

EUROPEAN DATA PROTECTION SUPERVISOR

Udtalelse nr. 4/2015

Mod en ny digital etik

Data, værdighed og teknologi



11. september 2015

Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) er en uafhængig EU-institution, der i henhold til artikel 41, stk. 2, i forordning 45/2001 har "til opgave at sikre, at fællesskabsinstitutionerne og -organerne respekterer fysiske personers grundlæggende rettigheder og frihedsrettigheder, især retten til privatlivets fred i forbindelse med behandling af personoplysninger" og "[...] rådgive disse institutioner og organer samt de registrerede om alle spørgsmål vedrørende behandling af personoplysninger". Han blev sammen med den assisterende tilsynsførende udpeget i december 2014 med den specifikke opgave at være mere konstruktiv og proaktiv. EDPS offentliggjorde i marts 2015 en femårig strategi for, hvordan han agter at løse denne opgave, og hvordan han agter at stå til ansvar for, at det sker.

Denne udtalelse ligger i forlængelse af EDPS' tidligere udtalelse om den generelle forordning om databeskyttelse, der havde til formål at hjælpe EU's primære institutioner med at nå frem til den rette konsensus om et brugbart, fremtidsorienteret regelsæt, som styrker fysiske personers rettigheder og frihedsrettigheder. Ligesom udtalelsen om mobilsundhedsydelse i begyndelsen af 2015 behandler den udfordringerne i forbindelse med databeskyttelsens "digitalisering" – det tredje mål i EDPS' strategi – "tilpasning af de eksisterende databeskyttelsesprincipper til den globale digitale arena", også i lyset af EU's planer for det digitale indre marked. Den er i overensstemmelse med Artikel 29-Gruppens tilgang til databeskyttelsesaspekterne ved anvendelsen af nye teknologier, f.eks. "tingenes internet", hvortil EDPS bidrog som fuldgældigt medlem af gruppen.



Dignity	Værdighed
Future-oriented rules and enforcement	Fremtidsorienterede regler og håndhævelse
Accountable controllers	Ansvarlige registeransvarlige
Empowered individuals	Beføjelser til fysiske personer
Innovative privacy engineering	Innovativ privatlivsbevidst konstruktion
Ethics	Etik

"Den menneskelige værdighed er ukrænkelig. Den skal respekteres og beskyttes".

Artikel 1, EU's charter om grundlæggende rettigheder

Den grundlæggende ret til privatlivets fred og til beskyttelse af personoplysninger er blevet vigtigere for beskyttelsen af den menneskelige værdighed end nogensinde før. Disse rettigheder er nedfældet i EU-traktaterne og i EU's charter om grundlæggende rettigheder. De giver fysiske personer mulighed for at udvikle deres egen personlighed, leve et uafhængigt liv, innovere og udøve andre rettigheder og frihedsrettigheder. De databeskyttelsesprincipper, der er fastsat i EU-chartret – nødvendighed, proportionalitet, rimelighed, dataminimering, formålsbegrænsning, samtykke og gennemsigtighed – gælder for hele databehandlingen, for såvel indsamling som for anvendelse.

Teknologien bør ikke diktere værdier og rettigheder, men forholdet mellem dem bør heller ikke reduceres til et falsk modsætningsforhold. Den digitale revolution giver forventning om fordele for sundheden, miljøet, den internationale udvikling og den økonomiske effektivitet. I forbindelse med EU's planer for et digitalt indre marked anses cloudcomputing, "tingenes internet", big data og andre teknologier for at være af central betydning for konkurrenceevne og vækst. Forretningsmodeller udnytter ny kapacitet til massiv indsamling, øjeblikkelig videregivelse, kombination og genbrug af personoplysninger til uforudsete formål og begrundet i omfattende og utilgængelige privatlivspolitikker. Dette har sat databeskyttelsesprincipperne under nyt pres, hvilket kræver nytænkning af, hvordan de anvendes.

I dagens digitale miljø er det ikke tilstrækkeligt at overholde loven, vi skal tage den etiske dimension af databehandling i betragtning. EU-lovgivningen giver allerede mulighed for fleksible, specifikke beslutninger og sikkerhedsforanstaltninger ved håndtering af personoplysninger. Reformen af lovgivningen vil være et godt skridt fremad. Men der er mere dybtgående spørgsmål med hensyn til indvirkningen af tendenser i det datadrevne samfund på værdigheden, den enkeltes frihed og demokratiets funktion.

Disse spørgsmål har tekniske, filosofiske, juridiske og moralske konsekvenser. I denne udtalelse fremhæves en række vigtige teknologiske tendenser, som kan være forbundet med en uacceptabel behandling af personoplysninger eller gøre indgreb i retten til privatlivets fred. Den beskriver et firstrengnet "big data protection ecosystem" (økosystem til beskyttelse af big data) med henblik på at tage den digitale udfordring op: en kollektiv indsats, der understøttes af etiske overvejelser.

- (1) En fremtidsorienteret regulering af databehandling og retten til respekt for privatlivets fred og til databeskyttelse.
- (2) Ansvarlige registeransvarlige, som fastlægger behandlingen af personoplysninger.
- (3) Privatlivsbevidst konstruktion og design af databehandlingsprodukter og -tjenester.
- (4) Beføjelser til fysiske personer.

Den Europæiske Tilsynsførende for Databeskyttelse ønsker at sætte gang i en åben og informeret debat i og uden for EU, med inddragelse af civilsamfundet, designere, virksomheder, akademikere, offentlige myndigheder og reguleringsmyndigheder. EU's nye etiske databeskyttelsesråd, som vi vil oprette hos EDPS, vil være med til at definere en ny

digital etik, som giver bedre mulighed for at opnå fordelene ved teknologien for samfundet og økonomien på måder, som styrker fysiske personers rettigheder og frihedsrettigheder.

INDHOLDSFORTEGNELSE

1. Data overalt: Tendenser, muligheder og udfordringer	7
1.1 BIG DATA	7
1.2 "TINGENES INTERNET"	8
1.3 AMBIENT COMPUTING	8
1.4 CLOUDCOMPUTING	8
1.5 FORRETNINGSMODELLER, DER AFHÆNGER AF PERSONOPLYSNINGER	9
1.6 DRONER OG AUTONOME KØRETØJER	9
1.7 TENDENSER MED POTENTIELT STØRRE INDVIRKNING PÅ LÆNGERE SIGT	10
2. Et økosystem til beskyttelse af big data.....	10
2.1 FREMTIDSORIENTERET REGULERING	11
2.2 ANSVARLIGE REGISTERANSVARLIGE	11
2.3 PRIVATLIVSBEVIDST KONSTRUKTION.....	12
2.4 BEFØJELSER TIL FYSISKE PERSONER	12
<i>Et producent-forbrugermiljø.....</i>	<i>12</i>
<i>Samtykke</i>	<i>12</i>
<i>Kontrol og "dataejerskab"</i>	<i>13</i>
3. Værdighed i centrum for en ny digital etik	13
3.1 VÆRDIGHED OG DATA.....	14
3.2 ET EUROPÆISK ETISK RÅDGIVENDE ORGAN.....	15
4. Konklusion: Tid til at uddybe debatten	16
Noter	17

1. Data overalt: Tendenser, muligheder og udfordringer

Stadig flere personoplysninger bliver indsamlet og behandlet på stadig mere uigennemsigtige og komplekse måder. Med den gradvise udbredelse af computere i virksomheder og offentlige administrationer i 1980'erne var der en udbredt opfattelse af, at den praksis, som magtfulde regeringer og selskaber benyttede til at behandle personoplysninger, reducerede fysiske personer til registrerede og udgjorde en trussel mod de grundlæggende rettigheder og frihedsrettigheder. Det, der kendetegner den nuværende bølge af integreret informations- og kommunikationsteknologi, er dens allestedsnærværelse og indflydelse.

