VERANTWOORDELIJK OMGAAN MET DIGITALISERING

Een oproep naar overheden en bedrijfsleven, waar ook de burger toe kan/moet bijdragen

Luc Bonte
Aimé Heene
Paul Verstraeten e.a.

KVAB STANDPUNTEN
61
Koninklijke Vlaamse Academie van België
voor Wetenschappen en Kunsten - 2018

VERANTWOORDELIJK OMGAAN MET DIGITALISERING

EEN OPROEP NAAR OVERHEDEN EN BEDRIJFSLEVEN, WAAR OOK DE BURGER TOE KAN/MOET BIJDRAGEN

KVAB Press

KVAB STANDPUNTEN
61

Ontwerp cover: Francis Strauven

De tekening van het Paleis der Academiën is een reproductie van het originele perspectief van Charles Vander Straeten in 1823. Jozef Cantré ontwierp het logo van de KVAB in 1947.
De KVAB Standpunten worden gepubliceerd door de Koninklijke Vlaamse Academie van België voor Wetenschappen en Kunsten, Hertogsstraat 1, 1000 Brussel.
Tel. 00 32 2 550 23 23 – info@kvab.be – www.kvab.be

VERANTWOORDELIJK OMGAAN MET DIGITALISERING

EEN OPROEP NAAR OVERHEDEN EN BEDRIJFSLEVEN, WAAR OOK DE BURGER TOE KAN/MOET BIJDRAGEN

Yolande Berbers
Luc Bonte
Hugo De Man
Jochanan Eynikel
Aimé Heene
Willy Van Overschée
Joos Vandewalle
Paul Verstraeten

D/2018/0455/11
ISBN 978 90 656 918 97

Aanbevolen citeerwijze: Luc Bonte, Aimé Heene, Paul Verstraeten e.a., *Verantwoordelijk omgaan met digitalisering. Een oproep naar overheden en bedrijfsleven, waar ook de burger toe kan/moet bijdragen*, KVAB Standpunt 61, 2018.

Drukkerij Universa

Verantwoordelijk omgaan met digitalisering
Een oproep naar overheden en bedrijfsleven, waar ook de burger toe kan/moet bijdragen

INHOUD

Samenvatting

De explosieve toename van het verzamelen van data en van de verwerkingscapaciteit van deze data in een gedigitaliseerde wereld dwingt bedrijven en overheden ertoe een strategie te ontwikkelen om verantwoord met deze 'disruptie' om te gaan. Deze noodzaak spruit voort uit vier belangrijke problemen:

- de bezorgdheid van consumenten en overheden over het gebruik van persoonsgegevens;
- de impact en de uitdagingen van automatisering en robotisering;
- het gevaar van onethisch gebruik van de nieuwe technologieën;
- het gevaar van toenemende ongelijkheid.

Persoonsgegevens maken zowat drie kwart uit van alle digitaal verzamelde en verwerkte data (2). Dit percentage neemt toe naargelang bedrijven er meer en meer gebruik van willen maken om hun productaanbod te personaliseren op basis van de voorkeuren en gewoontes van hun klanten, om te innoveren en om nieuwe markten te veroveren.

Het gebruik van persoonsgegevens door bedrijven is een commerciële troef, maar ook een gevaar: volgens een enquête van Accenture (2) is drie kwart van de bedrijven het erover eens dat een verantwoord, verantwoordelijk en veilig gebruik van persoonsgegevens een strategisch belangrijk thema is geworden, dat op het hoogste bestuursniveau behandeld moet worden. Twee derde van de bedrijven die deelnamen aan de enquête verklaarden een *chief data/privacy officer*[1] (ook soms *data protection officer* genaamd) of iemand in een equivalente functie aangesteld te hebben.

Dit Standpunt brengt een synthese van de recente literatuur die over verantwoord en verantwoordelijk omgaan met persoonsgegevens is gepubliceerd en toetst die met de praktijkervaring en inzichten van experts uit het onderzoeksveld en ervaringsdeskundigen uit de bedrijfswereld. Het Standpunt kwam tot stand in een reeks workshops waarin de stellingen en bevindingen uit de literatuur werden voorgelegd aan panels van deskundigen uit de onderzoekswereld en het bedrijfsleven. (Voor de samenstelling van de panels: zie pagina 46.)

Dit Standpunt is als volgt opgebouwd:

I. Technologische doorbraken bij het begin van de 21ste eeuw
II. Risico's verbonden aan deze technologisch aangestuurde ontwrichting (disruptie)

[1] In de literatuur over het onderwerp van dit Standpunt, en ook in de dagelijkse taal, worden veel Engelse vaktermen gebruikt (ICT-jargon). Waar mogelijk hanteren we in dit Standpunt een equivalente Nederlandse term, maar voor de vlotte leesbaarheid opteerden we toch ook vaak voor de algemeen ingeburgerde Engelse terminologie.

