JURIDISKA FAKULTETEN
vid Lunds universitet

Felicia Johansson

Profilering och Big Data

Hur dataskyddsförordningen och teknologin hamnar på kollisionskurs

LAGF03 Rättsvetenskaplig uppsats

Kandidatuppsats på juristprogrammet
15 högskolepoäng

Handledare: Karol Nowak

Termin: HT 2019

Innehåll

Summary

Today, technological advancements enable the constant collection and analysation of extensive amounts of data as well as decision making based on that processing. This undeniably holds true for the processing of personal data to create customer profiles for marketing purposes.

The General Data Protection Regulation is the EU's response to the increased possibilities to draw far-reaching conclusions about individuals from personal data. The regulation's aim is to hand the control of personal data back to the individuals and, by doing so, facilitate economic growth in the EU's internal market. In this essay, two of the regulation's fundamental principles – purpose limitation and data minimisation – as well as the prohibition to process special categories of personal data are examined in relation to personal data in a big data context. The purpose of the scrutiny is to evaluate if the regulation is compatible with the digital, big data driven society we live in. The essay also examines what private companies involved in customer profiling should keep in mind regarding the regulation's rules and principles.

The essay shows that the General Data Protection Regulation to a large extent limits the possibilities to lawfully carry out big data processing for marketing purposes, by aiming to give individuals strong privacy protection. The EU data protection is not adapted to how personal data is currently used. Furthermore, some evidence shows that the current legislation does not give individuals the protection the EU aims for, even when the regulation is complied with during big data processing. Even though it will prove difficult for private companies to lawfully carry out large scale processing of personal data, it is suggested that companies show restraint if they do decide to process customers' personal data for marketing purposes. The aim should be to preserve costumers trust.

Sammanfattning

Tekniska lösningar möjliggör idag att omfattande mängder data ständigt samlas in, analyseras och används som beslutsunderlag. Inte minst gäller detta behandling av personuppgifter för att skapa kundprofiler i marknadsföringssyfte.

Dataskyddsförordningen är EU:s respons på de ökade möjligheterna att dra långgående slutsatser om enskilda individer utifrån personuppgifter. Lagens syfte är att åter ge individer kontroll över sina personuppgifter, vilket i längden även ska främja ekonomisk tillväxt inom unionen. I uppsatsen utreds hur två av dataskyddsförordningens grundläggande principer – ändamålsbegränsning och uppgiftsminimering – samt förbudet mot att behandla känsliga personuppgifter förhåller sig till big data när denna data är hänförlig till personuppgifter. Syftet med utredningen är att utvärdera om lagstiftningen är förenligt med det digitaliserade, big data drivna samhället vi idag lever i. Hur privata företag engagerade i kundprofilering ska förhålla sig till bestämmelserna och de underliggande principerna undersöks också.

Uppsatsen visar att dataskyddsförordningen, genom målsättningen att ge individer långtgående integritetsskydd, i stor utsträckning inskränker möjligheterna att utföra lagenlig behandling av big data i marknadsföringssyfte. Dataskyddsbestämmelserna är inte anpassade till hur personuppgifter faktiskt tillvaratas. Visst stöd ges dessutom för att nuvarande lagstiftning vid behandling av big data inte ger individer det skydd som eftersträvas av EU, även när regelverket följs. Även om lagenlig personuppgiftsbehandling för företag kan vara svåruppnått, föreslås viss återhållsamhet om behandling av kunders personuppgifter ändock genomförs. Att bevara kunders tillit bör utgöra en ledstjärna.

Förkortningar

Artikel 29-gruppen	Europeiska Unionens rådgivande och oberoende organ för dataskyddsfrågor. Efter införande av dataskyddsförordningen ersattes organet av European Data Protection Board (edpb). På de områden dataskyddsförordningen är oförändrad i förhållande till den äldre lagstiftningen innehar artikel 29-gruppens rådgivning fortfarande relevans.
Dataskyddsdirektivet	Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.
Dataskyddsförordningen	Europaparlamentets och rådets förordning (eu) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/eg. Förkortad GDPR på engelska.
EESC	EU:s Europeiska ekonomiska och sociala kommitté.
EKMR	Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna
ENISA	Europeiska unionens byrå för nät- och informationssäkerhet.
ePrivacy-direktivet	Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och

	integritetsskydd inom sektorn för elektronisk kommunikation.
EU	Europeiska unionen.
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna.
FEUF	Fördraget om Europeiska unionens funktionssätt.

1 Inledning

1.1 Bakgrund

På bara några decennier har data gått från att vara dyr och begränsad till att finnas tillgänglig för alla som så önskar i outtömliga mängder. Jämte denna utveckling har artificiell intelligens främjat tillvaratagandet av dessa enorma datauppsättningar. Big data, det vill säga stora mängder data som kräver automatiska processer för att behandlas, har blivit ett vardagsord.

Massbehandlingen av information om individer och profilering i syfte att individanpassa tjänster och produkter är en av följderna med en utveckling mot ett allt mer datadrivet samhället. Googles före detta VD, Eric Schmidt, har uttalat att "we know roughly who you are, roughly what you care about, roughly who your friends are".[1] Privatägda företag i form av klädesaffärer och till och med matbutiker riktar sina produktkampanjer till de kunder som tack vare big data kan förutses ha störst intresse av de specifika varorna.

Samtidigt har ikraftträdandet av EU:s General Data Protection Regulation, mer känt som GDPR eller dataskyddsförordningen, undgått få. Dataskyddsförordningen är EU:s respons på de tekniska framsteg som på kort tid har gjorts kring informationsbehandling och utgör unionens huvudsakliga lagstiftning för att skydda individers personuppgifter.

Mot bakgrund av det nya datadrivna och rättsliga landskapet väcks givetvis frågan om personlig integritet och kontroll över personuppgifter. Än mer än så, uppstår en mängd frågor om huruvida behandling av big data över huvud taget kan förenas med, stävjas eller främjas av lagstiftarens penna.

[1] Cit. Deans, Jason, publicerad 18 augusti 2010, https://www.theguardian.com/media/2010/aug/18/google-facebook, The Guardian, besökt 23 december 2019

1.2 Syfte och frågeställning

Uppsatsen syftar till att kritiskt granska om EU:s dataskyddsregler lämpar sig i ett datadrivet samhälle. Härvidlag syftar uppsatsen mer specifikt till att utvärdera om de principer som är vägledande för dataskyddsförordningen går att upprätthålla när de möter den omfattande insamling och bearbetningen av personuppgifter som big data utgör.

Uppsatsen har även som mål att undersöka vilken inverkan dataskyddsförordningen har på privata företag som ämnar använda sig av big data i marknadsföringssyfte. Av denna anledning är företags användning av information om konsumenter ett genomgående tema i uppsatsen.

Frågeställningen är således:

- Kan behandling av big data, när denna data hänför sig till personuppgifter som behandlas i syfte att fatta beslut som påverkar enskilda individer, samexistera med EU:s dataskyddsförordning?
- Hur bör privata företag som utför kundprofilering förhålla sig till dataskyddsbestämmelserna?

1.3 Avgränsning

Uppsatsen utgår från ett EU-perspektiv och av den anledningen behandlas endast lagstiftningen på unionsgemensam nivå. Tid och utrymme har saknats för att utreda ett ännu bredare, internationellt perspektiv. Enbart dataskyddsförordningen behandlas. Det har saknats utrymme att nämna annan EU-lagstiftning om dataskydd, exempelvis ePrivacy-direktivet och dess förväntade efterträdare ePrivacy-förordningen.

Fokus i denna uppsats ligger uteslutande på de fall där big data används i syfte att påverka enskilda individer genom behandling av deras personuppgifter. Personuppgiftsbehandling i statistiskt syfte beskrivs inte. Sådan

personuppgiftsbehandling som utförs av stater exkluderas och uppsatsen riktar i stället in sig på privata aktörers behandling av big data.

