

EUROPEAN DATA PROTECTION SUPERVISOR

## Advies 4/2015

# Naar een nieuwe digitale ethiek:

*data, waardigheid en technologie*



EDPS

11 september 2015

*De Europese Toezichthouder voor gegevensbescherming (EDPS) is een onafhankelijke instelling van de EU, die er overeenkomstig artikel 41, lid 2, van Verordening (EG) nr. 45/2001 voor zorgt "dat de fundamentele rechten en vrijheden van natuurlijke personen, met name het recht op bescherming van de persoonlijke levenssfeer, bij de verwerking van persoonsgegevens, door de communautaire instellingen en organen in acht worden genomen", en ook zorgt voor "(...) het verstrekken van advies aan de communautaire instellingen en organen en aan de betrokkenen inzake de verwerking van persoonsgegevens". De toezichthouder is in december 2014 samen met de adjunct-toezichthouder benoemd met als specifieke opdracht zich constructiever en proactiever op te stellen. De EDPS heeft in maart 2015 een vijfjaarsstrategie gepubliceerd waarin uiteengezet wordt hoe hij deze opdracht wil gaan uitvoeren en hoe hij daarvoor ter verantwoording kan worden geroepen.*

*Dit advies volgt op het eerdere advies van de EDPS inzake de Algemene Verordening betreffende gegevensbescherming, waarmee hij beoogde de belangrijkste instellingen van de EU te helpen bij het bereiken van de juiste consensus over een werkbare, toekomstgerichte reeks voorschriften die de rechten en vrijheden van natuurlijke personen versterken. Net als het advies over mobiele gezondheid dat begin 2015 werd uitgebracht, gaat dit advies in op de uitdaging van de "digitalisering" van de gegevensbescherming – de derde doelstelling van de EDPS-strategie – "de aanpassing van de bestaande gegevensbeschermingsbeginselen aan de mondiale digitale arena", mede in het licht van de EU-plannen voor een digitale interne markt. Het advies stemt overeen met de benadering van de Artikel 29-Groep betreffende de gegevensbeschermingsaspecten van het gebruik van nieuwe technologieën, zoals het "internet van de dingen", waaraan de EDPS als volwaardig lid van de groep heeft bijgedragen.*



Dignity	waardigheid
Future-oriented rules and enforcement	toekomstgerichte voorschriften en handhaving
Accountable controllers	verantwoordelijken met verantwoordingsplicht
Empowered individuals	weerbare natuurlijke personen
Innovative privacy engineering	innovatieve privacytechnieken
Ethics	ethiek

**"De menselijke waardigheid is onschendbaar. Zij moet worden geëerbiedigd en beschermd."**

#### **Artikel 1, EU-Handvest van de grondrechten**

**De grondrechten van bescherming van de persoonlijke levenssfeer en bescherming van de persoonsgegevens zijn belangrijker voor de bescherming van de menselijke waardigheid dan ooit tevoren.** Zij zijn verankerd in de Europese Verdragen en in het EU-Handvest van de grondrechten. Zij stellen mensen in staat om hun eigen persoonlijkheid te ontwikkelen, een onafhankelijk leven te leiden, te innoveren en andere rechten en vrijheden uit te oefenen. De in het EU-handvest gedefinieerde beginselen voor de gegevensbescherming – noodzakelijkheid, evenredigheid, eerlijkheid, gegevensminimalisatie, doelbinding, toestemming en transparantie – gelden voor het hele proces van gegevensverwerking, zowel de verzameling als het gebruik.

**De technologie mag geen normen en rechten dicteren, maar mag hun relatie evenmin reduceren tot een valse dichotomie.** De digitale revolutie stelt voordelen op het gebied van gezondheid, milieu, internationale ontwikkeling en economische efficiëntie in het vooruitzicht. In de EU-plannen voor een digitale interne markt worden cloudcomputing, het "internet van de dingen", "big data" en andere technologieën gezien als de sleutel voor concurrentiekracht en groei. In ondernemingsmodellen worden nieuwe mogelijkheden voor de massale verzameling, de onmiddellijke overdracht en het combineren en hergebruiken van persoonsinformatie benut voor onvoorziene doeleinden, en gerechtvaardigd door lang en ondoorgroondelijk privacybeleid. Hierdoor zijn de beginselen voor gegevensbescherming weer onder druk komen te staan, waardoor opnieuw over hun toepassing moet worden nagedacht.

**In de huidige digitale omgeving kan niet worden volstaan met de naleving van de wetgeving; ook de ethische dimensie van gegevensverwerking moet door ons in overweging worden genomen.** Het regelgevingskader van de EU laat reeds ruimte voor flexibele beslissingen en waarborgen op individuele basis bij de omgang met persoonsgegevens. De hervorming van het regelgevingskader zal een goede stap voorwaarts betekenen. Maar er zijn dieperliggende vragen ten aanzien van de gevolgen van tendensen in een door gegevens gestuurde maatschappij voor de waardigheid, de individuele vrijheid en het functioneren van de democratie.

**Deze vraagstukken hebben technische, filosofische, juridische en morele implicaties.** Dit advies belicht een aantal belangrijke technologische tendensen die een onaanvaardbare verwerking van persoonsinformatie met zich mee kunnen brengen of die inbreuk op het recht op bescherming van de persoonlijke levenssfeer kunnen maken. Het schetst de contouren van een uit vier lagen bestaand ecosysteem ter bescherming van "big data" als reactie op de digitale uitdaging: een gezamenlijke inspanning, onderbouwd door ethische overwegingen.

- (1) Een toekomstgerichte regulering van de gegevensverwerking en het eerbiedigen van het recht op bescherming van de persoonlijke levenssfeer en het recht op gegevensbescherming.
- (2) Verantwoordingsplichtige verantwoordelijken die de verwerking van persoonsgegevens bepalen.
- (3) Een privacybewust(e) ontwikkeling en ontwerp van producten en diensten op het gebied van gegevensbescherming.

(4) Weerbare natuurlijke personen.

**De Europese Toezichthouder voor gegevensbescherming wil zowel binnen als buiten de EU een open en goed geïnformeerd debat stimuleren**, waaraan wordt deelgenomen door het maatschappelijk middenveld, ontwikkelaars, het bedrijfsleven, academici, overheidsinstanties en toezichthouders. De nieuwe ethische commissie voor gegevensbescherming die wij bij de EDPS gaan opzetten, zal helpen om een nieuwe digitale ethiek te formuleren, waarmee de voordelen van technologie voor de samenleving en de economie beter kunnen worden gerealiseerd op manieren die de rechten en vrijheden van natuurlijke personen versterken.

## INHOUDSOPGAVE

<b>1. Gegevens zijn overal: tendensen, kansen en uitdagingen</b> .....	<b>7</b>
1.1 BIG DATA.....	7
1.2 "INTERNET VAN DE DINGEN" .....	8
1.3 "AMBIENT COMPUTING" .....	8
1.4 CLOUDCOMPUTING .....	9
1.5 PERSOONLIJKE GEGEVENSafhankelijke ONDERNEMINGSMODELLEN .....	9
1.6 DRONES EN AUTONOME VOERTUIGEN .....	10
1.7 TENDENSEN MET MOGELIJK GROTERE EN LANGDURIGE GEVOLGEN .....	10
<b>2. Een ecosysteem ter bescherming van big data</b> .....	<b>11</b>
2.1 TOEKOMSTGERICHTE REGULERING .....	11
2.2 VERANTWOORDELIJKEN MET VERANTWOORDINGSPLICHT .....	12
2.3 PRIVACYBEWUSTE ONTWIKKELING.....	12
2.4 WEERBARE NATUURLIJKE PERSONEN .....	13
<i>Een "prosumentenomgeving"</i> .....	13
<i>Toestemming</i> .....	13
<i>Controle en "eigendom" van gegevens</i> .....	14
<b>3. Waardigheid als de kern van een nieuwe digitale ethiek</b> .....	<b>14</b>
3.1 WAARDIGHEID EN GEGEVENS.....	15
3.2 EEN EUROPESE ETHISCHE ADVIESCOMMISSIE .....	16
<b>4. Conclusie: tijd voor verdieping van de discussie</b> .....	<b>17</b>
<b>Noten</b> .....	<b>18</b>

# 1. Gegevens zijn overal: tendensen, kansen en uitdagingen

Er worden steeds meer persoonlijke gegevens verzameld en verwerkt op steeds minder doorzichtige en steeds complexere wijze. Dankzij de steeds grotere inzet van computers in ondernemingen en bij de overheid in de jaren 1980 ontstond bij velen de opvatting dat de praktijken van machtige regeringen en ondernemingen bij de verwerking van persoonsgegevens ertoe leidden dat personen werden gereduceerd tot gegevensonderwerpen en de grondrechten en vrijheden in het gedrang zouden komen. De huidige golf van geïntegreerde informatie- en communicatietechnologie onderscheidt zich door zijn alomtegenwoordigheid en macht.

