatiserat beslutsfattande. Slutligen föreskriver undantaget i artikel 22.2 c att automatiskt beslutsfattande är tillåtet om uttryckligt samtycke från den registrerade föreligger.¹⁶⁸

4.2.3 Särskilda rättigheter för den enskilde

Automatiskt beslutsfattande som åsyftas i artikel 22 GDPR sker allt oftare. Sådana beslut fattas automatiskt på förinlagda parametrar, eller också genom AI som utvecklar egna beslutsparametrar, samt genom information som enskild individ tillhandahållit. Automatiskt beslutsfattande kan exempelvis ske vid beslut rörande kreditvärderingar, hantering av jobbansökningar och marknadsföring grundat på profilering.¹⁶⁹

Risken att inskränka enskildas rättigheter vid automatiserat beslutsfattande, inklusive profilering, ställer krav på att den personuppgiftsansvarige vidtar åtgärder för att säkerställa insyn i behandlingen till syfte att skydda den registrerade. Enskilda som blir föremål för automatiserat beslutsfattande, med stöd av undantaget i artikel 22.2, erhåller därför vissa rättigheter.

¹⁶⁷ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 24; Frydlinger m.fl. (2018) s. 223 f.

¹⁶⁸ Frydlinger m.fl. (2018) s. 224.

¹⁶⁹ Frydlinger m.fl. (2018) s. 221.

Artiklarna 13.2 f, 14.2 g och 15.1 h ger den enskilde rätt att få meningsfull information om både den bakomliggande logiken som underbyggt beslutet samt betydelsen och följderna av beslutet. Skäl 71 föreskriver även att personuppgiftsbehandling bör:

”omgärdas av lämpliga skyddsåtgärder, som bör inkludera specifik information till den registrerade och rätt till mänskligt ingripande, att framföra sina synpunkter, att erhålla en förklaring till det beslut som fattas efter sådan bedömning och att överklaga beslutet”

Skäl 71 ligger i linje med artikel 22.3 GDPR, vilken anger att om undantagen i artikel 22.2 punkt a eller c är tillämpliga föreligger en skyldighet för den personuppgiftsansvarige att vidta ”lämpliga åtgärder för att säkerställa den registrerades rättigheter, friheter och rättsliga intressen” och särskilt ge den registrerade förutsättningar till att invända och bestrida beslutet.¹⁷⁰

En intressant fråga är huruvida enskilda individer har rätt till *förklaring* eller endast en rätt till *information* om det automatiserade beslutet. Skäl 71 GDPR föreskriver en rätt till förklaring medan artiklarna 13–15 endast ger enskilda en rätt till meningsfull men begränsad information om beslutet och processens logik samt beslutets konsekvenser. Vid en granskning av GDPR kan det konstateras att en rätt till förklaring upptas enbart i skäl 71. Skälen i GDPR avser enbart att ge vägledning för hur artiklarna ska tolkas och är inte rättsligt bindande. Legitima förväntningar på en *rätt till förklaring* följer således inte genom skäl 71. Detta minskar kravet på transparens vid automatiserade beslut.¹⁷¹ Forskarna Wachter, Mittelstadt och Floridi anser att ovan nämnda tvetydighet visar avsaknad av ett precist språk i GDPR.

¹⁷⁰ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 37.

¹⁷¹ Wachter m.fl. ‘Why a right to explanation of automated decision-making does not exist in the general data protection regulation’ (2017) s. 80.

Brist på tydliga och väldefinierade bestämmelser riskerar vidare efterlevnaden av enskildas integritetsskyddande rättigheter.¹⁷²

4.2.4 Datautvinning eller algoritmiskt beslutsfattande?

Algoritmiskt beslutsfattande kan utgöras av mer eller mindre komplexa algoritmer samt innebära olika grader av autonomi jämfört med mänsklig inblandning och kontroll. Naarttjärvi, forskare inom juridik, AI och mänskliga rättigheter, påtalar att separation av algoritmiskt beslutsfattande från sammanhanget datautvinning, där det ofta används, kan vara svårt. Datautvinning syftar till att synliggöra dolda samband, mönster och trender. Storskalig datautvinning är ett välkänt kommersiellt verktyg för företag och organisationer inom en rad områden.¹⁷³ Som exempel kan nämnas Target-fallet med den gravida tonårskvinnan, där datautvinning skedde i syfte att precisera kundreklamen för ökad försäljning.

Algoritmiskt beslutsfattande kan beskrivas som en sammansättning av två parallella processer. Den första processen avser att utvinna ny kännedom och förståelse ur stora tillgängliga datamängder. Den andra processen är utvecklingen inom maskininlärning och AI som möjliggör att algoritmer lär sig analysera självständigt. De två parallella processerna skapar tillsammans ett värde. Stora mängder data skapar i regel mer precisa maskininlärda algoritmer. Större nytta av maskininlärda algoritmer och AI skapar i sin tur mer autonoma beslutssystem.¹⁷⁴

Datautvinning och algoritmiskt beslutsfattande är avhängigt någon form av automatiserad algoritmisk behandling vars komplexitet varierar. En enklare och kontrollerbar process är när beslutet fastställts automatiskt men där

¹⁷² Wachter m.fl. 'Why a right to explanation of automated decision-making does not exist in the general data protection regulation' (2017) s. 76, s. 97 och s. 99.

¹⁷³ Naarttjärvi 'Rättsstatlighet och algoritmiska svarta lådor' (2017) s. 248 f.

¹⁷⁴ Naarttjärvi 'Rättsstatlighet och algoritmiska svarta lådor' (2017) s. 249

mänsklig programmering utgör processens förutsättningar.¹⁷⁵ Mer avancerade processer sker vid den maskininlärning som kallas djupinlärning. Beslutsfattande genom djupinlärning utgörs av en ogenomskådlig och icke-transparent logik, vilket därför har kommit att benämnas som algoritmiska 'svarta lådor'.¹⁷⁶ Beslutet, exempelvis förutsägelsen eller sannolikheten, är tydligt men beslutsprocessens beräkning framgår inte. Behovet av transparens i tekniskt komplexa processer som påverkar enskilda individer återspeglas i GDPR, särskilt i artikel 22 GDPR.¹⁷⁷ Den möjliga efterlevnaden av denna reglering avser kommande kapitel att undersöka.

¹⁷⁵ Mittelstadt m.fl. 'The ethics of algorithms: Mapping the debate' (2016) s. 2 f.

¹⁷⁶ Mittelstadt m.fl. 'The ethics of algorithms: Mapping the debate' (2016) s. 6; McKinsey Analytics 'An executive's guide to AI' (2018) s. 6; Mer om 'svarta lådor' i kommande avsnitt 5.1.1.

¹⁷⁷ Naarttijärvi 'Rättsstatlighet och algoritmiska svarta lådor' (2017) s. 249 f.

5 Teknik möter juridik

Redogörelsen ovan visar att den tekniska utvecklingen inom AI och datautvinning möjliggör den profilering och det automatiserade beslutsfattandet vi dagligen kommer i kontakt med. I de kommande avsnitten analyseras vilka rättsliga problem som följer av detta.

Lösningsförslag på problematiken presenteras. En genomgående analys av hur de belysta riskerna och problemen påverkar efterlevnaden av enskildas integritetsskyddande rättigheter följer även i de nedanstående avsnitten.

5.1 Problem och utmaningar

Lagstadgade bestämmelser i GDPR ställer krav på att informationen om personuppgiftsbehandlingen klart och tydligt kommuniceras till den registrerade. Informationen och kommunikationen ska framställas kortfattat, kärnfullt, i lättillgänglig form samt med ett tydligt språk. Sammantaget ger artiklarna 12, 13 och 14 GDPR en rätt för enskilda att bli informerade och upplysta. Vid automatiserat beslutsfattande, inklusive profilering, ska även information om logiken bakom det automatiserade beslutet kommuniceras meningsfullt.¹⁷⁸

Det är viktigt att rättigheterna lagförs och att de teoretiskt sett ger enskilda ett skydd vid deras personuppgiftsbehandling. Men det är minst lika viktigt att enskilda är medvetna om sina rättigheter, vilket förutsätts för att de ska kunna utöva dessa. De föreskrivna rättigheterna i GDPR tillförsäkrar enskilda ett skydd vid personuppgiftsbehandling, vilket bygger på ett skyddsvärde hos den personliga integriteten. Det är därför relevant att undersöka hur väl enskildas tillgång till rättigheterna *i praktiken är* och undersöka om tekniken bakom AI inverkar på bedömningen av enskildas tillgång till deras lagstadgade rättigheter.

¹⁷⁸ Se artiklarna 12, 13.2 f och 14.2 g GDPR.

Undersökningen *Special Eurobarometer 487a* från 2019 visar att två tredjedelar av medborgarna i EU har hört talas om GDPR. Av de två tredjedelarna är endast ungefär hälften medvetna om vad GDPR handlar om samt dess innebörd.¹⁷⁹ Medvetenheten hos enskilda om deras rättigheter som garanteras genom GDPR varierar emellertid beroende på rättighet. Generellt har majoriteten av EU-medborgarna hört talas om rättigheterna som finns i GDPR, med undantag för rätten att yttra sig när beslut skett genom automatiserat beslutsfattande, vilket inbegriper profilering, då endast 41% känner till denna rättighet.¹⁸⁰

Vidare visar undersökningen att ungefär hälften av respondenterna anser att de delvis har kontroll över den personliga informationen som samlats in över nätet. 62% av de som känner att de har delvis eller ingen kontroll över den information de tillhandahåller på internet är oroliga över detta.¹⁸¹ Drygt en av fem anser att de alltid är informerade om villkoren för insamling och användningen av deras personuppgifter online. Vidare påtalar endast 7 % att de aldrig ombeds att lämna personlig information vid internetuppkoppling.¹⁸² Vid en jämförelse från 2015 till 2019 har medvetenheten hos EU-medborgarna kring villkoren för insamling och användning av personuppgifter online minskat. Medvetenheten i Sverige har emellertid ökat sedan 2015.¹⁸³

Undersökningen visar vidare att sex av tio internetanvändare svarade att de läser integritetspolicys online. Dock svarade endast en minoritet på 13% av dessa att de läser dem fullständigt.¹⁸⁴ Integritetspolicyernas längd är den främsta anledningen till att endast en minoritet läser dem. Nästan en tredjedel anser att integritetspolicyerna är otydliga och svåra att förstå.¹⁸⁵

¹⁷⁹ Special Eurobarometer 487a (2019) s. 20.