Ingen närmare förklaring ges av de underliggande tekniska lösningarna till behandling av big data, då detta faller utanför denna juridiska uppsats syfte. Varifrån data samlas in behandlas inte heller i detalj.

Det tredje och fjärde kapitlet i uppsatsen belyser tre aspekter. Dessa aspekter är av intresse för att förstå EU:s dataskyddsförordnings koppling till big data och marknadsföring genom behandlingen av big data. Avgränsningen har gjorts utifrån vad som är mest förekommande i doktrinen samt utifrån vad som tydligast framhäver problematiken med att reglera big data. Artikel 22 dataskyddsförordningen utvecklas inte, då tröskeln för att denna artikel ska vara tillämplig är högt ställd.[2] Det har saknats utrymme att ingående beskriva de lagliga grunderna för behandling, exempelvis samtycke, som finns stadgade i artikel 6 dataskyddsförordningen.[3] Generellt kan anges att möjligheterna att erhålla giltigt samtycke är något mer begränsad vid behandling av big data än annan personuppgiftsbehandling.[4]

1.4 Metod, material och perspektiv

I uppsatsen används rättsdogmatisk metod för att tolka gällande rätt med stöd av de allmänt accepterade rättskällorna.[5] Den rättsdogmatiska metoden har som syfte att finna lösningar på konkreta rättsliga problem genom att tillämpa rättsregler.[6] Dataskyddsförordningen utgör EU-lagstiftning och följaktligen

[2] Artikel 29-gruppen, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 2018, s. 21; Paterson, Moira och McDonagh, Maeve, *data protection in an era of big data: the challenges posed by big personal data*, Moash University Law Review, Volume 44 Issue 1, 2018, s. 23.
[3] För en sammanfattad beskrivning av berättigat intresse som laglig grund vid kundprofilering, se Frydlinger, David, Edvardsson, Tobias, Olstedt Carlström, Caroline, Beyer, Sandra, *GDPR: juridik, organisation och säkerhet enligt datasskyddsförordningen*, Nordsteds juridik, 2018, s 181.
[4] Paterson and McDonagh, s. 18.
[5] Nääv, Maria och Zamboni, Mauro, *Juridisk metodlära*, 2 uppl., Studentlitteratur, 2018, s. 21.
[6] Nääv och Zamboni, s. 21.

tolkas lagstiftningen i enlighet med EU-metoden. Bland annat innehar soft law, det vill säga icke-bindande juridiska dokument framtagna av EU-organ, en framträdande roll.[7] Soft law besitter en i praktiken normerande effekt.[8] I stället för förarbeten utarbetade på svenskt vis, presenteras i EU-rättsakter en preambel med icke-bindande men auktoritativa uttalanden om rättsaktens mål och syften.[9] Allmänna principer får stort utrymme inom EU.[10]

Materialet består främst av lagtext, vägledande uttalanden från EU-organ samt doktrin. Skälen i dataskyddsförordningens preambel används främst för att beskriva dess ändamål. Eftersom dataskyddsförordningen är relativt ny och reglerna som behandlas till viss del är oförändrade används i stor utsträckning artikel 29-gruppens uttalanden om dataskyddsdirektivet. Rättsfall hänvisas till i begränsad omfattning.

Uppsatsen handlar om samspelet mellan dagens datadrivna samhälle och juridiken, vilket innebär att ämnet faller under rättsinformatik.[11] Det perspektiv som präglar uppsatsen är kritik mot dataskyddets bristande anpassning till den marknadsmässiga nyttan av big data, även om individers intressen inte förbises i uppsatsen.

1.5 Forskningsläge

Dataskyddsförordningen har varit i kraft i drygt ett år och ett halvt år och omfattande klargöranden från praxis likväl som doktrin saknas. Big data generellt och kundprofilering specifikt är dessutom ett ungt fenomen som fortfarande befinner sig i en utvecklingsfas. Praxis och doktrin om big data i förhållande till EU:s dataskyddsreglering är därmed begränsad, men på

[7] Nääv och Zamboni, s. 127f.
[8] Nääv och Zamboni, s. 128.
[9] Bernitz, Ulf, Carlsson, Mia, Heuman, Lars, Leijonhufvud, Madeleine, Magnusson Sjöberg, Cecilia, Seipel, Peter, Warnling-Nerep, Wiweka och Vogel, Hans-Heinrich, *finna rätt: juristens källmaterial och arbetsmetoder*, 14 uppl., Wolters Kluwer, 2017, s.113.
[10] Nääv och Zamboni, s. 122 och 126; Bernitz m.fl., s. 67.
[11] Magnusson Sjöberg, Cecilia, *Rättsinformatik: juridiken i det digitala informationssamhället*, uppl. 3, Studentlitteratur, 2018, s. 19.

uppsving. Mayer-Schönberger, Tene och Zarsky är några av de forskare som ofta återkommer i doktrin om omfattande personuppgiftsbehandling.

1.6 Disposition

Efter inledningen följer ett kapitel som förklarar vad big data och kundprofilering är samt hur kundprofilering används. Därefter, i tredje kapitlet, beskrivs två principer och ytterligare en bestämmelse i dataskyddsförordningen som har inverkan på big data. I fjärde kapitel kopplas de i föregående kapitel framställda aspekterna till big data och kundprofilering. Upplägget i fjärde kapitlet innebär att ändamålsbegränsning och uppgiftsminimering – två principer som visar sig gå hand i hand – först behandlas. Utläggningen övergår sedan till känsliga personuppgifter och mer utrymme ges åt individanpassad marknadsföring.

En analys om lagstiftningens förenlighet med big data och implikationerna för individers personliga integritet samt för företag som engagerar sig i riktad marknadsföring följer av uppsatsens femte och sista kapitel. I femte kapitlet besvaras de frågor som ställts i avsnitt 1.2.

2 Big data – vad och varför?

2.1 Big data som begrepp

Inledningsvis bör det noteras att big data inte utgör en legal term. Därtill saknas en enhetlig definition.[12] Laney har dock formulerat en klassisk definition av begreppet.[13] Han beskriver big data som tredimensionellt, utifrån begreppen ”volume”, ”velocity” och ”variety”[14], numera allmänt kända som ”de tre V:na”.[15] Big data kan utifrån Laneys begrepp förstås som en mycket omfattande och rörlig samling data, hämtad från ett brett omfång av källor, vilken kräver automatiska processer som arbetar i realtid för att utröna användbart material.

Vidare kan big data förstås som en trestegsprocess: insamling, analys och slutligen tillvaratagande av resultaten funna genom analysen.[16] I uppsatsen används fortsättningsvis begreppet ”behandling” för att beskriva samtliga steg i big datas livscykel, då det speglar den beskrivning av termen som går att finna i artikel 4(2) dataskyddsförordningen.

De ökade möjligheterna att genomföra avancerade analyser på data samt denna datas komposition särskiljer big data från annan data.[17] Härutöver medför de tekniska lösningar som ligger till grund för big datas framgång att automatiserade beslut kan tas med avstamp i befintliga data, i motsats till att hypoteser om vad som kommer kunna utrönas sätter den yttersta ramen för

[12] Corrales, Marcelo, Fenwick, Mark, Forgó, Nikolaus, *New Technology, Big Data and the Law*, Springer, 2017 s. 20; Information Commissioner’s Office, *Big data, artificial intelligence, machine learning and data protection*, 2.2 uppl., 2017, s. 6.
[13] Laney, Doug, *3D Data Management: Controlling Data Volume, Velocity and Variety*, META group, 2001.
[14] Laney, s. 1f.
[15] Se exempelvis European Union Agency For Network And Information Security (ENISA), *Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics*, 2015, s.10; Corrales m.fl., s. 20f.
[16] Corrales m.fl., s. 21f.
[17] ENISA, s. 14.

insamlingen.[18] Den senare processen omnämns på engelska som ”data mining”[19] och översatt till svenska som ”datautvinning”.