Sidste år blev det rapporteret, at der var flere enheder med internetforbindelse på planeten end mennesker¹. Større processorkapacitet², lagring og transmissionsbåndbredde betyder, at der er gradvist færre tekniske begrænsninger for at behandle personoplysninger. "Tingenes internet" og big data-analyser ventes at konvergere med kunstig intelligens, natursprogsbehandling og biometriske systemer som udgangspunkt for applikationer med maskinlæring til avanceret intelligens. Regeringer og virksomheder kan udvide "data mining" til "reality mining", som findes i hverdagsoplevelser, kommunikation og endda tanker³. I takt med at samfundet tilpasser sig kravene på det digitale marked, gøres der nu igen bestræbelser for at lære små børn at programmere⁴. At styrke disse tendenser i en sektor, hvor EU er en førende forbruger, men halter efter med hensyn til at levere tjenester, er et tilbagevendende tema i Kommissionens strategi for det digitale indre marked⁵.

Disse tendenser og mange af de begreber, der anvendes i dag, er trods deres udbredelse svage og overlappende. For at bidrage til at skabe en debat ønsker vi at fremhæve specifikke tendenser, som – om end de ikke er udtømmende – efter vores opfattelse stiller de vigtigste etiske og praktiske spørgsmål vedrørende anvendelsen af principperne om databeskyttelse.

1.1 Big data

"Big data"⁶ henviser til den praksis, hvor enorme mængder meget forskellige oplysninger kombineres og analyseres, ofte ved hjælp af selvlærende algoritmer, med henblik på at træffe informerede beslutninger. Disse oplysninger er ikke altid personoplysninger: data, der er genereret af sensorer til overvågning af fysiske eller atmosfæriske fænomener som vejrforhold eller forurening eller til overvågning af de tekniske aspekter af fremstillingsprocesser, vedrører ikke "en identificeret eller identificerbar fysisk person"⁷. Men en af de største værdier af big data for virksomheder og regeringer stammer fra overvågningen af *menneskelig* adfærd, både kollektivt og individuelt, og ligger i deres prædiktive potentiale⁸.

Et resultat heraf er fremkomsten af en indtægtsmodel for internetvirksomheder, der benytter sporing af onlineaktiviteter til at optimere den økonomiske værdi af transaktioner til tjenesteydere, ikke kun til målrettet markedsføring, men også betingelser for og priser på forsikringspolicer, lån og andre kontraktforhold. På det konkurrenceprægede marked for brugernes opmærksomhed er de færreste mennesker klar over det store omfang af denne sporing⁹. Sådanne "big data" bør også anses for at være personoplysninger, selv om der er anvendt anonymiseringsteknikker. Det bliver stadig lettere at udlede en persons identitet ved at kombinere angiveligt "anonyme" data med andre datasæt, herunder offentligt tilgængelige oplysninger, f.eks. på de sociale medier¹⁰. Når disse data handles, navnlig på tværs af grænser og jurisdiktioner, bliver ansvaret for at behandle oplysningerne vage og vanskelige at fastslå eller håndhæve i henhold til databeskyttelseslovgivningen, navnlig i mangel af internationale standarder.

1.2 "Tingenes internet"

Der findes allerede mange helt almindelige enheder, som er forbundet til internettet, som smartphones, tablets og maskiner til kontanthævninger og til indcheckning på fly. Konnektivitet forudses inden 2020 at blive en standardfunktion med 25 mia. internetforbundne objekter (sammenlignet med 4,8 mia. i 2015) bestående af alt fra telemedicin til køretøjer, fra intelligente målere til en lang række nye stationære og mobile enheder, der anvendes i intelligente byer¹¹.

Disse sensorer vil give øjeblikkelige og granulerede oplysninger, som statistikbureauer og undersøgelser ikke kan nå frem til i dag, men som ikke nødvendigvis er mere præcise og endda kan være potentielt misvisende¹². De anslåede 1,8 mia. autonome forbindelser mellem maskiner inden 2022 kan reducere ulykker og forurening samt øge produktiviteten og gøre ældre og handicappede mere selvhjulpne¹³. "Wearables" som tøj og ure vil behandle personoplysninger på samme måde som andre internetforbundne enheder. De kan opdage blodpropper og overvåge både sundhed og sårheling, ligesom internetforbundne tekstiler kan beskytte mod ekstreme miljøer, f.eks. i forbindelse med brandslukning. Disse enheder vil uploade personoplysninger direkte til lagring i skyen, være forbundet til sociale netværk og potentielt offentliggøre oplysningerne, hvilket gør det muligt at identificere brugere og spore fysiske personers og gruppers adfærd og bevægelser¹⁴.

Den måde, disse oplysninger behandles på, kan påvirke privatlivets fred, ikke kun for brugerne af enhederne, herunder ved brug på arbejdspladsen, men også rettighederne for andre, der observeres og registreres af enheden. Selv om der er meget lidt, der tyder på egentlig forskelsbehandling, er det klart, at den store mængde personoplysninger, som indsamles af "tingenes internet" er af stor interesse med hensyn til at maksimere indtægterne gennem mere personlige priser, alt efter den sporede adfærd, navnlig inden for sygeforsikringssektoren¹⁵. Andre domænespecifikke regler vil også blive udfordret, f.eks. hvor enheder, der omfatter behandling af sundhedsoplysninger, ikke rent teknisk kan kategoriseres som medicinsk udstyr og falder uden for forordningens anvendelsesområde¹⁶.

1.3 Ambient computing

Ambient eller usynlig computing henviser til den teknologi, der ligger til grund for "tingenes internet". En af dets mest oplagte anvendelsesmuligheder er "intelligente hjem" og "intelligente kontorer", som består af enheder med indbygget og sofistikeret kapacitet til behandling af oplysninger, som lover større energieffektivitet og mere oplyste personer, som kan fjernstyre deres forbrug (om end dette ville kræve, at beboeren var uafhængig af udlejeren eller bygningsadministratoren). Det skal stå klart, hvem der er ansvarlig for formålet med og midlerne til behandling af de personoplysninger, som anvendes til ambient computing, ikke kun for at beskytte fysiske personers grundlæggende rettigheder, men også for sikre en korrekt ansvarsfordeling og overholdelse af de overordnede krav til systemsikkerheden.

1.4 Cloudcomputing

Cloudcomputing er kendt som en central teknologi, både med hensyn til de avancerede analyse- og miningfunktioner, indsamling af big data og analyser og strømmen af oplysninger fra "tingenes internet", som aktuelt anvendes af omkring en femtedel af alle personer og virksomheder i EU¹⁷. Cloudcomputing gør det muligt at samle data fra de utallige enheder,

som er forbundet til "tingenes internet", og udnytter tilgængeligheden og konnektiviteten af enorme mængder data i enorme lagrings- og behandlingsfaciliteter i hele verden¹⁸. En bredere anvendelse af cloudcomputing¹⁹ i den private og offentlige sektor anslås at føje i alt 449 mia. EUR til EU28's BNP (0,71 % af EU's samlede BNP).

Kontrol over personoplysninger deles ofte mellem kunden og udbyderen af cloudtjenesten, og det er ikke altid klart, hvem der bærer ansvaret for databeskyttelsesforpligtelserne. Dette kan betyde, at der i praksis gives utilstrækkelig beskyttelse. Disse forpligtelser gælder uanset **datalagerets fysiske placering**. Endvidere kan infrastrukturen for cloudcomputing, selv om den kun er en baggrundsteknologi, der understøtter virksomheden, i sig selv blive en kritisk infrastruktur og skabe større ubalancer i markedspositionerne, idet 30 % af virksomhederne har haft problemer med at afmelde abonnementer eller ændre udbyder²⁰.

1.5 Forretningsmodeller, der afhænger af personoplysninger

Disse teknologier har åbnet mulighed for nye forretningsmodeller, som gør brug af oplysninger, der ikke kun genereres af leverede tjenester, men også af andre kilder som sociale medier, til at vurdere risiko og kreditværdighed og maksimere indtægterne. En fremtrædende forretningsmodel i dag findes i form af platforme, som forbinder sælgere og købere, således at de kan dele og omfordele produkter, tjenesteydelser, færdigheder og aktiver. Disse platforme kaldes ofte "deleøkonomi", "samarbejdsforbrug" eller online og mobile fagfælleplatforme²¹ og kan tilbyde klassiske økonomiske fordele ved at give markedet en konkurrencemæssig indsprøjtning og reducere spild. Deres globale værdi skønnes at blive firedoblet fra 26 til 110 mia. USD i de kommende år²². Sådanne datadrevne forretningsmodeller skaber allerede enorme indtægter inden for deling af biler og udlejning af private hjem og inden for finansiel teknologi og sociale lån. Undersøgelser viser, at forbrugerne værdsætter deres tilsyneladende mere overkommelige priser og større bekvemmelighed²³.