Vorig jaar werd gerapporteerd dat er meer verbonden apparaten op de planeet waren dan mensen<sup>1</sup>. De toename in de capaciteit van processoren<sup>2</sup>, opslag en transmissiebandbreedte houdt in dat er steeds minder technische beperkingen zijn voor de verwerking van persoonsgegevens. Het is de verwachting dat het internet van de dingen (Internet of Things) en big data-analyses zullen convergeren met kunstmatige intelligentie, natuurlijke taalverwerking en biometrische systemen zodat toepassingen automatisch kunnen leren en zo steeds intelligenter worden. Regeringen en ondernemingen kunnen verdergaan dan "data mining" en overgaan op "reality mining", dat nog verder in het dagelijks leven, de communicatie en zelfs gedachten<sup>3</sup> binnendringt. Terwijl de samenleving zich aanpast aan de behoeften van de digitale marktplaats, vinden er nu nieuwe inspanningen plaats om programmeren te leren aan jonge kinderen<sup>4</sup>. Gebruikmaken van deze tendensen in een sector waar de EU een toonaangevende consument is, maar achterloopt in de dienstverlening, is een thema dat vaker terugkomt in de strategie van de Commissie voor een digitale interne markt<sup>5</sup>.

De tendensen en veel van de concepten die tegenwoordig worden gebruikt, komen weliswaar veel voor, maar zijn vaag en overlappen elkaar. We willen, om een discussie te helpen stimuleren, specifieke tendensen benadrukken die naar onze mening, zonder uitpuittend te willen zijn, de belangrijkste ethische en praktische vraagstukken naar voren brengen bij de toepassing van de gegevensbeschermingsbeginselen.

## 1.1 Big data

Met de term "big data"<sup>6</sup> wordt verwezen naar de praktijk waarin grote hoeveelheden informatie afkomstig uit verschillende bronnen worden gecombineerd en geanalyseerd, vaak met behulp van zelflerende algoritmen, om weldoordachte besluiten te nemen. Deze informatie is niet altijd persoonlijk van aard: gegevens die worden gegenereerd door sensoren voor het controleren van natuurlijke of atmosferische gebeurtenissen, zoals het weer of vervuiling, of voor het bewaken van de technische aspecten van een productieproces, houden geen verband met een "geïdentificeerde of identificeerbare natuurlijke persoon"<sup>7</sup>. Maar een van de grootste waardevolle eigenschappen van big data voor ondernemingen en overheden is afgeleid van de monitoring van *menselijk* gedrag, zowel gezamenlijk als individueel, en huist in het voorspellende potentieel<sup>8</sup>.

Eén gevolg is de opkomst van een inkomstenmodel voor internetbedrijven waarbij online activiteiten worden bijgehouden om de economische waarde van transacties voor dienstverleners te optimaliseren, niet alleen in gerichte advertenties, maar ook in de voorwaarden en tarieven van verzekeringen, leningen en andere contractuele relaties. In de concurrerende markt voor de aandacht van de gebruiker, zijn de meeste mensen zich niet bewust van de omvang waarin gegevens worden bijgehouden<sup>9</sup>. Dergelijke "big data" moeten als persoonlijk worden beschouwd, zelfs wanneer anonimiseringstechnieken zijn toegepast:

het wordt steeds eenvoudiger om de identiteit van een persoon te achterhalen door middel van het combineren van vermeende "anonieme" gegevens met andere gegevensreeksen, waaronder openbaar beschikbare informatie op bijvoorbeeld sociale media<sup>10</sup>. Wanneer deze gegevens worden verhandeld en dan met name over de grens en in andere rechtsgebieden, wordt de verantwoordingsplicht ten aanzien van de gegevensverwerking schimmig en moeilijk vast te stellen of te handhaven op grond van gegevensbeschermingswetgeving, met name door de afwezigheid van internationale normen.

## 1.2 "Internet van de dingen"

Veel apparaten die met internet zijn verbonden, zijn alom aanwezig, zoals smartphones, tablets, geldautomaten en incheckzuilen op de luchthaven. Het is de verwachting dat connectiviteit tegen 2020 een standaardfunctie is met 25 miljard verbonden objecten (in vergelijking met 4,8 miljard in 2015), variërend van telegeneeskunde tot voertuigen, van slimme meters tot een hele reeks aan nieuwe vaste en mobiele apparaten om slimme steden mogelijk te maken<sup>11</sup>.

Deze sensoren bieden directe en gedetailleerde informatie die statistiekbureaus en vragenlijsten momenteel niet kunnen samenstellen, maar die niet noodzakelijkerwijs nauwkeuriger is en zelfs misleidend zou kunnen zijn<sup>12</sup>. De geraamde 1,8 miljard verbindingen tussen voertuigen onderling tegen 2022, kunnen ongelukken en vervuiling verminderen en de productiviteit en autonomie van ouderen en gehandicapten vergroten<sup>13</sup>. Kleding en horloges verwerken bijvoorbeeld persoonsgegevens net als andere verbonden apparaten. Ze zijn in staat om bloedproppen te ontdekken en houden de fitheid en de heling van wonden bij. Verbonden vezels kunnen beschermen tegen extreme omstandigheden, bijvoorbeeld bij brandbestrijding. Deze apparaten laden persoonsgegevens rechtstreeks naar een cloudopslag, zijn verbonden met sociale netwerken en kunnen mogelijk in het openbaar uitzenden, zodat gebruikers kunnen worden geïdentificeerd en het gedrag en de bewegingen van individuen en menigten kunnen worden bijgehouden<sup>14</sup>.

De verwerking van deze informatie kan van invloed zijn op niet alleen de persoonlijke levenssfeer van de gebruikers van de apparaten, onder andere wanneer ze worden gebruikt op de werkvloer, maar ook op de rechten van anderen die door het apparaat worden geobserveerd en vastgelegd. Hoewel er weinig bewijzen zijn van daadwerkelijke discriminatie, is het duidelijk dat het enorme volume aan persoonsgegevens dat wordt verzameld door het internet van de dingen van groot belang is als middel om inkomsten te maximaliseren met behulp van een meer gepersonaliseerde prijsstelling overeenkomstig het bijgehouden gedrag, met name in de gezondheidszorgsector<sup>15</sup>. Ook andere domeinspecifieke voorschriften zullen worden aangetast, bijvoorbeeld wanneer apparaten die gezondheidsgegevens verwerken technisch niet worden ingedeeld als medische apparaten en dus buiten het toepassingsgebied van regulering vallen<sup>16</sup>.

## 1.3 "Ambient computing"

**Ambient of onzichtbare computing** verwijst naar een belangrijke technologie die ten grondslag ligt aan het internet van de dingen. Een van de meest zichtbare toepassingen zijn "slimme huizen" en "slimme kantoren" die bestaan uit apparaten met ingebouwde en geavanceerde capaciteit voor gegevensverwerking die een grotere energie-efficiëntie beloven en waarbij geïnformeerde personen hun verbruik op afstand kunnen beïnvloeden (al is dat afhankelijk van de onafhankelijkheid van de bewoner van de eigenaar of de



gebouwbeheerder). Er moet duidelijk zijn wie er verantwoordelijk is voor het doeleinde van en de middelen voor de verwerking van de persoonsgegevens die betrokken zijn bij toepassingen op het gebied van ambient computing, niet alleen voor de bescherming van de grondrechten van personen, maar ook voor de juiste toewijzing van de aansprakelijkheid om te waarborgen dat de algemene beveiligingseisen van het systeem in acht worden genomen.

#### 1.4 Cloudcomputing

Cloudcomputing staat bekend als een centrale ontsluitingstechnologie voor zowel de geavanceerde analyses en mogelijkheden voor "mining", de verzameling en analyse van big data en de stroom aan gegevens afkomstig van het internet van de dingen, die momenteel wordt gebruikt door ongeveer twintig procent van de personen en ondernemingen in de EU<sup>17</sup>. Het maakt het mogelijk om gegevens te concentreren vanuit de ontelbare apparaten die zijn verbonden met het internet van de dingen en vertrouwt op de beschikbaarheid en connectiviteit van enorme hoeveelheden gegevens in grootschalige opslag- en verwerkingsfaciliteiten over de hele wereld<sup>18</sup>. Een breder gebruik van cloudcomputing<sup>19</sup> door de publieke en de private sector wordt geraamd in totaal 449 miljard EUR bij te dragen aan het bbp van de EU-28 (0,71 % van het totale bbp van de EU).

De controle over persoonsgegevens wordt vaak gedeeld tussen de klant en de aanbieder van de clouddiensten en de verantwoordelijkheid voor de verplichtingen uit hoofde van gegevensbescherming is niet altijd duidelijk. Dit kan inhouden dat er in de praktijk onvoldoende bescherming wordt verleend. Deze verplichtingen zijn niet afhankelijk van de **fysieke locatie van de gegevensopslag**. Bovendien kan de infrastructuur voor cloudcomputing, die momenteel slechts een achtergrondtechnologie is ter ondersteuning van de bedrijfstoeepassingen, zelf een kritieke infrastructuur worden en de ongelijkheden in de marktmacht vergroten, aangezien 30 % van de ondernemingen recentelijk heeft aangegeven moeilijkheden te ondervinden bij het afmelden bij of veranderen van aanbieder<sup>20</sup>.