2.2 Kundprofilering som begrepp

Big data möjliggör på grund av sin omfattning profilering. Även före big data slog igenom har profilering förekommit, men automatiska processer har främjat dess tillämpning.[20] Profilering avser den automatiska behandlingen av personuppgifter som består i bedömning av personliga egenskaper hos en fysisk person. Genom profileringen analyseras personliga aspekter och framtida ageranden och intressen kan förutses. I Artikel 4(4) dataskyddsförordningen radas ett antal aspekter upp som tas hänsyn till vid profilering, däribland hälsa, personliga preferenser, vistelseort och förflyttningar.[21]

2.3 Exempel på hur kundprofilering tillämpas av privata företag

För privata aktörers del har kundprofilering en framträdande roll.[22] Företag har allt större möjlighet att skräddarsy upplevelsen till varje potentiell konsument[23] och därmed öka chanserna att denne köper företagets tjänster eller varor.

[18] Mayer-Schönberger, Viktor och Padova, Yann. *Regime Change? Enabling Big Data Throug Europe's New Data Protection Regulation*, the Columbia Science & Technology Law Review volume XVII, 2016, s. 319.
[19] Hildebrandt, Mireille & Gutwirth, Serge, *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer, 2008 s. 18.
[20] Hildebrandt, s.23f och s. 30f.
[21] För en mer utförlig uppradning av aspekter som kan utrönas via big data profilering, se Gutwirth, Serge, Leenes, Ronald, De Hert, Paul, Poullet, Yves, *European Data Protection: In Good Health?*, Springer, 2012 s. 56.
[22] Frydlinger m.fl., s. 176.
[23] Konsument definieras här som en fysisk person som i huvudsak handlar för privat bruk, jfr 1 § tredje stycket konsumentköplagen (1990:932).

Ökade intäkter har rapporterats som en följd av implementering av riktade försäljningsstrategier.[24] Dessutom rapporteras i ett flertal omfattande studier, dock utfärdade av främst internetbaserade teknikföretag, att konsumenter i stor utsträckning förväntar sig individanpassad marknadsföring.[25] Konsumenters efterfrågan av individanpassad marknadsföring är dock inte slutgiltigt utredd, då en studie från EU visat att detta saknar stöd hos en majoritet av de omkring tjugotusen tillfrågade EU-medborgarna.[26]

Differentiell prissättning, det vill säga individanpassade priser utifrån individers uppfattade benägenhet att betala en viss summa[27], är ett tillämpningsområde för kundprofilering som visat sig medföra ökade intäkter för företag.[28] Det är dock profilering i syfte att sända riktade e-postmeddelande som förefaller kvarstå som det vanligaste tillämpningsområdet för kundprofilering vid marknadsföring.[29]

Utöver ovan angivna marknadsföringsföringsstrategier kan kundprofilering användas för att bättre anpassa företags tjänster till enskilda användares intressen. Ett exempel på ovanstående är det svenska företaget Spotify, som skapar individanpassade spellistor utifrån lyssnarens preferenser.[30] På liknande vis rekommenderar streamingjätten Netflix innehåll baserat på aspekter såsom tittarens betygsättning av filmer och serier.[31] Företagares förhoppning med kundprofilering av detta slag är att kundens upplevelse av plattformen förbättras i och med att det mest eftertraktade också blir mest lättillgängligt.

---

[24] Researchscape International & Evergage, Inc., *2019 Trends in Personalization*, 2019, s. 29.
[25] Salesforce research, *State of the Connected Customer*, 2 uppl., 2018, s. 10f; Segment, The 2017 State of Personalization Report, 2017, s. 3, 5 och 7; Infosys, *Rethinking Retail: insights from consumers and retailers into an omni-channel shopping experience*, 2013, s.3; Salesforce research, *State of the Connected Customer*, 3 uppl.,2019 s. 8.
[26] Europeiska kommissionen, *Special Eurobarometer 431, Data Protection*, 2015, s. 39.
[27] ENISA, s. 14.
[28] Tanner, Adam, *Different Customers, Different Prices, Thanks To Big Data,* Forbes, publicerad 26 mars 2014, https://www.forbes.com/sites/adamtanner/2014/03/26/different-customers-different-prices-thanks-to-big-data/#caac0c457305, Forbes.
[29]Researchscape International & Evergage, Inc.,*2019 Trends in Personalization*, 2019, s. 6.
[30] Spotify, *Playlists*, https://artists.spotify.com/guide/playlists.
[31] Netflix, *Så här fungerar Netflix system för rekommendationer,* https://help.netflix.com/sv/node/100639.

Det går inte att bortse från skräddarsydd internetreklam när kundprofilering beskrivs. Utifrån en outtömlig mängd källor kan företag hämta information om personer som används för att förutse vilka produkter de kan tänkas vara intresserade av. Data som samlats in säljs konstant i snabba transaktioner mellan olika annonsörer och den som bjuder högst på informationen om personen vinner plats att annonsera.[32] Enbart den relevanta reklamen visas sedan för personen, oberoende av hemsida och plattform. Exempelvis kan internetplattformer på så vis bli tillgängliga gratis för användaren. Ett överanvänt, men för riktad reklam mycket talande allmänt känt uttryck, är *om du inte är konsument är du produkt*. Hundratals miljarder amerikanska dollar spenderas årligen världen över på digital marknadsföring.[33] Stora internetföretag, såsom Google och Facebook, har under lång tid utvecklat skräddarsydd reklam,[34] men dessa företag är inte ensamma på marknaden.[35]

För att förstå omfattningen av kundprofilering kan nämnas att en forskare har beskrivit det som att ”digital marketing *watches us*”.[36] Självklart är inte enbart forskare medvetna om resultaten av kundprofilering. En analytiker för det stora lågprisvaruhuset Target har citerats säga ”[w]e’ll be sending you coupons for things you want before you even know you want them”.[37]

[32] Gutwirth m.fl., s. 58.
[33] Enberg, Jasmine, *What’s Shaping the Digital Ad Market*, publicerad 28 mars 2019, https://www.emarketer.com/content/global-digital-ad-spending-2019, eMarket
[34]Gutwirth m.fl., s. 54.
[35] Researchscape International & Evergage, Inc., s.7; Gutwirth, s. 61.
[36] Cit. Gutwirth m.fl., s. 53.
[37] Cit. Duhigg, Charles, *How Companies Learn Your Secrets*, publicerad 16 februari 2012, https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html, the New York Times Magazine

3 Dataskyddsförordningen

3.1 Allmänt

Inom EU finns ingen lagstiftning som riktar sig uteslutande till big data generellt eller big data som används i marknadsföring specifikt. Fenomenet behandlas i stället främst i dataskyddsförordningen. Förordningen reglerar all typ av data genom att ställa upp krav på integritetsskydd. Nedan presenteras först de allmänna målen med dataskyddsförordningen. Därefter följer en beskrivning av de aspekter av dataskyddsförordningen som främst inverkar på behandlingen av big data.

3.2 Bakgrund och ändamål

Den 25 maj 2018 trädde dataskyddsförordningen i kraft och ersatte det dataskyddsdirektiv som hade varit i kraft sedan 1995. Det är mot bakgrund av snabb teknisk utveckling och ökad globalisering, vilket möjliggjort behandling av personuppgifter i mycket stor omfattning, som dataskyddsförordningen tillkommit.[38]

Dataskyddsförordningen ämnar finna enad balans inom Europeiska unionen mellan å ena sidan hög skyddsnivå för personuppgifter och å andra sidan det fria flödet av personuppgifter inom den inre marknaden.[39] Skydd för personuppgifter som rör enskilda är en grundläggande rättighet inom Europiska unionen, stadgad i artikel 8 EU-stadgan. Skyddet ses som ett uttryck för den grundläggande rätten till privatliv.[40] Det kan nämnas att skydd för privatliv finns stadgat bland annat i artikel 7 EU-stadgan och artikel 8

[38] Skäl 6 dataskyddsförordningen; Europeiska kommissionen, *Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska Ekonomiska Sociala Kommitten samt Regionkommittén, Skydd av den personliga integriteten i en uppkopplad värld: En europeisk ram för personuppgiftsskydd för tjugohundratalet*, COM (2012) 9 final, 2012, s. 2.
[39] Skäl 6 och 10 Dataskyddsförordningen.
[40] Dom av den 13 maj 2014, Google Spain, C-131/12, ECLI:EU:C:2014:317, punkt 3 och 68; Dom av den 6 oktober 2015, Schrems, C-362/14, ECLI:EU:C:2015:650, punkt 39.