Executive summary

Responsible digitalisation: an appeal to governments and companies to which the public can and should contribute

The tremendous growth of data collecting and data processing in a digitalised world is forcing governments and companies to develop a strategy to cope with this disruption in a responsible way. Four major issues found this necessity:

- concern of consumers and governments about the use of personal data;
- impact and challenges of automation and robotization;
- risk of unethical use of new technologies;
- risk of growing inequality.

Personal data represent about 75% of all digitally collected and processed data. This percentage increases with the tendency of companies to use such data more and more for personalising their product offer based on their customers' preferences and habits, for innovation and for conquering new markets.

The use of personal data by companies is a commercial advantage, but also a risk: according to a survey of Accenture (2) three quarters of all companies agree that a responsible and safe use of personal data has become a strategically important issue that needs to be taken care of at the highest management levels. Two thirds of the companies that participated in the survey declared to have appointed a chief data/privacy officer (sometimes named data protection officer) or to have created an equivalent function.

This Position Paper contains a synthesis of recent literature about responsible personal data processing and a challenge of it based upon the experiences and insights of experts from research institutes and companies. Workshops were organised in order to confront positions and views from literature with panels of experts from research institutes and companies. (Participants in the workshops: see page 46)

The structure of this Position Paper is as follows:

I. Technological breakthroughs at the beginning of the 21st century
II. Risks linked to this technology driven disruption
III. Europe leads the pack in protection of personal data
IV. Influence of digitalisation on companies
V. Current and future (r)evolutions
VI. Coping responsibly with digitalisation
VII. Recommendations and conclusions

Voorwoord

De reeks Standpunten van de Academie is een bijdrage tot een wetenschappelijk onderbouwd debat over actuele maatschappelijke en artistieke thema's. De auteurs, leden en werkgroepen van de Academie schrijven in eigen naam, onafhankelijk en met volledige intellectuele vrijheid. De goedkeuring voor publicatie door een of meerdere Klassen van de Academie waarborgt de kwaliteit van de publicatie. Dit Standpunt werd goedgekeurd voor publicatie door de Klasse van de Technische Wetenschappen op 22 november 2018.

Een transparante en verantwoordelijke omgang met persoonsgegevens is voor heel wat bedrijven en organisaties een belangrijke prioriteit geworden. De heisa rond Cambridge Analytica heeft het thema in het voorjaar van 2018 ook onder de aandacht van het grote publiek gebracht.

Op 25 mei 2018 werd in de Europese Unie de GDPR (*General Data Protection Regulation)* van kracht, op basis van een verordening van het Europees Parlement en de Europese Raad. Zoals op andere vlakken neemt Europa ook op het vlak van de bescherming van persoonsgegevens hiermee het voortouw.

De fenomenale toename van de rekenkracht van computers maakt dat gigantische hoeveelheden data door bedrijven en instellingen verzameld en verwerkt kunnen worden. Het succes van sociale media en het internet leidt ertoe dat de gebruikers vaak veel meer waarde hechten aan de aangeboden producten en diensten dan dat zij zich zorgen maken over mogelijke inbreuken op hun *privacy*.

Artificiële intelligentie en robotica zullen ongetwijfeld ook een toenemende impact hebben op het toekomstige werkaanbod, zowel in volume als in aard. Verwacht wordt dat routinematige en repetitieve administratieve jobs nog veel meer dan nu reeds het geval is door machines overgenomen zullen worden. Daartegenover staat dat de werknemer in de toekomst meer ruimte zal krijgen voor creatief werk, wat theoretisch tot meer jobtevredenheid moet kunnen leiden (19).

In de Verenigde Staten heeft het huis van afgevaardigden CEO's van technologiebedrijven uitgenodigd voor een debat over *Corporate Digital Responsibility* (CDR). De focus lag op de volgende thema's (1):

- Antitrustwetgeving: schaden bedrijven als Google en Facebook de vrije markt? Of maakt hun dominantie hun diensten net goedkoop of zelfs gratis? Vormen onlineadvertenties en zoekmachines een inbreuk op de vrije concurrentie?
- Politieke beïnvloeding: mogen sociale media nieuws verspreiden met het oog op steun voor een politieke ideologie? President Trump laakte reeds herhaaldelijk nepnieuws van sociale media, maar de enquête van Cambridge Analytica zou net bijgedragen hebben tot zijn verkiezing.

– Niet-transparante algoritmes: ‘onfaire’ algoritmes kunnen leiden tot misbruiken, bijvoorbeeld in de gezondheidszorg, de verzekeringswereld, veiligheidsbewaking, militaire toepassingen. Moeten technologiebedrijven een inspectie van hun algoritmes toestaan? Mogen technologiebedrijven in strikte geheimhouding samenwerken met het militaire apparaat?