Valutaen for sådanne platforme er typisk brugernes omdømme, fagfællebedømmelser og identitetskontrol. Dette kan potentielt ses som øget gennemsigtighed og ansvarlighed, men ikke nødvendigvis i forhold til platformudbyderen selv. Store aktører på disse markeder er blevet kritiseret for angiveligt at tilbageholde oplysninger om omdømme for de individuelle brugere, som oplysningerne netop vedrører. Der er en stor risiko for, at fysiske personer udelukkes fra tjenester på grundlag af omdømme, der er baseret på unøjagtige oplysninger, som de ikke kan anfægte eller anmode om at få slettet. Anvendelsen af data fra flere forskellige kilder sætter også spørgsmålstegn ved princippet i EU-lovgivningen om dataminimering. Omfanget af disse og fremtidige teknologibaserede forretningsmodellers indvirkning på fysiske personer og samfundet i fremtiden giver stof til eftertanke²⁴.

1.6 Droner og autonome køretøjer

Droner eller halvautonome luftfartøjer tjener i dag mange militære formål, men anvendes i stigende grad til overvågning, kortlægning, transport, logistik og offentlig sikkerhed som f.eks. til at inddæmme naturbrande²⁵. Billeder, videoer og andre personlige data, som indsamles af droner, kan udveksles via telenet. Brug af droner medfører en alvorlig risiko for indgreb i privatlivets fred og har en skræmmende effekt på ytringsfriheden. Spørgsmålet er, hvordan deres design og anvendelse effektivt kan reguleres, så de registrerede kan udøve deres ret til adgang til de data, der indsamles af disse maskiner.

På jorden vil autonome køretøjer eller førerløse biler ændre den måde, individuelle rejser anvendes og tilrettelægges på, og dette kan sløre forskellen mellem privat og offentlig

transport. Det anslås, at der vil være 12 mio. helt autonome og 18 mio. delvist autonome køretøjer i 2035, og at Europa vil være blandt de første brugere²⁶. De algoritmer, der styrer bilerne, vil påvirke de beslutninger, som direkte kan påvirke den fysiske integritet og endog liv eller død for fysiske personer, for eksempel med hensyn til det indprogrammede valg i tilfælde af et uundgåeligt sammenstød. Ud over det åbenlyse behov for klarhed om, hvem der er ansvarlig og hæfter for datastyring og datasikkerhed, rejser disse applikationer en række etiske spørgsmål.

1.7 Tendenser med potentielt større indvirkning på længere sigt

3D-bioprinting af organiske dele, som bruger kopier af patienters celler og "biobandager" af kollagen (dvs. følsomme oplysninger i henhold til EU-lovgivningen) til at fastlægge række på række af levende celler, vurderes snart at blive tilgængelige²⁷. Det vil gøre det lettere at levere specialfremstillede menneskelige anatomiske dele og være særlig værdifuldt i fattige dele af verden og post-konfliktområder. Bioprinting rejser indlysende spørgsmål vedrørende medicinsk etik, beskyttelse af intellektuel ejendom og forbrugerbeskyttelse, men også, da bioprinting bygger på behandling af fortrolige og følsomme oplysninger om fysiske personers helbred, vedrørende anvendelse af reglerne om databeskyttelse.

Kunstig intelligens, såsom robotteknologi, henviser til et teknologisk krav om autonome maskiner, stationære såvel som mobile. I takt med at de udvikles, vil deres potentiale vokse enormt i forhold til i dag. "Deep learning"-computere lærer sig selv opgaver ved at behandle store datasæt ved hjælp af (bl.a.) neurale netværk, der synes at efterligne hjernen. Forskere og virksomheder søger at skabe bedre læring uden opsyn. Algoritmer kan allerede forstå og oversætte sprog, genkende billeder, skrive nyhedsartikler og analysere medicinske oplysninger²⁸. Sociale medier leverer enorme mængder af personoplysninger, som personer selv har mærket. Dette kan være den seneste i en række af kognitive forbedringer til at øge den menneskelige hjernes evne, som papiret eller kuglerammen eller, integreret i autonome maskiner, robotter, men nu er det tid til at overveje de bredere konsekvenser for både fysiske personer og samfundet²⁹.

2. Et økosystem til beskyttelse af big data

EU har nu mulighed for at føre an og vise, hvordan regeringer, reguleringsmyndigheder, registeransvarlige, designere, udviklere og fysiske personer bedre kan arbejde sammen om at styrke rettigheder og styre, ikke blokere for teknologisk innovation. Den tendens, som er beskrevet i afsnit 2, har, ifølge en kommentator, "udvidet kløften mellem det, der er muligt, og det, der er lovligt"³⁰. I modsætning til visse påstande er privatliv og databeskyttelse en platform for et bæredygtigt og dynamisk digitalt miljø, ikke en hindring. Uafhængige databeskyttelsesmyndigheder som EDPS spiller en central rolle i forhold til at aflive sådanne myter og imødekomme fysiske personers reelle bekymringer over at miste kontrollen med deres personoplysninger³¹.

Den næste generation af personoplysninger vil sandsynligvis være endnu mindre tilgængelig for de personer, som den vedrører. Ansvar for at forme et bæredygtigt digitalt indre marked er nødvendigvis spredt, men det er også, ligesom et økosystem, indbyrdes afhængigt og kræver et effektivt samspil mellem udviklere, virksomheder og reguleringsmyndigheder til gavn for den enkelte. I dette afsnit beskriver vi, hvordan disse fire vigtige spillere kan bidrage til dette.

2.1 Fremtidsorienteret regulering

Vi opfordrede for nylig EU til at gribe den historiske mulighed for at indføre mere enkle regler for behandling af personoplysninger, som vil forblive relevante for en hel generation³². Forhandlingerne om den generelle forordning om databeskyttelse og databeskyttelsesdirektivet i politiet og retsvæsenet er gået ind i de sidste faser, og opmærksomheden vil snart blive rettet mod fremtiden for direktivet om databeskyttelse inden for elektronisk kommunikation og den nye forordning om, hvordan EU's institutioner og organer selv behandler personoplysninger. Da de økonomiske omkostninger ved at indsamle og lagre data er tæt på ubetydelige, vil det være op til databeskyttelsesmyndighederne at håndhæve disse regler konsekvent for at undgå den moralske risiko, der er forbundet med overdreven databehandling³³.

I strategien for det digitale indre marked anerkendes sammenhængen mellem kontrol med store mængder data og markedsstyrke. Strategien følger samme overbevisning, som vi udtrykte i vores foreløbige udtalelse i 2014 om privatlivets fred og konkurrenceevne i big data-tidsalderen ("Privacy and Competitiveness in the Age of Big Data"), om, at der er behov for mere sammenhæng blandt reguleringsmyndighederne. EU har allerede redskaberne til at genoprette de styrkemæssige ubalancer på det digitale marked. Som eksempel er Europa-Kommissionens verserende antitrustsag en tilkendegivelse af, at mobile enheder dominerer markedet med hensyn til adgang til internettet. Det er muligt at foretage en mere holistisk håndhævelse inden for de eksisterende juridiske rammer, f.eks. gennem et clearing house i EU, hvor tilsynsmyndighederne kan overveje, om individuelle sager kan anfægte overholdelsen af konkurrence-, forbruger- og databeskyttelsesreglerne. F.eks.:

- Krav om større prisgennemsigtighed – kontant eller anden betaling – for en tjeneste, kan præge og lette analysen af konkurrencesager³⁴.
- Sporing af urimelig prisdiskrimination på grundlag af dårlig datakvalitet og urimelig profilering og korrelationer³⁵.