EKMR. Dataskyddsförordningen ska vidare stimulera ekonomisk tillväxt i den inre marknaden genom att enskilda innehar förtroende för att deras personuppgifter erhåller starkt skydd.[41] Individers rätt till kontroll över sina personuppgifter är ett centralt koncept inom EU:s dataskyddsreglering, vilket också genomsyrar dataskyddsförordningen. Samtidigt belyses i skäl 4 dataskyddsförordningen att det grundläggande skyddet för personuppgifter inte är en absolut rättighet, utan en rättighet som måste vägas mot andra grundläggande rättigheter.

Att individer i stor utsträckning anser sig sakna full kontroll och även önskar kontroll över de personuppgifter de lämnar ut på internet är väldokumenterat.[42] Kontroll över vilka personuppgifter som samlas in och transparens om hur dessa behandlas har dessutom belysts som en central aspekt för att generera konsumenters tillit till företag.[43]

Genom formen av en förordning är de nya bestämmelserna direkt tillämpliga i samtliga EU-medlemsstater, vilket undanröjer ett behov av genomgripande nationell lagstiftning på dataskyddsområdet samt medför en ökad harmoniseringen. Majoriteten av de regler som gick att finna i dataskyddsdirektivet återfinns i dataskyddsförordningen. Den främsta skillnaden mot dataskyddsdirektivet är ökad territoriell tillämplighet, ett större fokus på efterlevnad av bestämmelserna, och – vilket troligen har undgått få – höga straffavgifter i de fall reglerna överträds.

3.3 Personuppgifter

För en bättre förståelse kring varför dataskyddsförordningen är tillämplig på omfattande behandling av data i de fall denna data är hänförlig till en individ är det viktigt att förstå vad som utgör personuppgifter.

[41] Europeiska kommissionen (2012), s.2.
[42] Europeiska kommissionen, *Special Eurobarometer 487a, the General Data Protection Regulation*, 2019 s. 34f och 39. Det bör dock poängteras att Europeiska unionen inte är en objektiv part, då unionens dataskydd till stor del bygger på personlig kontroll.
[43] Salesforce research (2018), s. 21 och 55.

Begreppet personuppgifter definieras i artikel 4(1) dataskyddsförordningen som varje upplysning som avser en identifierad eller identifierbar levande fysisk person. En person anses identifierbar om hen, med beaktande av alla hjälpmedel, med rimlig sannolikhet utifrån specifika faktorer kan komma att identifieras.[44] Det har i ett rättsfall beskrivits att risken för identifiering i praktiken inte ska vara försumbar.[45]

Även indirekta uppgifter, det vill säga uppgifter som måste kombineras med andra uppgifter för att en fysisk person ska kunna identifieras, utgör personuppgifter i dataskyddsförordningens mening enligt artikel 4. Det kan också nämnas att både metadata – data som förklarar kontexten bakom annan data – och cookies kan omfattas av dataskyddsförordning.[46]

3.4 Ändamålsbegränsning

Ändamålsbegränsning är en av de grundläggande principer som fastslås i artikel 5 dataskyddsförordningen, närmare bestämt art 5(1)(b). Härutöver går principen även att finna i artikel 8(2) EU-stadgan. Principen fanns tidigare stadgad i artikel 6 dataskyddsdirektivet. Aspekten av individuell kontroll är starkt förankrad i principen om ändamålsbegränsning.[47] Individer ska kunna förutsätta i vilka syfte data om dem behandlas och detta ska bevara tillit.[48]

Principen riktar sig till insamlingsfasen av data och innebär enligt dataskyddsförordningen att det krävs ”särskilda, uttryckligt angivna och berättigade ändamål” för att insamling av personuppgifter ska få ske. Det är tillåtet att ange fler ändamål än ett och varje enskilt ändamål ska nå upp till

[44] Skäl 26 dataskyddsförordningen.
[45] Dom av den 19 oktober 2016, Patrick Breyer v Bundesrepublik Deutschland, C-582/14, ECLI:EU:C:2016:779, punkt 46.
[46] C-582/14, Patrick Breyer v Bundesrepublik Deutschland; skäl 30 dataskyddsförordningen.
[47] Artikel 29-gruppen, *Opinion 03/2013 on Purpose Limitation*, 2013, 4.
[48] Artikel 29-gruppen (2013), s. 4.

de krav som ställs i artikel 5.[49] Berättigade ändamål syftar främst till de rättsliga grunder som följer av artikel 6, nämligen samtycke från den enskilde och fem olika slags nödvändighet att samla in data.[50] Gällande samtycke kan nämnas att kraven för att samtycket ska vara giltigt är högt ställda.[51]

Ändamålsspecificering följer också av principen om ändamålsbegränsning.[52] För den personuppgiftsansvarige eller för personuppgiftsbiträdet – det vill säga de kategorier av person som utför behandlingen[53] – innebär specificeringsrekvisitet att en utvärdering av i vilket eller vilka syften personuppgifterna kommer att användas måste genomföras och att personuppgifter endast får samlas in för dessa syften.[54] De angivna ändamålen måste dessutom vara specifika.[55] Insamlares möjligheter att på laglig väg ange vaga ändamål i syfte att kringgå ändamålsprincipen är därmed begränsade.[56]

Vidare innebär ändamålsprincipen att ytterligare behandling inte får ske på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling, nedan benämnt vidarebehandling[57], utgör enligt artikel 29-gruppen all behandling som går utöver den initiala insamlingen av personuppgifterna.[58] Viss mån av avsteg från de ursprungligen satta ändamålen är tillåtet, men enbart inom ramen för vad som inte är inkompatibelt.[59] Enligt artikel 6(4) kan en mer eller mindre ingående bedömning utifrån exempelvis kopplingen mellan ändamålen, konsekvenser för individen, och behovet av särskilda skyddsåtgärder behöva övervägas vid vidarebehandling. Artikel 6(4) är en

[49] Artikel 29-gruppen (2013), s. 16.
[50] Artikel 29-gruppen (2013) s. 19f.
[51] Magnusson Sjöberg, s. 182ff; se även Mayer-Schönberger och Padova, s.325f.
[52] Artikel 29-gruppen (2013), s. 15.
[53] För en definition av begreppen, se artikel 4(7) och 4(8) dataskyddsförordningen, se även artikel 3(1) och 3(2).
[54] Artikel 29-gruppen (2013), s. 15.
[55] Artikel 29-gruppen (2013), s. 15; skäl 39 dataskyddsförordningen.
[56] Zarsky, Tal, *incompatible: The GDPR and the Age of Big Data,* Seton Hall Law Review, Volume 47,No. 4(2), s.995-1020, 2017, s. 1006.
[57] Jämför prop. 2017/18:105, s. 110.
[58] Artikel 29-gruppen (2013), s. 21.
[59] Artikel 29-gruppen (2013), s. 21.

implementering av vad artikel 29-gruppen flera år tidigare föreslagit som lämpliga bedömningskriterier.[60]

3.5 Uppgiftsminimering

Principen om uppgiftsminimering, vilken följer av art 5(1)(c) dataskyddsförordningen, innebär att personuppgifter måste vara adekvata, relevant och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Av skäl 39 framgår att behandling av personuppgifter endast bör ske ”om syftet med behandlingen inte rimligen kan uppnås genom andra medel.” Således får endast de personuppgifter som nödvändigtvis måste behandlas för att ändamålet ska uppnås genomgå behandling.[61]

3.6 Särskilda kategorier av personuppgifter

Dataskyddsförordningen föreskriver i artikel 9(1) ett förbud mot behandling av personuppgifter som avslöjar vissa särskilda kategorier av personuppgifter. I skälen till dataskyddsförordningen och i nationell svensk rätt benämns dessa särskilda kategorier av personuppgifter som ”känsliga uppgifter”[62] respektive ”känsliga personuppgifter”[63]. Nedan används det sistnämnda begreppet.

