

EUROPEAN DATA PROTECTION SUPERVISOR

Yttrande 4/2015

Mot en ny digital etik:

data, värdighet och teknik



11 september 2015

Europeiska datatillsynsmannen (EDPS) är en oberoende institution inom EU som enligt artikel 41.2 i förordning (EG) nr 45/2001 ansvarar för att "vad gäller behandling av personuppgifter ... säkerställa att fysiska personers grundläggande fri- och rättigheter, särskilt deras rätt till privatliv, respekteras av gemenskapsinstitutionerna och gemenskapsorganen" och för att "... ge råd till gemenskapsinstitutionerna och gemenskapsorganen och de registrerade i alla frågor som rör behandling av personuppgifter." Han utsågs i december 2014 tillsammans med den biträdande datatillsynsmannen, med särskild befogenhet att arbeta mer konstruktivt och aktivt. I mars 2015 publicerade Europeiska datatillsynsmannen en femårig strategi där han angav hur han avser att fullgöra sitt ansvarsområde och se till att målen uppnås.

Detta yttrande är en fortsättning på Europeiska datatillsynsmannens föregående yttrande om den allmänna uppgiftsskyddsförordningen, vilket syftade till att hjälpa EU:s huvudinstitutioner att nå rätt samförstånd om en praktiskt genomförbar, framtidsorienterad uppsättning regler som stärker den enskildes rättigheter och friheter. Liksom yttrandet om mobil hälsa i början av 2015 handlar detta yttrande, bland annat mot bakgrund av EU:s planer för den digitala inre marknaden, om utmaningen att göra dataskyddet "digitalt", vilket motsvarar det tredje målet i Europeiska datatillsynsmannens strategi, som är "att anpassa befintliga dataskyddsprinciper till den globala digitala arenan". Yttrandet är förenligt med artikel 29-gruppens syn på dataskyddsaspekterna av användningen av ny teknik, exempelvis "sakernas internet", till vilken Europeiska datatillsynsmannen har bidragit som fullvärdig medlem av gruppen.



Dignity	Värdighet
Future-oriented rules and enforcement	Framtidsorienterade regler och verkställighet
Accountable controllers	Ansvarsskyldiga dataregisteransvariga
Empowered individuals	Självbestämmande individer
Innovative privacy engineering	Innovativ integritetsteknik
Ethics	Etik

”Människans värdighet är okränkbar. Den ska respekteras och skyddas.”

Artikel 1, EU:s stadga om de grundläggande rättigheterna

Den grundläggande rätten till integritet och skydd av personuppgifter är viktigare än någonsin tidigare för skyddet av människans värdighet. Dessa rättigheter är inskrivna i EU-fördragen och EU:s stadga om de grundläggande rättigheterna. De ger den enskilde möjlighet att utveckla sin egen personlighet, leva ett oberoende liv, finna nya vägar samt utöva andra rättigheter och friheter. De dataskyddsprinciper som fastställs i EU:s stadga – nödvändighet, proportionalitet, lagenlighet, dataminimering, ändamålsbegränsning, samtycke och insyn – gäller uppgiftsbehandlingen i sin helhet, såväl insamling som användning.

Tekniken bör inte diktera värden och rättigheter, men förhållandet mellan dem bör inte heller reduceras till en falsk uppdelning. Den digitala revolutionen skapar nya möjligheter inom områdena hälsa, miljö, internationell utveckling och ekonomisk effektivitet. I EU:s planer för en digital inre marknad betraktas molntjänster, sakernas internet, stordata och annan teknik som avgörande för konkurrenskraft och tillväxt. Olika affärsmodeller utnyttjar de nya möjligheterna till omfattande insamling, omedelbar överföring, sammanslagning och återanvändning av personuppgifter för oförutsedda syften som motiveras med omfattande och ogenomträngliga integritetspolicier. Detta sätter dataskyddsprinciperna på hårda prov, vilket kräver nya tankegångar om hur de ska tillämpas.

I dagens digitala miljö räcker det inte med att följa lagen, vi måste även titta på den etiska dimensionen i uppgiftsbehandlingen. EU:s regelverk ger redan utrymme för flexibla beslut och säkerhetsåtgärder i det enskilda fallet vid behandling av personuppgifter. Reformen av regelverket är ett stort steg framåt. Men det finns djupare frågor som handlar om hur utvecklingen i ett datadrivet samhälle påverkar värdigheten, den individuella friheten och demokratins funktion.

Dessa frågor får konsekvenser på det tekniska, filosofiska, rättsliga och moraliska planet. I det här yttrandet belyser vi några viktiga områden där den tekniska utvecklingen kan leda till oacceptabel behandling av personuppgifter eller inkräkta på rätten till integritet. I yttrandet beskrivs ett fyrdelat ”ekosystem för skydd av stordata” i syfte att möta den digitala utmaningen: en kollektiv insats som underbyggs av etiska överväganden.

- (1) En framtidsorienterad reglering av uppgiftsbehandlingen och respekt för rätten till integritet och uppgiftsskydd.
- (2) Ansvarsskyldighet för dataregisteransvariga som styr behandlingen av personuppgifter.
- (3) Medvetenhet om integritetsfrågor vid utveckling och utformning av produkter och tjänster för uppgiftsbehandling.
- (4) Självbestämmande individer.

Europeiska datatillsynsmannen vill ha en öppen och initierad diskussion i och utanför EU, där det civila samhället, utvecklare, företag, akademiker, offentliga myndigheter och lagstiftare deltar. Den nya etiknämnd för dataskydd i EU som vi kommer att inrätta vid Europeiska datatillsynsmannen ska bidra till att utforma en ny digital etik som kommer att göra det lättare för samhället och ekonomin att dra nytta av tekniken på ett sätt som stärker individens rättigheter och friheter.

INNEHÅLLSFÖRTECKNING

1. Data överallt – trender, möjligheter och utmaningar	6
1.1 STORDATA.....	6
1.2 SAKERNAS INTERNET	7
1.3 OSYNLIGA DATORTJÄNSTER	7
1.4 MOLNBASERADE DATORTJÄNSTER.....	7
1.5 AFFÄRSMODELLER SOM ÄR BEROENDE AV PERSONUPPGIFTER.....	8
1.6 DRÖNARE OCH AUTONOMA FORDON.....	8
1.7 TRENDER SOM KAN FÅ STÖRRE INVERKAN PÅ LÄNGRE SIKT	9
2. Ett ekosystem av stordataskydd	9
2.1 FRAMTIDSORIENTERAD REGLERING.....	10
2.2 ANSVARSSKYLDIGA DATAREGISTERANSVARIGA.....	10
2.3 INTEGRITETSMEDVETEN TEKNIK.....	11
2.4 SJÄLVBESTÄMMANDE INDIVIDER.....	11
<i>En prosumentmiljö.....</i>	<i>11</i>
<i>Samtycke</i>	<i>11</i>
<i>Kontroll och "ägande" av uppgifter.....</i>	<i>12</i>
3. Världighet i centrum för en ny digital etik	12
3.1 VÄRDIGHET OCH DATA	12
3.2 EN EUROPEISK RÅDGIVANDE ETIKNÄMND	14
4. Slutsats: Det är dags att fördjupa diskussionen	14
Fotnoter	16

1. Data överallt – trender, möjligheter och utmaningar

Allt större mängder personlig information samlas in och behandlas på allt mer ogenomskinliga och komplicerade sätt. När datorer gradvis började användas i företag och offentliga förvaltningar på 1980-talet fanns det en utbredd uppfattning om att mäktiga regeringar och företag behandlade personuppgifter på ett sätt som reducerade enskilda personer till poster i ett register, vilket var ett hot mot grundläggande fri- och rättigheter. Det speciella med dagens våg av integrerad informations- och kommunikationsteknik är att den finns överallt och har så stort inflytande.

Förra året fanns det enligt uppgift fler uppkopplade enheter på planeten än det fanns människor¹. Ökad processorkapacitet², lagring och bandbredd för överföring innebär att de tekniska hindren för behandling av personuppgifter minskar. Sakernas internet och stordatanalys väntas löpa samman med artificiell intelligens, bearbetning av naturligt språk och system för biometrisk matchning – och möjliggöra applikationer med maskininlärningsförmåga för avancerad intelligens. Regeringar och företag kan gå vidare från datautvinning till ”verklighetsutvinning”, som tränger in i vardagsupplevelser, kommunikation och till och med tankar³. I takt med att samhället anpassar sig till den digitala marknadsplatsen görs nu förnyade ansträngningar att lära små barn att programmera⁴. Hur denna utveckling ska tas till vara i en sektor där EU är ledande som konsument men släpar efter som tjänsteleverantör är ett återkommande tema i kommissionens strategi för den digitala inre marknaden⁵.