¹⁸⁰ Special Eurobarometer 487a (2019) s. 23 och s. 50.

¹⁸¹ Special Eurobarometer 487a (2019) s. 34 och s. 39.

¹⁸² Special Eurobarometer 487a (2019) s. 42.

¹⁸³ Special Eurobarometer 487a (2019) s. 44.

¹⁸⁴ Special Eurobarometer 487a (2019) s. 47.

¹⁸⁵ Special Eurobarometer 487a (2019) s. 51.

Undersökningen visar respondenterna är mindre benägna att läsa integritetspolicyerna 2019 än vad de var 2015.¹⁸⁶

Sammantaget visar det presenterade resultatet av undersökningen en problematisk situation. EU-medborgarnas medvetenhet över GDPR:s existens och förståelsen för deras rättigheter lagförda i GDPR är begränsad. Det är enligt mig oroväckande att ungefär hälften av EU-medborgarna anser att de endast har delvis kontroll över den personliga informationen som samlas in över internet samt att en majoritet av dem oroliga över hur deras personuppgifter hanteras. Det ska i sammanhanget noteras att det enbart är 7% som påstår sig aldrig ha uppmanats till att lämna personliga information på internet. Med den statistiken kan det konstateras att en klar majoritet uppmanas lämna information vid internetanvändning, de flesta känner en begränsad kontroll över hur deras uppgifter hanteras och en stor oro kring detta föreligger.

Undersökningen markerar även att EU-medborgarnas medvetenhet och benägenheten att känna till villkoren för behandlingen av deras personuppgifter har minskat sedan 2015 fram tills 2019. Av särskilt intresse är den avvikande statistiken kring rätten att invända vid automatiserat beslutsfattande. Det föreligger således en minskad medvetenhet om enskildas rättigheter vid automatiserat beslutsfattande i förhållande till GDPR:s övriga lagstadgade rättigheter. Frågan är om denna avvikande statistisk kan förklaras genom att profilering och automatiserat beslutsfattande särskiljande är den rättighet som utgörs av en tekniskt komplex process innefattande AI, vilket GDPR möjligen inte tagit höjd för alternativt förmått att reglera. Vidare uppstår funderingar kring om tekniken påverkar organisationers och företags möjligheter att uppfylla och efterleva de lagstadgade bestämmelserna i GDPR, särskilt informationskraven och öppenhetsprincipen. Dessa reflektioner avser kommande framställning undersöka.

¹⁸⁶ Special Eurobarometer 487a (2019) s. 47.

5.1.1 Algoritmisk bristande transparens

Vikten av kunskap kring bristande transparens påvisas genom att EU-kommissionen har inlett en djupgående studie av algoritmiskt beslutsfattande. Undersökningen utförs i syfte att öka medvetenheten, få kunskap samt utreda utmaningar och möjligheter med algoritmiskt beslutsfattande. Studien avser att fokusera på hur algoritmer formar och personifierar informationsflödet till mottagaren, med andra ord påverkan av profilering och särskilt personalisering. EU-kommissionen påtalar att sökmotorer styr vår informationstillgång, vilket har stora konsekvenser för samhällets konsumenter.¹⁸⁷ Kommande redogörelse avser att i linje med EU-kommissionens studie undersöka bristen av transparens vid automatiserat beslutsfattande och profilering.

Enskildas rätt till insyn och information vid profilering och automatiserat beslutsfattande ställer krav på att algoritmerna är transparenta. Kravet på algoritmisk transparens ställer den personuppgiftsansvariga inför en svår uppgift.¹⁸⁸ Artikel 29-gruppen påtalar nämligen att maskininlärningens snabba tillväxttakt tillsammans med den tekniska komplexiteten försvårar förståelsen och förklaringen av hur en automatiserad beslutsprocess eller profilering fungerar – en bristande transparens kan således föreligga.¹⁸⁹

De algoritmer som använts för det automatiserade beslutet ska enligt GDPR framställas begripligt för den enskilde.¹⁹⁰ Artikel 29-gruppen menar att informationen åtminstone ska framställas så tydligt att den enskilde förstår skälen till beslutet.¹⁹¹

¹⁸⁷ EU-kommissionen, 'Algorithmic Awareness-Building' (uppdaterad 9 juni 2020).

¹⁸⁸ Frydinger m.fl. (2018) s. 164 f.

¹⁸⁹ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 26.

¹⁹⁰ Frydinger m.fl. (2018) s. 165.

¹⁹¹ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 26.

Vidare påtalar Artikel 29-gruppen, baserat på skäl 58 GDPR, att den tekniska komplexiteten inte utgör en godtagbar ursäkt för bristande transparens och därmed inskränkning av informationskravet.¹⁹² Skäl 58 stadgar följande:

”Öppenhetsprincipen kräver att all information som riktar sig till allmänheten eller till registrerade är kortfattad, lättåtkomlig och lättbegriplig samt utformad på ett tydligt och enkelt språk [...]. Detta är särskilt relevant i situationer där mängden olika aktörer och den tekniska komplexiteten gör det svårt för den registrerade att veta och förstå om personuppgifter som rör honom eller henne samlas in, vem som gör det och för vilket syfte, exempelvis i fråga om reklam på nätet.”

Skäl 58 föreskriver med andra ord ett tydlighetskrav och meningsfull information poängteras, oavsett dess tekniska komplexitet. Meningsfull information innebär inte krav på tekniska utläggningar utan betyder snarare att logiken bakom och kriterier till grund för det automatiserade beslutet förklaras.¹⁹³ Kravet på algoritmisk transparens medför krav på att tydligt förklara den automatiserade processens syfte, vilken data processen behandlar, möjliga och förutsedda utfall av beslutet samt beslutets konsekvens för den registrerade. Det uppställs däremot inga krav på att förklara hur algoritmerna tekniskt fungerar.¹⁹⁴

Vid diskussion om algoritmisk transparens vid profilering och automatiserat beslutsfattande används begreppet ‘black box’ eller som det benämns på svenska ‘svart låda’. Pasquale menar att begreppet ‘svarta lådor’ syftar till system eller processer vars transparens är bristande, innebärande en oförmåga för människan att veta hur och på vilka parametrar ett algoritmiskt beslut fattats.¹⁹⁵ Burrell anser att algoritmers bristande transparens innebär

¹⁹² Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 26 fotnot 40.

¹⁹³ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 26; Frydlinger m.fl. (2018) s. 165.

¹⁹⁴ Frydlinger m.fl. (2018) s. 165.

¹⁹⁵ Pasquale (2015) s. 3.

att en mottagare av en algoritms utgång, exempelvis mottagare av en banks lånebeslut eller mottagare av personifierad reklam online, sällan får en konkret förståelse för hur eller varför beslutet genererats från den givna indata. Denna brist på transparens har kommit att kallas 'svarta lådor'.¹⁹⁶

Larsson menar att vid en undersökning av transparensproblemen inom AI och maskininlärning behövs det nyanseras vad transparens är, för vem finns ett transparensbehov och i vilket syfte föreligger behovet. Intressant inom ramen för denna uppsats är transparensbehovet för enskilda individer vars syfte är att skydda den personliga integriteten och upprätthållandet av de grundläggande fri- och rättigheterna.¹⁹⁷

Vad transparens är har Burrell definierat genom en uppdelning av transparensproblemen i tre kategorier. Den första är avsiktlig avsaknad av transparens, vilket föreligger hos bland annat företag med intresse att bevara företagshemligheter. Den andra är avsaknad av transparens på grund av oförmåga att översätta tekniska termer i tal och skrift. Den tredje härrör från maskininlärningsalgoritmers tekniska komplexitet vilket krävs för att tillämpa dem på ett användbart sätt.¹⁹⁸

Det pågår en diskussion kring orsaker och lösningar av bristande transparens vid algoritmiskt beslutsfattande. Larsson menar att en bidragande faktor till transparensproblemen är intressekonflikter hos aktörer och enskilda individer. Exempelvis föreligger det ett företagsintresse i att inte vilja avslöja och synliggöra deras AI-tekniska lösningar. Företagens mjukvara och dess algoritmer kan ses som värdefulla företagshemligheter.¹⁹⁹ Argumentet är i linje med Burrells första kategori av transparensproblem – avsiktlig avsaknad av transparens. Denna bristande

¹⁹⁶ Burrell 'How the machine 'thinks': Understanding opacity in machine learning algorithms' (2016) s. 1.

¹⁹⁷ Larsson 'Sju nyanser av transparens: Om artificiell intelligens och ansvaret för digitala plattformars samhällspåverkan' (2018) s. 25 f.

¹⁹⁸ Burrell 'How the machine 'thinks': Understanding opacity in machine learning algorithms' (2016) s. 1 f.

¹⁹⁹ Larsson 'Sju nyanser av transparens: Om artificiell intelligens och ansvaret för digitala plattformars samhällspåverkan' (2018) s. 25 f.

transparens beror inte på algoritmens tekniska komplexitet utan kan åtgärdas genom reglering och tillsyn.²⁰⁰

Utvecklingen av maskininlärning bidrar till maskinell autonomi.²⁰¹ Vidare anses förståelsen och förklaringen av algoritmer minska i takt med ökad autonomi.²⁰² *Lärande* algoritmer skapar en egen beslutslogik för beslutsfattandet och denna förändras i takt med att algoritmen *lärt sig*. Även om en maskininlärningsalgoritms logik kan förklaras, är det i praktiken osannolikt att en sådan förklaringsbar algoritm är särskilt användbar, det vill säga genererar träffsäkra förutsägelser. Burrell påvisar att maskininlärningsmodeller som visar sig vara användbara, särskilt när det gäller klassificeringens noggrannhet, har en oundviklig komplexitet.²⁰³ De två sistnämnda argumenten ligger i linje med Burrells första och andra kategorier av transparensproblem – oförmåga att översätta de algoritmiska processernas koder i förståeligt språk samt teknikens komplexitet.