#### 1.5 Persoonlijke gegevensafhankelijke ondernemingsmodellen

Deze technologieën hebben nieuwe ondernemingsmodellen mogelijk gemaakt die vertrouwen op informatie die niet alleen wordt vergaard bij het verlenen van een dienst, maar ook vanuit andere bronnen, zoals de aanwezigheid op sociale media, om risico's en kredietwaardigheid te beoordelen en inkomsten te maximaliseren. Een prominent ondernemingsmodel dat momenteel erg populair is, zijn platformen waar verkopers en kopers aan elkaar worden gekoppeld, en die het delen en herdistribueren van producten, diensten, vaardigheden en activa mogelijk maken. Deze platformen worden vaak aangeduid met "deeleconomie", "deelconsumptie" of online en mobiele peer-to-peer-bedrijfsplatformen<sup>21</sup> en kunnen klassieke economische efficiëntie aanbieden, de markt concurrerender maken en afval verminderen. De raming is dat de waarde in de komende jaren zal verviervoudigen, van 26 miljard dollar naar 110 miljard dollar<sup>22</sup>. Dergelijke door gegevens gestuurde ondernemingsmodellen genereren al enorme inkomsten op het gebied van het delen van auto's en huizenverhuur en in de financiële technologie en sociale leenvormen. Uit vragenlijsten blijkt dat consumenten de klaarblijkelijke betere betaalbaarheid en het gemak waarderen<sup>23</sup>.

Het bestaansrecht van dergelijke platforms wordt meestal gevormd door de reputatie van de gebruiker, beoordelingen door medegebruikers en identiteitsverificatie. Dat kan worden gezien als een verbetering van de transparantie en de verantwoordingsplicht, maar dat geldt niet noodzakelijkerwijs voor de aanbieder van het platform zelf. Grote spelers op deze markten zijn bekritiseerd voor het vermeend achterhouden van reputatiegegevens voor de

afzonderlijke gebruikers waarop de gegevens betrekking hebben. Er bestaat een groot risico dat personen kunnen worden uitgesloten van diensten op basis van een reputatie die is gebaseerd op onjuiste gegevens die zij niet kunnen weerleggen en niet kunnen verzoeken deze te verwijderen. Door te vertrouwen op gegevens afkomstig uit meerdere bronnen, komt ook het beginsel in de EU-wetgeving van gegevensminimalisatie in het gedrang. De omvang van de toekomstige gevolgen voor personen en de samenleving van deze en toekomstige ondernemingsmodellen die technologieën mogelijk maken, moeten zorgvuldig worden onderzocht<sup>24</sup>.

## 1.6 Drones en autonome voertuigen

Drones of semiautonome vliegtuigen worden momenteel nog voornamelijk gebruikt door het leger, maar worden steeds vaker gebruikt voor surveillance, cartografie, vervoer, logistiek en openbare veiligheid, zoals het beperken van natuurbranden<sup>25</sup>. Foto's, video's en andere persoonsgegevens die door drones worden verzameld, kunnen worden uitgewisseld via telecommunicatienetwerken. Het gebruik van drones kan leiden tot ernstige inbreuken op de privacy en een schrikbarend effect op de vrijheid van meningsuiting. De vraag doet zich voor hoe het ontwerp en gebruik ervan op doeltreffende wijze kan worden gereguleerd, zodat betrokkenen hun rechten kunnen uitoefenen en toegang kunnen krijgen tot de gegevens die door deze machines worden vastgelegd.

Op de grond zullen autonome voertuigen of zelfrijdende auto's een verandering teweegbrengen in de manier waarop afzonderlijk vervoer wordt gebruikt en georganiseerd en kan het verschil tussen particulier en openbaar vervoer vervagen. Er wordt geraamd dat er tegen 2035 12 miljoen volledig autonome en 18 miljoen deels autonome voertuigen zullen zijn, waarbij het gebruik in Europa voorop loopt<sup>26</sup>. De algoritmen die de besturing van de auto verzorgen nemen beslissingen die direct betrekking kunnen hebben op de fysieke integriteit en zelfs het leven of de dood van individuen, bijvoorbeeld bij de keuze die is geprogrammeerd in geval van een onvermijdelijke botsing. Niet alleen moet duidelijk worden wie er verantwoordelijk en aansprakelijk is voor de gegevenscontrole en de veiligheid van gegevens, maar deze toepassingen geven ook aanleiding tot ethische vraagstukken.

## 1.7 Tendensen met mogelijk grotere en langdurige gevolgen

Het is de verwachting dat het **3D-bioprinten** van organische voorwerpen, waarbij gebruikgemaakt wordt van kopieën van cellen van patiënten en "biologische verbanden" van collageen (onder de EU-wetgeving valt dit onder gevoelige gegevens) om opeenvolgende rijen levende cellen te maken, binnenkort algemeen beschikbaar wordt<sup>27</sup>. Het zou de levering van aangepaste menselijke anatomische delen vereenvoudigen en met name waardevol zijn in armere gebieden en voormalige conflictgebieden overal ter wereld. Bioprinten geeft uiteraard aanleiding tot zorgen op het gebied van de medische ethiek, het beschermen van intellectueel eigendom en consumentenbescherming, maar ook, aangezien het vertrouwt op het verwerken van intieme en gevoelige gegevens over de gezondheid van personen, over de toepassing van voorschriften op het gebied van gegevensbescherming.

**Kunstmatige intelligentie**, zoals robotica, verwijst naar een technologische eis voor zowel vaste als mobiele autonome machines. De verdere ontwikkeling hiervan biedt enorme mogelijkheden die verdergaan dan de huidige toepassingen. Zogenaemde "deep learning"-computers leren zichzelf taken door grote gegevensreeksen te verwerken met behulp van (onder andere) neurale netwerken die de hersenen lijken na te bootsen. Onderzoekers en ondernemingen streven ernaar om leren zonder toezicht te verbeteren. Het is al zo dat

algoritmen talen kunnen begrijpen en vertalen, afbeeldingen kunnen herkennen, nieuwsartikelen kunnen schrijven en medische gegevens kunnen analyseren<sup>28</sup>. Sociale media leveren enorme hoeveelheden persoonlijke informatie op die in feite al door de personen zelf van een etiket is voorzien. Dit zijn mogelijk de laatste ontwikkelingen in een reeks cognitieve verbeteringen om de mogelijkheden van het menselijk brein te vergroten, zoals papier of de abacus of geïntegreerd in autonome machines, robots, maar dit is het moment om de gevolgen voor individuen en de samenleving als geheel in overweging te nemen<sup>29</sup>.

## 2. Een ecosysteem ter bescherming van big data

De EU heeft nu de mogelijkheid om voorop te lopen en te laten zien hoe regeringen, toezichthouders, voor de verwerking verantwoordelijken, ontwerpers, ontwikkelaars en individuen beter kunnen samenwerken om hun rechten te versterken en sturing te geven aan technologische innovatie en deze niet te blokkeren. De tendensen die worden beschreven in hoofdstuk 2 hebben, volgens één commentator, "de kloof verbreed tussen wat er mogelijk is en wat er wettelijk is toegestaan"<sup>30</sup>. In tegenstelling tot wat door sommigen wordt beweerd, zijn privacy en gegevensbescherming een platform voor een duurzame en dynamische digitale omgeving en vormen zij geen belemmering. Onafhankelijke gegevensbeschermingsinstanties, zoals de EDPS, spelen een belangrijke rol in het ontcrachten van deze fabeltjes en in het reageren op de werkelijke zorgen die personen hebben over het verlies van controle over hun persoonsgegevens<sup>31</sup>.

De volgende generatie persoonsgegevens wordt waarschijnlijk nog minder toegankelijk voor de personen waarop de gegevens betrekking hebben. De verantwoordelijkheid voor het inrichten van één duurzame digitale interne markt wordt noodzakelijkerwijs door meerdere instanties gedeeld, maar is ook onderling afhankelijk, net als een ecosysteem, en er dient effectieve interactie plaats te vinden tussen ontwikkelaars, ondernemingen en toezichthouders in het belang van het individu. In dit hoofdstuk beschrijven we wat deze vier onmisbare spelers kunnen bijdragen.

### 2.1 Toekomstgerichte regulering

We hebben de EU recentelijk aangespoord om de historische kans te benutten om eenvoudigere regels te introduceren voor de verwerking van persoonsgegevens die een generatie lang van toepassing blijven<sup>32</sup>. De onderhandelingen over de Algemene Verordening gegevensbescherming en de richtlijn voor gegevensbescherming bij politie en justitie bevinden zich in het laatste stadium en binnenkort zal de aandacht worden gevestigd op de toekomst van de e-Privacy-richtlijn betreffende elektronische communicatie en de nieuwe verordening waarin wordt geregeld hoe de instellingen en organen van de EU zelf persoonsgegevens verwerken. Nu de economische kosten voor het verzamelen en opslaan van gegevens bijna verwaarloosbaar zijn, komt het neer op de gegevensbeschermingsinstanties om deze regels op consistente wijze te handhaven en het "morele gevaar" van overmatige gegevensverwerking te voorkomen<sup>33</sup>.