Dessa trender och många av de koncept som används i dag är trots sin allmänna spridning vaga och överlappande. För att stimulera en debatt vill vi lyfta fram vissa trender som visserligen inte är heltäckande, men som vi anser medför de största etiska och praktiska problemen för tillämpningen av uppgiftsskyddsprinciperna.

1.1 Stordata

Med *stordata*⁶ avses bruket att slå ihop enorma mängder uppgifter från en rad olika källor och att analysera dem för att få fram ett beslutsunderlag, ofta med hjälp av självlärande algoritmer. Det handlar inte alltid om personuppgifter; data som genereras av sensorer för övervakning av naturliga eller atmosfäriska fenomen som väder eller föroreningar eller för att övervaka tekniska aspekter av tillverkningsprocesser avser till exempel inte ”en identifierad eller identifierbar fysisk person”⁷. Något av det mest värdefulla som företag och regeringar får ut av stordata hämtas dock från övervakningen av *mänskligt* beteende, kollektivt eller individuellt, och detta värde ligger i möjligheten att göra förutsägelser⁸.

Ett resultat är framväxten av en intäktsmodell för internetföretag som utgår från spårning av onlineaktivitet för att optimera transaktionernas ekonomiska värde för tjänsteleverantörerna, inte bara inom riktad reklam utan också i villkoren för och priserna på försäkringar, lån och andra kontraktbaserade förhållanden. I den hårda konkurrensen om användarnas uppmärksamhet är de flesta omedvetna om hur utbredd denna spårning är⁹. Den här typen av stordata skulle kunna betraktas som personuppgifter även när avidentifieringsteknik har använts: det blir allt enklare att härleda en persons identitet genom att lägga samman så kallade avidentifierade uppgifter med andra uppsättningar data, däribland offentligt tillgängliga uppgifter på t.ex. sociala medier¹⁰. När dessa uppgifter sedan säljs, särskilt över gränser och mellan jurisdiktioner, blir ansvarsskyldigheten för uppgiftsbehandlingen otydlig och svår att säkerställa eller verkställa inom ramen för lagen om uppgiftsskydd, särskilt eftersom det saknas internationella normer.

1.2 Sakernas internet

Många enheter som är anslutna till internet är redan en del av vår vardag: smarta telefoner, surfplattor och maskiner för kontantuttag eller incheckning på flyget. År 2020 väntas anslutningskapacitet ha blivit en standardfunktion och 25 miljarder föremål vara anslutna (jämfört med 4,8 miljarder 2015), vilket omfattar allt från telemedicin till fordon, från smarta mätare till en rad nya fasta och mobila enheter för att möjliggöra smarta städer¹¹.

Dessa sensorer kommer att ge direkt och detaljerad information som statistikbyråer och undersökningar inte kan få fram i dag, men som inte nödvändigtvis är mer korrekta utan rentav kan vara vilseledande¹². De 1,8 miljarder maskin-till-maskin-anslutningar i fordon som man beräknar kommer att finnas 2022 kan leda till färre olyckor och mindre utsläpp, öka produktiviteten och ge äldre och personer med funktionsnedsättning ökad autonomi¹³. Kroppsnära artiklar som kläder och klockor kommer att behandla personuppgifter precis som andra anslutna enheter. De kommer att kunna upptäcka blodproppar och övervaka kondition och sårhäkning. Tyger med internetanslutning kan skydda mot extrema miljöer, t.ex. vid brandbekämpning. Dessa enheter kommer att ladda upp personuppgifter direkt till molnlagring, länka till sociala nät och eventuellt sända offentligt, vilket gör det möjligt att identifiera användare och spåra beteenden och förflyttningar hos enskilda personer och grupper¹⁴.

Hur uppgifterna hanteras kan påverka inte bara användarnas integritet, t.ex. om enheterna används på arbetsplatsen, utan även rättigheterna för andra som observeras och registreras av enheten. Det finns få belegg för verklig diskriminering, men det är uppenbart att den enorma mängd personlig information som samlas in av sakernas internet är högintressant som ett sätt att maximera intäkter genom skraddarsydd prissättning baserad på spårat beteende, inte minst för sjukförsäkringssektorn¹⁵. Andra områdesspecifika regler kommer också att ifrågasättas, t.ex. när enheter som behandlar hälsouppgifter inte formellt klassas som medicintekniska produkter och därför inte omfattas av lagstiftningen¹⁶.

1.3 Osynliga datortjänster

Ambienta eller osynliga datortjänster handlar om en central teknik som ligger till grund för sakernas internet. En av de mer uppenbara tillämpningarna är så kallade smarta hem och smarta kontor, med enheter som har inbyggd sofistikerad kapacitet för att behandla information. Dessa kan leda till ökad energieffektivitet och mer välinformerade användare som kan påverka sin förbrukning på distans (även om detta beror på hur oberoende den boende kan agera i förhållande till hyresvärderna eller fastighetsskötaren). Det måste klargöras vem som har ansvaret för ändamålet med och metoden för behandling av personuppgifter i samband med osynliga databehandlingstillämpningar, inte bara för att skydda enskilda personers grundläggande rättigheter utan också för att fördela ansvaret för uppfyllandet av de allmänna kraven på systemsäkerhet på ett lämpligt sätt.

1.4 Molnbaserade datortjänster

Molnbaserade datortjänster är en central möjliggörande teknik, både för avancerad analys- och utvinningsförmåga och för flödet av uppgifter från sakernas internet. Dessa tjänster används i dag av ungefär en femtedel av alla personer och företag i EU¹⁷. Med dessa tjänster går det att koncentrera uppgifter från den uppsjö av enheter som ingår i sakernas internet. Tjänsterna är beroende av att det går att få tillgång och ansluta till de enorma mängder

uppgifter som lagras och behandlas i stor skala vid anläggningar runt om i världen¹⁸. Om molnbaserade datortjänster skulle börja användas mer allmänt¹⁹ i de privata och offentliga sektorerna skulle detta kunna höja BNP i EU28 med sammanlagt 449 miljarder euro (0,71 procent av EU:s totala BNP).

Kontrollen över personuppgifterna delas ofta mellan kunden och molntjänsteleverantören och det är inte alltid klart vem som har ansvar för att uppfylla kraven på uppgiftsskydd. Detta kan innebära att skyddet i praktiken blir bristfälligt. Dessa skyldigheter gäller oavsett **var uppgifterna lagras fysiskt**. Även om infrastrukturen för molnbaserade datortjänster bara är en bakgrundsteknik till stöd för affärstillämpningar kan den **dessutom** i sig bli en kritisk infrastruktur och öka skillnaderna i marknadsinflytande. Nyligen uppgav 30 procent av företagen att de ansåg att det var svårt att avsluta abonnemang eller byta leverantörer²⁰.

1.5 Affärsmodeller som är beroende av personuppgifter

Den här tekniken har öppnat för nya affärsmodeller som är beroende av information som inte bara genereras av tillhandahållandet av tjänsten utan också hämtas från andra källor, som närvaro i sociala medier, för att bedöma risk och kreditvärdighet och maximera intäkterna. I dag är plattformar som kopplar samman säljare och köpare en viktig affärsmodell som gör det möjligt att dela och omfördela produkter, tjänster, färdigheter och tillgångar. Dessa plattformar ingår i det som ofta kallas ”delningsekonomin”, ”den gemensamma konsumtionen” eller webbaserade och mobila peer-to-peer-plattformar²¹ och kan erbjuda klassiska ekonomiska skalfördelar, öka konkurrenskraften på marknader och minska mängden avfall. Enligt beräkningar kommer deras globala värde att fyrdubblas från 26 till 110 miljarder US-dollar de närmaste åren²². Den här typen av datadrivna affärsmodeller ger redan enorma intäkter i bildelning och bostadsuthyrning samt i finansiell teknik och social utlåning. Dessa modeller är till synes mer prisvärda och bekväma, och undersökningar visar att konsumenterna uppskattar detta²³.