En tættere dialog mellem reguleringsmyndigheder fra forskellige sektorer kan fremkalde en reaktion på den stigende efterspørgsel efter globale partnerskaber, som kan skabe et "fællesareal" for åbne data, hvor data og idéer, såsom statistikker og kort, kan flyde frit og være til rådighed og udveksles i offentlighedens interesse med mindre risiko for overvågning og give fysiske personer større indflydelse på beslutninger, der vedrører dem³⁶.

2.2 Ansvarlige registeransvarlige

Ansvarlighed kræver, at der indføres interne politikker og kontrolsystemer, som sikrer overholdelse og giver relevante beviser, især til uafhængige tilsynsmyndigheder.

Vi har argumenteret for at fjerne bureaukratiet i databeskyttelseslovgivningen ved at minimere kravene til unødvendig dokumentation for at give så meget plads som muligt til mere ansvarlige initiativer fra virksomhederne støttet af vejledning fra databeskyttelsesmyndighederne. Princippet om, at personoplysninger kun bør behandles på måder, der er kompatible med det eller de specifikke formål, som de blev indsamlet til, er afgørende med hensyn til at respektere den enkeltes berettigede forventninger. For eksempel kan adfærdskodekser, revisioner, certificering og en ny generation af kontraktbestemmelser og bindende virksomhedsregler hjælpe med at opbygge en solid tillid til det digitale marked. De ansvarlige for at behandle personoplysninger bør være langt mere dynamiske og proaktive og bevæge sig væk fra den såkaldte "sorte boks"-tendens til at benytte hemmeligholdelse og

uigennemsi g tighed i deres forretningsmetoder, samtidig med, at de kræver stadig større gennemsi g tighed hos kunderne³⁷.

2.3 Privatlivsbevidst konstruktion

Menneskelig innovation har altid været et produkt af aktiviteter i særlige sociale grupper og specifikke sammenhænge, der som regel afspejler tidens samfundsmæssige normer³⁸. Men beslutninger om teknologisk design bør ikke diktere vores samfundsmæssige interaktion og strukturen i vores samfund, men støtte vores værdier og grundlæggende rettigheder.

EU bør udvikle og fremme konstruktionsteknikker og -metoder, der gør det muligt at gennemføre databehandlingsteknologier, der fuldt ud respekterer den enkeltes værdighed og rettigheder. System- og softwareudviklere skal være bedre til at forstå og anvende principperne om privatlivsbevidst konstruktion i nye produkter og tjenester i alle konstruktionens faser samt teknologier. Ansvarlighed skal understøttes af mere forskning i og udvikling af metoder og værktøjer, der sikrer nøjagtige revisioner og klarlægger, om registeransvarlige og registerførere overholder reglerne, f.eks. ved at "tagge" alle personoplysninger med "metadata", der beskriver databeskyttelseskravene.

Tekniske løsninger bør styrke de personer, der ønsker at beskytte deres privatliv og frihed gennem anonymitet. EU bør fremme udformningen og gennemførelsen af algoritmer, der skjuler identiteter og aggregerer data for at beskytte den enkelte og samtidig udnytter den prædiktive effekt af dataene³⁹.

I dag skal vi lægge grunden til at løse disse opgaver ved at samle udviklere og databeskyttelsesekspertter fra forskellige områder i brede netværk som f.eks. IPEN (Internet Privacy Engineering Network), som bidrager til en frugtbar tværfaglig udveksling af idéer og strategier.

2.4 Beføjelser til fysiske personer

Et producent-forbrugermiljø

Fysiske personer er ikke blot passive objekter, der kræver lovens beskyttelse mod udnyttelse. De ovenfor beskrevne digitale tendenser er en positiv mulighed for at styrke den enkeltes rolle. For eksempel både producerer og forbruger mennesker nu indhold og tjenester og kan i stigende grad anses for sammen med tjenesteudbydere at have et fælles ansvar for at behandle personoplysninger, medmindre det udelukkende sker til "husbehov"⁴⁰ (begrebet producent-forbruger skal beskrive netop denne udvikling⁴¹). I mellemtiden tilbyder virtuelle valutaer brugerne anonymitet og omgåelse af tredjemandskontrol af transaktioner og dermed lavere transaktionsomkostninger til betaling for varer og tjenesteydelser på tværs af grænserne. På anden side kan den anonyme karakter af disse virtuelle valutaer på tværs af jurisdiktioner (eller, kan det hævdes, *uden jurisdiktion*) gøre fysiske personer sårbare over for svig og kriminelle markeder, som er svære at opdage og undersøge. Ud over reguleringsmyndighedernes, virksomhedernes og teknikernes pligter har borgerne også et ansvar for at være opmærksomme, agtpågivende, kritiske og informerede, når de foretager valg både online og offline⁴².

Samtykke

Endvidere er det, stik mod traditionel tankegang, ikke al menneskelig adfærd, som kan forklares med økonomiske principper, der antager, at mennesker er helt gennem rationelle og

følsomme over for økonomiske incitament⁴³. Dette er relevant for den rolle, som den enkeltes samtykke i fremtiden kommer til at spille i forhold til behandling af personoplysninger. I henhold til EU-lovgivningen er samtykke ikke det eneste legitime grundlag for de fleste former for behandling. Selv hvor samtykke spiller en vigtig rolle, fritager det ikke de registeransvarlige fra deres ansvar for, hvad de gør med oplysningerne, navnlig hvor der er indhentet et generelt samtykke til behandling til en lang række formål.

Kontrol og "dataejerskab"

Fysiske personer skal kunne anfægte fejl og urimelige fordomme som følge af den logik, der anvendes af algoritmer til at bestemme formodninger og antagelser. Som et eksempel kan nævnes en amerikansk undersøgelse af næsten 3 000 kreditrapporter for 1 000 forbrugere, hvor det blev konstateret, at 26 % havde "væsentlige" fejl – problemer, som var tilstrækkeligt alvorlige til at påvirke forbrugernes kreditvurdering og dermed omkostningerne ved at opnå kredit⁴⁴.

Data anses ofte som en ressource, der ligesom olie ideelt set handles af lige informerede transaktionsparter⁴⁵. Kunderne modtager ikke rimelig kompensation for deres personoplysninger, som handles, og der er hørt røster til støtte for en dataejerskabsmodel. Det er imidlertid svært at garantere absolut kontrol over personoplysninger – der vil være andre bekymringer som offentlige interesser og andres rettigheder og frihedsrettigheder. Kontrol er nødvendigt, men ikke tilstrækkeligt⁴⁶. Menneskelig værdighed er imidlertid altid konstant, og i henhold til EU-lovgivningen kan ejendomsretten ikke anvendes analogt med personoplysninger, som har en iboende tilknytning til individuelle personer. Der er ingen bestemmelser i EU's databeskyttelseslovgivning om, at en person kan give afkald på denne grundlæggende rettighed.

En alternativ metode til at give mennesker bedre kontrol over deres data, hvem der kan få adgang og til hvilket formål, kunne være at bruge lagre til personoplysninger eller "databokse"⁴⁷. Idéen om et sådant "personligt lager" kræver sikkerhedsmekanismer, der sikrer, at det kun er de enheder, som den registrerede har godkendt, der kan få adgang til oplysningerne, og kun til de dele, som de er godkendt til. Lagre til personoplysninger vil være mest effektive, hvis de vedrører aktuelle og konstant opdaterede oplysninger såsom geospatiale oplysninger eller tegn på liv. Ud over de tekniske beskyttelsesforanstaltninger ville brugerne være forpligtede til at overholde reglerne om udveksling og brug af oplysninger. Konkurrence og muligheden for at ændre den tjeneste, man bruger, er forbrugernes mest effektive styrke til at påvirke det marked for tjenester, som er til rådighed for dem. At sikre at forbindelser kan overføres, herunder identifikatorer og kontaktoplysninger, har vist sig at være en kraftig katalysator for konkurrencen og reducerede reelt forbrugerpriserne, da telekommarkedet blev liberaliseret. Dataportabilitet, det vil sige den faktuelle og praktiske mulighed for at overføre de fleste af ens egne oplysninger fra én tjenesteyder til en anden, er et effektivt udgangspunkt for at skabe de rigtige betingelser for ægte forbrugervalg.