Sammantaget visar utredningen att det lagförda informationskravet som åläggs den personuppgiftsansvarige ställer vidare krav på algoritmisk transparens. Redogörelsen visar att transparensen riskeras vid algoritmiskt komplexa processer, liksom profilering och automatiserat beslutsfattande utförd av AI. Den personuppgiftsansvarige förmår inte att uppfylla informationskravet som stadgas i GDPR om processerna är ogenomskådliga och oförklarliga. Jag menar därför att de rådande transparensproblemen vid algoritmisk databehandling, innefattande profilering och automatiserat beslutsfattande, äventyrar lagbestämmelsernas efterlevnad och riskerar att försvaga enskildas integritetsskyddande rättigheter.

²⁰⁰ Burrell 'How the machine 'thinks': Understanding opacity in machine learning algorithms' (2016) s. 3 f.

²⁰¹ Naarttijärvi 'Rättsstatlighet och algoritmiska svarta lådor' (2017) s. 252.

²⁰² Mittelstadt m.fl. 'The ethics of algorithms: Mapping the debate' (2016) s. 11.

²⁰³ Burrell 'How the machine 'thinks': Understanding opacity in machine learning algorithms' (2016) s. 5.

5.1.2 Ingripande datainsamling och framställning av personuppgifter

Problemen som teknikutvecklingen skapar vid profilering och automatiserat beslutsfattande kan inte enbart hänföras till bristande transparens hos algoritmerna. Burrell menar att de nya genomgripande teknikerna för datainsamling som möjliggör en omfattande lagring och skapande av nya personuppgifter är problematiska. Bekymmer kring enskildas integritet och möjligheten, eller oroväckande omöjligheten, att självständigt göra val i livet uppkommer i sammanhanget.²⁰⁴

Mängden och värdet av enskildas personuppgifter ökar som ett resultat av digitaliseringen och vår ständigt uppkopplade tillvaro i kombination med teknikens förmåga att utvinna information ur denna data som därmed genereras.²⁰⁵ Redogörelsens resonemang kring GDPR:s definition av personuppgifter och domstolens bedömning i fallet Nowak mot Data Protection Commission föranleder att personuppgifter inte enbart avser upplysningar likt namn, telefonnummer och adress. Bedömningar och förutsägelser om en enskild individ skapade genom profileringsprocessen kan också anses vara personuppgifter.²⁰⁶ Vidare kan även enskildas inköpsbeteende och personliga preferenser baserade på bland annat länkklick online utgöra personuppgifter.²⁰⁷

Hur väl rättigheterna till information, radering, rättelse och begränsning i artiklarna 14 och 16–18 GDPR efterlevs i praktiken är intressant att fundera över. Hildebrandt och Gutwirth belyser att information genererad av profilering inte nödvändigtvis är verklighetsenlig eller sann eftersom informationen är baserad på bedömningar.²⁰⁸ De uppgifter som

²⁰⁴ Burrell 'How the machine 'thinks': Understanding opacity in machine learning algorithms' (2016) s. 2.

²⁰⁵ Burrell 'How the machine 'thinks': Understanding opacity in machine learning algorithms' (2016) s. 2.

²⁰⁶ Se avsnitt 4.1.4.1; C-434/16 Peter Nowak mot Data Protection Commissioner p. 34.

²⁰⁷ Burrell 'How the machine 'thinks': Understanding opacity in machine learning algorithms' (2016) s. 2.

²⁰⁸ Hildebrandt och Gutwirth 'Concise Conclusions: Citizens Out of Control' (2008) s. 365.

profileringsprocessen skapar, bedömningar om en enskilds egenskaper eller förutsägelser om dennes beteendemönster, kan således med stor sannolikhet för den enskilde vara felaktiga. Funderingar uppkommer kring om de enskilda som blir föremål för profilering ens är medvetna om profileringens bedömningar, bedömningar som dessutom kan anses utgöra personuppgifter. Utan en medvetenhet om personuppgifternas existens kan rätten att påkalla rättelse, radering och begränsning undermineras. Dock kvarstår informationsskyldigheten för den personuppgiftsansvarige enligt artikel 14 GDPR som diskuterats i ovanstående kapitel, vilket ger enskilda rätt att få reda på de personuppgifter som skapats genom profileringen. Det kan däremot i praktiken verka komplicerat för den personuppgiftsansvarige att tillämpa artikel 14 och således informera den enskilde om dennes personliga egenskaper framkomna av profileringsprocessen. Vidare kan det sannolikt upplevas obehagligt och integritetskränkande för den enskilde att ett företag har information om dennes personliga egenskaper, information som den enskilde kanske inte själv ens är medveten om eller anser är korrekt. Med det i åtanke äventyras sannolikt efterlevnaden av de uppställda rättigheterna i GDPR till information, radering, rättelse och begränsning.

GDPR är en integritetsskyddande lagstiftning som är uppbyggd på de grundläggande fri- och rättigheterna. Som belysts i redogörelsens avsnitt 4.1.4.3 bör principen om korrekthet förstås i ljuset av enskildas rätt till självbestämmande.²⁰⁹ Det kan diskuteras huruvida de personuppgifter som skapats ur en profileringsprocess är i enlighet med korrekthetsprincipen i artikel 5.1 d GDPR. Dels riskerar bedömningarna och förutsägelseerna om en enskild individ att utgöra felaktig information som dessutom individen inte nödvändigtvis får ta del av, dels riskerar uppgifterna begränsa individens valmöjlighet och självbestämmerätt eftersom den enskilde genom profileringen kategoriserats in i fack och utifrån klassificering presenteras ett sorterat urval. Ur ett integritetsperspektiv kan enskildas rätt till självbestämmande inskränkas om rättigheterna enligt GDPR och

²⁰⁹ Frydlinger m.fl. (2018) s. 36.

korrekthetsprincipen inte efterlevs, vilket riskeras vara fallet på grund av de genomgripande teknikerna för datainsamling.

5.2 Lösningförslag på problemen

EU-kommissionen konstaterar att algoritmisk transparens är ett viktigt skydd för rättvist automatiserat beslutsfattande samt att förståelsen av dess funktion är nyckeln till utformningen av välarbetat politiskt beslutsfattande.²¹⁰ Lösningförslagen på de problem och utmaningar som redogjorts ovan varierar. Nedanstående avsnitt avser att belysa utvalda föreslagna lösningar, inbegripet EU-strategin.

Artikel 29-gruppen tar upp ett par åtgärder för att personuppgiftsansvariga ska kunna uppfylla kraven i GDPR vid profilering och automatiserat beslutsfattande. Det krävs till att börja med att de som behandlar personuppgifter har stabila och utarbetade rutiner för att garantera efterlevnaden av artiklarna 12–22 i GDPR. Lämpliga åtgärder för företag är bl.a. att kontinuerligt fullfölja kvalitetssäkringskontroller av de använda AI-systemen, genomföra algoritmgranskning av de algoritmer som utvecklas av maskininlärningssystem samt att införa verktyg för mänskligt ingripande. Vidare föreslår Artikel 29-gruppen lösningförslag likt certifiering för personuppgiftbehandlingar och uppförandekoder vid granskningen av algoritmerna för att lösa rådande problem.²¹¹

Burrell menar att kombinationen av regelverk och någon form av utbildning till en bredare samhällsgrupp i kodskrivning kan vara lösningen för att minska transparensproblemen vid profilering och automatiserat beslutsfattande. Den rådande kunskapen om kodning och därmed förståelsen för den automatiserade beslutsprocessen innehas idag endast av en liten homogen teknikkunnig krets. Burrell problematiserar vidare sitt

²¹⁰ EU-kommissionen ‘Algorithmic Awareness-Building’ (uppdaterad 9 juni 2020).

²¹¹ Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017) s. 32 ff. och fotnot 52.

lösningsförslag och konstaterar att lösningen inte är tillräcklig vid beslutsfattande genererat av maskininlärda algoritmer. En maskininlärd algoritms beslutsprocess utvecklas och lärs med tiden utan mänsklig inblandning. Processen överensstämmer inte med det människan uppfattar som ”naturliga” förklaringar, vilket också gäller för specialutbildade datavetare.²¹²

Hildebrandt och Gutwirths uppfattning är i linje med Burrells. Profileringsprocessens bristande transparens härrör från att algoritmer behandlar data på ett sätt som överstiger den mänskliga hjärnkapaciteten.²¹³ Burrell konstaterar vidare att lösningen på transparensproblemen inte uppnås med enbart ett verktyg. Lösningen, eller snarare lindringen av de negativa konsekvenserna, är enligt Burrell en kombination av lagregler och teknisk granskning av algoritmernas koder och funktionssätt.²¹⁴ Hildebrandt och Gutwirth menar också att lösningen på problemen är dels rättsliga verktyg (i form av lagstadgade bestämmelser som rätt till information och transparens), dels tekniska verktyg (som möjliggör enskildas utövande av de lagstadgade rättigheterna).²¹⁵ Transparensproblematikens lösning är således enligt Burrell, Hildebrandt och Gutwirth avhängigt kombinationen av väl utformade lagregler och tekniska verktyg.

5.2.1 Rättsliga verktyg

Hildebrandt och Gutwirth anser att lagens uppställda dataskyddsregler teoretiskt sett är tillämpliga på profileringsprocessens olika delar men att profileringsens komplexa tekniker är en ’svart låda’, vilket i praktiken riskerar resultera i en ineffektiv dataskyddslagstiftning.²¹⁶ Dock anförde

²¹² Burrell ‘How the machine ‘thinks’: Understanding opacity in machine learning algorithms’ (2016) s. 10.

²¹³ Hildebrandt och Gutwirth ‘Concise Conclusions: Citizens Out of Control’ (2008) s. 366.

²¹⁴ Burrell ‘How the machine ‘thinks’: Understanding opacity in machine learning algorithms’ (2016) s. 10.

²¹⁵ Hildebrandt och Gutwirth ‘Concise Conclusions: Citizens Out of Control’ (2008) s. 366.