In de strategie voor de digitale interne markt wordt erkend dat er een link bestaat tussen de controle over grote hoeveelheden gegevens en marktmacht. De strategie deelt de overtuiging, zoals verwoord in ons voorlopige advies inzake privacy en concurrentievermogen in het tijdperk van big data uit 2014, dat er behoefte bestaat aan meer samenhang tussen de toezichthouders. De EU beschikt al over de middelen voor het herstellen van de machtsongelijkheden op de digitale markt: zo zijn bijvoorbeeld de lopende procedures voor de bestrijding van kartels door de Europese Commissie een erkenning van de dominantie van

mobiele apparaten bij de toegang tot internet. Een meer holistische handhaving is binnen het bestaande rechtskader mogelijk, bijvoorbeeld door een Europees clearinginstituut op te richten voor toezichthoudende autoriteiten waar kan worden bekeken of afzonderlijke gevallen aanleiding geven tot twijfels op het gebied van de voorschriften inzake mededinging, consumenten- en gegevensbescherming. Bijvoorbeeld:

- het verplichten van meer transparantie van de prijs, contant of anderszins, voor een dienst kan de analyse van mededingingszaken informeren en faciliteren<sup>34</sup>, en
- het opsporen van oneerlijke prijsdiscriminatie op basis van slechte gegevenskwaliteit en oneerlijke profielvorming en correlaties<sup>35</sup>.

Een nauwere dialoog tussen toezichthouders uit verschillende sectoren kan leiden tot een reactie op de toenemende oproepen tot globale partnerschappen die een "marktgrond" van open gegevens kunnen creëren, waar gegevens en ideeën, zoals statistieken en kaarten, in het algemeen belang beschikbaar kunnen zijn en kunnen worden uitgewisseld, met minder risico op surveillance, zodat individuen meer invloed hebben over besluiten die op hen van toepassing zijn<sup>36</sup>.

## **2.2 Verantwoordelijken met verantwoordingsplicht**

Voor de verantwoordingsplicht is het noodzakelijk dat intern beleid en controlesystemen worden ingericht die naleving waarborgen en relevante bewijsstukken bieden aan onafhankelijke toezichthoudende instanties.

We hebben gepleit voor het afschaffen van de bureaucratie in de gegevensbeschermingswetgeving door de eisen voor onnodige documentatie te minimaliseren om zo de ruimte te maximaliseren voor meer verantwoordelijke initiatieven door ondernemingen, ondersteund door adviezen van de gegevensbeschermingsinstanties. Het beginsel dat persoonsgegevens uitsluitend mogen worden verwerkt op manieren die verenigbaar zijn met het specifieke doeleinde/de specifieke doeleinden waarvoor zij zijn verzameld, is van essentieel belang bij de eerbiediging van de legitieme verwachtingen van een persoon. Bijvoorbeeld gedragscodes, audits, certificeringen en een nieuwe generatie contractsbepalingen en bindende bedrijfsvoorschriften kunnen helpen bij het opbouwen van een solide vertrouwen in de digitale markt. De verantwoordelijken voor de verwerking van persoonsgegevens moeten veel dynamischer en proactiever zijn en afstand nemen van de neiging tot geheimhouding en ondoorzichtigheid (de zogenoemde "Black Box"-tendens) van bedrijfspraktijken terwijl steeds meer transparantie wordt gevraagd van de klanten<sup>37</sup>.

## **2.3 Privacybewuste ontwikkeling**

De menselijke innovatie is altijd het product geweest van activiteiten door specifieke sociale groepen en specifieke contexten, die meestal de maatschappelijke normen van dat moment weerspiegelen<sup>38</sup>. Technologische ontwerpbesluiten mogen echter niet onze maatschappelijke interacties en de structuur van onze gemeenschappen dicteren, maar moeten onze waarden en grondrechten juist ondersteunen.

De EU moet ontwikkelingstechnieken en -methodologieën uitwerken en bevorderen die het mogelijk maken gegevensverwerkende technologieën in te voeren die de waardigheid en rechten van het individu volledig eerbiedigen. Systeem- en softwareontwikkelaars moeten de beginselen van privacy-by-design begrijpen en beter toepassen in nieuwe producten en diensten in de ontwerpfasen en in technologieën. De verantwoordingsplicht moet worden

ondersteund door meer onderzoek en de ontwikkeling van methoden en hulpmiddelen om nauwkeurige audits te waarborgen en om de naleving door voor de verwerking verantwoordelijken en verwerkers van de voorschriften te bepalen, door bijvoorbeeld elke eenheid persoonlijke informatie te taggen met metadata waarin de eisen op het gebied van gegevensbescherming worden beschreven.

Technische oplossingen moeten personen die hun persoonlijke levenssfeer en vrijheid door middel van anonimiteit willen behouden weerbaarder maken. De EU moet het ontwerp en de uitvoering van algoritmen bevorderen die identiteiten verhullen en gegevens samenvoegen om het individu te beschermen, maar tegelijkertijd toch gebruik te maken van de voorspellende kracht van de gegevens<sup>39</sup>.

We moeten nu de fundamenten leggen voor het vervullen van deze taken door ontwikkelaars en deskundigen op het gebied van gegevensbescherming uit verschillende gebieden samen te brengen in brede netwerken, zoals het Internet Privacy Engineering Network (IPEN), dat bijdraagt aan een vruchtbare interdisciplinaire uitwisseling van ideeën en benaderingen.

## 2.4 Weerbare natuurlijke personen

### Een "prosumentenomgeving"

Personen zijn niet slechts passieve objecten die door de wet moeten worden beschermd tegen uitbuiting. De hiervoor beschreven digitale tendensen bieden positieve kansen voor het versterken van de rol van het individu. Zo consumeren mensen bijvoorbeeld niet meer alleen inhoud en diensten, maar produceren ze deze ook. Ze kunnen ook steeds meer samen met de dienstverlener verantwoordelijk worden geacht voor de verwerking van persoonsgegevens, tenzij dit uitsluitend voor "huishoudelijke" doeleinden<sup>40</sup> is (voor de beschrijving van deze ontwikkeling is het begrip "prosument" ontstaan<sup>41</sup>). Ondertussen bieden virtuele valuta gebruikers anonimiteit en omzeilen zij de externe verificatie van transacties, waardoor de transactiekosten bij grensoverschrijdende betalingen voor goederen en diensten lager worden. Anderzijds zorgen de anonimiteit en de rechtsgebiedoverschrijdende (of, zo kan worden gesteld, de *rechtsgebiedloze*) aard van deze virtuele valuta ervoor dat individuen kwetsbaar worden voor fraude en criminele markten, die moeilijk op te sporen en te onderzoeken zijn. Naast de taken van toezichthouders, ondernemingen en ontwikkelaars, hebben ook burgers de verantwoordelijkheid bewust, alert, kritisch en geïnformeerd te zijn bij het maken van zowel online als offline keuzes<sup>42</sup>.

### Toestemming

Bovendien kan, in tegenstelling tot de traditionele gedachtegang, niet al het menselijk gedrag worden verklaard aan de hand van economische beginselen die ervan uitgaan dat mensen volledig rationeel zijn en gevoelig zijn voor economische stimulansen<sup>43</sup>. Dit is van belang voor de toekomstige rol van toestemming van de betrokkene voor de verwerking van persoonsgegevens over hem of haar. Op grond van de EU-wetgeving is toestemming niet de enige legitieme basis voor de meeste vormen van verwerking. Zelfs als de toestemming een belangrijke rol speelt, ontslaat dit de voor de verwerking verantwoordelijken niet van hun verantwoordingsplicht ten aanzien van wat zij met de gegevens doen, met name wanneer er algemene toestemming is verkregen voor de verwerking ten behoeve van een groot aantal doeleinden.

## Controle en "eigendom" van gegevens

Personen moeten fouten en oneerlijke vooroordelen kunnen aanvechten die het gevolg zijn van de logica die wordt gebruikt door algoritmen om aannamen en voorspellingen vast te stellen. Ter illustratie, bij een onderzoek in de VS van 3 000 kredietverslagen afkomstig van 1 000 consumenten, werd vastgesteld dat er in 26 % van de gevallen sprake was van "wezenlijke" fouten: problemen die zo ernstig waren dat ze van invloed waren op de kredietscores van de consumenten en derhalve op de kosten voor het verkrijgen van een krediet<sup>44</sup>.

Gegevens worden vaak gezien als hulpbronnen, zoals olie, die kunnen worden verhandeld, idealiter door partijen bij de transactie die alle even goed zijn geïnformeerd<sup>45</sup>. Klanten ontvangen geen eerlijke compensatie voor de persoonsgegevens die worden verhandeld en er zijn mensen die pleiten voor een model van gegevenseigendom. Absolute controle over persoonsgegevens is echter moeilijk te garanderen: er is dan sprake van andere moeilijkheden, zoals het openbaar belang en de rechten en vrijheden van anderen. Controle is noodzakelijk, maar niet toereikend<sup>46</sup>. De menselijke waardigheid is echter altijd een constante en op grond van de EU-wetgeving kan de analogie van eigendom niet als zodanig worden toegepast op persoonsgegevens, die intrinsiek zijn verbonden aan individuele personen. Er is in de EU-wetgeving geen bepaling waardoor een persoon afstand kan doen van dit grondrecht.