I. Technologische doorbraken bij het begin van de 21ste eeuw

De technologische evolutie aan het begin van het derde millennium wordt beheerst door de indrukwekkende toename van de rekencapaciteit van computers en de eraan gekoppelde digitalisering van tal van processen, in vrijwel alle sectoren van de menselijke activiteit. Het gaat om een (r)evolutie die reeds in het midden van de 20ste eeuw begon met de ontwikkeling van de eerste *mainframes*, maar die eigenlijk pas nu tot volle maturiteit aan het komen is. Precies omdat deze disruptie zo ingrijpend is in alle facetten van ons dagelijks leven, wordt George Orwells *Big Brother* uit zijn wereldberoemde cultroman *1984* heel reëel en is een verantwoorde omgang met de digitalisering van persoonsgegevens een bijzonder actueel thema geworden.

In de 20ste eeuw ging het vooral om digitale **innovatie**: het digitaliseren/automatiseren van sinds lang bestaande processen. Doelstelling was meestal een besparing op de werkingskosten door het vervangen van dure menselijke arbeid door machines.

Momenteel gaat de digitale **transformatie** een hele stap verder: het gaat om compleet nieuwe businessmodellen en nieuwe samenwerkingsverbanden, zoals *blockchain* (zie hieronder). Deze modellen zijn vaak gebaseerd op artificiële intelligentie (AI), *Internet of Things (IoT)* (Internet der Dingen), *big data*, *deep learning* en zijn vaak als disruptief (of ontwrichtend) te catalogiseren.

I.1. Big data (3)

De term *big data* verwijst naar machinaal leesbare digitale informatie die computersystemen kunnen verwerken. De informatie is direct verbonden met technieken (algoritmes) die het doorzoeken en analyseren mogelijk maken van grote hoeveelheden data van zeer verscheiden aard, die niet noodzakelijk op voorhand gesorteerd zijn.

Het verschil tussen gegevensverzameling in het verleden en *big data* nu schuilt in de drie 'V's': *volume*, *velocity* en *variety*. Soms (4) wordt hier nog een vierde 'V' aan toegevoegd: *veracity*, waarheidsgetrouwheid van de gegevens. De hoeveelheid verzamelde gegevens is exponentieel toegenomen, de verwerking ervan kan *in real time* gebeuren en de data kunnen van heel diverse aard zijn (tekst, beeld, geluid) en uit diverse bronnen afkomstig zijn (e-mails, blogs, sensoren, camerabeelden enzovoort).

I.2. Deep learning

Door de enorme toename van de rekenkracht en de opslagcapaciteit van computers kan men nu almaar grotere hoeveelheden gegevens, aangeleverd door

diverse bronnen en sensoren, verwerken met algoritmes. ('Wet van Moore': elke 24 maand een verdubbeling van het aantal transistoren in een geïntegreerde schakeling. Dit was eerder een voorspelling dan een 'wet'. Gordon Moore van computerprocessorenmaker Intel deed ze al in 1965!)

De wet van Moore in termen van 'aantal transistoren per chip' lijkt overigens op zijn laatste benen te lopen, omdat de miniaturisering van transistoren bij 3 nm op haar fysische limieten stoot. Dit wil niet zeggen dat rekenkracht en dataopslag niet verder exponentieel groeien door 3D-integratie[2] en het invoeren van nieuwe computerarchitecturen, zoals neuromorfe computerchips, die veel minder energie verbruiken en aangepast zijn aan de AI-algoritmes. Op lange termijn – meer dan tien jaar – leven er hoge verwachtingen over de zogeheten quantumcomputers.

Vroeger programmeerde men machines om aan de hand van een aantal door de programmeur bepaalde vaste stappen een specifiek vooropgesteld resultaat te bereiken. De machine kon niet autonoom haar gedrag verbeteren. Met machineleren (*machine learning)* verbetert de machine zelf haar gedrag op basis van voorbeelden of van intrinsieke elementen in de data, zoals *clusters*, om een doel dat de gebruiker kiest, zo goed mogelijk te realiseren. Voor data, zoals deze gemeten door sensoren (IoT), neemt het AI-programma op basis van dat leerproces op het juiste moment de correcte beslissingen om bijvoorbeeld een productieproces aan te sturen of een zelfrijdende auto te besturen. Deze datagebaseerde benadering heeft geleid tot een nieuwe stroomversnelling voor AI, die in de vorige decennia vooral kennisgebaseerd was: het ging om kennis van menselijke experts die in de vorm van regels in algoritmes vertaald was. (5)

Recent kwam men met *deep learning* tot een spectaculaire kwaliteitsverbetering van de performantie voor beeld-, spraak- en taalverwerking en voor veel industriële toepassingen. (3) De ontwerpers en gebruikers kunnen zelf het doel kiezen dat het lerende systeem zal nastreven. Ontwerpers en gebruikers zullen echter slechts in beperkte mate kunnen verklaren waarom hun algoritmes deze buitengewone prestaties bereiken: men spreekt van een 'zwarte doos'.