Det avgörande för sådana plattformar brukar vara anseendet hos användarna, användarrecensioner och identitetsverifiering. Detta kan uppfattas som en förbättring av insynen och ansvarsskyldigheten, men inte nödvändigtvis i fråga om plattformslieferantören i sig. Stora aktörer inom dessa marknader har kritiserats för påstått undanhållande av uppgifter som påverkar deras anseende från just de enskilda användare som uppgifterna avser. Det finns en mycket stor risk att enskilda personer utesluts från tjänster på grundval av rykten som baseras på felaktiga uppgifter som de inte kan ifrågasätta eller begära att få raderade. Beroendet av uppgifter från flera källor äventyrar också EU-lagstiftningens princip om uppgiftsminimering. Det är viktigt att noga tänka igenom hur stor inverkan dessa och framtidens teknikbaserade affärsmodeller får på enskilda personer och på samhället²⁴.

1.6 Drönare och autonoma fordon

Drönare, eller halvautonoma luftfartyg, används i dag främst för militära ändamål men allt oftare även för övervakning, kartläggning, transport, logistik och allmän säkerhet, t.ex. för att begränsa skogsbränder²⁵. Bilder, filmer och andra personuppgifter som samlas in av drönare kan skickas över telekommunikationsnät. Deras användning riskerar att leda till allvarliga intrång i privatlivet och få en s.k. avkylande effekt på yttrandefriheten. Frågan är hur deras utformning och användning ska kunna regleras på ett effektivt sätt, så att de registrerade kan utöva sin rätt att få tillgång till uppgifter som fångas in av dessa maskiner.

På marken kommer autonoma fordon eller förarlösa bilar att ändra enskilda personers resvanor och kanske sudda ut gränsen mellan privata transporter och kollektivtrafik. Man

beräknar att det kommer att finnas 12 miljoner helt autonoma och 18 miljoner delvis autonoma fordon 2035, samt att EU kommer att vara bland de första att införa den nya tekniken²⁶. De algoritmer som styr bilarna kommer att vara avgörande för beslut som direkt kan påverka enskilda personers fysiska integritet och rentav liv eller död, t.ex. beroende på vilket val som har programmerats in för en oundviklig kollision. Utöver det uppenbara behovet av tydlighet när det gäller vem som är ansvarig för datastyrning och datasäkerhet väcker dessa tillämpningar även flera etiska frågor.

1.7 Trender som kan få större inverkan på längre sikt

3D-bioskrivning av organiska föremål som utgår från kopior av patienters celler och ”biobandage” av kollagen (dvs. känsliga uppgifter enligt EU-lagstiftningen) för att skriva ut lager på lager av levande celler väntas snart bli lättillgänglig²⁷. Detta skulle göra det lättare att få fram skraddarsydda mänskliga anatomiska delar och vara särskilt värdefullt i fattigare och konfliktdrabbade områden i världen. Bioskrivning väcker uppenbara frågor om medicinsk etik, skydd av immateriella rättigheter och konsumentskydd, men även om tillämpningen av dataskyddsreglerna, eftersom den baseras på behandling av privata och känsliga uppgifter om enskilda personers hälsa.

Artificiell intelligens, t.ex. robotteknik, handlar om ett tekniskt krav på såväl fasta som mobila autonoma maskiner. Framstegen med detta kommer att skapa enorma möjligheter utöver de nuvarande tillämpningarna. Djuplärande datorer lär sig uppgifter på egen hand genom att analysera stora uppsättningar data med hjälp av (bl.a.) neurala nätverk som verkar efterlikna hjärnan. Forskare och företag siktar på att förbättra självständigt lärande. Redan i dag kan algoritmer förstå och översätta språk, känna igen bilder, skriva nyhetsartiklar och analysera medicinska uppgifter²⁸. Sociala medier tillhandahåller enorma mängder personlig information som i praktiken är förhandssorterade av individerna själva. Detta kan vara den senaste i en rad kognitiva förbättringar för att höja den mänskliga hjärnans förmåga, som papper eller kulramen, eller integreras i autonoma maskiner och robotar, men det är dags att tänka närmare på de bredare konsekvenserna för enskilda personer och för samhället²⁹.

2. Ett ekosystem av stordataskydd

Nu har EU möjlighet att gå i bräsch genom att visa hur regeringar, lagstiftare, registeransvariga, konstruktörer, utvecklare och enskilda personer kan agera bättre tillsammans för att förstärka rättigheterna och styra, inte hindra, den tekniska innovationen. De trender som beskrivs i avsnitt två har enligt en kommentator ”ökat klyftan mellan vad som är möjligt och vad som är lagligt”³⁰. Till skillnad från vad vissa påstår är integritets- och uppgiftsskydd en plattform, inte ett hinder, för en hållbar och dynamisk digital miljö. Oberoende dataskyddsmyndigheter som Europeiska datatillsynsmannen har en avgörande roll för att skingra dessa myter och besvara enskilda personers uppriktiga oro över att de ska förlora kontrollen över sina personuppgifter³¹.

Nästa generations personuppgifter kommer sannolikt att vara ännu mindre tillgängliga för de enskilda personer som de berör. Ansvar för att utforma en hållbar digital inre marknad är av nödvändighet utspritt men det innefattar också ett ömsesidigt beroende, som ett ekosystem, där det krävs att utvecklare, företag och lagstiftare agerar tillsammans för den enskildes bästa. I detta avsnitt beskriver vi hur dessa fyra centrala aktörer kan bidra.

2.1 Framtidsorienterad reglering

Vi uppmanade nyligen EU att ta vara på denna historiska möjlighet att införa enklare regler för behandling av personuppgifter som kan vara relevanta i en generation³². Förhandlingarna om den allmänna uppgiftsskyddsförordningen och direktivet om dataskydd inom polis- och rättsväsendet befinner sig i slutskedet och snart kommer uppmärksamheten att riktas mot framtiden för direktivet om integritet och elektronisk kommunikation och den nya förordningen om hur EU:s institutioner och organ själva behandlar personuppgifter. När den ekonomiska kostnaden för att samla in och lagra data är så gott som försumbar kommer det att vara upp till dataskyddsmyndigheterna att se till att reglerna följs konsekvent för att undvika den ”moraliska risken” för alltför omfattande uppgiftsbehandling³³.

I strategin för den digitala inre marknaden erkänns denna koppling mellan kontroll över stora mängder data och marknadsinflytande. Där uttrycks samma övertygelse som vi framförde i vårt preliminära yttrande 2014 om privatliv och konkurrenskraft i stordataåldern, nämligen att det krävs större samstämmighet mellan lagstiftarna. EU har redan verktygen för att avhjälpa den bristande balansen i inflytande på den digitala marknaden: Europeiska kommissionens pågående anti-trustförfaranden är t.ex. ett erkännande av de mobila enheternas dominans när det gäller åtkomst till internet. Det är möjligt med en mer helhetsinriktad tillämpning inom den nuvarande rättsliga ramen, t.ex. genom ett EU-samordningskontor för tillsynsmyndigheter, för att överväga om enskilda fall kan väcka frågor om efterlevnad av konkurrens-, konsument- och dataskyddsreglerna. Några exempel:

- Ett krav på större insyn i priset – i kontanter eller annat – på en tjänst kan bidra till och underlätta analysen av konkurrensärenden³⁴.
- Identifiering av oskälig prisdiskriminering på grundval av dålig kvalitet i uppgifter, ogrundad profilering och ogrundade korrelationer³⁵.

En närmare dialog mellan lagstiftare från olika sektorer kan leda till en lösning på de växande kraven på globala partnerskap som kan skapa en gemensam mötesplats för öppna data, där data och idéer som statistik och kartor kan flöda, vara tillgängliga och utbytas i det allmänna intresset, med mindre risk för övervakning, för att ge enskilda personer större inflytande över beslut som påverkar dem³⁶.

2.2 Ansvarsskyldiga dataregisteransvariga

Ansvarsskyldighet innebär att det måste införas interna policyer och kontrollsystem som garanterar efterlevnad och tillhandahåller relevant bevisning, framför allt för oberoende tillsynsmyndigheter.