²¹⁶ Hildebrandt och Gutwirth ‘Concise Conclusions: Citizens Out of Control’ (2008) s. 367 f.

Hildebrandt och Gutwirth detta innan GDPR trädde ikraft, vilket aktualiserar funderingar kring om dataskyddet effektiviserats efter GDPR ikraftträdande. Följande undersökning av Wahlgren, professor och forskare inom lagstiftningsläran, och Holtz, lektor i IT-rätt, avser att utreda detta samt undersöka effektiva alternativ till traditionell lagstiftning.

Wahlgren har undersökt lagstiftning i allmänhet och menar att lagstiftningen utsätts för allt större påfrestningar. En bidragande faktor är den ökade förändringstakten i samhället. Wahlgren menar att traditionella sätt att formulera lagar passar mindre väl när problem präglas av en snabb utvecklingstakt. En del områden uppvisar en komplexitet där bakgrundskunskaper krävs för att finna en optimal lösning men där tiden är otillräcklig. Regleringarna av områden som påverkas av tekniska förändringar förefaller därför vara onödigt komplicerade och svagheterna enkla att finna. Wahlgren menar att den tekniska utvecklingen som präglar samhället innebär att problem som skyddet för den personliga integriteten uppkommer inom allt fler områden.²¹⁷

Vidare menar Wahlgren att lagstiftning består av tre delar: lagstiftningens rationalitet, lagstiftningens problem och lagstiftningsteknikens möjliga utveckling. Lagstiftningens rationalitet åsyftar lagarnas ändamålsenlighet. Lagstiftningen ska verka för att fungera på bästa möjliga sätt och vara välanpassad till olika områdets förutsättningar. Kunskap om lagstiftningens problem är en förutsättning för att förstå hur lagstiftningstekniken kan utvecklas. Lagstiftningsteknikens utveckling handlar om möjligheterna att anpassa lagen till omgivningens förändringar, omgivningen där lagen avser att verka. Det avser dels att uppdatera traditionella lagstiftningstekniken, dels undersöka möjligheterna att introducera praktiska lösningar.²¹⁸

Holtz har ställt sig kritisk till GDPR:s avsaknad av uttryckliga regleringar av viktiga företeelser som präglar dataskyddet. Han exemplifierar sociala

²¹⁷ Wahlgren (2014) s. 18.

²¹⁸ Wahlgren (2014) s. 17 f.

medier, sökmotorer och Big data och menar att explicita regleringar hade kunnat bidra till ett mer praktiskt dataskydd. Holtz menar att GDPR:s teknikneutrala utformning går miste om chansen att reglera problem och utmaningar som uppkommer och förmodligen fortsättningsvis riskeras uppkomma på grund av teknikens utveckling.²¹⁹ Sammantaget anser Holtz att GDPR är utformad med bristande ändamålsenlighet, vilket enligt Wahlgrens uppdelning föranleder brister i lagstiftningens rationalitet. Holtz efterlyser en anpassad lagstiftningsteknik i förhållande till den teknologiska utvecklingen som skett och som även kommer ske. Lagstiftningsteknikens utveckling avser att finna praktiska lösningar, vilket Wahlgren förklarar enligt följande.

Wahlgren diskuterar möjligheten att uttrycka lagar på olika sätt och introducera mer praktiska lösningar, bland annat genom inbyggda lagar i den fysiska miljön. Inbyggda lagar är direktverkande på ett operativt sätt och utformningen kan variera. Det handlar om att översätta samt komplettera lagregler med en uppsättning precisa instruktioner. Exempelvis kan de precisa instruktionerna om regelfunktionerna återges i flödesscheman eller bestå av datorprogram. De inbyggda lagarna kräver en konkret utformning, vilket vanligtvis är en integrering i tekniska system. Wahlgren menar att en teknisk integrering av ett regelverk eller regelfunktioner är mer effektivt jämfört med en uteslutande traditionell lagutformning.²²⁰ Möjligheterna att införliva lagstiftningen med tekniska skyddsmekanismer är vidsträckt. Denna möjlighet kommer även öka i takt med användning av mer avancerad teknik. Wahlgren menar också att tekniken har börjat användas för att stärka dataskydd och skyddet för personlig integritet.²²¹

I linje med Wahlgrens inbyggda lagar menar Hildebrandt och Gutwirth att det, i brist på praktiskt relevant dataskyddslagstiftning, krävs en integrering

²¹⁹ Holtz 'Den nya allmänna dataskyddsförordningen – några anmärkningar' (2018) s. 240 och s. 243.

²²⁰ Wahlgren (2014) s. 219 f.

²²¹ Wahlgren (2014) s. 223; Se t.ex. European Union Agency For Network and Information Security 'A tool on Privacy Enhancing Technologies (PETs) knowledge management and maturity assessment' (2018).

av lagliga transparensnormer i tekniska enheter. Dessa transparensregler ska kunna översätta det tekniska händelseförloppet som sker vid profileringsprocessen och det automatiserade beslutsfattandet. Syftet är att det ska skapa en förståelse för processen och en möjlighet för företag att förklara hur och på vilka parametrar en profilering och ett automatiserat beslut genererats. Enskilda kan således återfå viss kontroll över konsekvenserna av deras handlingsätt, vilket stärker skyddet för den personliga integriteten.²²²

5.2.2 Tekniska verktyg

Inbyggda lagar och transparensnormer i tekniska enheter som redogjorts för ovan är rättsliga verktyg integrerade i tekniska system, vilket därför delvis utgör tekniska verktyg. Nedan följer en vidare redogörelse av vilka tekniska verktyg som kan utgöra tänkbara lösningar på transparensproblemen.

Marshall m.fl. har inom ramen för Microsofts dokumentation och utbildning utarbetat dokumentet *Framtidens säkra artificiella intelligens och maskininlärning med Microsoft*. Materialet är tänkt att användas av Microsoft och branschpartners. Författarna belyser att forskning och kunskap inom AI krävs för att inte riskera att framtidens AI blir en 'svart låda'. Författarnas efterforskning visar att oroväckande stor tillit ges till resultatet från AI-baserade beslutsprocesser med tanke på att transparensproblematiken utesluter en förståelse och förklaring av hur besluten exakt kommit till.²²³

Enligt Marshall m.fl. måste det utarbetas nya ramverk och strategier för att åtgärda brister i AI-baserade tjänster. För att säkerställa integritet, transparens och visa riktigheten i algoritmiskt beslutsfattande är det viktigt

²²² Hildebrandt och Gutwirth 'Concise Conclusions: Citizens Out of Control' (2008) s. 367 f.

²²³ Marshall m.fl. 'Framtidens säkra artificiella intelligens och maskininlärning med Microsoft' (2018) se under rubrik "Sammanfattning".

att AI-tjänster kan granskas och spåras på algoritmnivå. Det kräver att AI har inbyggda *datautredningsfunktioner*, funktioner som identifierar när beslut fattas, vilken data som påverkat beslutet och tillförlitligheten i den använda datan. Företag och organisationer kan genom tekniskt inbyggd datautredning demonstrera hur den algoritmiska beslutsprocessen fungerar, vilket även möjliggör företagens förmåga att justera eventuellt felaktiga beslut. Resultatet av en fungerande inbyggd datautrednings- och säkerhetsloggning vid AI-användning ger den registrerades rätt till information och transparens. Det möjliggör vidare enskildas rätt till rättelse eller radering. Sammantaget bidrar inbyggda dataskyddsfunktioner till ett förtroende och skydd för enskildas integritet.²²⁴

Resultatet av fungerande datautredningsfunktioner skiljer sig inte mycket från det önskvärda resultatet av lagliga transparensnormer i tekniska enheter, vilka presenterades i ovanstående avsnitt. Sammanfattningsvis kan rättsliga verktyg samt krav likt certifiering och uppförandekoder i kombination med tekniska verktyg skapa transparens vid profilering och automatiserat beslutsfattande, vilket möjliggör en efterlevnad av GDPR:s integritetskyddande bestämmelser.

5.2.3 EU-strategin

Larsson anför att när det diskuteras reglering av AI, behov av ny eller eftersläpning av befintlig, ska inte den nuvarande regleringen glömmas bort. Det utvecklade regelverket för dataskydd, GDPR, är tillämpligt för många processer där AI används. Problemen grundar sig förmodligen inte i avsaknad av lagregler utan snarare på implementeringen av regleringen vid användning av mer autonoma system. Larsson menar att branschöverenskommelser, utveckling av standarder och certifieringar kan

²²⁴ Marshall m.fl. 'Framtidens säkra artificiella intelligens och maskininlärning med Microsoft' (2018) se under rubrik 'Nya säkerhetstekniska utmaningar' och 'Transparens och ansvarstagande förutsätter att AI har inbyggd datautredning- och säkerhetsloggning'.

krävas som komplement till lagreglering för att lösa problemen.²²⁵ Detta aktualiserar funderingar kring vad EU-strategin om framtida AI-hanteringens betyder. Kan det utgöra startskottet till det komplementet Larsson kräver eller den strategi som Marshall m.fl. efterlyser för komma till rätta med problematiken? Vidare uppstår frågan om det påverkar tillämpningen och implementeringen av de uppställda rättigheterna i GDPR.

EU-kommissionen har utarbetat olika åtgärdsförslag som framlagts i EU-strategin till syfte att främja utvecklingen och användningen av AI samt adressera riskerna kopplade till AI-användning.²²⁶ EU-strategin består av två huvudsakliga åtgärdsdelar. Den första delen behandlar åtgärder i syfte att skapa spetskompetens. Samarbete mellan medlemsstaterna betonas, behov av forskning och innovation understryks och kommissionen framhåller att åtgärder för kompetensbrister inom AI måste stödjas.²²⁷ I denna del kan åtgärderna och den kompetenshöjande forskningen inom AI minska transparensproblemen. Den andra delen upptar utformningen av ett framtida AI-regelverk för att skapa en gemensam europeisk ram i syfte att öka enskilda individers förtroende.²²⁸ Detta regelverk ska vara inriktat på att minimera riskerna med AI, särskilt de risker som äventyrar enskildas grundläggande rättigheter och enskildas skydd till personlig integritet.²²⁹

Vidare belyser EU-kommissionen att bristen på transparens hos AI försvårar identifieringen av eventuella lagöverträdelser, inkluderat överträdelser eller icke-efterlevnad av bestämmelser som skyddar de grundläggande rättigheterna. EU-kommissionen anför därför att det kan krävas en anpassning och förtydligande av befintlig lagstiftning för att möjliggöra en effektiv efterlevnad och kontroll av både EU-lagstiftning och nationell lagstiftning.²³⁰

²²⁵ Larsson 'Artificiell intelligens som normativ samhällsutmaning: partiskhet, ansvar och transparens' (2019) s. 363.