Följande känsliga personuppgifterna finns stadgade i artikel 9(1), vilka utgör en uttömmande uppräkning:

[60] Se artikel 29-gruppen (2013), s.23-27; för en kort analys av artikel 6(4) dataskyddsförordningen, se kapitel 4.3 i Holtz, Hajo Michael, *Den nya allmänna dataskyddsförordningen — några anmärkningar*, publicerad 2018, https://svjt.se/svjt/2018/253, Svensk Juristtidning.
[61] I dataskyddsförordningens engelska version används i artikel 5(1)(c) uttrycket ”limited to what is necessary in relation to the purposes”.
[62] Se exempelvis skäl 10 och 51 dataskyddsförordningen.
[63] Se exempelvis lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning kapitel 3.

> etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

De i artikel 9(1) uppradade personuppgifterna anses särskilt skyddsvärda eftersom behandlingen av sådana uppgifter riskerar intrång i grundläggande rättigheter och friheter.[64] Det är risken att personer utsätts för ofördelaktig behandling om de anses falla under någon av kategorierna som behandlingsförbudet har för avsikt att skydda individer ifrån.[65]

Ett antal undantag från behandlingsförbudet följer av artikel 9(2), varav majoriteten gäller specifika situationer såsom domstolars dömande verksamhet och folkhälsovårdens allmänintresse. Den registrerades *uttryckliga* samtycke, ett högre ställt krav än vad som gäller enligt artikel 6(1)(a), till behandlingen för ett eller flera specifika ändamål är dock ett mer generellt föreskrivet undantag, stadgat i artikel 9(2)(a).

[64] Skäl 51 dataskyddsförordningen.
[65] Rouvroy, Antionette, *"Of Data and Men": Fundamental Rights and Freedoms in a World of Big Data*, Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ets 108], 2016, s. 28.

4 Dataskyddsförordningens koppling till big data

4.1 Big data kontra principer?

Ändamålsbegränsning, särskilt ändamålsspecificering, och behandling av big data är eventuellt den mest diskutera oenigheten mellan lagstiftningen och big data.[66] Fördelen med big data är möjligheten att dra slutsatser som till en början inte var förutsedda, tack vare datautvinningen bakom behandling av big data.[67] Dessutom är det genom kombinationen av personuppgifter från flera olika källor som det fulla värdet av big data främst framkommer.[68] Även om ett syfte i likhet med ”profilering i marknadsföringssyfte” anges, är detta troligen inte tillräckligt specificerat för att vara förenligt med rekvisitet ändamålsspecificering.[69] Zarsky, som utgår från att enskilda inte eftersträvar tillit kring hur deras personuppgifter behandlas[70], har argumenterat att det kan utgöra en kostsam och eventuell omöjlig process att håll sig inom ramarna för det tillåtna vid behandling av big data.[71] Han kritiserar även principen för att vara bristfällig och generera oklarhet.[72]

Vidare är återanvändning av personuppgifter vanligt inom behandling av big data.[73] Ändamålsbegränsning blir som bekant aktuell även vid sådan vidarebehandling av personuppgifter. Som ovan angivits godkänner ändamålsprincipen viss flexibilitet i och med att vidarebehandling får ske även om visst avsteg från det ursprungliga ändamålet görs. Gällande särskilt profilering i syfte att genomföra direktmarknadsföring och liknande

[66] Se exempelvis Corrals m.fl. kap 2; Zarsky, s. 1003-1009; Esayas, Samson, *The idea of ‘emergent properties’ in data privacy: towards a holistic approach*, International Journal of Law and Information Technology vol 25, s. 139–178, s. 143; Mayer-Schönberger och Padova; Paterson, s. 19.
[67] Mayer-Scönberger och Padova, s. 319f.
[68] Mayer-Scönberger och Padova, s. 320.
[69] Artikel 29-gruppen (2013), s. 16.
[70] Zarsky, s. 1003.
[71] Zarsky, s. 1006; angående kostnader för den personuppgiftsansvarige eller personuppgiftsbiträdet, se även Corrales m.fl., s. 40.
[72] Zarsky, s. 1009.
[73] Mayer-Scönberger och Padova, s. 319f; ENISA, s. 13 och 19; Esayas, s. 140.

individanpassade behandlingar bör frivilligt, specifikt, informerat och otvetydigt ”opt-in” samtycke i många fall utgöra ett krav för att vidarebehandling ska anses tillåtet, samt även transparens kring beslutfattningsprocessen och slutsatserna dragna därifrån.[74] Mayer-Scönberger och Padova har poängterat att det är mycket svårt att erhålla det breda samtycke som krävs för att utföra vidarebehandling av personuppgifter, på grund av de höga krav som ställs på giltigt samtycket.[75]

Här bör erinras om ändamålsbegränsningens syfte, nämligen personlig kontroll. Principen om ändamålsbegränsning är en hörnsten inom EU-rätten eftersom den vördar individers förväntningar om varför data samlas in och är central för att bevara tillit.[76] Esayas är dock av åsikten att de talrika syften för vilka personuppgifter samlas in och återanvänds i kombination med annan data för olika användningsområden underminerar denna kontroll – oberoende av om kontroll i form av ändamålsbegränsning preserveras för varje enskilt fall.[77] Han stadgar följande:

> the individualistic approach is based on the underlying assumption that there are well-delineated, distinct processing activities serving distinct purposes, with every piece of data fitting into those delineated individual boxes of processing activities. However, in light of the increasing commercial value of personal data and big data practices, this assumption is a half-truth at best.[78]

Esayas proklamerar att helheten är större än summan av delarna.[79] Således går han ett steg längre än Zasky i sin utvärdering av principen om ändamålsbegränsning. Den sistnämnda forskaren fokuserar på de problem

[74] Artikel 29-gruppen (2013), s. 46f.; se vidare kap 3.4 samt artikel 29-gruppen (2013) s. 23-27.
[75] Mayer-Scönberger och Padova, s. 326; för andra svårigheter med att erhålla samtycke, se Tene, Omer och Polonetsky, Jules, *Big Data for All: Privacy and User Control in the Age of Analytics*, Northwestern Journal of Technology and Intellectual Property, volume 11, issue 5, s. 240.273, 2013, s. 260ff.
[76] Artikel 29-gruppen (2013), s. 4.
[77] Esayas, s. 140.
[78] Cit. Esayas, s. 140.
[79] Esayas, se bland annat s.140, s. 148. “Emergent properties”, är dessutom benämningen på det koncept som beskriver att helheten innehar mer än delarna.

som ändamålsbegränsning står inför i varje enskilt fall av datainsamling när principen möter det komplexa systemet av behandling av big data. Esayas anser att även om individer i det enskilda fallet upprätthåller kontroll över sina personuppgifter tack vare en på riktigt vis implementerad ändamålsbegränsning, kvarstår de problem med kontroll som principen eftersträvar att skydda.