Vi har förespråkat att dataskyddslagstiftningen ska bli mindre krånglig genom att kraven på onödig dokumentation ska minimeras, för att ge största möjliga utrymme för mer ansvarstagande initiativ från företagen, med stöd av vägledning från dataskyddsmyndigheterna. Principen att personuppgifter enbart ska behandlas på sätt som är förenliga med de specifika ändamål för vilka de samlades in är avgörande för att infria enskilda personers rättmätiga förväntningar. Uppförandekoder, granskningar, certifieringar, revisioner och en ny uppsättning avtalsvillkor och bindande företagsbestämmelser kan bidra till att skapa ett starkt förtroende för den digitala marknaden. De som ansvarar för hanteringen av personuppgifter bör vara mycket mer dynamiska och aktiva och överge den s.k. svarta lådan-utvecklingen, med hemlighetsmakeri och ogenomskinliga affärsmetoder samtidigt som det ställs krav på allt större öppenhet från kundernas sida³⁷.

2.3 Integritetsmedveten teknik

Mänsklig innovation har alltid varit ett resultat av verksamhet inom specifika sociala grupper och specifika sammanhang, som oftast återspeglar de aktuella samhällsnormerna³⁸. Tekniska utformningsbeslut bör dock inte styra vårt sociala samspel och strukturen i våra samhällen utan i stället stödja våra värderingar och grundläggande rättigheter.

EU bör utveckla och främja konstruktionsteknik och metoder som gör det möjligt att använda databehandlingsteknik i syfte att fullt ut respektera den enskilda personens värdighet och rättigheter. System- och programvaruingenjörer måste förstå och i högre grad tillämpa principerna för inbyggt integritetsskydd i nya produkter och tjänster, genom alla konstruktionsfaser och i all teknik. Ansvarsskyldigheten måste få stöd av mer forskning och utveckling av metoder och verktyg som kan garantera tillförlitliga granskningar och fastställa att registeransvariga och registerförare följer reglerna, t.ex. genom att ”tagga” varje enhet i personuppgifter med ”metadata” som beskriver uppgiftsskyddskraven.

Tekniska lösningar bör ge enskilda personer möjlighet att skydda sin personliga integritet och frihet genom avidentifiering. EU bör främja utformningen och genomförandet av algoritmer som döljer identiteter och aggregerar data för att skydda den enskilda personen och samtidigt ta vara på uppgifternas prediktiva förmåga³⁹.

Vi måste redan nu lägga grunden för att ta itu med dessa uppgifter genom att sammanföra utvecklare och uppgiftsskyddsexperter från olika områden i breda nätverk, t.ex. nätverket för integritetsteknik på internet (Internet Privacy Engineering Network, IPEN), som bidrar till ett givande tvärvetenskapligt utbyte av idéer och metoder.

2.4 Självbestämmande individer

En prosumentmiljö

Enskilda personer är inte bara passiva objekt som måste skyddas mot exploatering med hjälp av lagar. De digitala trender vi beskriver ovan innebär också positiva möjligheter att stärka individens roll. Nuförtiden är människor t.ex. både producenter och konsumenterna av innehåll och tjänster och kan i allt högre grad betraktas som medansvariga tillsammans med tjänsteleverantörerna för behandlingen av personuppgifter, såvida det inte är för rena ”hushållsändamål”⁴⁰ (begreppet *prosument* har vuxit fram för att beskriva denna företeelse⁴¹). Under tiden erbjuder virtuella valutor anonymitet och möjligheten att kringgå tredjepartsverifiering av transaktioner, vilket sänker transaktionskostnaderna för gränsöverskridande betalningar av varor och tjänster. Å andra sidan innebär anonymiteten och de jurisdiktionsöverskridande (eller rentav *a-jurisdiktionsella*) egenskaperna hos dessa virtuella valutor att den enskilda personen blir sårbar för bedrägerier och kriminella marknader som är svåra att spåra och utreda. Utöver de skyldigheter som åligger lagstiftare, företag och tekniker, har även invånarna ett ansvar för att vara medvetna, uppmärksamma, kritiska och informerade när de gör sina val såväl på som utanför nätet⁴².

Samtycke

I motsats till den traditionella uppfattningen kan allt mänskligt beteende inte heller förklaras med ekonomiska principer som förutsätter att människor är fullständigt rationella och mottagliga för ekonomiska incitament⁴³. Detta är relevant för den roll som individens samtycke ska spela i framtiden för behandling av personuppgifter om honom eller henne. Enligt EU-lagstiftningen är samtycke inte den enda legitima grunden för de flesta former av

behandling. Även i de fall där samtycke har en viktig roll, befriar detta inte de registeransvariga från deras ansvar när det gäller vad de gör med uppgifterna, särskilt inte när ett generellt samtycke för behandling för en rad olika ändamål har inhämtats.

Kontroll och ”ägande” av uppgifter

Enskilda personer måste kunna påtala fel och ogrundad snedvridning till följd av den logik som algoritmerna tillämpar för att göra antaganden och förutsägelser. Som exempel kan nämnas att en amerikansk undersökning av nästan 3 000 kreditprövningar av 1 000 konsumenter visade att 26 procent innehöll ”väsentliga” fel som var tillräckligt allvarliga för att påverka konsumenternas kreditbetyg och därmed kostnaden för att få lån⁴⁴.

Data betraktas ofta som en resurs, som olja, som helst ska köpas och säljas mellan två lika välinformerade parter⁴⁵. Kunderna får ingen skälig ersättning när deras personuppgifter säljs och vissa har argumenterat för en ägarmodell för data. Det är dock svårt att garantera fullständig kontroll över personuppgifter – det kommer att finnas annat att ta hänsyn till – som det allmänna intresset och andra personers fri- och rättigheter. Det är nödvändigt med kontroll, men det räcker inte⁴⁶. Mänsklig värdighet är dock en konstant faktor och enligt EU-lagstiftningen kan analogin med ägande inte tillämpas som sådan på personuppgifter, som ju är oupplösligt kopplade till enskilda personer. Det finns inga bestämmelser i EU:s dataskyddslagstiftning som gör det möjligt för en enskild person att avstå från denna grundläggande rättighet.

En annan metod för att ge enskilda personer bättre kontroll över sina uppgifter, över vem som kan få tillgång till dem och för vilka ändamål, skulle kunna vara att använda personliga uppgiftslager eller ”datavalv”⁴⁷. För en sådan ”personlig lagring” krävs säkerhetsåtgärder som garanterar att bara de enheter som har fått tillstånd av den registrerade kan få tillgång till uppgifterna och endast till de delar som de har fått tillstånd för. Personliga uppgiftslager skulle vara effektivast när de gäller aktuell och ständigt uppdaterad information, t.ex. geomatiska uppgifter eller livstecken. Utöver de tekniska skyddsåtgärderna skulle uppgiftsanvändarna vara skyldiga att respektera reglerna för att dela och använda uppgifterna. Konkurrens och möjlighet att byta den tjänst man använder är det allra viktigaste verktyg som konsumenterna har för att påverka den marknad av tjänster som finns tillgänglig för dem. Att se till att anslutningar går att flytta, inklusive identifieringar och kontaktuppgifter, har visat sig vara en viktig faktor för att möjliggöra konkurrens och har effektivt sänkt konsumentpriserna när telekommunikationsmarknaden har avreglerats. Portabilitet för uppgifter, dvs. den faktiska och konkreta möjligheten att föra över större delen av sina egna uppgifter från en tjänsteleverantör till en annan, är en effektiv inkörsport för att skapa förutsättningar för verklig valfrihet för konsumenterna.

3. Värdighet i centrum för en ny digital etik

Detta digitala ekosystem måste bygga på en etisk ram. Europeiska datatillsynsmannen anser att en bättre respekt och ett bättre skydd för mänsklig värdighet skulle kunna utgöra en motvikt till den utbredda övervakning och asymmetriska makt som den enskilda individen nu möter. Detta bör stå i centrum för en ny digital etik.

3.1 Värdighet och data

Efter den industriella revolutionen på 1700- och 1800-talen strävade människorättsrörelsen efter att trygga det allmänna bästa i vidare bemärkelse genom att minska hindren för respekt

för den enskilde. EU har nu genom EU-stadgan om de grundläggande rättigheterna och enligt den allmänna förklaringen om de mänskliga rättigheterna och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna tagit den mänskliga värdighetens okränkbarhet som sin utgångspunkt. En människas värdighet är inte bara en grundläggande rättighet i sig utan också en förutsättning för de efterföljande fri- och rättigheterna, däribland rätten till integritet och uppgiftsskydd⁴⁸. En människas värdighet kan t.ex. kränkas om personen behandlas som ett objekt och som ett verktyg för någon annans syften⁴⁹. Integritet är en omistlig del av den mänskliga värdigheten och rätten till dataskydd utformades ursprungligen på 1970- och 1980-talen för att uppväga risken för att integritet och värdighet skulle urholkas av storskalig behandling av personuppgifter. I Tyskland grundades rätten ”att bestämma över information om sig själv” på rätten till personlig värdighet och fri personlig utveckling i enlighet med artiklarna 1 och 2 i den tyska konstitutionen⁵⁰.