Een alternatieve methode om personen meer controle te geven over hun gegevens, wie daartoe toegang heeft en voor welk doeleinde, kan het gebruik zijn van persoonlijke gegevensopslag of "gegevenskluisen"<sup>47</sup>. Het concept van zo'n "persoonlijke opslag" vereist beveiligingsmechanismen die waarborgen dat alleen die entiteiten die van de betrokkene toestemming hebben gekregen toegang krijgen tot de gegevens en dan alleen tot die delen waarvoor toestemming is verleend. Persoonlijke gegevensopslag is het meest effectief wanneer dit betrekking heeft op actuele en voortdurend bijgewerkte informatie, zoals geospatiale gegevens of levenstekenen. In aanvulling op de technische beschermingsmaatregelen moeten gebruikers van gegevens worden verplicht de voorschriften inzake het delen en gebruiken van gegevens te eerbiedigen. Mededinging en de mogelijkheid om de dienst die wordt gebruikt te wijzigen, is de meest doeltreffende macht van een consument om invloed uit te oefenen op de diensten die hem ter beschikking staan. Het verzekeren van de portabiliteit van verbindingen, met inbegrip van identificatiemiddelen en contactgegevens, is aantoonbaar nuttig gebleken voor de mededinging en heeft de consumentenprijzen daadwerkelijk doen dalen na de liberalisatie van de telecommarkt. De portabiliteit van gegevens, dat wil zeggen de feitelijke en praktische mogelijkheid om de meeste gegevens over te zetten van de ene dienstenaanbieder naar de andere, is een effectief startpunt voor het creëren van de juiste omstandigheden voor daadwerkelijke consumentenkeus.

### **3. Waardigheid als de kern van een nieuwe digitale ethiek**

Een ethisch kader is nodig als basis voor de bouwstenen van dit digitale ecosysteem. De EDPS is van mening dat betere eerbiediging en bescherming van de menselijke waardigheid tegenwicht kan bieden aan de indringende surveillance en machtsongelijkheid waarmee personen tegenwoordig worden geconfronteerd. Dit moet de kern vormen van een nieuwe digitale ethiek.

### 3.1 Waardigheid en gegevens

Na de industriële revolutie in de 18<sup>e</sup> en de 19<sup>e</sup> eeuw streefde de mensenrechtenbeweging ernaar het bredere sociale goed veilig te stellen door de belemmeringen voor eerbiediging van het individu te verkleinen. De EU heeft nu, met het Handvest van de grondrechten en in navolging van de Universele Verklaring van de rechten van de mens en het Europees Verdrag voor de rechten van de mens de onschendbaarheid van de menselijke waardigheid als haar uitgangspunt genomen. De waardigheid van de mens is niet alleen een grondrecht op zich, maar ook het fundament voor andere vrijheden en rechten, waaronder het recht op eerbiediging van de persoonlijke levenssfeer en de bescherming van persoonsgegevens<sup>48</sup>. Objectificatie, waarbij een persoon wordt behandeld als middel ten behoeve van de doeleinden van een ander, kan worden beschouwd als een schending van de waardigheid<sup>49</sup>. Privacy maakt integraal onderdeel uit van de menselijke waardigheid en het recht op gegevensbescherming is oorspronkelijk geïntroduceerd in de jaren 1970 en 1980 als compensatie voor de mogelijke afbrokkeling van privacy en waardigheid als gevolg van de grootschalige verwerking van persoonsgegevens. In Duitsland was het recht op "informatieele zelfbeschikking" gebaseerd op het recht op persoonlijke waardigheid en op het recht op de vrije ontwikkeling van de persoonlijkheid, zoals vastgelegd in de artikelen 1 en 2 van de Duitse grondwet<sup>50</sup>.

In de eerst jaren van de 21<sup>e</sup> eeuw worden personen steeds vaker verplicht veel meer persoonsgegevens via internet bekend te maken om deel te nemen aan sociale, administratieve en zakelijke aangelegenheden en wordt de mogelijkheid om hiervan af te zien steeds kleiner. Nu alle activiteiten altijd online kunnen zijn, wordt het begrip van vrije en geïnformeerde toestemming onder enorme druk gezet. Elke minuut worden er "digitale broodkruimels" achtergelaten en gecombineerd om personen in realtime in te delen en om meerdere en soms tegenstrijdige profielen te maken. Deze profielen kunnen binnen microseconden worden gedistribueerd zonder dat de persoon daarvan op de hoogte is en worden gebruikt als basis voor belangrijke beslissingen die op hem of haar van toepassing zijn.

Profielen die worden gebruikt om het gedrag van mensen te voorspellen, lopen het risico stigmatiserend te zijn en bestaande stereotypen, sociale en culturele segregatie en uitsluiting te versterken<sup>51</sup>, waarbij deze "collectieve inlichtingen" de individuele keuze en gelijke kansen ondermijnen. Deze "filterbubbels" of "persoonlijke echoruimten" kunnen ertoe leiden dat de creativiteit, innovatie, vrijheid van meningsuiting en vrijheid van vereniging worden onderdrukt die er juist voor hebben gezorgd dat de digitale technologie tot bloei kon komen.

Ondertussen wordt er nog steeds een uitzonderingsstatus toegekend op grond van de "veiligheid" als rechtvaardiging voor de meerdere lagen aan indringende technieken voor het monitoren van de activiteiten van personen<sup>52</sup>. Voor het begrijpen van deze toegenomen surveillance is een langetermijnperspectief nodig op de algemene gevolgen voor de samenleving en gedrag.

De EU moet, net als derde landen, nauwkeurig kijken hoe deze waarden kunnen worden gewaarborgd en niet slechts op papier worden geëerbiedigd terwijl ze in werkelijkheid in cyberspace worden geneutraliseerd. Met name de EU heeft nu een "kritieke periode" voor het massaal aannemen van deze technologieën om waarden in te bouwen in digitale structuren die onze samenleving zullen definiëren<sup>53</sup>. Hiervoor is een nieuwe beoordeling nodig van de vraag of de mogelijke voordelen van de nieuwe technologieën daadwerkelijk afhankelijk zijn van de verzameling en analyse van persoonlijk identificeerbare gegevens van miljarden

individuen. Een dergelijke beoordeling kan ontwikkelaars uitdagen om producten te ontwerpen die in realtime enorme hoeveelheden ongeorganiseerde informatie van persoonlijke kenmerken ontdoen om het zo moeilijker of onmogelijk te maken er één persoon uit te halen.

We erkennen al dat bepaalde vormen van gegevensverwerking, bijvoorbeeld genetische gegevens, niet alleen moeten worden gereguleerd, maar ook door de bredere maatschappij moeten worden beoordeeld, zoals door ethische commissies. Genetische gegevens hebben door hun aard niet slechts betrekking op één persoon, maar ook op diens voorouders en nakomelingen. Genetische gegevens dienen niet alleen ter identificatie van familierelaties, maar elementen die worden aangetroffen in de genen van één persoon, kunnen ook informatie geven over diens ouders en kinderen en leiden tot besluiten van voor de verwerking verantwoordelijken die van invloed zijn op hun kansen in het leven, zelfs al voordat ze geboren zijn. De mogelijke concentratie van genetische persoonsgegevens in de handen van een aantal grote spelers op de markt, heeft gevolgen voor de markteconomie en voor de betrokkenen. Een toenemende afhankelijkheid van een wereldwijd systeem van verzameling en analyse van een voortdurende gegevensstroom, kan de samenleving en de economie kwetsbaarder maken voor ongekende fouten in de beveiliging en kwaadaardige aanvallen.

Het bestaande kader kan falen als we de toekomst niet met behulp van innovatief denken benaderen. Er is sprake van een toenemende vraag en behoefte om de betrokkene te beschouwen als een individu en niet slechts als consument of gebruiker. Werkelijk onafhankelijke gegevensbeschermingsinstanties spelen een cruciale rol in het voorkomen van een toekomst waarin individuen worden bepaald door algoritmen en de voortdurende variaties daarvan. Ze moeten worden uitgerust met een "zorgplicht" jegens individuen en hun online waardigheid. Traditionele opvattingen en beginselen over privacy en gegevensbescherming bevatten al ethische nuances voor de bescherming van de waardigheid, zoals werkgelegenheid en gezondheid. De huidige tendensen hebben echter een heel nieuw hoofdstuk geopend en er bestaat een behoefte om te verkennen of de beginselen solide genoeg zijn voor het digitale tijdperk<sup>54</sup>. Het begrip "persoonsgegeven" zelf zal waarschijnlijk radicaal veranderen wanneer de technologie individuen steeds meer in staat stelt om opnieuw te worden geïdentificeerd aan de hand van vermeende anonieme gegevens. Daarnaast zullen machinelere en het samenvoegen van menselijke en kunstmatige intelligentie de concepten van de rechten en verantwoordelijkheden van een individu ondermijnen.

### **3.2 Een Europese ethische adviescommissie**

Met het voorgaande wilden wij geen alarmerend beeld van een dystopie schetsen. Er worden al discussies gevoerd binnen de juridische, politieke, economische, sociale, wetenschappelijke en zelfs religieuze wereld<sup>55</sup>. Simplistische benaderingen die eenzijdig voordeel bieden aan economische winst of surveillance voor veiligheid, zijn waarschijnlijk niet nuttiger dan een al te beperkte toepassing van bestaande wetgeving die innovatie en vooruitgang zou beperken. De EDPS stelt daarom voor een uitgebreide, brede en multidisciplinaire analyse uit te voeren om aanbevelingen te doen en een maatschappelijk debat te informeren over hoe een vrije, democratische samenleving het hoofd moet bieden aan de technologische uitdagingen.