Även uppgiftsminimeringsprincipen och behandling av big data lyfts av många forskare som två motstridiga företeelser. Som ovan framgått föreskriver uppgiftsminimeringsprincipen att behandling av personuppgifter måste begränsas till minsta möjliga omfattning.[80] Behandling av omfattande mängder data är emellertid ett karaktäriserande drag för big data-analyser.[81] En forskare har gått så långt som att påstå att uppgiftsminimering ”is simply no longer the market norm”.[82] Till följd av omfattningen av big data är det först efter behandling som det går att utröna vad som har varit relevant.[83] Företag som behandlar personuppgifter om sina kunder, likväl som andra personuppgiftsansvariga, har dessutom incitament att bevara uppgifterna under längre tid, i hopp om att nya användningsområden kan finnas i framtiden.[84]

En del forskare anser att de fundamentala principer som ovan beskrivits står i sådan skarp kontrast till big data att de omöjligt kan samverka med big data. Forskare med denna åsikt trycker på att främst uppgiftsminimering och ändamålsbegränsning bör tillskrivas en mer begränsad roll, till förmån för riskbedömningar av skada för individen när personuppgifter behandlas, ökad transparens eller individers tillgång till sin data.[85]

---

[80] Europeiska ekonomiska och sociala kommittén (EESC), *The ethics of Big Data: Balancing economic benefits and ethical questions of Big Data in the EU policy context*, 2017, s. 37.
[81] Frydlinger m.fl., s. 39.
[82] Cit. Tene m.fl., s. 260.
[83] Frydlinger m.fl., s. 39; Paterson and McDonagh, s. 19.
[84] Zarsky, s. 1011.; Artikel 29-gruppen (2018), s. 11.
[85] Tene m.fl., s. 263; Zarsky, s. 1011; Artikel 29-gruppen, *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*, 2014, s. 2; se även Esayas, s. 172, som lägger stor vikt vid personlig integritet; se även Dainow, Brandt, *Digital*

De två principernas roll vid behandling av big data diskuterades år 2014 av artikel 29-gruppen.[86] I sitt uttalande besvarade arbetsgruppen den kritik som väckts gällande EU-rättens fundamentala principers ansedda oförenlighet med kommande utveckling av big data. Härvidlag stod arbetsgruppen fast vid att principerna om ändamålsbegränsning och uppgiftsminimering, jämte andra principer för dataskydd, var fortsatt giltiga och lämpliga även för big data.[87] Arbetsgruppen tog även ställning för att det gällande ramverket besitter en nyckelroll i skapandet och upprätthållandet av tillit, som de påpekade att intressenter behöver för att utveckla stabila företagsmodeller baserade på behandling av big data.[88] Ett liknande resonemang har förts av ENISA. ENISA vidhåller att integritet lägger grunden för tillit och att dessa komponenter är centrala för att behandling av big data ska frodas.[89] De kallar det ”big data with privacy”, i stället för ”big data versus privacy”.[90] Zarsky har däremot kallat argumentation av det slaget för önsketänkande.[91]

4.2 Känsliga personuppgifter och personers känslor

Känsliga personuppgifter är ytterligare en aspekt som har belysts inom doktrinen om behandling av big data.[92] Behandling av big data kan medföra, när icke känsliga kategorier av personuppgifter kombineras, att känsliga kategorier av personuppgifter skapas.[93] Liknande resonemang har förts av artikel 29-gruppen gällande specifikt profilering.[94]

alienation as the foundation of online privacy concerns, Acm Sigcas Computers and Society Volume 45 Issue 3, s. 109-117, September 2015, s. 115.
[86] Artikel 29-gruppen (2014).
[87] Artikel 29-gruppen (2014), s. 2.
[88] Artikel 29-gruppen (2014), s. 2.
[89] ENISA, s. 17ff.
[90] Cit. ENISA, s. 49.
[91] Zarsky, s. 1003.
[92] Se exempelvis Esayas s. 163; Zarsky, s. 1012-1015; Tene m.fl., s. 253f och 270; se även en generell analys av känsliga personuppgifter i förhållande till snabb teknisk utveckling i Ohm, Paul, *sensitive information*, southern California Law Review, vol. 88, 2015.
[93] Zarsky, s. 1013; Esayas, s. 163.; Rouvroy, s. 27; se även Ohm, s. 1148.
[94] Artikel 29-gruppen (2018), s. 15.

Ett konkret exempel på vilka slutsatser som kan dras utifrån icke känsliga uppgifter vid riktad marknadsföring är den välkända incidenten kring det amerikanska lågprisvaruhuset Target. I syfte att använda riktad reklam för att locka kunder till att handla mer hos företaget analyserades gravida kvinnors shoppingvanor och hur dessa ändrade sig under graviditetens gång. Benägenheten att handla vissa av företagets produkter visade sig indikera sannolikheten på att en kvinna var gravid. Det gällde exempelvis parfymfria krämer och tvålar, handdesinfektion och bomullstussar i storpack. Genom en sådan analys listade företaget år 2012 ut att en ung kvinna var gravid och skickade riktad reklam till henne – före det att hon hade berättat om graviditeten för sin familj. Till och med en av de analytiker som låg bakom det framgångsrika konceptet noterade att kunder kunde uppleva obehag om det applicerades på fel vis. Företaget har sedermera ändrat hur informationen om gravida kvinnor förmedlas till kunder, för att det inte lika tydligt ska framgå att företaget besitter vetskapen.[95]

Graviditets-algoritmer är inte det enda förekommande exemplet på hur big data har använts för att skapa träffsäkra och känsliga profiler. Liknande har utförts avseende bland annat individers hälsa[96] samt politiska åsikter och sexuella läggning.[97]

Inom doktrinen belyser både Dainow och Esayas att kombinationen av massiva mängder personuppgifter från flera olika privata källor kan liknas vid övervakning[98] och möjligheten att från övervakningen dra slutsatser om känsliga uppgifter framgår både direkt och implicit av den senare forskarens utläggning.[99] Överexponeringen argumenteras av Esayas skapa uppgivna individer och medgörliga konsumenter, vilket kränker den personliga

[95] Duhigg.
[96] Rouvroy s, s. 27; se även Ohm, s. 1170.
[97] Två forskare av-anonymiserade och drog klara slutsatser om individers politiska åsikter och sexuella läggning genom kombinationen av uppgifter från två databaser om betygsättning av filmer, Narayanan, *Arvind &* Shmatikov, Vitaly, *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset),* the University of Texas at Austin, 2008, s. 11 och 16.
[98] Dainow, s. 112; Esayas, s. 157; se även EESC, s. 32.
[99] Esayas, se exempelvis s. 155f och s. 163.

autonomin, integriteten och digniteten som EU:s dataskyddsregler ska värna om.[100]

Till följd av att information som för många individer kan anses privat görs lättillgänglig genom profilering har, på ett rent lagstiftningsmässigt plan, uppdelningen i känsliga och övriga personuppgifter kritiserats för att vara artificiell.[101] Zarsky har dessutom påpekat att uppdelningen riskerar bli mycket kostsam för lagstiftare och för parter när innebörden av känsliga uppgifter ska tolkas i domstol, samt riskerar att skapa stor osäkerhet för företag som avser tillämpa behandling av big data.[102]

EU är inte av samma åsikt som forskare som invänder mot systemet med känsliga personuppgifter i dess helhet. Utöver i artikel 9 dataskyddsförordningen behandlas känsliga personuppgifter i artikel 6(4)(c).[103] Av bestämmelsen framgår att ett kriterium att ta hänsyn till, vid bedömning av om vidarebehandling av personuppgifter är giltig, är uppgifternas art och därvidlag särskilt sådana känsliga personuppgifter som faller under artikel 9. Artikel 29-gruppen har också betonat vikten av respekt för känsliga uppgifter för att vidarebehandling av personuppgifter ska ske i enlighet med principen om ändamålsbegränsning och den underliggande personliga kontroll principen föreskriver, även vid big data behandling.[104] Till skillnad från lagstiftningen begränsade sig inte artikel 29-gruppen i sin redogörelse till den uttömmande lista på vad som enligt dataskyddsförordningen utgör känsliga personuppgifter, utan tydliggjorde att andra typer av personuppgifter som kräver särskilt skydd bör tas med i bedömningen.[105] Vilken typ av information arbetsgruppen syftade till kan bland annat urskönjas i en studie utförd av det rådgivande EU-organet EESC. I studien sammanfattades vilka personuppgifter en individ normalt genererar

[100] Esayas, s. 158.
[101] Zarsky, s. 1013; se även Tene m.fl., s. 270.
[102] Zarsky, s. 1014.
[103] Se även kap. 3.4.
[104] Artikel 29-gruppen (2013), s. 25 och 35.
[105] Artikel 29-gruppen (2013), s. 25.