²²⁶ Vitbok om artificiell intelligens (2020) s. 1.

²²⁷ Vitbok om artificiell intelligens (2020) s. 5 ff.

²²⁸ Vitbok om artificiell intelligens (2020) s. 10.

²²⁹ Vitbok om artificiell intelligens (2020) s. 12 och s. 15.

²³⁰ Vitbok om artificiell intelligens (2020) s. 15.

Tillsammans med vitboken presenterade EU-kommissionen två meddelanden: *Att forma EU:s digitala framtid* och *En EU-strategi för data*.²³¹ Meddelandet om datastrategi för EU belyser att enskilda individer genererar allt större datamängder och således ökar tillgängliga datavolymer. Detta ställer i sin tur högre krav på att den data som samlas in beaktar individens grundläggande rättigheter. För att allmänheten ska vara med i den digitala utvecklingen och bruka datadrivna innovationer måste enskilda inneha förtroende för att delning och spridning av deras personuppgifter sker i enlighet med reglerna i GDPR.²³² EU-kommissionen anser att översyn och kontroll av GDPR är användbara åtgärder för att skapa ett ökat förtroende och efterlevnad av regelverket.²³³

Vidare menar EU-kommissionen att det föreligger ett flertal problem som hindrar EU från att förverkliga en datadriven ekonomi. Ett av problemen är möjligheten för enskilda individer att utöva sina rättigheter. GDPR stadgar en hög skyddsnivå som i teorin främjar enskilda personers grundläggande rättigheter. Kommissionen anser däremot att det saknas tekniska verktyg och standarder för att enskilda individer ska kunna utöva sina rättigheter på ett relativt enkelt vis. Kommissionen lyfter rörelsen MyData och liknande aktörer²³⁴ som presenterat åtgärder i syfte att ge enskilda personer konkreta verktyg och metoder för att få insyn, ta kontrollen och beslutanderätten över hur deras data och personuppgifter hanteras. De potentiella verktygen består främst av applikationer och kooperativ för personuppgifter, vilka avser att vara mellanhänder i ekonomin för personuppgifter.²³⁵

²³¹ Kommissionens meddelande; 'En EU-strategi för data' (2020) och 'Att forma EU:s digitala framtid' (2020).

²³² Kommissionens meddelande 'En EU-strategi för data' (2020) s. 1.

²³³ Kommissionens meddelande 'En EU-strategi för data' (2020) s. 4.

²³⁴ Se t.ex. DECODE, Solid och RadicalxChange.

²³⁵ Kommissionens meddelande 'En EU-strategi för data' (2020) s. 6 och s. 10 f.

6 Diskussion och avslutande reflektioner

Avhandlingen har i ljuset av AI-utvecklingen granskat regleringen av profilering och automatiserat beslutsfattande, med fokus på skyddet för enskildas grundläggande fri- och rättigheter. Uppsatsens första frågeställning om vilka risker och problem som uppstår när profilering och automatiserat beslutsfattande utförs av AI har besvarats i fjärde och femte kapitlet. Problemen är bristande algoritmisk transparens, ingripande datainsamling och skapandet av nya personuppgifter. Ur dessa problem skapas i sin tur vidare problem, vilket är risken för en minskad efterlevnad av enskildas integritetsskyddande rättigheter i GDPR och de efterföljande effekter av detta som tredje frågeställningen tar sikte på.

Uppsatsens andra frågeställning om GDPR kan hantera de belysta problemen eller om kompletterande lösningar krävs samt förslag på åtgärder har besvarats i femte kapitlet. Slutsatsen är att kompletterande lösningar krävs samt att lösningsåtgärderna bör bestå av både rättsliga- och tekniska verktyg för att komma till bukt med problemen. En slutlig reflektion av detta framställs nedan. I femte kapitlet har EU-strategin och dess åtgärdsförslag presenterats, en vidare diskussion om EU-strategins *betydelse* följer i syfte att besvara andra frågeställningens delfråga.

Uppsatsens tredje och sista frågeställning, hur de belysta riskerna och problemen av profilering och automatiserat beslutsfattande påverkar efterlevnaden av enskildas integritetsskyddande rättigheter, har genomgående tagits upp i avhandlingen och avser vidare att besvaras i nedanstående diskussion. Det som framkommit i avhandlingen är att efterlevnaden av enskildas rättigheter äventyras, vilket sedermera riskerar att resultera i integritetsintrång och inskränkning i enskildas självbestämmanderätt.

Uppsatsens frågeställningar ska inte upprepas och besvaras på nytt. Istället följer en avslutande och sammanfattande integritetspräglad diskussion och reflektion av uppsatsens syfte och de redan besvarade frågeställningarna. Diskussionen fokuserar på om enskildas lagstadgade rättigheter kan tillvaratas, om regleringen i GDPR är ändamålsenlig samt vad som krävs för att regleringen ska vara tillfredställande ur ett integritetsperspektiv när AI används vid profilering och automatiserat beslutsfattande.

6.1 En faktisk medvetenhet...

För att enskildas rättigheter ska kunna tillvaratas vid profilering och automatiserat beslutsfattande som utförs av AI krävs det att två förutsättningar är uppfyllda. För det första måste en *faktisk medvetenhet hos den enskilde* föreligga, en medvetenhet om att en aktuell integritetskränkande profilering och/eller automatiserat beslutsfattande existerar samt vilka rättigheter som den enskilde kan åberopa. För det andra krävs en *praktisk möjlighet för företag och organisationer att tillämpa* och efterleva den befintliga lagstiftningen, här specifikt enskildas integritetsskyddande rättigheter i GDPR vid profilering och automatiserat beslutsfattande.

En intressant reflektion när den faktiska medvetenheten diskuteras är om GDPR är utformad med en övertro på individernas förståelse för vilka åtgärder de är föremål för, särskilt när AI involveras. Som tagits upp är GDPR en integritetsskyddande lagstiftning som genomsyras av laglighet-, korrekthet- och öppenhetsprinciperna. Principerna framgår av ett antal artiklar som gemensamt ger enskilda rätt till information vid behandling av deras personuppgifter. Främjande av öppenhet och insyn är sedan länge etablerat i EU, varav syftet är att skapa förtroende i processer som påverkar medborgarna för att ge dem möjlighet att, vid behov, utmana och ifrågasätta processerna.

Utredningen av profilering visar att de flesta individer är omedvetna om att de blir föremål för profilering, särskilt personalisering. En enskilds möjlighet att tillvarata och åberopa sina rättigheter, när den enskilde är omedveten om att en integritetskränkande situation föreligger, är begränsad. Undersökningen i Special Eurobarometer 487a kan anses påvisa att en ökad teknisk involvering minskar enskildas medvetenhet och förståelse för hur deras personuppgifter hanteras samt vilka rättigheter de har i sammanhanget. Detta är problematiskt eftersom en minskad eller obefintlig medvetenhet sannolikt minskar möjligheten för enskilda att tillvarata sina integritetsskyddande rättigheter. Det lär även minska företagens incitament att efterleva rättigheterna i GDPR. Talesättet ”det man inte vet, tar man ingen skada av” är möjligen felaktigt i sammanhanget, men beskriver samtidigt företagens synsätt väl. Företagen har uppenbarligen brustit i eller inte haft förmågan att informera enskilda om deras rättigheter i samband med automatiserat beslutsfattande innefattande profilering, något individer förblir ovetandes om. Den tekniska utvecklingen av AI lär inte sakta ner, snarare tvärtom. En vidare undersökning och forskning av de framkomna problemen och praktiska lösningsförslag är således viktigt för att undvika upprepning av de problem som i dagsläget föreligger.

I sammanhanget kan det noteras att uppsatsens utredning visar att användbar information vid profilering och automatiserat beslutsfattande är mer än en enskilds uppsättning personuppgifter. Först när personuppgifterna analyseras i sin kontext och bearbetas på nytt skapas ett mervärde och en fullständig profil kan framställas. Om bristande medvetenhet föreligger kring den ursprungliga hanteringen av den enskildes personuppgifter, föreligger sannolikt en ytterligare minskad medvetenhet hos individen om företagens fortsatta behandling av dennes personuppgifter. Den fortsatta behandlingen riskerar dessutom att hantera personuppgifterna i skilda syften och sammanhang än de ursprungliga. En konkret överenskommelse med individen bortfaller och resulterar i en från integritetsperspektiv oönskad omedvetenhet.

I realiteten är de individspecificerade rekommendationerna och valen som når den enskilda individen noga utvalda utifrån en analys av individens beteende och personliga preferenser, vilket med andra ord är resultatet av profileringsprocessen. Profilering riskerar att gå enskilda individen omedvetet men inte obetydligt förbi, eftersom det riskerar att undergräva individens lagstadgade självbestämmanderätt och rätt att självständigt göra val i livet. En problematisk situation uppstår och en negativ informationsasymmetri mellan företag och enskilda skapas. Huruvida GDPR tagit höjd för detta kan ifrågasättas. Ett argument kan tänkas vara att GDPR avsett att balansera asymmetrin genom att ålägga den personuppgiftsansvarige en informationsplikt. Denna informationsplikt förutsätter att regleringen är praktiskt möjlig att efterleva för den personuppgiftsansvarige vid användningen av AI. Detta har tidigare i avhandlingen besvarats delvis nekande men diskuteras vidare nedan.

6.2 ... och en praktisk möjlig tillämpning...