De strategie van de EDPS<sup>56</sup> die is gericht op de ontwikkeling van een ethische benadering van gegevensbescherming waarbij wordt erkend dat "haalbaar, nuttig of winstgevend, niet gelijkstaat aan duurzaam" en waarin de "verantwoordingsplicht wordt benadrukt ten opzichte van de mechanische naleving van de letter van het recht". We streven ernaar ook de



gemeenschappen buiten vertegenwoordigers van de EU, advocaten en IT-deskundigen te bereiken en eminente personen te benaderen die in staat zijn de gevolgen op de middellange en lange termijn te beoordelen van de technologische wijzigingen en de reacties daarop van de toezichthouders. De komende maanden zullen we binnen onze onafhankelijke instelling een externe adviescommissie samenstellen over de ethische dimensie van gegevensbescherming om de relatie te verkennen tussen mensenrechten, technologie, markten en ondernemingsmodellen in de 21<sup>e</sup> eeuw.

Onze ethische adviescommissie zal bestaan uit een selecte groep onderscheiden personen afkomstig uit de ethiek en filosofie, sociologie, psychologie, technologie en de economie, die indien nodig zullen worden bijgestaan door deskundigen met kennis en ervaring op het gebied van gezondheid, vervoer en energie, sociale interactie en media, economie en financiën, governance en democratie en veiligheid en politieel toezicht. Ze worden uitgenodigd de bredere ethische gevolgen te beoordelen van de manier waarop persoonsgegevens ontstaan en worden gebruikt, waarbij hun overwegingen op maximale wijze transparant worden gemaakt.

#### **4. Conclusie: tijd voor verdieping van de discussie**

De bescherming van de persoonlijke levenssfeer en gegevensbescherming zijn onderdeel van de oplossing, niet het probleem. Voorlopig wordt de technologie door mensen gecontroleerd. Het is niet eenvoudig om deze potentiële ontwikkelingen simpelweg te classificeren als goed of slecht, wenselijk of schadelijk, voordelig of nadelig, en nog minder indien een aantal mogelijke tendensen in context moet worden gezien. Beleidsmakers, technologieontwikkelaars, activiteitenontwikkelaars en wij allen moeten serieus nadenken of en hoe wij invloed willen uitoefenen op de ontwikkeling van technologie en de toepassing daarvan. Maar even belangrijk is dat de EU met spoed gaat kijken naar de ethiek en de plaats van de menselijke waardigheid in de technologieën van de toekomst.

De beginselen voor gegevensbescherming hebben bewezen dat zij natuurlijke personen en hun persoonlijke levenssfeer kunnen beschermen tegen de risico's van onverantwoorde gegevensverwerking. Maar de tendensen van vandaag vergen mogelijk een geheel nieuwe benadering. Daarom geven wij de aanzet voor een nieuw debat over de vraag in welke mate de toepassing van beginselen zoals eerlijkheid en rechtmatigheid afdoende is. Degenen die bij de gegevensbescherming betrokken zijn, kunnen een nieuwe rol spelen met gebruikmaking van bestaande instrumenten, zoals voorafgaande controles en autorisaties – omdat er geen andere organisaties toegerust zijn om een dergelijke gegevensverwerking aan een onderzoek te onderwerpen. Nu de technologie, mondiale innovatie en menselijke verbondenheid zich pijlsnel ontwikkelen, hebben wij de kans om aandacht te vragen, belangstelling te wekken en consensus te bereiken.

Met dit advies hopen wij een kader te bieden voor een bredere en diepere discussie over hoe de EU de integriteit van haar normen en waarden kan waarborgen, terwijl zij tegelijkertijd de voordelen van de nieuwe technologieën omarmt.

Gedaan te Brussel, 11 september 2015

**(getekend)**

Giovanni BUTTARELLI

Europese toezichthouder voor gegevensbescherming

## Noten

---

<sup>1</sup> Bron: GSMA Intelligence.

<sup>2</sup> De "wet van Moore", dat het aantal transistors dat op een microchip kan worden geplaatst elke achttien maanden verdubbelt, is over het algemeen juist gebleken; Moore, Gordon E. (19-4-1965). "Cramming more components onto integrated circuits", *Electronics*. 22-8-2011.

<sup>3</sup> Nathan Eagle, Alex (Sandy) Pentland, "Reality mining: sensing complex social systems", *Journal Personal and Ubiquitous Computing* Volume 10 Issue 4, maart 2006, blz. 255–268. Shoshana Zuboff schrijft in "Big Other: surveillance capitalism and the prospects of an information civilization", *Journal of Information Technology* (2015) 30, blz. 75-89: "As a result of pervasive computer mediation, nearly every aspect of the world is rendered in a new symbolic dimension as events, objects, processes, and people become visible, knowable, and shareable in a new way". Zuboff voorziet een "toename van een nieuwe universele architectuur" die zij "Big Other" noemt, "a ubiquitous networked institutions regime that records, modifies, and commodifies everyday experience from toasters to bodies, communication to thought, all with a view to establishing new pathways to monetization and profit"; blz. 77, 81.

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

<sup>5</sup> Volgens de update op 31 maart 2015 van *PWC Global Top Ten Companies by Market Capitalisation* is geen van de tien grootste ondernemingen in de technologiesector op basis van marktkapitalisatie gevestigd in de EU (acht ondernemingen zijn gevestigd in de VS, één in China en één in Taiwan).

<sup>6</sup> "Big data refers to the exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed (hence the name: analytics) using computer algorithms", advies nr. 3/2013 van de Artikel 29-Groep betreffende doelbinding. In een verslag van het Witte Huis uit 2014 wordt big data beschreven als: "The growing technological ability to capture, aggregate, and process an ever-greater volume, velocity, and variety of data", zie "Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President" ("Podesta-verslag"), mei 2014.

<sup>7</sup> In de EU-wetgeving wordt onder "persoonsgegevens" verstaan: iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon ("betrokkene"); als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit", artikel 2, onder a), van Richtlijn 95/46/EG. Deze definitie is in brede zin vergelijkbaar met de definitie die is vastgesteld door de Raad van Europa in het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ook bekend als "Verdrag nr. 108") en in de OESO-richtsnoeren inzake de bescherming van de privacy en het grensoverschrijdende verkeer van persoonsgegevens. Zie voor een uitgebreide analyse advies 4/2007 van de Artikel 29-Groep over het begrip persoonsgegevens, WP 136.

<sup>8</sup> Zie bijvoorbeeld een toespraak door de voorzitter van de Federale Handelscommissie van de Verenigde Staten (FTC) in 2014: "The proliferation of connected devices, the plummeting cost of collecting, storing, and processing information, and the ability of data brokers and others to combine offline and online data means that companies can accumulate virtually unlimited amounts of consumer information and store it indefinitely. Using predictive analytics, they can learn a surprising amount about each of us from this", inleidende opmerkingen van de voorzitter van de FTC, Edith Ramirez, "Big Data: A Tool for Inclusion or Exclusion?", Washington, DC, 15 september 2014. Sandy Pentland merkt het volgende op: "Social physics is a quantitative social science that describes reliable, mathematical connections between information and idea flow on the one hand and people's

---

behaviour on the other (...) it enables us to predict the productivity of small groups, of departments within companies and even of entire cities." Dit "is what is required to build better social systems" (blz. 4, 7) en om "allow (government officials, industry managers, and citizens) to use the tools of social network incentives to *establish new norms of behavior*" (blz. 189) (cursief door ons); Pentland, *Social Physics: How Good Ideas Spread: The Lessons from a New Science*.

<sup>9</sup> Speciale Eurobarometer 431 inzake gegevensbescherming, juni 2015, en een enquête van het onderzoekspanel van Pew uit januari 2014 over de openbare perceptie van privacy en veiligheid na de onthullingen van Snowden. Een gemiddeld bezoek aan één website leidt volgens een onderzoek tot 56 gevallen waarin gegevens worden verzameld, volgens Julia Angwin *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, 2012). In het verslag van het Witte Huis over big data uit 2014 wordt gesteld dat "unprecedented computational power and sophistication (...) create an asymmetry of power between those who hold the data and those who intentionally or inadvertently supply it"; "some of the most profound challenges revealed during this review concern how big data analytics may (...) create such an opaque decision-making environment that individual autonomy is lost in an impenetrable set of algorithms."

<sup>10</sup> Met behulp van de anonieme gegevens uit de volkstelling van 1990 kan 87 % van de Amerikaanse bevolking waarschijnlijk worden geïdentificeerd aan de hand van hun vijfcijferige postcode in combinatie met het geslacht en de geboortedatum; zie hiervoor Paul Ohm "Broken promises of privacy: responding to the surprising failure of anonymisation", *UCLA Law Review* 2010 en "Record linkage and privacy: issues in creating new federal research and statistical info", april 2011. Dna is uniek (behalve bij eeneiige tweelingen) en blijft het hele leven stabiel. Het bevat informatie over etniciteit, aanleg voor ziekten en kan andere familieleden identificeren. In januari 2013 konden onderzoekers individuen en personen identificeren aan de hand van anonieme dna-gegevens uit openbaar toegankelijke geneologiedatabases; Gymrek, M., McGuire, A. L., Golan, D., Halperin, E. & Erlich, Y. *Science* 339, 321–324 (2013). Zie ook "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/> (laatst geraadpleegd op 10.9.2015). Zie ook de volgende adviezen van de Artikel 29-Groep: nr. 4/2007 over het begrip persoonsgegevens, nr. 3/2013 over doelbinding, nr. 6/2013 over open gegevens en hergebruik van overheidsinformatie, en nr. 5/2014 over anonimiseringstechnieken.