Hedendaagse toepassingen zijn bijvoorbeeld de behandeling van kredieten in financiële instellingen, het bestellingenbeheer in supermarkten (op het juiste moment de minimaal nodige hoeveelheid producten laten aanleveren), aanbiedingen op het internet, de diagnose van toestellen en patiënten enzovoort. Het belangrijkste probleem met *deep learning* is dat het bijzonder moeilijk blijkt

[2] Sequentiële 3D-integratie is een veelbelovend alternatief voor de schaalverkleining van chips. Sequentiële 3D-integratie (S3D) is een relatief nieuwe technologie die belooft bepaalde problemen van klassieke tweedimensionale chipfabricatie (2D CMOS) aan te pakken. Volgens de S3D-integratietechniek wordt een chip of systeem sequentieel in verschillende lagen 'geprocest' en verticaal geïntegreerd.

om de verklaring voor beslissingen die de algoritmes nemen in 'mensentaal' om te zetten. Krachtige oplossingen zullen moeten komen van een symbiose van menselijke kennis en vaardigheden enerzijds en AI anderzijds: in dit verband spreekt men meer en meer over IA (*intelligence amplification*) of *augmented intelligence* dan over de klassieke AI. (5)

Modellen voor *machine learning* worden per definitie getraind met statistische gegevens uit het verleden. Aangezien de wereld continu verandert zal het 'getrainde' model na verloop van tijd meer fouten beginnen maken en zullen aanpassingen noodzakelijk zijn. (6)

I.3. Blockchain (7)

De digitale munt *bitcoin* is sinds kort een bekend begrip*. Blockchain* is dat nog niet helemaal, hoewel de *bitcoin* een typisch voorbeeld is van de *blockchain*-filosofie. Deze recente digitale technologie bestaat er namelijk in bij transacties tussen twee partijen de tussenkomst van een derde, controlerende partij uit te schakelen, bijvoorbeeld van een bank of een notaris. *The Economist* noemt *blockchain* een *trust machine*. (8)

Blockchain werkt via een decentraal 'grootboek' dat alle partijen rechtstreeks beheren. Elke transactie krijgt een cryptografische handtekening (*hash*) die maakt dat elke wijziging aan de transactie onmiddellijk door alle partijen gezien wordt (de *hash* verandert).

Dit kan uiteraard heel wat kosten van tussenpersonen uitschakelen en de efficiëntie en de snelheid van transacties significant verhogen. Multinationals uit de voedingssector, zoals Nestlé en Unilever, passen *blockchain* toe om de veiligheid van hun producten te borgen, omdat dit een koppeling van de hele ketting van producent tot consument garandeert. De Antwerpse haven gebruikt *blockchain* om containeroverslag te beveiligen. De toepassingen in België hinken in vergelijking met landen als Dubaï, Duitsland en Oostenrijk globaal genomen echter nog achterop.

Een belangrijke kanttekening: het netwerk zelf en de *blockchain* die de *bitcoin* overeind houdt verbruiken heel veel elektriciteit. De website *Digiconomist* houdt bij hoeveel energie de verwerking van cryptotransacties gebruikt: voor het verifiëren van transacties in het *bitcoin*-netwerk komt dat op 30,14 terawattuur (TWh) per jaar of 30,14 miljard kilowattuur. Dat is meer dan het totale elektriciteitsverbruik van Ierland! Met dat elektriciteitsverbruik zou elke *bitcoin*-transactie omgerekend zowat 300 kWh elektriciteit gebruiken. Hierdoor is cryptogeld geen echt zuinig betaalmiddel. (36)

Een van de redenen achter al dat energieverbruik is de manier waarop de transacties worden afgehandeld. Elke transactie wordt geverifieerd en vastgezet

in een versleutelde keten, de *blockchain*. Elke gebruiker kan vervolgens een kopie van die hele keten op zijn computer zetten. Het rekenwerk achter al die encryptie en de verificatie van de transacties gebeuren door *miners*, computers die ervoor zorgen dat alles blijft draaien en die daarvoor beloond worden met nieuw geld.

I.4. Internet der Dingen

Het Internet der Dingen *(Internet of Things: IoT)*) refereert aan de situatie dat door mensen bediende computers (*desktops, laptops, tablets, smartphones*) in de minderheid zullen zijn op het internet. De meerderheid van de internetgebruikers zal in deze visie bestaan uit semi-intelligente apparaten, zogenaamde geïntegreerde systemen (*embedded systems*). Alledaagse voorwerpen worden hierdoor een entiteit op het internet, die kunnen communiceren met personen en met andere objecten, en die op grond hiervan autonome beslissingen kunnen nemen.

'Slimme' objecten spelen een sleutelrol in het Internet der Dingen: met gebruik van sensors kunnen zij hun omgeving in zich opnemen en via ingebedde netwerktechnologie kunnen ze met elkaar communiceren, internetdiensten gebruiken en met mensen interageren. In de huidige betekenis refereert de term 'Internet der Dingen' dus aan 'dingen' die zelf computers zijn en via internet hun omgeving monitoren en regelen.