3. Værdighed i centrum for en ny digital etik

En etisk ramme skal understøtte dette digitale økosystems byggesten. EDPS mener, at mere respekt for og bedre beskyttelse af menneskers værdighed kan være en modvægt til den gennemtrængende overvågning og magtasymmetri, som den enkelte nu står over for. Dette bør være i centrum for en ny digital etik

3.1 Værdighed og data

I kølvandet på den industrielle revolution i det 18. og 19. århundrede forsøgte menneskerettighedsbevægelsen at beskytte de sociale vilkår ved at reducere hindringerne for respekten for den enkelte. EU har nu med chartret om grundlæggende rettigheder og efter den universelle erklæring om menneskerettigheder og den europæiske menneskerettighedskonvention taget udgangspunkt i den menneskelige værdigheds ukrænkelighed. En persons værdighed er ikke blot en grundlæggende rettighed i sig selv, men også et grundlag for deraf følgende frihedsrettigheder og rettigheder, herunder retten til privatlivets fred og til beskyttelse af personoplysninger⁴⁸. Krænkelser af værdighed kan omfatte objektivering, hvor en person behandles som et redskab, der tjener en andens formål⁴⁹. Privatlivets fred er en integreret del af den menneskelige værdighed, og retten til databeskyttelse blev oprindeligt udtænkt i 1970'erne og 80'erne som en metode til at kompensere for muligheden for at underminere privatlivets fred og værdighed gennem storstilet behandling af personoplysninger. I Tyskland var retten til "oplysende selvbestemmelse" baseret på retten til personlig værdighed og til fri udvikling af personligheden som fastsat i artikel 1 og 2 i den tyske forfatning⁵⁰.

Men i starten af det 21. århundrede skal fysiske personer i stigende grad give flere og flere personoplysninger over internettet for at deltage i sociale, administrative og handelsmæssige anliggender, og muligheden for at vælge dette fra bliver stadig mere begrænset. Når alle aktiviteter potentielt set altid foregår online, kommer idéen om frit og oplyst samtykke under stadig større pres. Der kastes hele tiden "digitale brødkrummer", som kombineres for at klassificere personer i realtid og skabe flere og til tider modstridende profiler. Disse profiler kan rundsendes på mikrosekunder uden personernes vidende og bruges som grundlag for vigtige beslutninger, der påvirker dem.

Profiler, der bruges til at forudsige folks adfærd, risikerer at blive udsat for stigmatisering, som styrker eksisterende stereotyper, social og kulturel adskillelse og udstødelse⁵¹, idet en sådan "kollektiv intelligens" undergraver individuelle valg og lige muligheder. Sådanne "filterbobler" eller "personlige ekkokamre" kan ende med at sætte en stopper for al den kreativitet, innovation og ytrings- og forsamlingsfrihed, som har gjort det muligt for den digitale teknologi at blomstre.

I mellemtiden bruges en form for undtagelsestilstand begrundet i "sikkerhed" til at retfærdiggøre de mange lag af indgribende teknikker til overvågning af fysiske personers aktiviteter⁵². For at kunne forstå denne "onde overvågningscirkel" er det nødvendigt at se på den overordnede virkning for samfund og adfærd på langt sigt.

EU skal sammen med tredjelande se nøje på, hvordan det sikres, at disse værdier ikke blot respekteres på papiret, mens de reelt set neutraliseres i cyberspace. Især EU har nu et "kritisk vindue" frem til massevedtagelsen af disse teknologier til at forme værdierne for de digitale strukturer, som kommer til at definere vores samfund⁵³. Dette kræver en ny vurdering af, om de potentielle fordele ved nye teknologier reelt set afhænger af indsamling og analyse af personligt identificerbare oplysninger for milliarder af fysiske personer. En sådan vurdering kan anspore udviklere til at designe produkter, som i realtid afpersonaliserer enorme mængder uorganiserede oplysninger og dermed gør det vanskeligere eller umuligt at identificere en person.

Vi anerkender allerede, at visse former for databehandling, af f.eks. genetiske data, ikke kun skal være genstand for lovgivning, men også for vurderinger af mere samfundsmæssige

bekymringer i f.eks. etiske udvalg. Genetiske data vedrører af natur ikke blot én person, men også dennes forfædre og efterkommere. Genetiske data bruges ikke kun til at identificere familieforhold, men elementer fundet i generne hos en enkelt person kan også give oplysninger om dennes forældre og børn og føre til, at registeransvarlige træffer beslutninger, som påvirker deres muligheder i livet, selv før de fødes. Den potentielle koncentration af genetiske personoplysninger i hænderne på et par store markedsaktører har konsekvenser for både markedsøkonomier og registrerede. En voksende afhængighed af et globalt system for indsamling og analyse af en konstant strøm af data kan gøre samfundet og økonomien mere sårbare over for hidtil usete sikkerhedshuller og ondsindede angreb.

De eksisterende rammer kan slå fejl, hvis vi ikke går fremtiden i møde med nytænkning. Der er en stigende efterspørgsel efter og behov for at se registrerede som individer og ikke blot som forbrugere eller brugere. Reelt uafhængige databeskyttelsesmyndigheder spiller en afgørende rolle i forhold til at forhindre en fremtid, hvor fysiske personer bestemmes af algoritmer og løbende variationer deraf. De skal sættes i stand til at udøve en "omsorgspligt" over for fysiske personer og deres værdighed online. Traditionelle idéer og principper om privatliv og databeskyttelse indeholder allerede etiske nuancer til beskyttelse af værdighed, som f.eks. beskæftigelse og sundhed. Men nutidens tendenser har åbnet et helt nyt kapitel, og der er behov for at undersøge, om principperne er robuste nok til den digitale tidsalder⁵⁴. Begrebet personoplysninger vil i sig selv sandsynligvis blive ændret radikalt i takt med, at teknologien i stigende grad gør det muligt at identificere fysiske personer ud fra tilsyneladende anonyme data. Derudover vil maskinlæring og sammenlægningen af menneskelig og kunstig intelligens undergrave begreber som fysiske personers rettigheder og ansvar.

3.2 Et europæisk etisk rådgivende organ

Det er ikke hensigten at male et alarmerende dystopisk billede. Allerede nu drøftes dette i juridiske, politiske, økonomiske, sociale, videnskabelige og endda religiøse kredse⁵⁵. En enkel strategi, der ensidigt fremmer økonomisk overskud eller overvågning af sikkerhedsårsager, er sandsynligvis ikke mere nyttig end en alt for restriktiv anvendelse af den eksisterende lovgivning, der kvæler innovation og fremskridt. EDPS foreslår derfor en grundig, bred og tværfaglig analyse, der skal udmønte sig i anbefalinger og præge den samfundsmæssige debat om, hvordan et frit og demokratisk samfund bør møde den teknologiske udfordring.

EDPS lovede i sin strategi⁵⁶ at udvikle en etisk tilgang til databeskyttelse og anerkendte, at "mulig, nyttig eller rentabel ikke er lig med bæredygtig", og understregede et "ansvar over for mekanisk overensstemmelse med lovens bogstav". Vi agter at nå ud til andre end blot EU's tjenestemænd, advokater og it-specialister og ud til fremtrædende personer, som er i stand til at vurdere konsekvenserne af de teknologiske ændringer og lovgivningsmæssige svar på mellemlangt og langt sigt. I de kommende måneder vil vi i vores uafhængige institution nedsætte en ekstern rådgivende gruppe om den etiske dimension af databeskyttelse, som skal undersøge forholdet mellem menneskerettigheder, teknologi, markeder og forretningsmodeller i det 21. århundrede.

Vores etiske rådgivende organ vil bestå af en udvalgt gruppe af fremtrædende personer inden for etik og filosofi, sociologi, psykologi, teknologi og økonomi med den fornødne støtte fra eksperter med viden og ekspertise på områder som sundhed, transport og energi, social interaktion og medier, økonomi og finansiering, forvaltning og demokrati og sikkerhed og

politiarbejde. De vil blive opfordret til at overveje de bredere etiske konsekvenser af, hvordan personlige data opfattes og bruges med størst mulig gennemsigtighed i deres overvejelser.