Om vi antar att enskilda faktiskt vet vilka profilerings- och automatiserade beslutssituationer de blir föremål för samt vilka rättigheter de kan åberopa i aktuella situationer, kvarstår en praktisk möjlig tillämpning av de integritetsskyddande rättigheterna. Denna tillämpning är en förutsättning för efterlevnaden av enskildas integritetsskyddande rättigheter i GDPR.

Som redogörelsen undersökt har AI särskilda egenskaper som medför utmaningar. Bristande transparens i form av 'svarta lådan'-effekten, teknisk komplexitet, autonomt beteende vid maskininlärningsalgoritmer och oförutsebara resultat är de egenskaper hos AI som medför de största problemen och svårigheterna. Svårigheterna består i att praktiskt möjligt tillämpa, eller praktiskt möjligt kontrollera tillämpligheten, av reglerna i GDPR hänförliga till profilering och automatiserat beslutsfattande.

GDPR är en teknikneutral reglering och är i teorin tillämplig oavsett AI:s involvering. Min utredning har emellertid visat att den personuppgiftsansvariges möjlighet att efterleva den registrerades rättigheter till information, radering, rättelse och begränsning föreskrivna i artiklarna 12–18 GDPR kan vara begränsad när profileringsprocessen och förfarandet vid automatiserat beslutsfattande består av icke-transparenta algoritmer. GDPR är således i dessa delar ineffektiv och icke ändamålsenlig eftersom en praktisk möjlig tillämpning av hänförliga integritetsskyddande bestämmelser äventyras.

Vid diskussion om ändamålsenligheten och efterlevnaden av de integritetsskyddande artiklarna i GDPR är det intressant att uppmärksamma den föreliggande skillnaden mellan beslutsprocesser där människan inte *behöver* involveras jämfört med beslutsprocesser där människan inte *förmår* att involveras. Artiklarna 13.2 f och 14.2 g samt skäl 58 GDPR förutsätter att personuppgiftsansvarig förmår att ge den registrerade information och insyn i beslutsprocessen, åtminstone för att processen ska vara laglig. Här åsyftas beslutsprocessen bakom det automatiserade beslutsfattandet, inklusive profilering, som undantaget i artikel 22 GDPR rättfärdigar. En laglig automatiserad beslutsprocess enligt artikel 22 tar således sikte på beslut vars process sker automatiskt men där personuppgiftsansvariga inte *behöver*, men likväl *förmår*, att involveras i. Utifrån det resonemanget kan automatiserat beslutsfattande som rättfärdigas av artikel 22 antas vara av tekniskt enklare sort eftersom personuppgiftsansvarige förmår att involveras och insyn i processen är möjlig, vilket sedermera möjliggör uppfyllandet av informationskravet. De mer komplexa icke-transparenta algoritmiska beslutsprocesserna som personuppgiftsansvariga inte förmår att involveras i eller överblicka resulterar sannolikt i något av de två följande scenarion. Antingen föreligger en svårighet i att praktiskt kontrollera tillämpligheten av artikel 22 och det integritetsskyddande informationskravet, eller också faller sannolikt situationen utanför artikel 22 tillämpningsområde och personuppgiftsansvariga brister i sin informationsplikt. GDPR:s befintliga utformning med avsaknad av explicita regleringar av tekniska förfaranden, i

detta fall automatiserat beslutsfattande med AI, anser jag med anledning av nyss anförda diskussion sannolikt bidrar till en bristande möjlig efterlevnad av enskildas integritetsskyddande rättigheter föreskrivna i GDPR.

I anknytning till algoritmisk bristande transparens kan diskussion om profilering som mänskligt tänkande uppmärksammas. Resultat i form av klassificeringar och förutsägelser som baserats på erfarenheter och fördomar är inte unikt för AI. Som tagits upp i avsnitt 4.1.2 fungerar mänskligt tänkande på samma sätt. Förklaringen av logiken bakom hur mänskligt tänkande processar erfarenheter och fördomar som slutligen genererar förutsägelser är svårt. Lika svårt kan förståelsen vara av logiken bakom maskininlärningsalgoritmer som genererar ett automatiserat beslut, vilket innefattas i det informationskrav som GDPR uppställer för laglig personuppgiftshantering. Burrell menar att maskininlärd algoritmer skapar egen föränderlig beslutslogik samt att användbara algoritmer med träffsäkra resultat är de algoritmiska processer vars logik är oförklarlig.²³⁶ Hur väl möjligheten, med dagens givna förutsättningar, att tillämpa de integritetsskyddande reglerna i GDPR när maskininlärd algoritmer utför profilering och automatiserat beslutsfattande ställer jag mig mot bakgrund av ovan frågande till.

Framtidens AI, särskilt maskin- och djupinlärning, kommer troligtvis utvecklas till att jämföras med mänskligt tänkande. Likt Burrells ställningstagande är användbara maskininlärningsalgoritmer de som har en oundviklig komplexitet med en oförklarbar beslutsprocess.²³⁷ Det räcker inte att GDPR uppställer lagbestämmelser om dessa inte är möjliga att tillämpa och efterleva i samtiden-, och med största sannolikhet, framtidens algoritmstyrda processer. Risken är att enskilda individers integritet inskränks på grund av bristande samspel mellan teknik och juridik. Det krävs således lösningar och åtgärder för hur en praktiskt möjlig tillämpning

²³⁶ Se avsnitt 5.1.1.

²³⁷ Se avsnitt 5.1.1.

av GDPR:s grundläggande värden och regler kan stärkas i dagens digitaliserade miljö, vilket kommande avsnitt avser att diskutera.

6.3 ... förutsätter men garanterar inte efterlevnaden av enskildas rättigheter föreskrivna i GDPR

Som rubriken antyder garanteras inte efterlevnaden av enskildas integritetsskyddande rättigheter vid profilering och automatiserat beslutsfattande av att en faktisk medvetenhet och en praktisk tillämpning av GDPR:s bestämmelser. Medvetenhet är en förutsättning men det är inte någon garanti för regleringens efterlevnad. Garanti, eller i realiteten ökad chans, till efterlevnad av de integritetsskyddande reglerna kan främjas genom avhandlingens avsnitt 5.2 upptagna lösningsförslag.

Uppsatsens diskussion belyser de problem som riskeras uppkomma om en bristande faktisk medvetenhet och en bristande möjlig tillämpning av GDPR:s bestämmelser föreligger. Det är två problem ur en situation: profilering respektive automatiserat beslutsfattande utförd av AI. Hur ska enskilda individer kunna fatta egna val i livet och verka självbestämmande när problem likt dessa föreligger? Är Wahlgrens inbyggda lagar lösningen? Eller är lösningen integrering av transparensnormer i tekniska processer som Hildebrandt och Gutwirth anför? Eller är det kombinationen av Burrell, Hildebrandt och Gutwirths lösningar kring ökad kunskap, ändamålsenliga lagregler och tekniska verktyg som är nyckeln till efterlevnad av GDPR? Alternativt är Artikel 29-gruppens förslag om kontinuerliga kvalitetssäkringskontroller av AI-system och dess maskininlärda algoritmerna, verktyg för mänsklig involvering samt certifiering och uppförandekoder lösningen på problemen?²³⁸

²³⁸ Se avsnitt 5.2.

Min slutsats är att GDPR:s befintliga utformning i samtidens kontext kräver kompletterande lösningar för att ha en chans att verka ändamålsenligt och minimera de negativa konsekvenserna som riskeras uppstå för enskilda individen. Efterlevnaden av enskildas rättigheter i GDPR kräver praktiska lösningar där rättigheterna enligt mig bör integreras i tekniska system för att få verklig nytta. Ett närmare ställningstagande om det mest effektiva lösningsförslaget lämnar jag till läsaren. Däremot följer en fortsatt diskussion om EU-strategins betydelse.

För att lösa de belysta problemen efterlyses inte sällan åtgärder i form av strategier och ramverk. EU-strategin är förvisso en strategi, men med generella riktlinjer och mål. Åtgärder likt kunskapshöjande arbete och forskning mellan medlemsstaterna presenteras i EU-strategin. Vidare poängteras företagens ansvar i sammanhanget. EU-strategin föreslår att företag vidtar interna kontroller och processer för att möjliggöra en transparent AI-användning. En större ansvarsbörda vid AI-användning och vid data som appliceras på AI-applikationer åläggs företagen. De strategier och ramverk som efterfrågas är sannolikt mer konkreta branschöverenskommelser och direkta riktlinjer för företag att tillgå, likt ”checklistor” vid hanteringen av AI. Vad EU-strategin kommer att leda till kan ingen i dagsläget svara på. Framtiden får utvisa om EU-strategin leder fram till ett AI-regelverk, eller slutar vid en självreglering eller enbart resulterar i instruktioner och riktlinjer.

För att konkretisera och besvara den andra delfrågeställningen följer ett par meningar om min personliga uppfattning av EU-strategins betydelse i sammanhanget. EU-strategin framhäver vikten av att värna om och upprätthålla de grundläggande europeiska värdena vid den framtida utvecklingen och hanteringen av AI. Vid både en explicit och implicit läsning av EU-strategin syftar den till att stärka skyddet för slutkonsumenten, den enskilda individen, som brukar AI-lösningen. I realiteten driver USA och Kina AI-utvecklingen medan Europa avser att använda omvärldens framställda AI-applikationer. En viktig betydelse av

EU-strategin är således enligt mig att strategin uppmärksammar omvärlden på vikten av EU:s grundvärden och vikten av att skapa och integrera ett skyddsnet för enskilda individen när AI-applikationer framställs. Denna värdeskapande betydelse av EU-strategin är välkomnat ur ett integritetsperspektiv.

6.4 Avslutande reflektioner

Uppsatsen har granskat profilering och automatiserat beslutsfattande innefattande AI ur ett integritetsperspektiv. Problem och konsekvenser har belysts och de positiva effekterna har medvetet lämnats utanför redogörelsen. Huruvida digitaliseringen och utvecklingen av AI som möjliggjort nutida profilering och automatiserat beslutsfattande slutligen är till övervägande nytta eller skada lämnar därför jag okommenterat. Det är omöjligt att ge en enhetlig och korrekt kommentar. Ett eventuellt ställningstagande från min sida hade skiljt sig åt beroende på utifrån vilket perspektiv det analyserats och beroende på vilka lösningsförslag som använts.