De vele 'slimme' apparaten zijn feitelijk niet meer dan computers bestaande uit hard- en software. Ze kunnen kwetsbaar zijn, wat door kwaadwilligen misbruikt kan worden. Gecompromitteerde apparaten kunnen hierdoor een bedreiging vormen voor de *privacy*, bijvoorbeeld wanneer kwaadwillende lui informatie onderscheppen uit het apparaat.

Voorbeelden van toepassingen zijn zelfrijdende wagens, gezondheids-'bewaking' op afstand via *wearables* (bijvoorbeeld *smartwatches*) en de talloze camera's op openbare plaatsen.

Is big brother watching us?

In de workshops bleek de overtuiging te overheersen dat, indien het een IoT-gebruik betreft dat goed is voor de maatschappij (veiligheid op de weg, criminaliteitsbestrijding, een betere preventieve gezondheidszorg enzovoort), er ook wel een draagvlak voor zal zijn. Als het een louter persoonlijk voordeel oplevert voor individuele personen, dan kan er een probleem zijn en men mag ook niet voorbijgaan aan het risico van *hacking* van de data voor minder positieve doelen. Maar het lijkt er wel op dat het publiek 'went' aan het feit dat onze dagelijkse activiteiten meer en meer opgevolgd worden.

De perceptie is duidelijk aan het verschuiven, zoals dat ook gebeurd is met duurzaamheidsrapportage in bedrijven: aanvankelijk heerste er grote argwaan

(vrees voor gerechtelijke vervolging bijvoorbeeld bij het overschrijden van milieunormen), maar vandaag de dag erkennen ook bedrijven het grote voordeel van duurzaam ondernemen voor alle partijen.

Na het schandaal met Cambridge Analytica hebben maar zeer weinig mensen hun *Facebookaccount* opgezegd. Dataverzameling is immers niets meer dan het vergaren van alles wat nodig is om aan een probleem een geïntegreerde oplossing te geven. De data zijn slechts een *enabler*, zij maken het mogelijk om die oplossing vorm te geven, maar ze kunnen inderdaad ook misbruikt worden. Algemeen gesproken zou een meer geïnterconnecteerde maatschappij beter moeten functioneren, en dus zou digitalisering altijd een stap vooruit moeten betekenen. Waakzaamheid blijft echter geboden.

II. Risico's verbonden aan deze technologisch gestuurde ontwrichting (disruptie)

II.1. Gebrek aan transparantie van algoritmes

Algoritmes volgen de logica van wie ze bouwt: ze zetten – met een bepaald doel voor ogen – data om in informatie, maar zijn daarin niet onfeilbaar en dat kan nare gevolgen hebben. Zo kunnen bedrijven die zich baseren op onlinepersoonsgegevens om sollicitanten te beoordelen daar foute conclusies uit trekken, bijvoorbeeld omdat de software subjectieve parameters hanteert: gender, leeftijd, ras, religie, Facebookcontacten enzovoort.

Discriminatie op grond van dergelijke parameters is wettelijk verboden, maar wanneer een machine die data verwerkt is de transparantie zeer klein. De systemen beschikken over heel wat informatie over ons, maar wij kennen de systemen niet (informatie-asymmetrie) en de zelflerende systemen worden bovendien bijzonder complex, waardoor de oorspronkelijke architect ervan ook geen zuiver beeld meer heeft van hoe het systeem werkt. Dat kan ertoe leiden dat een sollicitant of een investeerder op grond van irrelevante gegevens naast een baan of lening grijpt.

In haar boek *Weapons of math destruction* (9) geeft de wiskundige Cathy O'Neil van Columbia University/Occupy Wall Street een resem voorbeelden van de gevaren van algoritmes:

- de *rating* van hypotheekleningen (gebaseerd op foute algoritmes die risicovolle leningen onvoldoende identificeerden) leidde tot de vastgoedzeepbel van 2008, die op zijn beurt de grootste financiële crisis sinds de depressie van de jaren 1930 inleidde;
- de *rating* van leerkrachten aan Amerikaanse hogescholen en universiteiten: omdat deze ratings grotendeels gebaseerd waren op de resultaten van de studenten, ontstond er een vertekening waardoor goeie leraars in scholen met een populatie met veel minderheden slechtere scores kregen en zo snel mogelijk verhuisden naar scholen met kansrijke studenten. Dit vergrootte de concentratie van minder goeie leerkrachten in 'arme' scholen in plaats van ze te verkleinen;
- de scheiding van 'fortuinlijken' en 'onfortuinlijken' op het internet (bijvoorbeeld in advertenties met algoritmes waarin financiële sterkte een groot gewicht krijgt) versterkt de bestaande segregatie;
- algoritmes die gebruikt worden in *deep learning* zijn gebaseerd op statistische data van het verleden en zijn potentieel gevaarlijker dan kennisgebaseerde algoritmes waarin menselijke expertise streeft naar continue verbetering. De datagebaseerde algoritmes bestendigen net de 'foute tendensen' van het verleden;
- mensen met een laag risicoprofiel kunnen goedkopere verzekeringen afsluiten dan mensen met een hoger risicoprofiel. Ook dit bestendigt ongelijkheid.