<sup>11</sup> Bron: Gartner.

<sup>12</sup> Zie bijvoorbeeld de paneldiscussie "What is the future of official statistics in the Big Data era?" van de Royal Statistical Society, Londen, 19 januari 2015; <http://www.odi.org/events/4068-future-official-statistics-big-data-era> (laatst geraadpleegd op 10.9.2015).

<sup>13</sup> "Ten technologies which could change our lives: potential impacts and policy implications", Eenheid Wetenschappelijke prognose, Onderzoeksdienst van het Parlement, januari 2015.

<sup>14</sup> Het werkprogramma van de EU voor de periode 2016-2017 in het kader van Horizon 2020 ondersteunt deze ontwikkelingen, met inbegrip van grootschalige proefprojecten waarbij wordt gekeken naar zorgpunten op het gebied van persoonlijke levenssfeer en ethiek.

<sup>15</sup> Verzekeringen zijn wel beschreven als het "native business model for the Internet of Things"; "From fitness trackers to drones, how the 'Internet of Things' is transforming the insurance industry", *Business Insider*, 11.6.2015. Het begrip "prijstdiscriminatie" in het mededingingsrecht, afgeleid van artikel 102 VWEU, waarin een dominante onderneming "het rechtstreeks of zijdelings opleggen van onbillijke aan- of verkoopprijzen of van andere onbillijke contractuele voorwaarden" wordt verboden, is zeer omstrede. Zie bijvoorbeeld Damien Gerardin en 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. Zie voor big data en het (volgens de auteurs nog niet gerealiseerde) potentieel om gepersonaliseerde prijzen te versnellen de publicatie van het Executive Office of the President of the United States, "Big Data and Differential Pricing" uit februari 2015, en een recente analyse waarin wordt geconcludeerd dat gepersonaliseerde prijzen over het

---

algemeen inhoudt dat persoonsgegevens moeten worden verwerkt en dat hierbij het transparantiebeginsel van de gegevensbeschermingswetgeving in acht moet worden genomen, zodat ondernemingen mensen moeten informeren over het doeleinde van de verwerking van hun persoonsgegevens: ondernemingen moeten het zeggen als ze prijzen personaliseren. En als een onderneming een cookie gebruikt om iemand te herkennen, is de onderneming op grond van de e-Privacy-richtlijn verplicht de persoon te informeren over het doel van de cookie; ontwerpdocument door Frederik Borgesius "Online Price Discrimination and Data Protection Law". Beschikbaar op [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2652665](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665) (laatst geraadpleegd op 10.9.2015).

<sup>16</sup> Medische apparaten worden in de EU-wetgeving gedefinieerd overeenkomstig Richtlijn 93/42/EEG van de Raad betreffende medische hulpmiddelen, gewijzigd bij Richtlijn 2007/47/EG van het Europees Parlement en de Raad van 5 september 2007. Zie advies nr. 1/2015 van de EDPS voor de gevolgen van "mobiele gezondheidszorg" voor de gegevensbescherming.

<sup>17</sup> Volgens Eurostat maakt 21 % van de personen en 19 % van de ondernemingen in de EU gebruik van cloudopslagdiensten.

<sup>18</sup> "If the worldwide Internet were a country, it would be the 12th-largest consumer of electricity in the world, somewhere between Spain and Italy. This represents roughly 1.1 to 1.5 percent of global electricity use (as of 2010) and the greenhouse gases generated annually by 70 to 90 large (500-megawatt) coal-fired power plants." Natural Resources Defense Council, Data Centre Efficiency Assessment: Scaling Up Energy Efficiency Across the Data Centre Industry: Evaluating Key Drivers and Barriers 2014.

<sup>19</sup> Verslag van het onderzoek "SMART 2013/0043 - Uptake of Cloud in Europe".

<sup>20</sup> Bron: Eurostat.

<sup>21</sup> De term "deeleconomie" wordt bekritiseerd als misleidend: "The Sharing Economy Isn't About Sharing at All", Giana M. Eckhardt en Fleura Bardhi, Harvard Business Review, 28.1.2015.

<sup>22</sup> Rachel Botsman en Roo Rogers, *What's Mine Is Yours: How Collaborative Consumption is Changing the Way We Live*, 2011.

<sup>23</sup> Future of Privacy Forum, "User Reputation: Building Trust and Addressing Privacy Issues in the Sharing Economy", juni 2015.

<sup>24</sup> Zie de workshop van 9 juni 2015 van de Federale Handelscommissie van de VS over "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/> (laatst geraadpleegd op 10.9.2015).

<sup>25</sup> Zie over de gevolgen voor gegevensbescherming van drones of op afstand bestuurd vliegtuigen het advies van de EDPS over de mededeling van de Commissie aan het Europees Parlement en de Raad: "Een nieuw tijdperk voor de luchtvaart De openstelling van de luchtvaartmarkt voor het veilige en duurzame civiele gebruik van op afstand bestuurd vliegtuigen" van november 2014.

<sup>26</sup> Bron: Boston Consulting Group.

<sup>27</sup> Gartner.

<sup>28</sup> Het algoritme van de DeepFace gezichtsherkenning op Facebook heeft een succesgraad van 97 % en doet het daarmee beter dan mensen, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification", gepubliceerd in een verslag over de IEEE-conferentie inzake computervisie en patroonherkenning, juni 2014.

<sup>29</sup> Robo is gedefinieerd als een "machine situated in the world that senses, thinks, and acts", Bekey, G, "Current trends in robotics: technology and ethics", in "Robot Ethics - The ethical and social implications of robotics", The MIT Press2, 2012, blz. 18. Er wordt geschat dat er tussen 2013 en 2016

---

22 miljoen dienstrobots worden verkocht, IRF World Robotics Report, 2013. Zie over kunstmatige intelligentie "Rise of the Machines", Economist, 9.5.2015 en het internetproject van het Pew Research Centre uit 2014. Een onderneming die actief was op het gebied van kunstmatige intelligentie stelde voor zijn overname door een leidinggevende technologische onderneming als voorwaarde dat er een ethische en veiligheidscommissie zou worden opgericht en er een verbod zou komen op het gebruik van kunstmatige intelligentie voor militaire doeleinden of voor de inlichtingendiensten, Forbes, Inside Google's Mysterious Ethics Board, 3.2.2014.

<sup>30</sup> Pentland, *Social physics*, blz. 147.

<sup>31</sup> Zie noot 9 hiervoor. Pentland, *Social physics*, blz. 153: "Great leaps in health care, transportation, energy and safety are all possible... the main barriers to achieving these goals are privacy concerns and the fact that we don't yet have any consensus around the trade-offs between personal and social values." De discussie rondom de ebola-pandemie in West-Afrika in 2014 illustreert hoe de valse dichotomie tussen de privacy van een individu en de behoeften van de samenleving tot stand komt. Ziekten worden vaak gevolgd en de levensduur ervan wordt gemeten via vragenlijsten en tellingen die eenvoudig achterhaald raken en die moeilijk te extrapoleren zijn om te anticiperen op waar de ziekte opnieuw zal toeslaan. Er bestaan enkele voorbeelden voor het gebruik van big data over het volgen van uitbraken van malaria in Namibië en Kenia en in 2009 om de doeltreffendheid bij te houden van gezondheidswaarschuwingen van de regering tijdens de Mexicaanse varkensgriepcrisis. Eén gegevensbron zijn de gegevens van mobiele telefoons, waaruit blijkt welke zendmast een gesprek heeft verwerkt en die in realtime een ruwe aanduiding kunnen geven van de locatie van mensen en waar ze naartoe gaan. Het verzamelen van deze gegevens is niet gericht, er kan geen onderscheid worden gemaakt tussen mensen met en zonder ebola. Een Zweedse ngo bracht heeft de mobiliteit van de bevolking in West-Afrika in kaart gebracht, maar de gegevens werden niet gebruikt, aangezien de aanbieders van mobiele telefonie deze niet wilden vrijgeven aan erkende externe onderzoekers, waarbij zij zich beriepen op het ontvangen van instructies van de regering, die zich op haar beurt weer beriep op zorgen met betrekking tot de privacy die niet konden worden gegarandeerd op grond van de EU-wetgeving; <http://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola>. (laatst geraadpleegd op 10.9.2015).

<sup>32</sup> Advies 3/2015 van de EDPS.

<sup>33</sup> De aanname op het gebied van big data dat "N=all" houdt in dat naar alle gegevenspunten moet worden gekeken en niet slechts een steekproef, Viktor Mayer-Schönberger en Kenneth Cukier, *The Rise of Big Data: How it's changing the way we think about the world*, 2013. De Raad van Lissabon en het Progressive Policy Institute stellen dat de welvaart zal toenemen door de "digitale dichtheid" - "de hoeveelheid gegevens die per inwoner wordt gebruikt in een economie" te maximaliseren <http://www.lisboncouncil.net/component/downloads/?id=1178> (laatst geraadpleegd op 10.9.2015). De Internationale Werkgroep inzake gegevensbescherming in de telecommunicatie (ook bekend als de "Berlijn-groep") heeft afwijkingen voorgesteld voor big data binnen de beginselen voor gegevensbescherming; [http://www.datenschutz-berlin.de/attachments/1052/WP\\_Big\\_Data\\_final\\_clean\\_675.48.12.pdf](http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf). (laatst geraadpleegd op 10.9.2015). Het World Economic Forum heeft opgeroepen zich te richten op het gebruik en niet op de verzameling en om afstand te nemen van het vereiste om toestemming te vragen voor het verzamelen van persoonsgegevens, "Unlocking the Value of Personal Data: From Collection to Usage, 2013.