4. Konklusion: Tid til at uddybe debatten

Privatlivets fred og databeskyttelse er en del af løsningen, ikke problemet. På nuværende tidspunkt kontrolleres teknologien af mennesker. Det er ikke let umiddelbart at klassificere denne potentielle udvikling som god eller dårlig, ønskelig eller skadelig, fordelagtig eller ufordelagtig, og dette endnu mindre, når en række potentielle tendenser skal ses i deres rette sammenhæng. Politiske beslutningstagere, teknologiudviklere, forretningsudviklere og vi alle skal seriøst overveje, om og hvordan vi ønsker at påvirke udviklingen af teknologier og anvendelsen heraf. Men lige så vigtigt er det, at EU hurtigst muligt tager fat på etikken og placeringen af menneskelig værdighed i fremtidens teknologier.

Databeskyttelsesprincipper har vist sig at være i stand til at beskytte fysiske personer og deres privatliv mod risiciene i forbindelse med en uansvarlig databehandling. Men nutidens tendenser kan kræve en helt ny tilgang. Vi indleder derfor en ny debat om, i hvilket omfang anvendelsen af principperne som rimelighed og legitimitet er tilstrækkelig. Databeskyttelseskredeene kan spille en ny rolle ved at anvende eksisterende værktøjer som forudgående kontrol og godkendelse – da ingen andre organer er rustede til at kontrollere en sådan databehandling. I betragtning af, at teknologien, den globale innovation og den menneskelig forbundethed udvikler sig ekstremt hurtigt, har vi mulighed for at tiltrække opmærksomhed, udløse interesse og opbygge en konsensus.

Med denne udtalelse håber vi at skabe rammerne for en bredere og dybere debat om, hvordan EU kan sikre integriteten af sine værdier og samtidig udnytte fordelene ved de nye teknologier.

Udfærdiget i Bruxelles, den 11. september 2015

(underskrevet)

Giovanni BUTTARELLI
Den Europæiske Tilsynsførende for Databeskyttelse

Noter

¹ Kilde: GSMA Intelligence.

² "Moore's lov" om, at det antal transistorer, som kan lægges ind i en mikrochip, fordobles ca. hver 18. måned, har vist sig at være nogenlunde præcis, Moore, Gordon E. (1965-04-19). "Cramming more components onto integrated circuits", Electronics. 22.08.2011.

³ Nathan Eagle, Alex (Sandy) Pentland, "Reality mining: sensing complex social systems", Journal Personal and Ubiquitous Computing Volume 10 Issue 4, marts 2006, s. 255-268. Shoshana Zuboff skriver i "Big Other: surveillance capitalism and the prospects of an information civilization", Journal of Information Technology (2015) 30, s. 75-89: "Som følge af gennemgribende computerformidling gengives næsten alle aspekter af verden i en ny symbolsk dimension som begivenheder, objekter og processer, og mennesker bliver synlige og vidende og deler information på en helt ny måde". Zuboff forudser "en ny universal arkitektur", som hun kalder "Big Other", "allestedsnærværende netværksforbundne institutioner, der registrerer, ændrer og kommercialiserer hverdagsoplevelser fra brødristerne til kroppe, fra kommunikation til tanke, med det entydige formål at finde nye veje til penge og profit", s. 77, 81.

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

⁵ Ingen af de 10 øverste virksomheder i teknologisektoren efter kursværdi ligger i EU (otte ligger i USA, én i Kina og én i Taiwan) ifølge PWC Global Top Ten Companies by Market Capitalisation, 31. marts 2015, opdatering.

⁶ "Big data henviser til den eksponentielle vækst både i tilgængelighed og i den automatiserede brug af oplysninger: det henviser til gigantiske digitale datasæt, som virksomheder, regeringer og andre store organisationer ligger inde med, og som analyseres gennemgribende (deraf navnet: analyser) ved hjælp af computeralgoritmer", WP29-udtalelse nr. 3/2013 om formålsbegrænsning. I en rapport fra Det Hvide Hus fra 2014 blev big data beskrevet som "den voksende teknologiske evne til at indfange, samle og behandle en stadig større mængde, hastighed og mangfoldighed af data", se "Big Data: Seizing Opportunities, Preserving Values", Executive Office of the President ("Podesta-rapport"), maj 2014.

⁷ I EU-lovgivningen defineres "personoplysninger" som "enhver form for information om en identificeret eller identificerbar fysisk person ("den registrerede"); ved identificerbar person forstås en person, der direkte eller indirekte kan identificeres, bl.a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet", artikel 2, litra a), i direktiv 95/46/EF. Denne definition er stort set sammenlignelig med de definitioner, der blev vedtaget af Europarådet i konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (kendt som konvention 108) og af OECD i retningslinjerne om beskyttelse af privatlivets fred og grænseoverskridende overførsel af personoplysninger. En indgående analyse findes i artikel 29-Gruppens (WP29) udtalelse nr. 4/2007 om begrebet personoplysninger, WP136.

⁸ Se f.eks. talen fra formanden for den amerikanske handelskommission, Federal Trade Commission, i 2014: "Udbredelsen af enheder, der er tilsluttet internettet, de faldende udgifter til indsamling, lagring og behandling af oplysninger, og dataformidlernes og andres evne til at kombinere offline- og onlinedata betyder, at virksomhederne kan akkumulere næsten ubegrænsede mængder af forbrugeroplysninger og lagre dem på ubestemt tid. Ved hjælp af prædiktive analyser kan de lære overraskende meget om hver enkelt af os af dette", indledning fra FTC's formand Edith Ramirez, "Big Data: A Tool for Inclusion or Exclusion?", Washington DC, 15. september 2014. Ifølge Sandy Pentland er "social fysik en kvantitativ samfundsvidenskab, der beskriver pålidelige, matematiske forbindelser mellem strømmen af oplysninger og idéer på den ene side og menneskers adfærd på den

anden... Den gør det muligt for os at forudsige produktivitet i små grupper, i afdelinger i virksomheder og endda i hele byer". Det er "det vi har brug for for at kunne skabe et bedre socialt system" (s. 4, 7) og "give (embedsmænd, ledere og borgere) mulighed for at bruge værktøjerne til sociale netværk til at *etablere nye former for adfærd*" (s. 189) (vores fremhævelse), Pentland, *Social Physics: How Good Ideas Spread: The Lessons from a New Science*.

⁹ Special Eurobarometer 431 om databeskyttelse, juni 2015, og Pew Research Panel Survey, januar 2014, om "Public Perceptions of Privacy and Security in the Post-Snowden Era". Ifølge én undersøgelse resulterer et gennemsnitligt besøg på et enkelt websted i 56 tilfælde af dataindsamling ifølge Julia Angwin *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, 2012). I Det Hvide Hus' rapport fra 2014 hævdes det, at "hidtil uset computerkraft og sofistikerede computere... skaber en asymmetrisk kraft mellem de, der er i besiddelse af data, og de, der forsætligt eller utilsigtet leverer dem", "nogle af de største udfordringer, der fremkommer under denne gennemgang, omhandler, hvordan big data-analyser kan ... skabe et så uigennemskueligt beslutningsmiljø, at individuel autonomi går tabt i et uigennemtrængeligt sæt af algoritmer".

¹⁰ Hvis man ser på offentligt optalte anonyme data fra 1990, kunne 87 % af den amerikanske befolkning identificeres ved hjælp af deres femcifrede postnummer kombineret med køn og fødselsdato, se Paul Ohm "Broken promises of privacy: responding to the surprising failure of anonymisation", *UCLA Law Review* 2010 og "Record linkage and privacy: issues in creating new federal research and statistical info", april 2011. DNA er unikt (med undtagelse af enæggede tvillinger) og stabilt livet igennem. Det indeholder oplysninger om etnicitet og anlæg for sygdomme og kan identificere andre familiemedlemmer. I januar 2013 kunne forskerne identificere fysiske personer og familier ud fra anonyme DNA-data fra offentligt tilgængelige slægtsforskningsdatabaser, Gymrek, M., McGuire, A. L., Golan, D., Halperin, E. & Erlich, Y. *Science* 339, 321–324 (2013). Se også "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/> (tilgået 10.9.2015). Se også WP29-udtalelse nr. 04/2007 om begrebet personoplysninger, WP29-udtalelse nr. 03/2013 om formålsbegrænsning, WP29-udtalelse nr. 06/2013 om videreanvendelse af åbne data og den offentlige sektors informationer (PSI) og WP29-udtalelse nr. 05/2014 om anonymiseringsteknikker.