I början av 2000-talet tvingas enskilda personer allt oftare att avslöja många fler personuppgifter via internet för att kunna delta i sociala, administrativa och kommersiella sammanhang och får allt mindre möjlighet att välja att avstå. När all aktivitet potentiellt alltid kan vara online uppstår det enorma påfrestningar för begreppet fritt och informerat samtycke. ”Digitala brödsmlor” sprids hela tiden och sammanställs för att klassificera enskilda personer i realtid till multipla och ibland motstridiga profiler. Dessa profiler kan spridas på en mikrosekund utan att den enskilda personen är medveten om det, och användas som underlag för viktiga beslut som påverkar dem.

Profiler som används för att förutsäga människors beteende kan leda till stigmatisering och förstärka befintliga stereotyper, social och kulturell segregation och utslagning⁵¹, där denna ”kollektiva information” undergräver individens valmöjligheter och lika möjligheter. Den här typen av ”filterbubblor” eller ”personliga ekokammare” kan i slutändan strypa just den kreativitet, innovation och yttrande- och organisationsfrihet som har gjort det möjligt för den digitala tekniken att blomstra.

Samtidigt används med hänvisning till ”säkerheten” ett oavbrutet undantagstillstånd för att motivera de många lagren av inkräktande metoder för att övervaka enskilda personers verksamhet⁵². För att förstå den här ”spärrhjulseffekten” i övervakningen krävs ett mer långsiktigt perspektiv på de övergripande effekterna på samhälle och beteende.

Tillsammans med tredjeländer måste EU noggrant undersöka hur man ska kunna garantera att dessa värden respekteras inte bara på papperet utan även i praktiken i cyberrymden. Framför allt har EU nu ett avgörande tillfälle att bygga in dessa värderingar i digitala strukturer som kommer att forma vårt samhälle, innan denna teknik blir allmänt utbredd⁵³. För detta krävs en ny bedömning av huruvida de möjliga fördelarna med den nya tekniken verkligen är beroende av att personligt identifierbara uppgifter om miljarder personer samlas in och analyseras. En sådan bedömning skulle kunna sporra utvecklarna att utforma produkter som i realtid aidentifierar enorma mängder oorganiserad information för att göra det svårare eller omöjligt att skilja ut en enskild person.

Vi är redan medvetna om att viss uppgiftsbehandling, av t.ex. genetiska data, inte bara måste vara reglerad utan också bedömas utifrån bredare samhällsfrågor, av t.ex. etiska nämnder. Genetiska data till sin natur sådana att de inte bara berör en enskild person, utan även deras förfäder och avkomma. Genetiska data kan användas inte bara för att fastställa familjerelationer. Egenskaper hos en enskild persons gener kan också ge information om dennes föräldrar och barn och leda till att registeransvariga fattar beslut som påverkar människors möjligheter i livet redan innan de har fötts. En eventuell koncentration av

genetiska personuppgifter i händerna på ett fåtal gigantiska marknadsaktörer påverkar marknadsekonomierna likaväl som de registrerade. Ett ökande beroende av ett globalt system för insamling och analys av ett ständigt flöde av data kan göra samhället och ekonomin mer sårbara för oförutsedda säkerhetsbrister och attacker med ont uppsåt.

Den nuvarande ramen kan misslyckas om vi inte tänker innovativt kring framtiden. Det finns ett växande krav på och behov av att betrakta den registrerade som en individ, inte bara som en konsument eller användare. Verkligt oberoende dataskyddsmyndigheter har en avgörande roll att spela för att förhindra en framtid där enskilda personer styrs av algoritmer och deras olika variationer. De måste vara rustade för att kunna utöva en ”skyldighet att beakta” enskilda personer och deras värdighet på nätet. De traditionella begreppen och principerna för integritets- och uppgiftsskydd omfattar redan etiska nyanseringar för att skydda värdigheten, t.ex. sysselsättning och hälsa. Men dagens trender har inlett ett helt nytt kapitel och vi måste undersöka om principerna är tillräckligt hållbara för den digitala eran⁵⁴. Begreppet personuppgifter kommer i sig sannolikt att ändras radikalt i takt med att tekniken ger allt större möjligheter att återidentifiera enskilda personer från förment avidentifierade uppgifter. Dessutom kommer maskininlärning och sammanslagningen av mänsklig och artificiell intelligens att undergräva föreställningarna om individens rättigheter och ansvar.

3.2 En europeisk rådgivande etiknämnd

Vårt mål är inte att måla upp en alarmistisk dystopi. Diskussioner förs redan i rättsliga, politiska, ekonomiska, sociala, vetenskapliga och även religiösa kretsar⁵⁵. Förenklade strategier som ger ensidiga fördelar för ekonomisk vinst eller övervakning för säkerhetsändamål är sannolikt inte mer användbara än alltför restriktiv tillämpning av befintliga lagar som hämmar innovation och framsteg. Därför föreslår Europeiska datatillsynsmannen en grundlig, bred och tvärvetenskaplig analys för att ta fram rekommendationer och bidra till samhällsdebatten om hur ett fritt, demokratiskt samhälle kan hantera den tekniska utmaningen.

I Europeiska datatillsynsmannens strategi⁵⁶ åtog vi oss att utveckla ett etiskt tillvägagångssätt för dataskydd som erkänner att ”genomförbar, användbar eller lönsam är inte lika med hållbar” och framhåller ”ansvarsskyldighet framför mekanisk efterlevnad av lagens bokstav”. Vi vill nå ut längre än till gruppen av EU-tjänstemän, advokater och it-specialister, till framträdande personer som kan bedöma den tekniska utvecklingens konsekvenser på medellång och lång sikt och hur de bör regleras. Under de kommande månaderna kommer vi att inrätta en extern rådgivande grupp om den etiska dimensionen i uppgiftsskyddet vid vår självständiga institution för att undersöka förhållandena mellan mänskliga rättigheter, teknik, marknader och affärsmodeller på 2000-talet.

Vår etiska rådgivande nämnd kommer att bestå av en utvald grupp framstående personer inom etik och filosofi, sociologi, psykologi, teknik och ekonomi som vid behov ska få stöd av andra experter med kunskap och expertis inom områden som hälsa, transport och energi, socialt samspel och medier, ekonomi och finans, styrning och demokrati samt säkerhet och polisverksamhet. De kommer att uppmanas att överväga de större etiska konsekvenserna av hur personuppgifter utformas och används och full insyn ges i deras diskussioner.

4. Slutsats: Det är dags att fördjupa diskussionen

Integritet och dataskydd är inte ett problem utan en del av lösningen. Än så länge kontrolleras tekniken av människan. Det är inte lätt att klassificera den potentiella utvecklingen som bra

eller dålig, önskvärd eller skadlig, positiv eller negativ, särskilt som flera potentiella trender måste ses utifrån sitt sammanhang. Politiska beslutsfattare, teknikutvecklare, affärsutvecklare och alla vi andra måste allvarligt fundera över om och hur vi vill påverka utvecklingen av tekniken och dess användning. Men lika viktigt är det att EU snarast möjligt överväger de etiska frågorna och vilken plats människans värdighet ska ha i framtidens teknik.

Dataskyddsprinciperna har visat sig kunna skydda individerna och deras integritet från risken för oansvarig uppgiftsbehandling. Men dagens utveckling kan kräva ett helt nytt synsätt. Därför vill vi inleda en ny debatt om huruvida det räcker att tillämpa principer såsom principerna om lagenlighet och legitimitet. De som arbetar med dataskydd skulle kunna fylla en ny funktion där de använder sig av befintliga verktyg såsom förhandskontroller och tillstånd, eftersom inga andra organ är rustade att granska behandlingen av personuppgifter. Tekniken, den globala innovationen och uppkopplingen människor emellan utvecklas i halsbrytande fart och vi har en möjlighet att fånga uppmärksamheten, väcka intresse och skapa samförstånd.