över sin livstid, i en ”vaggan till graven”-liknande beskrivning.[106] Gällande enbart information som anges vid online dejting radade EESC bland annat upp fotografier, fysisk deskription, sexuell läggning och rökvanor som känsliga personuppgifter.[107] I nära samband med artikel 29-gruppens påstående om känsliga uppgifter påpekade de även följande:

> emotional impacts also need to be taken into account, such as the irritation, fear and distress that may result from a data subject losing control over personal information, or realising that it has been compromised.[108]

[106] EESC, kap. 6.
[107] EESC, s. 52. Det bör dock anmärkas att majoriteten av dessa inte faller inom den uttömmande lista av känsliga uppgifter som återfinns i artikel 9 dataskyddsförordningen.
[108] Cit. Artikel 29-gruppen (2013), s. 26.

5 Analys

Före en diskussion kan föras över det ovan framförda materialet bör källornas vinklade perspektiv anmärkas på. EU är av naturliga skäl positivt inställd till dataskyddsförordningen. Därav framhäver unionen också ständigt den enskilda individens roll i behandlingen av personuppgifter, både via lagstiftning i sig och genom sina rådgivande organ. De rådgivande organen är enbart rådgivande, varför deras yttrande bör ses med viss skepsis. Doktrinen gällande big data går i stor utsträckning på ett helt annat spår. Här förringas skydd för individen och fokus läggs nästintill enbart på hur lagstiftningen begränsar användningen av big data. Zarsky är det tydligaste exemplet på den falangen inom doktrinen. Således kan EU:s inställning tolkas som en ytterlighet och doktrinens en annan. Att skapa en nyanserad analys utifrån ett svartvitt underlag – i hopp om att formalisera ett så dimmigt ämne som big data – är utmanande.

Uppsatsen visar att förhållandet mellan dataskyddsförordningen och big data inte är okomplicerat. Principerna om ändamålsbegränsning och uppgiftsminimering innebär att företag och andra personuppgiftsansvariga noggrant måste utarbeta hur de ämnar tillämpa den data som ska samlas in, före det att insamlingen sker. Den specificering och minimering som krävs enligt dataskyddsförordningen är en antites till hur behandling av big data genomförs för att informationen ska vara användbar. Till följd av konstruktionen av hur big data behandlas kan efterlevnad därmed innebära stora praktiska komplikationer. Svårtolkade rekvisit och höga kostnader för företag är konsekvenser som har förts fram inom doktrinen. Det kan anmärkas att höga kostnader för privata företag inte är ett direkt juridiskt dilemma. Invändningen är ändock värd att notera eftersom EU i dataskyddsförordningen explicit strävar efter ökad tillväxt i den inre marknaden.

Gällande känsliga personuppgifter åskådliggör det som presenterats att hela systemet med behandling av big data, särskilt vid profilering, riskerar vara förbjuden under gällande bestämmelser. Så är fallet eftersom omfattande mängder information kan skapa känsliga personuppgifter. Samtycke kan visserligen inhämtas, men som kort beskrivits kan detta enligt vissa forskare vara svårt att erhålla och behålla. Utöver de inom doktrin påstådda lagstiftningsmässiga svårigheterna med att reglera en allt mer omfattande mängd känsliga uppgifter i en datadriven big data värld, förs av EU-organ och inom doktrin även en diskussion om konsekvenserna för konsumenter. Rådgivande EU-organ och likaså näringsidkare pekar på de obehagskänslor som behandlingen riskerar medföra. Kopplingen till bristande kontroll och sviktande tillit är härvidlag tydlig.

Syftena bakom principerna och bestämmelserna som stadgas i dataskyddsförordningen bör således inte förbises när förhållandet mellan dataskyddsförordningen och big data analyseras. De finns till för att värna enskildas kontroll över sina personuppgifter. Det underliggande skälet förefaller vara att enskilda själva har bäst omdöme över i vilken utsträckning de vill skydda sina privatuppgifter och i förlängningen sitt privatliv. Emellertid går det inte att ignorera, inte ens för EU, att svårigheterna att skydda individers integritet blir större desto mer personuppgifter som finns tillgängliga på marknaden. Att trivial information kan leda till inkräktande kunskap om individers intressen och beteende är det yttersta beviset på de långtgående möjligheterna med big data och profilering. Gränsen mellan å ena sidan privatliv och individuell kontroll över personuppgifter och å andra sidan allmänt tillgänglig känslig information suddas ut när omfattande mängder data finns tillgänglig.

Problemen är dessutom än mer mångfacetterade än enbart en krock mellan omfattande personuppgiftsbehandling genom datautvinning och datasskyddsförordningens krav på att ett antal principer upprätthålls för att värna individers integritet. Som Esayas har belyst riskerar individer överexponeras av företag, även om reglerna hörsammas.

Unionens närmast tvångsartade påstående om att big data bör falla under samma föreskrifter som all annan typ av data framstår som ignorant i förhållande till nackdelarna likväl som fördelarna med big data. Ett sådant naivt tankesätt riskerar leda till att företag avvisar lagstiftningen i sin helhet som oförenlig med verkligheten och fortlöper med extremt avslöjande kundprofilering, så länge det leder till ekonomiska fördelar.

Kundprofilering bör emellertid inte enbart benämnas i negativ bemärkelse. Individanpassad marknadsföring är i hög grad redan implementerat av företag och efterfrågas enligt flertalet studier av konsumenter. Samtidigt har EU i upprepade studier visat att individer inte känner full tillit till hur deras personuppgifter behandlas. Under dessa förutsättningar är det inte rimligt att genom lagstiftning lämpa över allt ansvar på individerna själva, men det är precis lika orimligt att förvänta sig att företag som använder riktad konsumentmarknadsföring ska se förbi sitt eget vinstintresse och helhjärtat värna om personlig integritet och tillit. Både konsumenter och företag gynnas av de möjligheter som behandling av big data medför. Tillit, kontroll, konsumenters efterfrågan av individanpassad marknadsföring, den faktiska tillämpningen av big data i marknadsföringssamanhang och lagstiftningens utformning förefaller inte befinna sig i symbios. Hur big data bör regleras inom unionen för att bättre tillvarata personlig integritet likväl som ekonomisk nytta får besvaras i en annan uppsats.

För närvarande bör dock företag ha ett antal aspekter i åtanke när de profilerar konsumenter för att skapa individanpassad reklam och andra konsumentspecifika upplevelser. För det första lär de strikta principer som följer av dataskyddsförordningen inte lättvindigt försvinna. De gjorde inte sitt intåg via dataskyddsförordningen eller ens föregångaren dataskyddsdirektivets. Skydd för personuppgifter och rätt till privatliv är grundläggande rättigheter. Det kan finnas en poäng i att rätta sig efter lagstiftning som är stabil och oföränderlig över tid. För det andra är EU:s lagstiftning på området för dataskydd inte taget ur luften. Det är naturligt att

konsumenter känner obehag över att företag kan förstå att de väntar barn utifrån tendensen att handla bomullstussar i storpack, eller att få ett annat pris än en vän på en produkt. Konsumenter kommer känna sig övervakade, vilket aldrig innehar en positiv konnotation. Företag riskerar att förlora konsumenters tillit om marknadsföringen blir allt för aggressiv. Det är delvis detta lagstiftningen syftar till att försvara individer ifrån. Att skyddet inte är förenligt med befintliga tekniska lösningar är en annan sak. Vid något tillfälle kommer tröskeln passeras för när konsumenter anser att företag har gått för långt. Att då befinna sig på rätt sida om konsumenters förtroende är säkrast.