¹¹ Kilde: Gartner.

¹² Se f.eks. paneldiskussionen "What is the future of official statistics in the Big Data era?", the Royal Statistical Society, London 19. januar 2015, <http://www.odi.org/events/4068-future-official-statistics-big-data-era> (tilgået 10.9.2015).

¹³ "Ten technologies which could change our lives: potential impacts and policy implications", Scientific Foresight Unit, European Parliamentary Research Service, januar 2015.

¹⁴ EU's arbejdsprogram Horisont 2020, 2016-2017, støtter denne udvikling, herunder store pilotprojekter, som ser på privatlivsmæssige og etiske bekymringer.

¹⁵ Forsikring er beskrevet som den "oprindelige forretningsmodel for tingenes internet", "From fitness trackers to drones, how the "Internet of Things" is transforming the insurance industry", *Business Insider*, 11.6.2015. Tanken om prismæssig forskelsbehandling inden for konkurrenceretten, afledt af artikel 102 i TEUF, som forbyder en virksomhed i en dominerende stilling på et marked at foretage "direkte eller indirekte påtvingelse af urimelige købs- eller salgspriser eller af andre urimelige forretningsbetingelser", er meget omstridt, se f.eks. Damien Gerardin og 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. Om big data og deres (ifølge forfatterne endnu ikke realiserede) potentiale i forhold til at fremskynde personlige priser, se Executive Office of the President of the United States, "Big Data and Differential Pricing", februar 2015, og en ny analyse, hvori det konkluderes, at personlige priser generelt omfatter behandling af personoplysninger og derfor skal overholde databeskyttelseslovens

gennemsigtighedsprincip, ifølge hvilket virksomhederne skal underrette folk om formålet med at behandle deres personoplysninger: Virksomhederne skal sige, hvis de benytter personlige priser. Og hvis en virksomhed bruger en cookie til at genkende en person, stilles der i direktivet om databeskyttelse inden for elektronisk kommunikation krav om, at personen skal informeres om formålet med den relevante cookie", arbejdsudkast af Frederik Borgesius "Online Price Discrimination and Data Protection Law". Findes på http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665 (tilgået 10.9.2015).

¹⁶ Medicinske anordninger defineres i EU-retten i Rådets direktiv 93/42/EØF om medicinske anordninger, som ændret ved Europa-Parlamentets og Rådets direktiv 2007/47/EF af 5. september 2007. Om databeskyttelsens indvirkninger på "mobil sundhed", se EDPS' udtalelse 1/2015.

¹⁷ Ifølge Eurostat anvender 21 % af alle fysiske personer og 19 % af alle virksomheder i EU cloudlagringstjenester.

¹⁸ "Hvis det verdensomspændende internet var et land, ville det være verdens 12. største forbruger af elektricitet, et sted mellem Spanien og Italien. Dette svarer til ca. 1,1-1,5 % af den globale brug af elektricitet (i 2010) og de drivhusgasser, der årligt genereres af 70 til 90 store (500 megawatt) kulfyrede kraftværker". 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 fra undersøgelsen "SMART 2013/0043 – Uptake of Cloud in Europe".

²⁰ Kilde: Eurostat.

²¹ Begrebet "deleøkonomi" er blevet kritiseret som vildledende: "The Sharing Economy Isn't About Sharing at All", Giana M. Eckhardt og Fleura Bardhi, Harvard Business Review, 28.1.2015.

²² Rachel Botsman og 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 workshoppen af 9. juni 2015 fra den amerikanske Federal Trade Commission om "Competition, Consumer Protection, and Economic Issues Raised by the Sharing Economy", <https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators/> (tilgået 10.9.2015).

²⁵ Om droners eller fjernstyrede luftfartøjssystemers konsekvenser for beskyttelse af personoplysninger, se EDPS' udtalelse om meddelelsen fra Kommissionen til Europa-Parlamentet og Rådet om "En ny æra for luftfarten – Luftfartsmarkedet åbnes for civil anvendelse af fjernstyrede luftfartøjssystemer på en sikker og holdbar måde", november 2014.

²⁶ Kilde: Boston Consulting Group.

²⁷ Gartner.

²⁸ Facebooks ansigtsgenkendelsesalgoritme DeepFace har en succesrate på 97 % – hvilket er højere end menneskers, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification", offentliggjort i rapport om IEEE Conference on Computer Vision and Pattern recognition, juni 2014.

²⁹ Robo er defineret som en "maskine i verden, der føler, tænker og handler", Bekey, G, "Current trends in robotics: technology and ethics", i Robot Ethics – The ethical and social implications of robotics, The MIT Press, 2012, s. 18. Det anslås, at der mellem 2013 og 2016 vil blive solgt 22 mio. serviceroboter, IRF World Robotics Report, 2013. Om kunstig intelligens, se "Rise of the Machines", Economist, 9.5.15, og Pew Research Centre Internet Project 2014. En virksomhed for kunstig intelligens betingede sit salg til en førende teknologivirksomhed i 2014 af, at der blev oprettet et råd

for etik og sikkerhed, og at det blev forbudt at anvende kunstig intelligens til militære eller efterretningsmæssige formål, Forbes, Inside Google's Mysterious Ethics Board, 3.2.2014.

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

³¹ Se fodnote 9 ovenfor. Pentland *Social Physics*, s. 153: "Der er mulighed for at tage store spring inden for sundhedspleje, transport, energi og sikkerhed ... de største hindringer for at nå disse mål er privatlivets fred, og at vi endnu ikke har nået nogen konsensus omkring afvejningerne mellem personlige og sociale værdier". Debatten omkring den vestafrikanske Ebola-pandemi i 2014 viser denne falske sondring mellem privatlivets fred og samfundets behov. Sygdomme er som regel blevet sporet og deres levetid målt via undersøgelser og folketællinger, som let bliver forældede, og som er svære at ekstrapolere for at forudse, hvor sygdommen vil slå til næste gang. Der findes eksempler på brug af "big data" til sporing af malariaudbrud i Namibia og Kenya og i 2009 til at spore effektiviteten af offentlige sundhedsadvarsler under den mexicanske svineinfluenza. Én kilde til data er optegnelser over mobilopkald, som viser den basisstation, der håndterede opkaldet, og som i realtid kan give en nogenlunde idé om, hvor folk befinder sig, og hvor de skal hen. Indsamlingen af disse data er ikke målrettet – det er ikke muligt at skelne mellem mennesker med og uden Ebola. En svensk NGO kortlagde befolkningens mobilitet i Vestafrika, men dataene blev ikke brugt, da mobilsekskaberne ikke ville frigive dem til godkendte eksterne forskere, idet de hævdede, at de skulle have ordrer fra regeringen, som til gengæld anførte privatlivets fred, som ikke kunne garanteres i henhold til EU-lovgivningen, <http://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola>. (tilgået 10.9.2015)

³² EDPS' udtalelse nr. 3/2015.

³³ En big data-antagelse om, at "N=alle" henviser til at se på alle datapunkter og ikke kun et udsnit, Viktor Mayer-Schönberger og Kenneth Cukier, *The Rise of Big Data: How it's changing the way we think about the world*, 2013. Lisbon Council og Progressive Policy Institute har anført, at velfærden vil stige ved at maksimere den "digitale densitet" – den mængde data, der anvendes pr. indbygger i en økonomi" <http://www.lisboncouncil.net/component/downloads/?id=1178> (tilgået 10.9.2015). Den internationale arbejdsgruppe om databeskyttelse inden for telekommunikation ("Berlingruppen") har foreslået undtagelser for big data i forhold til databeskyttelsesprincipperne, http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf. (tilgået 10.9.2015). Det Verdensøkonomiske Forum har opfordret til at fokusere på brug og ikke indsamling og til at bevæge sig væk fra kravet om samtykke til indsamling af personoplysninger, "Unlocking the Value of Personal Data: From Collection to Usage", 2013.