Med detta yttrande hoppas vi tillhandahålla en ram för en bredare och djupare diskussion om hur EU både kan värna sina värderingar och välkomna den nya teknikens fördelar.

Utfärdat i Bryssel den 11 september 2015.

(namnteckning)

Giovanni Buttarelli
Europeisk datatillsynsman

Fotnoter

¹ Källa: GSMA Intelligence.

² ”Moore's lag” om att antalet transistorer som får plats på ett mikrochip fördubblas ungefär var artonde månad har i princip visat sig stämma. Moore, Gordon E (19 april 1965). ”Cramming more components onto integrated circuits”, *Electronics*, 22.8.2011.

³ Nathan Eagle, Alex (Sandy) Pentland, ”Reality mining: sensing complex social systems”, *Personal and Ubiquitous Computing*, volym 10 nr 4, mars 2006, s. 255–268. Shoshana Zuboff skriver följande i ”Big Other: surveillance capitalism and the prospects of an information civilization”, *Journal of Information Technology* (2015) 30, s. 75-89: ”I och med att datoranvändningen präglar allt får så gott som varje aspekt av världen en ny symbolisk dimension där händelser, föremål, processer och människor blir synliga, möjliga att lära känna och att dela på ett helt nytt sätt.” Zuboff ser framför sig ”framväxten av en ny universell arkitektur” som hon kallar ”Big Other”, ”en regim bestående av ett allestädes närvarande nät av institutioner som registrerar, modifierar och kommersialiserar allt i vardagen, från brödrostar till kroppar, från kommunikation till tanke, allt i syfte att upprätta nya möjligheter till monetarisering och vinst”, s. 77, 81.

⁴ ”BBC Micro Bit computer's final design revealed” 7.7.2015, <http://www.bbc.com/news/technology-33409311> (öppnad 10.9.2015), ”No assembler required: How to teach computer science in nursery school”, *The Economist*, 1.8.2015.

⁵ Inget av de tio främsta företagen inom tekniksektorn räknat efter börsvärde är baserat i EU (åtta företag finns i USA, ett vardera i Kina och Taiwan) enligt PWC:s Global Top Ten Companies by Market Capitalisation, 31 mars 2015.

⁶ Med *stordata* avses den exponentiella ökningen av såväl tillgång till som automatiserad användning av information: det handlar om enorma uppsättningar digitala data som lagras av företag, stater och andra stora organisationer och sedan utsätts för omfattande analyser med hjälp av datoralgoritmer”, artikel 29-arbetsgruppens yttrande 3/2013 om ändamålsbegränsning (*ej översatt till svenska*). I en rapport från Vita huset 2014 beskrevs stordata som den ökande tekniska förmågan att samla in, sammanställa och behandla en allt större mängd allt mer varierande data i allt snabbare takt, se *Big Data: Seizing Opportunities, Preserving Values*, presidentskansliet (”Podestarapporten”), maj 2014.

⁷ I EU-lagstiftningen definieras *personuppgifter* som ”varje upplysning som avser en identifierad eller identifierbar fysisk person (den registrerade). En identifierbar person är en person som kan identifieras, direkt eller indirekt, framför allt genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet”, artikel 2 a i direktiv 95/46/EG. Denna definition är i stora drag jämförbar med de definitioner som fastställs i Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (nedan kallad *konvention 108*) och i OECD:s riktlinjer för integritetsskydd och gränsöverskridande flöden av personuppgifter. En mer ingående analys finns i artikel 29-arbetsgruppens yttrande 4/2007 om begreppet personuppgifter, WP136.

⁸ Se t.ex. det tal som ordföranden för Förenta staternas federala handelskommission höll 2014: ”Spridningen av uppkopplade enheter, de snabbt sjunkande kostnaderna för att samla in, lagra och behandla uppgifter och datamäklares och andras förmåga att slå ihop fristående uppgifter med uppgifter online innebär att företag kan sammanställa så gott som obegränsade mängder konsumentuppgifter och lagra dem i oändlighet. Med hjälp av prediktiv analys kan de utifrån detta lära sig förvånansvärt mycket om var och en av oss.” Inledningsanförande av federala handelskommissionens ordförande Edith Ramirez, ”Big Data: A Tool for Inclusion or Exclusion?”, Washington, DC den 15 september 2014. Enligt Sandy Pentland är ”[s]ocialfysik en kvantitativ samhällsvetenskap som beskriver tillförlitliga matematiska kopplingar mellan å ena sidan flödet av information och idéer och å andra sidan människors beteende. Socialfysiken gör det möjligt för oss att förutsäga produktiviteten i små grupper, hos avdelningar inom företag och till och med i hela städer”.

Det är ”detta som krävs för att bygga bättre samhällssystem” (s. 4, 7) och ”göra det möjligt för (regeringstjänstemän, företagsledare och invånare) att använda de sociala nätens stimulansverktyg för att upprätta nya *beteendenormer*” (s. 189) (vår kursivering). Pentland *Social Physics: How Good Ideas Spread: The Lessons from a New Science*.

⁹ Särskild Eurobarometerundersökning 431 om uppgiftsskydd, juni 2015, och undersökning från Pew Research Panel i januari 2014 om allmänhetens uppfattning av integritet och säkerhet efter Snowden. Ett genomsnittligt besök på en enda webbplats leder enligt en undersökning till 56 tillfällen av uppgiftsinsamling, enligt Julia Angwin, *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, (2012). Enligt Vita husets rapport om stordata 2014 ”skapar en aldrig tidigare skådad datorkraft och sofistikerad ... en maktobalans mellan de som lagrar uppgifterna och de som avsiktligt eller oavsiktligt tillhandahåller dem”, ”några av de mest omvälvande förändringar som framkommit under denna granskning handlar om hur stordataanalys kan ... skapa en så ogenomskinlig beslutsmiljö att den enskilda människans oberoende går förlorat i en ogenomtränglig uppsättning algoritmer”.

¹⁰ Med hjälp av offentliga avidentifierade uppgifter från 1990 års folkräkning kan sannolikt 87 procent av USA:s befolkning identifieras genom sina femsiffriga postnummer kombinerat med kön och födelsedatum, se Paul Ohm, ”Broken promises of privacy: responding to the surprising failure of anonymisation”, *UCLA Law Review* 2010 och ”Record linkage and privacy: issues in creating new federal research and statistical info”, april 2011. DNA är unikt (utom för enäggstvillingar) och oföränderligt under en livstid. Det innehåller information om etnicitet, anlag för sjukdomar och kan identifiera andra familjemedlemmar. I januari 2013 kunde forskare identifiera enskilda personer och familjer utifrån avidentifierade DNA-uppgifter i offentligt tillgängliga genealogidatabaser, Gymrek, M., McGuire, A. L., Golan, D., Halperin, E. och Erlich, Y. *Science* 339, 321–324 (2013). Se även ”Poorly anonymized logs reveal NYC cab drivers’ detailed whereabouts”, 23.6.2014 <http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/> (öppnad 10.9.2015). Se även artikel 29-arbetsgruppens yttrande 4/2007 om begreppet personuppgifter, artikel 29-arbetsgruppens yttrande 3/2013 om ändamålsbegränsning, artikel 29-arbetsgruppens yttrande 6/2013 om öppna data och vidareutnyttjande av information från den offentliga sektorn och artikel 29-arbetsgruppens yttrande 5/2014 om avidentifieringsmetoder.

¹¹ Källa: Gartner.

¹² Se t.ex. paneldebatten om framtiden för offentlig statistik i stordataåldern, Royal Statistical Society, London den 19 januari 2015, <http://www.odi.org/events/4068-future-official-statistics-big-data-era> (öppnad 10.9.2015).

¹³ *Ten technologies which could change our lives: potential impacts and policy implications*, enheten för vetenskaplig framsyn vid Europaparlamentets generaldirektorat för parlamentarisk utredning och analys, januari 2015.

¹⁴ EU:s arbetsprogram 2016–2017 för Horisont 2020 stöder denna utveckling, bl.a. genom storskaliga pilotprojekt som ska behandla integritets- och etikfrågor.