Integritetskommitténs beskrivning av begreppet *integritet* och dess grundläggande skyddsvärde markerar en rätt för den enskilde individen till egna privata tankar, en rätt att bestämma vilken personlig information som ska tilldelas vem och hur informationen får användas. Mot bakgrund av redogörelsen är integritetsproblemen vid profilering och automatiserat beslutsfattande dubbel. För det första har digitaliseringen resulterat i ökad datainsamling, vilket betyder att det föreligger en ökad kännedom om och användning av enskilda individers personuppgifter. För det andra har utvecklingen av AI inom profilering möjliggjort skapandet av nya personuppgifter. Dessa uppgifter har den enskilde inte själv valt att dela med sig av utan som framställts vid sammanställning av stora datamängder och med hjälp av algoritmer. Sammantaget får integritetsproblemen därför dubbla konsekvenser, varpå den andra och sistnämnda konsekvensen

sannolikt är den mest problematiska. Denna problematik riskerar att underminera enskilda individers lagstadgade rättigheter i GDPR och det grundläggande skyddet för den personliga integriteten, särskilt rätten till självbestämmande.

Eller omkullkastas ovanstående slutsats av följande reflektion? Integritet är som redovisats subjektivt och förändras med samtiden. Kan synen på den personliga integriteten förskjutits och förändrats, i takt med samtidens teknikutveckling och vårt frivilliga bidragande till offentlighetens åskådning av våra liv på internet och sociala medier, att de integritetsproblem som ovan belysts normaliserats och inte ses som integritetskränkande? Jag ställer mig kritisk till nämnda resonemang men anser att det likväl tåls att fundera över.

Avslutningsvis välkomnar jag forskning och utredning med en tvärvetenskaplig utgångspunkt. Juridiska problem och efterlevnad av lagstadgade fundamentala rättigheter vid algoritmiska processer försvinner inte genom att problemen döljs i en matematisk dimma. Efterlevnad av lagstiftning, i denna framställning GDPR, löses inte enbart av en i teorin välutformad reglering. Det har granskningen av GDPR:s reglering av profilering och automatiserat beslutsfattande med beaktan av AI:s utveckling och involvering klarlagt.

Käll- och litteraturförteckning

Litteratur

Alpaydin, Ethem (2020), *Introduction to machine learning*, upplaga 4, The MIT Press, Cambridge, England. [cit. Alpaydin (2020)]

Anrig, Bernhard, Browne, Will och Gasson, Mark (2008), 'The Role of Algorithms in Profiling', i: Hildebrandt, Mireille och Gutwirth, Serge (red.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Science + Business Media B.V, Dordrecht, s. 65–87. [cit. Anrig, Browne och Gasson 'The Role of Algorithms in Profiling' (2008)]

Bakardjieva Engelbrekt, Antonina, Michalski, Anna och Oxelheim, Lars (2020) (red.), *EU och teknologiskiftet*, Santérus förlag, Stockholm. [cit. Bakardjieva Engelbrekt, Michalski och Oxelheim (2020)]

Benoist, Emmanuel (2008), 'Collecting Data for the Profiling of Web Users', i: Hildebrandt, Mireille och Gutwirth, Serge (red.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Science + Business Media B.V, Dordrecht, s. 169–184. [cit. Benoist 'Collecting Data for the Profiling of Web Users' (2008)]

Burrell, Jenna (2016), 'How the machine 'thinks': Understanding opacity in machine learning algorithms', i: *Big Data och Society*, Vol. 3, Nr. 1. [cit. Burrell 'How the machine 'thinks': Understanding opacity in machine learning algorithms' (2016)]

Canhoto, Ana och Backhouse, James (2008), 'General Description of the Process of Behavioural Profiling', i: Hildebrandt, Mireille och Gutwirth, Serge (red.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Science + Business Media B.V, Dordrecht, s. 47–63.

[cit. Canhoto and Backhouse 'General Description of the Process of Behavioural Profiling' (2008)]

Dahlman, Christian (2019), 'Begreppet rättskälla', i: Dahlman, Christian och Wahlberg, Lena (red.), *Juridiska grundbegrepp: en vänbok till David Reidhav*, upplaga 1, Studentlitteratur, Lund, s. 55–74. [cit. Dahlman 'Begreppet rättskälla' (2019)]

Franklin, Stan (2014), 'History, motivations, and core themes', i: Frankish, Keith och Ramsey, William M. (red.), *The Cambridge handbook of artificial intelligence*, Cambridge University Press, Cambridge, s. 15-33. [cit. Franklin 'History, motivations, and core themes' (2014)]

Frydlinger, David, Edvardsson, Tobias, Olstedt Carlström, Caroline och Beyer, Sandra (2018), *GDPR: juridik, organisation och säkerhet enligt dataskyddsförordningen*, upplaga 1, Norstedts juridik, Stockholm. [cit. Frydlinger m.fl. (2018)]

Gräns, Minna (2018), 'Allmänt om användningen av andra vetenskaper inom juridiken', i: Nääv, Maria och Zamboni, Mauro (red.), *Juridisk metodlära*, upplaga 2, Studentlitteratur, Lund, s. 429–441. [cit. Gräns 'Allmänt om användningen av andra vetenskaper inom juridiken' (2018)]

Gröning, Lotta (2014), 'Inledning', i: Almqvist, Kurt och Linder, P.J. Anders (red.), *Integritet*, Axel och Margareta Ax:son Johnsons stiftelse för allmännyttiga ändamål, Stockholm, s. 7–8. [cit. Gröning 'Inledning' (2014)]

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

Hildebrandt, Mireille och Gutwirth, Serge (2008), 'Concise Conclusions: Citizens Out of Control', i: Hildebrandt, Mireille och Gutwirth, Serge (red.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer

Science + Business Media B.V, Dordrecht, s. 365–368. [cit. Hildebrandt och Gutwirth 'Concise Conclusions: Citizens Out of Control' (2008)]

Hildebrandt, Mireille och Gutwirth, Serge (2008), 'General Introduction and Overview', i: Hildebrandt, Mireille och Gutwirth, Serge (red.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Science + Business Media B.V, Dordrecht, s. 1–13. [cit. Hildebrandt och Gutwirth 'General Introduction and Overview' (2008)]

Holtz, Hajo Michael (2018), 'Den nya allmänna dataskyddsförordningen – några anmärkningar', i: *SvjT* s. 240–264. [cit. Holtz 'Den nya allmänna dataskyddsförordningen – några anmärkningar' (2018)]

Isberg, Magnus och Eliason, Marianne, *Grundlagarna*, Norstedts Juridik, Stockholm, version 3A, uppdaterad den 1 januari 2019 (JUNO). [cit. Isberg och Eliason *Grundlagarna* (uppdaterad 1 januari 2019, JUNO)]

Janlert, Lars-Erik (2015), *Tänkande och beräkning: en inledning till datavetenskap och kognitionsvetenskap*, upplaga 2, Studentlitteratur, Lund. [cit. Janlert (2015)]

Jareborg, Nils (2004) 'Rättsdogmatik som vetenskap', i: *SvJT* s. 1–10. [cit. Jareborg 'Rättsdogmatik som vetenskap' (2004)]

Jermsten, Henrik, *Regeringsformen (1974:152) kommentar till 2 kap. 6 §*, Lexino, uppdaterade den 1 januari 2019 (JUNO). [cit. Jermsten *Regeringsformen, kommentar till 2 kap. 6 §* (uppdaterad 1 januari 2019, JUNO)]

Jordan, I. Michael (2019), 'Artificial Intelligence – The Revolution Hasn't Happened yet', i: *Harvard Data Science Review*, Creative Commons Attribution (CC BY 4.0) International license. [cit. Jordan 'Artificial Intelligence – The Revolution Hasn't Happened yet' (2019)]

Kleineman, Jan (2018), 'Rättsdogmatisk metod', i: Nääv, Maria och Zamboni, Mauro (red.), *Juridisk metodlära*, upplaga 2, Studentlitteratur, Lund, s. 21–46. [cit. Kleineman, 'Rättsdogmatisk metod' (2018)]

Larsson, Peter (2018), 'Sju nyanser av transparens: Om artificiell intelligens och ansvaret för digitala plattformars samhällspåverkan', i: Andersson Schwarz, Jonas och Larsson, Peter (red.) *Plattformssamhället: Den digitala utvecklingens politik, innovation och reglering*, Fores, Spektar, Bulgarien, s. 277–313. [cit. Larsson 'Sju nyanser av transparens: Om artificiell intelligens och ansvaret för digitala plattformars samhällspåverkan' (2018)]

Larsson, Peter (2019), 'Artificiell intelligens som normativ samhällsutmaning: partiskhet, ansvar och transparens', i: Banakar, Reza, Dahlstrand, Karl och Ryberg-Welander, Lotti (red.), *Festskrift till Håkan Hydén*, Juristförlaget, Lund, s. 339–370. [cit. Larsson 'Artificiell intelligens som normativ samhällsutmaning: partiskhet, ansvar och transparens' (2019)]

Larsson, Stefan, Anneroth, Mikael, Felländer, Anna, Felländer-Tsai, Li, Heintz, Fredrik, Cedering Ångström, Rebecka och Åström, Fredrik (2019), 'HÅLLBAR AI: Inventering av kunskapsläget för etiska, sociala och rättsliga utmaningar med artificiell intelligens', AI Sustainability Center, Stockholm. [cit. Larsson m.fl. 'HÅLLBAR AI: Inventering av kunskapsläget för etiska, sociala och rättsliga utmaningar med artificiell intelligens' (2019)]

Liebenau, Jonathan och Backhouse, James (1990), *Understanding information: an introduction*, upplaga 1, Macmillan, Basingstoke. [cit. Liebenau och Backhouse (1990)]

Lundqvist, Ulf (2020), 'Artificiell Intelligens – rättsordning och rättstillämpning', i: *SvJT* s. 382–415. [cit. Lundqvist 'Artificiell Intelligens – rättsordning och rättstillämpning' (2020)]