Sammanfattningsvis måste ett antal strikta principer efterlevas när big data hänförlig till personuppgifter behandlas inom EU för att behandlingen ska anses tillåten. Principernas syfte är att stärka personlig integritet och kontroll samt främja tillit till de som behandlar personuppgifterna. De skyddsvärda målen ska vidare gynna ekonomisk tillväxt på marknaden. Uppsatsen har dock visat att det vid omfattande personuppgiftsbehandling är omöjligt att uppfylla den eftersträvade balansen mellan skydd för personuppgifter och främjandet av ekonomisk tillväxt. I stor utsträckning förefaller principerna som ska skydda individer underminera fördelarna – för både konsumenter och företag – med behandling av big data, genom att i praktiken förbjuda behandlingen. Samtidigt riskerar behandling av big data vara totalt oförenlig med personlig integritet. Svaret på den första fråga är således att big data, när denna data behandlas i syfte att fatta beslut som påverkar enskilda individer, inte kan samexistera med befintlig EU-lagstiftning. Den andra frågan gällde hur företag bör förhålla sig till bestämmelserna. Företag bör undersöka hur omfattande insamling, bearbetning och lagring av personuppgifter faktiskt krävs för att på bästa sätt nå ut till konsumenter. Att minimera mängden personuppgifter och öka transparensen inför konsumenterna minskar risken för överträdelse av dataskyddsförordningens bestämmelser, även om total efterlevnad under befintligt regelverk verkar svåruppnått om behandling av big data genomförs. Sådan målsättning kan dock även undanröja faran för att konsumenter uttrycker missnöje eller vänder sig till konkurrerande företag när de inser att deras rätt till kontroll, om än illusorisk, åsidosatts.

Käll- och litteraturförteckning

EU – yttranden, vägledning och rapporter

Artikel 29-gruppen, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 2018

Artikel 29-gruppen, *Opinion 03/2013 on Purpose Limitation*, 2013

Artikel 29-gruppen, *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*, 2014

European Union Agency For Network And Information Security (ENISA), *Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics*, 2015

Europeiska kommissionen, *Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska Ekonomiska Sociala Kommitten samt Regionkommittén, Skydd av den personliga integriteten i en uppkopplad värld: En europeisk ram för personuppgiftsskydd för tjugohundratalet*, COM(2012) 9 final, 2012

Europeiska kommissionen, *Special Eurobarometer 431, Data Protection*, 2015

Europeiska kommissionen, *Special Eurobarometer 487a, the General Data Protection Regulation*, 2019

Europeiska ekonomiska och sociala kommittén (EESC), *The ethics of Big Data: Balancing economic benefits and ethical questions of Big Data in the EU policy context*, 2017

Rouvroy, Antionette, *”Of Data and Men”: Fundamental Rights and Freedoms in a World of Big Data*, Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ets 108], 2016

offentligt tryck

Storbritannien

Information Commissioner’s Office, *Big data, artificial intelligence, machine learning and data protection*, 2.2 uppl., 2017

Sverige

prop. 2017/18:105 *Ny dataskyddslag*

Litteratur

Bernitz, Ulf, Carlsson, Mia, Heuman, Lars, Leijonhufvud, Madeleine, Magnusson Sjöberg, Cecilia, Seipel, Peter, Warnling-Nerep, Wiweka och Vogel, Hans-Heinrich, *finna rätt: juristens källmaterial och arbetsmetoder*, 14 uppl., Wolters Kluwer, 201

Corrales, Marcelo, Fenwick, Mark, Forgó, Nikolaus, *New Technology, Big Data and the Law*, Springer, 2017

Dainow, Brandt, *Digital alienation as the foundation of online privacy concerns*, Acm Sigcas Computers and Society Volume 45 Issue 3, s. 109-117, 2015,

Esayas, Samson, *The idea of ‘emergent properties’ in data privacy: towards a holistic approach*, International Journal of Law and Information Technology volume 25, s. 139–178, 2017

Frydlinger, David, Edvardsson, Tobias, Olstedt Carlström, Caroline, Beyer, Sandra, *GDPR: juridik, organisation och säkerhet enligt datasskyddsförordningen*, Nordsteds juridik, 2018

Gutwirth, Serge, Leenes, Ronald, De Hert, Paul, Poullet, Yves, *European Data Protection: In Good Health?*, Springer, 2012

Hildebrandt, Mireille & Gutwirth, Serge, *Profiling the European Citizen: Cross-Disciplinary Perspectives,* Springer, 2008

Infosys, *Rethinking Retail: insights from consumers and retailers into an omni-channel shopping experience*, 2013.

Laney, Doug, *3D Data Management: Controlling Data Volume, Velocity and Variety,* META group, 2001

Magnusson Sjöberg, Cecilia, *Rättsinformatik: juridiken i det digitala informationssamhället*, uppl. 3, Studentlitteratur, 2018.

Mayer-Schönberger, Viktor och Padova, Yann. *Regime Change? Enabling Big Data Throug Europe's New Data Protection Regulation*, the Columbia Science & Technology Law Review volume XVII, 2016

Narayanan, *Arvind &* Shmatikov, Vitaly, *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset),* the University of Texas at Austin, 2008

Nääv, Maria och Zamboni, Mauro, *Juridisk metodlära*, 2 uppl., Studentlitteratur, 2018

Paterson, Moira och McDonagh, Maeve, *data protection in an era of big data: the challenges posed by big personal data*, Moash University Law Review volume 44 issue 1, 2018

Ohm, Paul, *sensitive information*, southern California Law Review, vol. 88, 2015

Researchscape International & Evergage, Inc., *2019 Trends in Personalization*, 2019

Salesforce research, *State of the Connected Customer*, 2 uppl., 2018

Salesforce research, *State of the Connected Customer*, 3 uppl., 2019

Segment, *The 2017 State of Personalization Report*, 2017

Tene, Omer & Polonetsky, Jules, *Big Data for All: Privacy and User Control in the Age of Analytics*, Northwestern Journal of Technology and Intellectual Property, volume 11, issue 5, s. 240-273, 2013

Zarsky, Tal, *incompatible: The GDPR and the Age of Big Data,* Seton Hall Law Review, Volume 47, No. 4(2), s. 995-1020, 2017

Elektroniska källor

Deans, Jason, publicerad 18 augusti 2010, https://www.theguardian.com/media/2010/aug/18/google-facebook, the Guardian, besökt 23 december 2019

Duhigg, Charles, *How Companies Learn Your Secrets*, publicerad 16 februari 2012, https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html, the New York Times Magazine, besökt 22 december 2019

Enberg, Jasmine, *What's Shaping the Digital Ad Market*, publicerad 28 mars 2019, https://www.emarketer.com/content/global-digital-ad-spending-2019, eMarket, besökt 22 december 2019

Holtz, Hajo Michael, *Den nya allmänna dataskyddsförordningen — några anmärkningar*, publicerad 2018, https://svjt.se/svjt/2018/253, Svensk Juristtidning, besökt 4 januari 2020

Netflix, *Så här fungerar Netflix system för rekommendationer*, https://help.netflix.com/sv/node/100639, besökt 22 december 2019

Spotify, *Playlists*, https://artists.spotify.com/guide/playlists, besökt 22 december 2019

Tanner Adam, *Different Customers, Different Prices, Thanks To Big Data*, Forbes, publicerad 26 mars 2014, https://www.forbes.com/sites/adamtanner/2014/03/26/different-customers-different-prices-thanks-to-big-data/#caac0c457305, Forbes, besökt 22 december 2019

Rättsfallsförteckning

EU-domstolen

Dom av den 13 maj 2014, Google Spain, C-131/12, ECLI:EU:C:2014:317

Dom av den 6 oktober 2015, Schrems, C-362/14, ECLI:EU:C:2015:650

Dom av den 19 oktober 2016, Patrick Breyer v Bundesrepublik Deutschland, C-582/14, ECLI:EU:C:2016:779