¹⁵ Försäkringar har beskrivits som ”originalaffärsmodellen för sakernas internet” i ”From fitness trackers to drones, how the ‘Internet of Things’ is transforming the insurance industry”, *Business Insider* 11.6.2015. Begreppet *prisdiskriminering* i konkurrenslagstiftningen härleds ur artikel 102 i EUF-fördraget. Enligt detta är det förbjudet för ett dominerande företag på marknaden att ”direkt eller indirekt påtvinga någon oskäligen inköps- eller försäljningspriser eller andra oskäligen affärsvillkor”. Begreppet är dock mycket omtvistat, se t.ex. Damien Gerardin and Nicolas Petit *Price Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting Principles* (juli 2005), Global Competition Law Centre Working Paper Series nr 07/05. När det gäller stordata och dess (enligt författarna ännu inte förverkligade) potential för att påskynda skräddarsydd prissättning, se Förenta staternas presidentskansli, *Big Data and Differential Pricing*, februari 2015, och en färsk analys som visar att skräddarsydd prissättning i allmänhet innebär behandling av personuppgifter och därför måste uppfylla dataskyddslagstiftningens krav på insyn, dvs. att företag måste informera

människor om ändamålet med behandlingen av deras personuppgifter: företagen måste informera om att de skräddarsyr priserna. Och om ett företag använder en kaka för att känna igen någon, måste företaget enligt direktivet om integritet och elektronisk kommunikation informera personen om ändamålet med kakan, arbetsutkast av Frederik Borgesius ”Online Price Discrimination and Data Protection Law”. Finns på http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665 (öppnad 10.9.2015).

¹⁶ Medicintekniska produkter definieras i EU-lagstiftningen i rådets direktiv 93/42/EEG om medicintekniska produkter, ändrat genom Europaparlamentets och rådets direktiv 2007/47/EG av den 5 september 2007. Se Europeiska datatillsynsmannens yttrande 1/2015 om vad ”mobil hälsa” innebär för uppgiftsskyddet.

¹⁷ Enligt Eurostat använder 21 procent enskilda personer och 19 procent företag i EU molnbaserade lagringstjänster.

¹⁸ ”Om internet var ett land skulle det vara den tolfte största elkonsumenten i världen, någonstans mellan Spanien och Italien. Detta motsvarar i grova drag 1,1 till 1,5 procent av den globala elförbrukningen (2010) och de växthusgaser som genereras årligen av 70 till 90 stora (500 MW) kolkraftverk.” Natural Resources Defense Council, *Data Centre Efficiency Assessment: Scaling Up Energy Efficiency Across the Data Centre Industry: Evaluating Key Drivers and Barriers* 2014.

¹⁹ Rapport från undersökningen *SMART 2013/0043 – Uptake of Cloud in Europe*.

²⁰ Källa: Eurostat.

²¹ Begreppet *delningsekonomi* har kritiserats för att det är vilseledande: ”The Sharing Economy Isn’t About Sharing at All”, Giana M. Eckhardt och Fleura Bardhi, *Harvard Business Review*, 28.1.2015.

²² Rachel Botsman och Roo Rogers, *What’s Mine Is Yours: How Collaborative Consumption is Changing the Way We Live*, 2011.

²³ Future of Privacy Forum, ”User Reputation: Building Trust and Addressing Privacy Issues in the Sharing Economy”, juni 2015.

²⁴ Se Förenta staternas handelskommissions workshop från den 9 juni 2015 om konkurrens, konsumentskydd och ekonomiska frågor som delningsekonomin leder till, <https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators/> (öppnad 10.9.2015).

²⁵ Angående drönare och fjärrstyrda luftfartygssystem inverkan på uppgiftsskyddet, se Europeiska datatillsynsmannens yttrande om kommissionens meddelande till Europaparlamentet och rådet *En ny era för luftfarten – luftfartsmarknaden öppnas för en säker och hållbar civil användning av fjärrstyrda luftfartygssystem*, november 2014.

²⁶ Källa: Boston Consulting Group.

²⁷ Gartner.

²⁸ Facebooks algoritm för att känna igen ansikten, DeepFace, sägs ha en träffsäkerhet på 97 procent, vilket är bättre än människor. ”DeepFace: Closing the Gap to Human-Level Performance in Face Verification”, offentliggjort i rapporten om IEEE:s konferens om datorsyn och mönsterigenkänning, juni 2014.

²⁹ Robo har definierats som en ”maskin i världen som känner, tänker och agerar”, Bekey, G, ”Current trends in robotics: technology and ethics”, i *Robot Ethics – The ethical and social implications of robotics*, The MIT Press2, 2012, s. 18. Man beräknar att det kommer att säljas 22 miljoner serviceroboter mellan 2013 och 2016; *IRF World Robotics Report*, 2013. Angående artificiell intelligens (AI), se ”Rise of the Machines”, *Economist*, 9.5.2015 och Pew Research Centre Internet Project 2014. Ett företag som arbetar med artificiell intelligens angav som villkor för sitt förvärv av ett ledande teknikföretag 2014 att det skulle inrättas en etik- och säkerhetsnämnd och införas ett

förbud mot användning av AI-arbete för militära ändamål och underrättelseändamål, Forbes, ”Inside Google’s Mysterious Ethics Board”, 3.2.2014.

³⁰ Pentland, *Social physics*, s. 147.

³¹ Se fotnot 9. Pentland *Social Physics* s. 153: ”Det är fullt möjligt att göra stora framsteg inom hälso- och sjukvård, transport, energi och säkerhet... de största hindren för att nå dessa mål är oro över den personliga integriteten och att vi ännu inte har uppnått samförstånd om avvägningen mellan den enskildes och samhällets värderingar.” Debatten kring ebolapandemin i Västafrika 2014 är ett bra exempel på denna falska uppdelning mellan den personliga integriteten och samhällets behov. Sjukdomar har tenderat att spåras och deras livslängd mätas genom undersökningar och folkräkningar som lätt blir föråldrade och som är svåra att extrapolera för att förutse var sjukdomen ska slå till nästa gång. Det finns några exempel på användning av stordata för att spåra malariautbrott i Namibia och Kenya. År 2009 användes stordata för att spåra effektiviteten i statliga hälsovarningar under utbrottet av svininfluensa i Mexiko. En uppgiftskälla är register över mobiltelefonsamtal som visar vilken basstation som hanterat samtalet och kan ge en grov realtidsbild av var människor befinner sig och vart de är på väg. Insamlingen av alla dessa uppgifter är inte riktad. Den kan inte göra åtskillnad mellan personer som har eller inte har ebola. En svensk ideell organisation kartlade befolkningens rörlighet i Västafrika, men uppgifterna användes inte eftersom mobiltelefonoperatörerna inte ville lämna ut uppgifterna till godkända externa forskare och hävdade att de måste få instruktioner från regeringarna, som i sin tur hänvisade till oro för den personliga integriteten, vilken var obefogad enligt EU-lagstiftningen <http://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola>. (öppnad 10.09.2015)

³² Europeiska datatillsynsmannens yttrande 3/2015.

³³ Stordataantagandet ”N=alla” handlar om att man tittar på alla datapunkter, inte bara ett urval, Viktor Mayer-Schönberger, and Kenneth Cukier, *The Rise of Big Data: How it’s changing the way we think about the world*, 2013. Lissabonrådet och Progressive Policy Institute har hävdade att välståndet kommer att öka när den ”digitala tätheten” – ”mängden data som används per capita i en ekonomi” – blir så stor som möjligt <http://www.lisboncouncil.net/component/downloads/?id=1178> (öppnad 10.9.2015). International Working Group on Data Protection in Telecommunications (nedan kallad *Berlingruppen*) har föreslagit undantag för stordata från principerna för uppgiftsskydd, http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf. (öppnad 10.9.2015). Världsekonometiskt forum har uppmanat till en inriktning mot användning, inte insamling, och en övergång från samtycke till insamling av personuppgifter, *Unlocking the Value of Personal Data: From Collection to Usage*, 2013.

³⁴ Se Europeiska datatillsynsmannens preliminära yttrande om privatliv och konkurrenskraft i stordataåldern.

³⁵ I artikel 21 i EU-stadgan om de grundläggande rättigheterna anges följande: ”All diskriminering på grund av bland annat kön, ras, hudfärg, etniskt eller socialt ursprung, genetiska särdrag, språk, religion eller övertygelse, politisk eller annan åskådning, tillhörighet till nationell minoritet, förmögenhet, börd, funktionshinder, ålder eller sexuell läggning ska vara förbjuden.” Många av dessa uppgiftskategorier (som ”avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter som rör hälsa och sexualliv”) får utökat skydd enligt artikel 8 i direktiv 95/46/EG.