³⁴ Se EDPS' foreløbige udtalelse om privatliv og konkurrenceevne i big data-tidsalderen ("Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data").

³⁵ I artikel 21 i chartret om grundlæggende rettigheder forbydes "enhver forskelsbehandling på grund af køn, race, farve, etnisk eller social oprindelse, genetiske anlæg, sprog, religion eller tro, politiske eller andre anskuelser, tilhørsforhold til et nationalt mindretal, formueforhold, fødsel, handicap, alder eller seksuel orientering". Mange af disse kategorier af data ("racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold og oplysninger om helbredsforhold og seksuelle forhold") beskyttes ekstra i artikel 8 i direktiv 95/46/EF.

³⁶ Om idéen om et digitalt fællesareal, se "Ambition numérique: Pour une politique française et européenne de la transition numérique", French Digital Council, juni 2015, s. 276, Bruce Schneier støtter oprettelsen af "frie offentlige rum" på internettet, som offentlige parker, *Data and Goliath*, s. 188-189, Sandy Pentland argumenterer for et "fællesareal for offentlige data", *Social Physics*, s. 179. Om vurdering af sikkerheden ved at offentliggøre aggregerede datasæt som åbne data, se WP29-udtalelse nr. 06/2013 om videreanvendelse af åbne data og den offentlige sektors informationer (PSI).

³⁷ "Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent" <http://crackedlabs.org/studie-kommerzielle-ueberwachung/info>. Om kvalificeret

gennemsigtighed, se f.eks. Frank Pasquale: *The Black Box Society: The Secret Algorithms that Control Money and Information*.

³⁸ "Bag den teknologi, der påvirker sociale relationer, ligger de selv samme sociale relationer", David Noble, "Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools", i *Case Studies in the Labor Process*, ed. Andrew Zimbalist, 1979. Se også Judy Wacjman, *Pressed for Time: The Acceleration of Life in Digital Capitalism*, 2014, s. 89-90, og Zuboff, "Big Other" (citeret i fodnote 3 ovenfor).

³⁹ Udtalelse nr. 05/2014 om anonymiseringsteknikker, vedtaget den 10. april 2014 (WP 216).

⁴⁰ Om snævert fortolket undtagelse fra databeskyttelsesreglerne udelukkende til personlige formål eller husbehov, se Domstolens dom i sag C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů*.

⁴¹ Begrebet producent-forbruger (på engelsk "prosumer") blev opfundet af Alvin Toffler i *The Third Wave*, 1980. En drøftelse om "producent-forbrugermiljøet" og hvordan der bør lovgives om det, findes i Ian Brown og Chris Marsden, *Regulating Code*, 2013.

⁴² Udtalelse fra Den Europæiske Gruppe vedrørende Etik inden for Naturvidenskab og Ny Teknologi til Europa-Kommissionen: "Ethics of Security and Surveillance Technologies", udtalelse nr. 28, 20.5.2015, s. 74.

⁴³ Se f.eks. Homer Economicus: *The Simpsons and Economics*, ed. Joshua Hall, 2014.

⁴⁴ Hvis man anvender den mest konservative definition af fejl, betyder dette, at 23 mio. amerikanere har væsentlige fejl i en forbrugerrapport. 5 % af undersøgelsens deltagere havde fejl, der, efter de blev rettet, forbedrede deres kreditvurdering, så de kunne opnå kredit til en lavere 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. Findes på SSRN: <http://ssrn.com/abstract=2432955>.

⁴⁵ WEF antager, at data er et værdifuldt personligt aktiv, som den enkelte kan vælge at give virksomheder og regeringer ret til at eje, anvende og sælge til gengæld for tjenesteydelser. Se også de seneste taler fra Kommissionens næstformand Ansip, f.eks. af 7.9.2015 til det årlige møde i Bruegel med titlen "Productivity, innovation and digitalisation – which global policy challenges?": "Ejerskab og forvaltning af datastrømme, brug og genbrug af data. Forvaltning og lagring af data. Disse understøtter vigtige nye sektorer som cloudcomputing, tingenes internet og big data".

⁴⁶ "Så hvem har ret til at bruge de oplysninger og data, som reelt ikke tilhører én selv? Dette spørgsmål går på tværs af grænserne for handel, etik og moral og medfører spørgsmål om privatlivets fred og beskyttelse af privatlivets fred", Al-Khouri, november 2012, http://www.academia.edu/6726887/Data_Owner_ship_Who_Owns_My_Data_036. Se også Margaret Jane Radin, "Incomplete Commodification in the Computerized World", i *The Commodification of Information* 3, 17, Niva Elkin-Koren & Neil Weinstock Netanel eds. 2002: "Der er stor forskel på, om privatlivets fred anses for at være en menneskerettighed, der følger mennesker i kraft af deres personlighed, eller en ejendomsret, som kan ejes og kontrolleres af mennesker. Menneskerettigheder kan formodentlig ikke mistes på markedet, hvorimod ejendomsrettigheder formodentlig kan."

⁴⁷ MIT's Computer Science and Artificial Intelligence Lab's Crosscloud-projekt, som støttes af flere virksomheder i EU, har til formål at "1) gøre det let at udvikle flerbrugersoftware (social software) udelukkende ved hjælp af front-end-udvikling og overholdelse af brugernes rettigheder og privatliv, og 2) give brugerne frihed til at bevæge sig let mellem applikationer, hardwareplatforme og sociale netværk og bevare deres oplysninger og sociale forbindelser", <http://openpds.media.mit.edu/#architecture> (tilgået 10.9.2015).

⁴⁸ Se forklaringen til artikel 1 i EU's charter om grundlæggende rettigheder.

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

⁵⁰ Dom af 15. december 1983, BVerfGE 65, 1-71, Volkszählung.

⁵¹ Se Den Europæiske Gruppe vedrørende Etik inden for Naturvidenskab og Ny Teknologi, udtalelse om etik og overvågning, s. 75. En undersøgelse har vist, at en annoncemålretningsalgoritme var diskriminerende, idet søgningerne i gennemsnit viste annoncer for flere højtbetalte job til mænd sammenlignet med kvinder, der besøgte jobsider, Carnegie Mellon University og International Computer Science Institute. Om tendensen til at digitale assistenter som standard har en kvindelig stemme, se f.eks. 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 og Jonathan King, "Big Data Ethics" (19. maj 2014), *Wake Forest Law Review*, 2014.

⁵⁴ BBC, forbrugerprogram undersøger salg af velgørenhedsdata, 1.9.2015.

⁵⁵ Se skrivelse fra Future of Life Institute. Den pavelige rundskrivelse *Laudato Si*: "Når medierne og den digitale verden bliver allestedsnærværende, kan deres indflydelse hindre folk i at lære, hvordan man lever klogt, tænker dybt og elsker generøst. I denne sammenhæng risikerer tidligere tiders store vismænd at blive overdøvet midt i støjen og forstyrrelserne fra de store informationsmængder. Der skal gøres en indsats for at hjælpe disse medier med at blive kilder til nye kulturelle fremskridt for menneskeheden og ikke en trussel mod vores dybeste rigdomme. Sand visdom er frugten af selvransagelse, dialog og generøse møder mellem personer og erhverves ikke ved en simpel ophobning af data, som i sidste ende fører til overbelastning og forvirring, en slags mental forurening. Reelle relationer med andre med alle de udfordringer, de nu engang medfører, har nu en tendens til at blive erstattet af en form for internetkommunikation, hvor vi kan vælge og vrage mellem relationer efter forgodtbefindende, hvilket giver anledning til en ny form for konstruerede følelser, som har mere at gøre med enheder og visninger end med andre mennesker og naturen. Medierne i dag gør det muligt for os at kommunikere og dele vores viden og kærlighed. Men ind imellem afholder de os også fra direkte kontakt med andres smerte, frygt og glæder og deres mange og komplekse personlige erfaringer. Vi skal derfor være bekymrede for, at der sammen med de spændende muligheder, som disse medier tilbyder, også kan opstå en dyb og melankolsk utilfredshed med personlige relationer eller en skadelig følelse af isolation."

⁵⁶ Se handling 4 i EDPS' strategi 2015-2020 om udvikling af en etisk dimension af databeskyttelse.