In de GDPR (zie par. III.1.) is een apart artikel (nr. 22) opgenomen over algoritmische besluitvorming: men spreekt over 'XAI' (*explainable artificial intelligence*), maar het is nog niet heel duidelijk hoe ver de 'uitlegbaarheid' van algoritimische besluiten strekt. Dit zal ongetwijfeld leiden tot een toename van audits van zelflerende algoritmes, iets waar organisaties zich beter op gaan voorbereiden. Een eerste stap zal zijn de data- en analyseprocessen binnen een organisatie duidelijk in kaart te brengen (*data protection impact assessment* of DPIA). (6)

Er zijn nog veel andere voorbeelden van risico's op een foute beoordeling van verwerkte persoonsgegevens. We bespreken zes voorbeelden.

Zelflerende misdaadvoorspelling (predictive policing) (10)

Door gebruik te maken van de software die seismologen gebruiken om naschokken na een aardbeving te voorspellen, ontwikkelde het Amerikaanse bedrijf PredPol programma's die voorspellen waar de kans het grootst is dat criminelen zullen toeslaan. Niet alleen de meest waarschijnlijke plaatsen worden voorspeld, maar ook de identiteit van de meest waarschijnlijke daders. Het programma maakt daarbij gebruik van de sociale media.

Het gevaar van deze software schuilt natuurlijk in de kwaliteit van de gebruikte algoritmes. Die hangt samen met de inzichten van de softwarearchitect, die vooringenomen kan zijn (fenomeen van vertekening (3)). Wijken die als 'gevaarlijk' ingekleurd worden, zullen meer politietoezicht krijgen, waardoor de bewoners zich nog meer gestigmatiseerd zullen voelen en nog minder vertrouwen in de politie zullen hebben. De algoritmes zijn bovendien zelflerend, waarbij de software louter toevallige correlaties als relevant kan interpreteren, met foute conclusies als gevolg.[3]

Wanneer in toeristische gidsen een buurt als 'onveilig' gekenmerkt wordt, zullen ook toeristen minder geneigd zijn er een hotelkamer te boeken of er te gaan dineren, waardoor de horeca er op termijn achteruitgaat of zelfs verdwijnt en de omgeving nog meer gaat verloederen.

Het spreekt vanzelf dat men het kind niet met het badwater mag weggooien. In Nederland werd bijvoorbeeld software gebruikt die gegevens van jongeren inzake spijbelgedrag en gezinsinkomen correleert met de kans dat zij gaan ontsporen. Dit stelt de overheid in staat om preventief op te treden, door die jongeren selectief te gaan begeleiden. In se is dit een legitieme en lovenswaardige doelstelling, maar het feit dat mensen niet steeds weten waarom overheden dergelijke gegevens gebruiken, zorgt voor argwaan. (10)

[3] Voorbeeld: wanneer er een reeks misdaden zou zijn gepleegd in buurten met veel treurwilgen, kan de software daaruit (ten onrechte) besluiten dat wijken met veel treurwilgen gevaarlijk zijn.

Manipulatie door zoekmachines (SEME: Search Engine Manipulation Effect)

Google kan door veranderingen in de volgorde van zoekresultaten surfers beïnvloeden in hun stem- of koopgedrag. *Search engine advertising* (3) speelt daarop in: ondernemingen betalen bedrijven die zoekmachines aanbieden om bij zoekopdrachten op een prominente plaats te staan, waardoor surfers meer kans maken om bij dat bedrijf uit te komen (32).

Bij *native advertising*, een vorm van sluikreclame, gaat het om door een bedrijf betaalde reclame die op websites van derden geplaatst wordt maar er niet als reclame uitziet. Het bedrijf gaat ervan uit dat potentiële klanten zeer waarschijnlijk die website zullen bezoeken en zich door de indirecte publiciteit tot een aankoop van haar producten of diensten zullen laten verleiden.

Tracking

First party tracking gaat over data die een bedrijf of organisatie verzamelt over bezoekers van zijn/haar website, om die vervolgens te kunnen gebruiken om gericht naar de eigen klanten te adverteren op basis van hun eerdere aankopen of van hun zoekopdrachten op de site van het bedrijf of de organisatie.

Third party tracking gaat een stap verder: bedrijven verkopen hun persoonsgegevens aan derde partijen (cf. Bisnode, zie IV.1), advertentienetwerken, *data brokers* die op allerlei sites mensen volgen en eventueel zelfs hun onlinegedrag koppelen aan offlinegedrag (aankopen in de supermarkt, financiële transacties enzovoort) of aan gegevens die ze halen uit *wearables* (*smartphones*, gps enzovoort). Zo krijgt de *data broker* een bijzonder compleet beeld van de voorkeuren, gewoontes en intenties van de gebruikers.