<sup>34</sup> Zie het voorlopig advies van de EDPS inzake privacy en concurrentievermogen in het tijdperk van big data.

<sup>35</sup> In artikel 21 van het Handvest van de grondrechten wordt "[e]lke discriminatie, met name op grond van geslacht, ras, kleur, etnische of sociale afkomst, genetische kenmerken, taal, godsdienst of overtuigingen, politieke of andere denkbeelden, het behoren tot een nationale minderheid, vermogen, geboorte, een handicap, leeftijd of seksuele geaardheid" verboden. Veel van deze gegevenscategorieën ("waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt,

---

alsook de verwerking van gegevens die de gezondheid of het seksuele leven betreffen") genieten grotere bescherming op grond van artikel 8 van Richtlijn 95/46/EG.

<sup>36</sup> Zie voor het idee van een digitale marktgrond "Ambition numérique: Pour une politique française et européenne de la transition numérique", Franse digitale raad, juni 2015 blz. 276; Bruce Schneier pleit voor het oprichten van "openbare ruimten zonder eigenaar" op internet, zoals openbare parken, *Data and Goliath*, blz. 188-189; Sandy Pentland pleit voor een "marktgrond voor openbare gegevens", *Social Physics*, blz. 179. Zie voor de beoordeling van de veiligheid van de publicatie van samengestelde gegevensreeksen als openbare gegevens advies nr. 6/2013 van de Artikel 29-Groep over open gegevens en hergebruik van overheidsinformatie.

<sup>37</sup> "Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent" <http://crackedlabs.org/studie-kommerzielle-ueberwachung/info>. Zie over gekwalificeerde transparantie bv. Frank Pasquale: *The Black Box Society: The Secret Algorithms that Control Money and Information*.

<sup>38</sup> "Behind the technology that affects social relations lie the very same social relations", David Noble, "Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools", in *Case Studies in the Labor Process*, ed. Andrew Zimbalist, 1979. Zie ook Judy Wacjman, *Pressed for Time: The Acceleration of Life in Digital Capitalism*, 2014 blz. 89-90, en Zuboff, "Big Other" (aangehaald in noot 3 hiervoor).

<sup>39</sup> Advies nr. 5/2014 over anonimiseringstechnieken, goedgekeurd op 10 april 2014 (WP 216).

<sup>40</sup> Zie voor een nauw geformuleerde uitzondering op de voorschriften inzake gegevensbescherming voor persoonlijke of huishoudelijke doeleinden het arrest van het HvJEU in de zaak C-212/13 *František Ryneš / Úřad pro ochranu osobních údajů*.

<sup>41</sup> De term "prosument" werd geïntroduceerd door Alvin Toffler in *The Third Wave*, 1980. Zie voor een discussie over de "prosumentenomgeving" en hoe deze moet worden gereguleerd Ian Brown en Chris Marsden, *Regulating Code*, 2013.

<sup>42</sup> Advies van de Europese groep ethiek van de exacte wetenschappen en de nieuwe technologieën aan de Europese Commissie: *Ethics of Security and Surveillance Technologies*, advies nr. 28, 20.5.2015, blz. 74.

<sup>43</sup> Zie bijvoorbeeld Homer Economicus: *The Simpsons and Economics*, ed. Joshua Hall, 2014.

<sup>44</sup> Op grond van de meest conservatieve definitie van "fout", houdt dit in dat in de consumentenverslagen van 23 miljoen Amerikanen wezenlijke fouten zitten. Bij vijf procent van de deelnemers aan het onderzoek was sprake van fouten die, na te zijn gecorrigeerd, de kredietscore zodanig verhoogden dat ze krediet konden verkrijgen tegen een lagere prijs; 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. Beschikbaar op SSRN: <http://ssrn.com/abstract=2432955>.

<sup>45</sup> Het World Economic Forum beschouwt gegevens als een waardevol activa van een persoon waarvan de rechten op bezit, gebruik en verwijdering kunnen worden verleend aan ondernemingen en overheden in ruil voor diensten. Zie recente toespraken, ook door de vicevoorzitter van de Commissie Ansip, bijvoorbeeld bij de jaarlijkse Bruegel-bijeenkomst op 7.3.2015, getiteld "Productivity, innovation and digitalisation - which global policy challenges?: "Ownership and management of data flows, use and re-use of data. Management and storage of data. These underpin important emerging sectors like cloud computing, the Internet of Things and big data."

<sup>46</sup> "So who possesses the right to use the information and data that truly do not belong to one's self? This is an issue that transcends borders of commerce, ethics, and morals, leading to privacy issues and the protection of privacy", Al-Khouri, november 2012, [http://www.academia.edu/6726887/Data\\_Ownership\\_Who\\_Owns\\_My\\_Data\\_036](http://www.academia.edu/6726887/Data_Ownership_Who_Owns_My_Data_036). Zie ook Margaret

---

Jane Radin, "Incomplete Commodification in the Computerized World", in *The Commodification of Information* 3, 17, Niva Elkin-Koren & Neil Weinstock Netanel eds. 2002: "It makes a big difference whether privacy is thought of as a human right, attaching to persons by virtue of their personhood, or as a property right, something that can be owned and controlled by persons. Human rights are presumptively market-inalienable, whereas property rights are presumptively market-alienable."

<sup>47</sup> Het project "Computer Science and Artificial Intelligence Lab's Crosscloud" van MIT dat door verschillende in de EU gevestigde ondernemingen wordt ondersteund, streeft naar het volgende "1) make it easy to develop multi-user ('social') software using only front-end development and respecting the rights and privacy of users. And 2) allow users the freedom to move easily among applications, hardware platforms, and social networks, keeping their data and social connections", <http://openpds.media.mit.edu/#architecture> (laatst geraadpleegd op 10.9.2015).

<sup>48</sup> Zie de toelichting bij artikel 1 van het Handvest van de grondrechten.

<sup>49</sup> Martha Nussbaum, "Objectification", in *Philosophy and Public Affairs* 24, 4, 1995.

<sup>50</sup> Arrest van 15 december 1983, BVerfGE 65, 1-71, Volkszählung.

<sup>51</sup> Zie het advies van de Europese groep ethiek van de exacte wetenschappen en de nieuwe technologieën inzake ethiek en surveillance, blz. 75. In een onderzoek is gesuggereerd dat een algoritme voor gerichte advertenties discrimineerde, omdat zoekopdrachten gemiddeld banen met een hoger salaris aan mannen liet zien in vergelijking tot vrouwen die banensites bezochten, Carnegie Mellon University en het International Computer Science Institute. Zie over de tendens om digitale assistenten standaard een vrouwenstem te geven bijvoorbeeld Judy Wajcman, "Feminist theories of technology", *Cambridge Journal of Economics*, 34 (1). blz. 143-152, 2010.

<sup>52</sup> Giorgio Agamben, *State of Exemption*, 2005.

<sup>53</sup> Neil Richards, Neil en Jonathan King, Big Data Ethics (19 mei 2014), *Wake Forest Law Review*, 2014.

<sup>54</sup> BBC, "Information watchdog investigates 'charity data sales'", 1.9.2015.

<sup>55</sup> Zie de brief van het Future of Life Institute. De pauselijke encycliciek *Laudato Si*: "(...) wanneer [media en de digitale wereld] alomtegenwoordig worden, [bevorderen zij] niet de ontwikkeling om wijs te leven, diep na te denken, edelmoedig lief te hebben. De grote wijzen van het verleden zouden in deze context het gevaar lopen hun wijsheid verstikt te zien te midden van het chaotische rumoer van de informatie. Dat vraagt van ons een krachtsinspanning dat deze middelen worden vertaald in een nieuwe culturele ontwikkeling van de mensheid en niet in een achteruitgang van haar grootste rijkdom. Ware wijsheid, de vrucht van reflectie, dialoog en edelmoedige ontmoeting tussen personen, verwerft men niet met een pure opeenhoping van data die uiteindelijk verzadigt en verwart in een soort geestelijke vervuiling. Tegelijkertijd is er de neiging de werkelijke relaties met de ander met al de uitdagingen die zij inhouden, te vervangen door een soort communicatie die door internet tot stand wordt gebracht. Dat maakt het mogelijk relaties te selecteren of te elimineren overeenkomstig onze willekeur, en zo wordt er vaak een nieuwe type kunstmatige emoties gegenereerd die meer van doen hebben met apparaten en schermen dan met personen en de natuur. De huidige middelen maken het mogelijk dat wij met elkaar communiceren en kennis en genegenheden delen. Soms verhinderen zij ons echter ook direct contact te krijgen met de angst, de vrees, de vreugde van de ander en de complexiteit van zijn persoonlijke ervaring. Daarom zou het feit niet moeten verbazen dat, samen met het overweldigende aanbod aan deze producten, een diepe en melancholische onvoldaanheid of schadelijk isolement groeit in de intermenselijke relaties."

<sup>56</sup> Zie actiepoint 4 in de strategie van de EDPS voor de periode 2015-2020 over de ontwikkeling van een ethische dimensie van gegevensbescherming.