³⁶ Angående tanken på en digital gemensam mötesplats, se *Ambition numérique: Pour une politique française et européenne de la transition numérique*, franska digitala rådet, juni 2015 s. 276. Bruce Schneier förespråkar inrättandet av ”offentliga rum utan ägare” på internet, ungefär som allmänna parker, *Data and Goliath*, s. 188–189. Sandy Pentland argumenterar för en ”gemensam mötesplats för offentlig data”, *Social Physics*, s. 179. Angående bedömning av säkerheten när aggregerade uppsättningar data offentliggörs som öppna data, se artikel 29-arbetsgruppens yttrande 6/2013 om öppna data och vidareutnyttjande av information från den offentliga sektorn.

³⁷ ”Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent” <http://crackedlabs.org/studie-kommerzielle-ueberwachung/info>. Angående kvalificerad insyn, se t.ex. Frank Pasquale: *The Black Box Society: The Secret Algorithms that Control Money and Information*.

³⁸ ”Bakom den teknik som påverkar sociala relationer ligger exakt samma sociala relationer”, David Noble, ”Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools”, i *Case Studies in the Labor Process*, red. Andrew Zimbalist, 1979. Se också Judy Wacjman, *Pressed for Time: The Acceleration of Life in Digital Capitalism*, 2014 s. 89–90, och Zuboff, ”Big Other” (se fotnot 3).

³⁹ Yttrande 5/2014 om avidentifieringsmetoder, antaget den 10 april 2014 (WP 216.)

⁴⁰ Angående ett snävt utformat undantag från dataskyddsreglerna för verksamhet som är av rent privat natur eller som har samband med en persons hushåll, se EU-domstolens dom i mål C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů*.

⁴¹ Begreppet prosument myntades av Alvin Toffler i *The Third Wave*, 1980. Angående en diskussion om ”prosumentmiljön” och hur den bör regleras, se Ian Brown och Chris Marsden, *Regulating Code*, 2013.

⁴² Yttrande från Europeiska gruppen för etik inom vetenskap och ny teknik till Europeiska kommissionen: *Ethics of Security and Surveillance Technologies*, yttrande nr 28, 20.5.2015, s. 74.

⁴³ Se t.ex. *Homer Economicus: The Simpsons and Economics*, red. Joshua Hall, 2014.

⁴⁴ Enligt den mest försiktiga definitionen av fel innebär detta att 23 miljoner amerikaner har väsentliga fel i en konsumentrapport. Bland deltagarna i undersökningen hade 5 procent fel som, när de hade korrigerats, förbättrade deras kreditbetyg så mycket att de kunde få kredit till ett lägre pris. *Federal Trade Commission, Report To Congress Under Section 319 Of The Fair And Accurate Credit Transactions Act Of 2003*, december 2012, Chris Jay Hoofnagle, *How the Fair Credit Reporting Act Regulates Big Data* (10 september 2013). *Future of Privacy Forum Workshop on Big Data and Privacy: Making Ends Meet*, 2013. Finns på SSRN: <http://ssrn.com/abstract=2432955>.

⁴⁵ Enligt Världsekonometiskt forum är data en värdefull tillgång för den enskilda personen och rätten att inneha, använda och disponera data får överlåtas till företag och regeringar i utbyte mot tjänster. Se anföranden nyligen även av kommissionens vice ordförande Andrus Ansup, t.ex. den 7 september 2015, vid det årliga Bruegelmötet, med titeln ”Produktivitet, innovation och digitalisering – vilka globala politiska utmaningar?”: ”Ägande och hantering av dataflöden, användning och återanvändning av uppgifter. Hantering och lagring av data. Detta utgör grunden för viktiga framväxande sektorer som molnbaserade datortjänster, sakernas internet och stordata.”

⁴⁶ ”Så vem äger rätten att använda information och data som faktiskt inte tillhör ens jag? Detta är en fråga som går utöver gränserna för handel, etik och moral och som leder till frågor om integritet och skydd av privatlivet”, Al-Khouri, november 2012, http://www.academia.edu/6726887/Data_Owner_Ship_Who_Owns_My_Data_036. Se också Margaret Jane Radin, ”Incomplete Commodification in the Computerized World”, i *The Commodification of Information* 3, 17, red. Niva Elkin-Koren och Neil Weinstock Netanel. 2002: ”Det är stor skillnad om man betraktar integritet som en mänsklig rättighet, som åtföljer personer på grund av att de är personer, eller som en äganderätt, något som personer kan äga och kontrollera. Mänskliga rättigheter antas vara oförytterliga på en marknad, medan äganderätt antas kunna säljas på en marknad.”

⁴⁷ Syftet med Crosscloud-projektet vid MIT:s laboratorium för datorvetenskap och artificiell intelligens, som får stöd av flera EU-baserade företag, är att ”1) göra det enkelt att utveckla (”social”) programvara för flera användare med enbart frontutveckling och med respekt för användarnas rättigheter och integritet, 2) ge användarna frihet att lätt förflytta sig mellan tillämpningar, hårdvaruplattformar och sociala nät och behålla sina uppgifter och sociala kopplingar”, <http://openpds.media.mit.edu/#architecture> (öppnad 10.9.2015).

⁴⁸ Se förklaring till artikel 1 i EU-stadgan om de grundläggande rättigheterna.

⁴⁹ Martha Nussbaum, ”Objectification”, i *Philosophy and Public Affairs* 24.4.1995.

⁵⁰ Dom av den 15 december 1983, BVerfGE 65, 1–71, Volkszählung.

⁵¹ Se Europeiska gruppen för etik inom vetenskap och ny teknik till Europeiska kommissionen: yttrande om etik och övervakning, s. 75. En undersökning visade att en reklamriktad algoritmer var diskriminerande, där sökningar i genomsnitt visade annonser för mer högvärlödade jobb för män än för kvinnor som besökte arbetsförmedlingssajter, Carnegie Mellon University och International Computer Science Institute. Angående att digitala assistenter tenderar att ha en kvinnlig röst som förinställt värde, se t.ex. Judy Wajcman, ”Feminist theories of technology”, *Cambridge Journal of Economics*, 34 (1). s. 143–152, 2010.

⁵² Giorgio Agamben, *State of Exemption*, 2005.

⁵³ Neil Richards, Neil och Jonathan King, ”Big Data Ethics” (19.5.2014), *Wake Forest Law Review*, 2014.

⁵⁴ BBC, Information watchdog undersöker ”välgörenhetsorganisationers försäljning av uppgifter”, 1.9.2015.

⁵⁵ Se skrivelse från Future of Life Institute. Påvens encyklika *Laudato Si*: ”När medier och den digitala världen blir allestädes närvarande kan deras inflytande hindra människor från att lära sig hur man ska leva med vishet, tänka djupt och älska generöst. I detta sammanhang riskerar gamla tiders vise män att försvinna i bruset och distraktionerna från en informationsöverdos. Det krävs ansträngningar för att hjälpa dessa medier att bli en källa till nya kulturella framsteg för mänskligheten och inte ett hot mot våra djupaste rikedomar. Sann visdom, som är resultatet av självreflektion, dialog och generösa möten mellan människor, går inte att förvärva genom en ren ansamling av uppgifter, som i slutänden leder till överbelastning och förvirring, en slags mental förorening. Verkliga relationer till andra, med alla de utmaningar som de medför, tenderar nu att ersättas med en typ av internetkommunikation där vi nyckvis kan välja eller välja bort förbindelser, vilket leder till en ny form av konstlade känslor som hänger mer ihop med apparater och skärmar än med människor och natur. Dagens medier ger oss möjlighet att kommunicera och dela med oss av våra kunskaper och känslor, men ibland skärmar de också av oss från direktkontakt med andras smärta, rädslor och glädjeämnen och det komplexa i deras personliga erfarenheter. Därför bör vi vara uppmärksamma på att samtidigt som dessa medier erbjuder spännande möjligheter, riskerar det också att växa fram ett djupt och melankoliskt missnöje med personliga relationer eller en skadlig upplevelse av isolering.”

⁵⁶ Se åtgärd 4 i Europeiska datatillsynsmannens strategi 2015–2020 för att utveckla en etisk dimension i dataskyddet (*ej översatt till svenska*).