Datamining is het opvolgen (*tracken*) van de persoonlijke voorkeuren en gewoontes van gebruikers van het internet om daarmee gerichte campagnes te voeren voor politieke, commerciële of andere doeleinden (*social engineering*).

Mensen zijn plug-ins geworden die het systeem voeden met data. Als je niet betaalt voor een product, ben je eigenlijk niet de klant of de consument: je bent zelf een product dat verkocht wordt. (3)(11)

Gericht adverteren: informatieasymmetrie (visie van de workshops)

Gebruik van persoonsgegevens voor gerichte reclame (*targeted advertising*) zal niet onmiddellijk als misbruik gepercipieerd worden, tenzij derde partijen er toegang toe krijgen, zoals bij de casus Facebook/Cambridge Analytica. Gebruikers lijken ook liever te hebben dat een computeralgoritme hun surfgedrag volgt en hen op basis daarvan gepersonaliseerde publiciteit van bedrijven toestuurt op

hun accounts bij sociale media dan dat een mens dit zou doen. Gerichte reclame vereist echter wel een zeker gericht toezicht.

Soms bestaan er relatief ongekende relaties tussen bedrijven (bijvoorbeeld tussen Facebook en Instagram), waardoor het onduidelijk wordt of het gebruik maken van elkaars persoonsgegevens als 'delen met een derde partij' beschouwd moet worden.

Dit illustreert het begrip informatieasymmetrie: bedrijven weten veel meer over hun klanten dan de consumenten weten over het bedrijf waarvan zij producten of diensten kopen.

Segmentering in sociale media (12)(13)(14)

Facebook en Twitter passen segmentering toe: het sturen van advertenties die aansluiten bij de gevoeligheden van surfers. Samen met het filterbubbel-algoritme dat surfers met boodschappen van gelijkgestemden omringt, kan dit leiden tot polarisering inzake politieke thema's. Het *liken* ('vind ik leuk') van nepnieuws (*fake news)* of het *retweeten* ervan versterkt de geloofwaardigheid van die valse berichten en dit wordt toegepast om ideologische boodschappen te verspreiden. Vooraleer *fact checking* de foute boodschappen heeft ontmaskerd, is het nepnieuws reeds miljoenen maal gedeeld.

Het verhaal van Cambridge Analytica

In maart 2018 brachten *The Observer* en *The New York Times* het bericht naar buiten dat Cambridge Analytica de persoonsgegevens van 50 miljoen Amerikaanse Facebookgebruikers inzamelde, er een psychologische profilering op deed en op basis daarvan het campagneteam van Donald Trump in 2016 hielp om gepersonaliseerde boodschappen te sturen naar potentiële kiezers. De gegevens werden ook gebruikt voor de beïnvloeding van het referendum over de Brexit in Groot-Brittannië. Ze werden dus niet *gehackt*, maar ingezameld met de onschuldig ogende enquête '*Thisisyourdigitallife*', een soort persoonlijkheidstest opgesteld door een gereputeerde psycholoog van de universiteit van Cambridge. Wie deelnam ('slechts' zowat 300.000 mensen) gaf echter niet alleen zijn eigen gegevens mee maar ook die van al zijn Facebookvrienden. Door het multiplicatoreffect kon het campagneteam van de toekomstige president 50 miljoen mensen profileren, zowat een kwart van de kiezers. In 2015 vroeg Facebook de persoonsgegevens te wissen, maar dat gebeurde niet.

'Sociale media zijn een moeras van nepnieuws, racistische, seksistische en extremistische inhoud. Delen van het internet hebben ons een miljoen mijl verwijderd van waar we hoopten dat we zouden raken.' Dat zei Keith Weed (Unilever), *chief marketing officer* van de Brits-Nederlandse multinational Unilever,

tijdens een speech op het jaarlijkse congres van het *Interactive Advertising Bureau* (IAB) in het Californische Palm Desert. (12)

Unilever – met een advertentiebudget van 7 miljard euro de op drie na grootste adverteerder ter wereld – dreigt ermee zijn reclame weg te halen bij Google en Facebook als die geen beter werk leveren in de tegenaanval tegen de verspreiding van nepnieuws en van berichten die als enige doel hebben mensen tegen elkaar op te zetten: 'Onze merken moeten door consumenten vertrouwd kunnen worden. We mogen niets doen dat dit vertrouwen zou kunnen beschadigen – de keuze van de platforms die we gebruiken om reclame te maken inbegrepen. 2018 wordt het jaar waarin sociale media dat vertrouwen moeten terugwinnen.'