Mireille Hildebrandt (2008), 'Defining Profiling: A New Type of Knowledge?', i: Hildebrandt, Mireille och Gutwirth, Serge (red.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Science + Business Media B.V, Dordrecht, s. 17–45. [cit. Hildebrandt 'Defining Profiling: A New Type of Knowledge?' (2008)]

Mittelstadt, Brent Daniel, Allo, Patrick, Taddeo, Mariarosaria, Wachter, Sandra och Floridi, Luciano (2016), 'The ethics of algorithms: Mapping the debate', i: *Big Data och Society*, Vol. 3, Nr. 2. [cit. Mittelstadt m.fl. 'The ethics of algorithms: Mapping the debate' (2016)]

Mohanty, Hrushiksha (2015), 'Big Data: An Introduction', i: Mohanty, Hrushiksha, Bhuyan, Prachet, Chenthati, Deepak (red.), *Big Data: A Primer*, Springer India, Indien, s. 1–28. [cit. Mohanty 'Big Data: An Introduction' (2015)]

Naarttijärvi, Markus (2017), 'Rättsstatlighet och algoritmiska svarta lådor', i: Edström, Örjan, Lindholm, Johan, Mannelqvist, Ruth (red.), *Jubileumsskrift till Juridiska institutionen 40 år*, Umeå universitet, Umeå, s. 245–259. [cit. Naarttijärvi 'Rättsstatlighet och algoritmiska svarta lådor' (2017)]

Pasquale, Frank (2015), *The black box society: the secret algorithms that control money and information*, Harvard University Press, Cambridge. [cit. Pasquale (2015)]

Reichel, Jane (2018), 'EU-rättslig metod', i: Nääv, Maria och Zamboni, Mauro (red.), *Juridisk metodlära*, upplaga 2, Studentlitteratur, Lund, s. 109–142. [cit. Reichel 'EU-rättslig metod' (2018)]

Sandgren, Claes (2005), 'Är rättsdogmatiken dogmatisk?' i: *Tidsskrift för rettsvetenskap* s. 648–656. [cit. Sandgren 'Är rättsdogmatiken dogmatisk?' (2005)]

Seipel, Peter (2004), *Juridik och IT: introduktion till rättsinformatiken*, upplaga 8, Norstedts juridik, Stockholm. [cit. Seipel (2004)]

Skarhed, Anna (2014), 'JK och den personliga integriteten' i: Almqvist, Kurt och Linder, P.J. Anders (red.), *Integritet*, Axel och Margaret Ax:son Johnsons stiftelse för allmännyttiga ändamål, Stockholm, s. 9–15. [cit. Skarhed 'JK och den personliga integriteten' (2014)]

Turban, Efraim, Aronson, Jay E. och Liang, Ting-Peng (2005), *Decision support systems and intelligent systems*, upplaga 7, Pearson Prentice Hall, U.S.A. [cit. Turban, Aronson och Liang (2005)]

van der Hof, Simone och Prins, Corien (2008), 'Personalisation and its Influence on Identities, Behaviour and Social Values', i: Hildebrandt, Mireille och Gutwirth, Serge (red.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Science + Business Media B.V, Dordrecht, s. 111–127. [cit. van der Hof och Prins 'Personalisation and its Influence on Identities, Behaviour and Social Values' (2008)]

Wachter, Sandra, Mittelstadt, Brent och Floridi, Luciano (2017), 'Why a right to explanation of automated decision-making does not exist in the general data protection regulation', i: Kuner, Christopher, Sventesson, Dan Jerker B., Cate, Fred H., Lynskey, Orla och Millard, Christopher (red.) *International Data Privacy Law*, 7(2), s. 76–99. [cit. Wachter m.fl. 'Why a right to explanation of automated decision-making does not exist in the general data protection regulation' (2017)]

Wahlgren, Peter (2014), *Lagstiftning: rationalitet, problem, möjligheter*, upplaga 2, Jure, Stockholm. [cit. Wahlgren (2014)].

Öman, Sören, *Dataskyddsförordningen (GDPR) m.m.: en kommentar*, Norstedts juridik, Stockholm, version 1A, uppdaterad den 29 februari 2020 (JUNO). [cit. Öman, *Dataskyddsförordningen en kommentar* (uppdaterad 29 februari 2020, JUNO)]

Källor

Offentligt tryck

Utredningsbetänkanden

SOU 2016:41 Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommittén. [cit. SOU 2016:41]

SOU 2017:52 Så stärker vi den personliga integriteten. [cit. SOU 2017:52]

Propositioner och regeringsskrivelser

Prop. 2009/10:80 En reformerad grundlag. [cit. prop. 2009/10:80]

Regeringskansliet (2018), 'Nationell inriktning för artificiell intelligens', Näringsdepartementet. [cit. Regeringskansliet (2018) 'Nationell inriktning för artificiell intelligens']

EU-rättsligt material

Kommissionens meddelande 'Artificiell intelligens för Europa', KOM(2018) 237 slutlig. [cit. Kommissionens meddelande 'Artificiell intelligens för Europa' (2018)]

Förslag till Rådets beslut om bemyndigande för medlemsstaterna att i Europeiska unionens intresse ratificera protokollet om ändring av Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (CETS nr 108), KOM(2018) 449 slutlig. [cit. Förslag till Rådets beslut om skydd för enskilda vid automatisk databehandling av personuppgifter (2018)]

Special Eurobarometer 487a (2019) 'The General Data Protection Regulation Report', EU-kommissionen. [cit. Special Eurobarometer 487a (2019)]

Kommissionens meddelande 'En EU-strategi för data', KOM(2020) 66 slutlig. [cit. Kommissionens meddelande 'En EU-strategi för data' (2020)]

Kommissionens meddelande 'Att forma EU:s digitala framtid', KOM(2020) 67 slutlig. [cit. Kommissionens meddelande 'Att forma EU:s digitala framtid' (2020)]

Vitbok om artificiell intelligens - en EU-strategi för spetskompetens och förtroende, KOM(2020) 65 slutlig. [cit. Vitbok om artificiell intelligens (2020)]

Soft law

Artikel 29-arbetsgruppen för skydd av personuppgifter, 'Yttrande 4/2007 om begreppet personuppgifter', WP136, antagna den 20 juni 2007. [cit. Artikel 29-gruppen om begreppet personuppgifter (2007)]

Artikel 29-arbetsgruppen för uppgiftsskydd, 'Riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/67', WP251, antagna den 3 oktober 2017, senast granskade och antagna den 6 februari 2018. [cit. Artikel 29-gruppen om automatiserat individuellt beslutsfattande och profilering enligt GDPR (2017)]

Övrigt

DECODO, <<https://www.decodeproject.eu/>>, besökt den 28 oktober. [cit. DECODE]

Duhigg, Charles, 'How Companies Learn Your Secrets', <<https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>>, uppdaterade den 16 februari 2012, besökt den 17 oktober 2020. [cit. Duhigg 'How Companies Learn Your Secrets' (uppdaterad 16 februari 2012)]

EU-kommissionen, 'Algorithmic Awareness-Building', <<https://ec.europa.eu/digital-single-market/en/algorithmic-awareness-building>>, uppdaterad den 9 juni 2020, besökt den 3 november 2020. [cit.

EU-kommissionen, 'Algorithmic Awareness-Building' (uppdaterad 9 juni 2020)]

European Union Agency For Network and Information Security 'A tool on Privacy Enhancing Technologies (PETs) knowledge management and maturity assessment', <<https://www.enisa.europa.eu/publications/pets-maturity-tool>>, publicerad den 7 mars 2018, besökt den 12 december 2020. [cit. European Union Agency For Network and Information Security 'A tool on Privacy Enhancing Technologies (PETs) knowledge management and maturity assessment' (2018)]

Haider, Jutta och Sundin, Olof, 'Internetguide #46 Algoritmer: Så påverkar de din vardag' (2016) <<https://internetstiftelsen.se/docs/Algoritmer.pdf>>, Internetstiftelsens internetguide, nr 46, besökt den 20 oktober 2020. [cit. Haider och Sundin 'Algoritmer: Så påverkar de din vardag' (2016)]

Marshall, Andrew, Rojas, Raul, Stokes, Jay och Brinkman, Donald, 'Framtidens säkra artificiella intelligens och maskininlärning med Microsoft' (2018) <<https://docs.microsoft.com/sv-se/security/engineering/securing-artificial-intelligence-machine-learning>>, besökt den 10 november 2020. [cit. Marshall m.fl. 'Framtidens säkra artificiella intelligens och maskininlärning med Microsoft' (2018)]

McKinsey Analytics, 'An executive's guide to AI' (2018), <<https://www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Analytics/Our%20Insights/An%20executives%20guide%20to%20AI/An-executives-guide-to-AI.ashx>>, besökt den 5 oktober 2020. [cit. McKinsey Analytics 'An executive's guide to AI' (2018)]

MyData Global, <<https://mydata.org/>>, besökt den 28 oktober. [cit. MyData]

Nationalencyklopedin, 'data mining', <<http://www.ne.se/uppslagsverk/encyklopedi/lång/data-mining>>, besökt den 21 oktober 2020. [cit. Nationalencyklopedin 'data mining']

RadicalxChange, <<https://radicalxchange.org/>>, besökt den 28 oktober. [cit. RadicalxChange]

Solid, <<https://solid.mit.edu/>>, besökt den 28 oktober. [cit. Solid]

Rättsfallsförteckning

EU-domstolen

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

C-434/16 *Peter Nowak mot Data Protection Commissioner*,
EU:C:2017:994. [cit. C-434/16 Peter Nowak mot Data Protection
Commissioner]

Europadomstolen

Application no. 6289/73 *Airey mot Ireland*, dom den 9 oktober 1979. [cit.
Airey mot Ireland]

Application no. 8978/80, *X och Y mot Nederländerna*, dom den 26 mars
1985. [cit. *X och Y mot Nederländerna*]

Application no. 5786/08, *Eliza Söderman mot Sverige*, dom den 12
november 2013. [cit. *Eliza Söderman mot Sverige*]