Klokkenluider Christopher Wylie, die bij Cambridge Analytica heeft gewerkt, formuleert het zo: sociale media zijn de nieuwe nutsbedrijven. Het is onmogelijk zonder stromend water of elektriciteit te leven. Het is nu ook bijna onmogelijk zonder internet, zonder sociaal platform te bestaan. Je kunt niet afstuderen als je niet googelt. Je kunt niet solliciteren zonder LinkedIn enzovoort. Je kan een functionerende democratie hebben waar op sociale media campagne gevoerd wordt, als er een regulering is. Of we moeten er genoegen mee nemen dat wij technologische vooruitgang remmen door online-ontwikkelingen te smoren, of we verkwanselen onze democratie. (13)

Eigenlijk is de reactie van Facebook op het misbruik van zijn data door Cambridge Analytica erger dan het misbruik op zich: vicepresident Andrew Bosworth van Facebook tweette dat er geen *hacking* of doorbreking van Facebooks databeveiliging in het spel was. Het *businessmodel* van Facebook bestaat uit het verzamelen, delen en verwerken van zo veel mogelijk data van Facebookgebruikers, zonder dat die gebruikers daar de toestemming voor hoeven te geven: '*This is the way Facebook works.*' (14) Je Facebookaccount wissen om je data te beveiligen is overigens ook geen oplossing, tenzij je ook alle apps verwijdert die je ooit via Facebook op je *smartphone, tablet, laptop* of PC hebt geïnstalleerd.

Het gevaar van de metadata

Bedrijven als Facebook houden naar verluidt ook de geschiedenis bij van het surfgedrag van hun gebruikers. Die delen met derden moet zeker als het overschrijden van een 'rode lijn' beschouwd worden.

Locatiegegevens kunnen een invloed hebben op de informatie die op sites gegeven wordt: zo kunnen prijzen van online aangeboden producten of diensten variëren naargelang van de locatie van de gebruiker. Surfers uit 'rijke' regio's betalen dan meer.

Apps voor routebeschrijving vragen aan hun gebruikers soms toegang tot hun fotomateriaal om de kwaliteit van de route-info te verbeteren. Als op die foto's echter mensen herkenbaar zijn, wordt de *privacy* aangetast.

Spionage

In de Verenigde Staten is het gebruik van Chinese software, bijvoorbeeld van Huawei, verboden omdat men vreest dat via die (soms niet transparante) software Amerikaanse knowhow ongezien in Chinese handen komt. Recente berichten over de mogelijke aanwezigheid van een Chinese microchip in servers die gebruikt worden door internetgiganten als Amazon en Google lijken te bevestigen dat er een reëel gevaar bestaat voor bedrijfs- of andere spionage via het internet.

Gebruik van sociale media door werknemers in bedrijven

De workshops leidden tot de volgende inzichten:

- In de meeste bedrijven is er geen verbod op het gebruik van sociale media door de werknemers. Wel zijn er beperkingen op de communicatie over het eigen bedrijf (enkel met toelating van de hiërarchie) of op het verspreiden van foto- of videomateriaal over bedrijfsprocessen.
- Ook hier moeten we een onderscheid maken tussen geanonimiseerd gebruik van persoonsgegevens en geïndividualiseerd gebruik. Vooral wanneer er commerciële belangen mee gepaard gaan is uiterste voorzichtigheid geboden.
- De sociale media zijn legaal gesproken de eigenaars van gedeelde informatie. Gebruikers zijn zich hiervan onvoldoende bewust wanneer ze zich registreren. Vooral de metadata zijn risicovol: zo kan het citeren uit artikels op het internet het auteursrecht schenden. De locatie van de gebruikers zit ook vaak ongemerkt in de metadata verscholen.
- Klassieke beperkingen zijn er uiteraard wel inzake het gebruik van internet op het werk, bijvoorbeeld voor het bezoeken van pornosites. 'Vertrouwen geven, geen politie spelen' is de stelregel.

III. Europa neemt het voortouw in de bescherming van persoonsgegevens

III.1. GDPR (AVG: Algemene Verordening Gegevensbescherming)

De *General Data Protection Regulation* is in de Europese Unie sinds 25 mei 2018 van kracht: het gaat om de uitwerking van verordening 2016/679 van het Europees Parlement en de Raad van Europa betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. De verordening moet persoonsgegevens beschermen tegen de risico's die gepaard gaan met *big data,* de *cloud* en het Internet der Dingen.

GDPR harmoniseerde de bestaande nationale wetgevingen inzake de bescherming van *privacy* en kende ook nieuwe rechten toe aan de burgers: recht op informatie, correctie en verwijdering van foute of strikt private informatie enzovoort. De verordening verzoent op die manier twee doelstellingen:

- een betere bescherming van persoonsgegevens;
- de eenmaking van de regelgeving in alle lidstaten in de digitale eengemaakte Europese markt.

Belangrijke elementen in de nieuwe verordening zijn: (15)

- gemakkelijker toegang tot de eigen persoonsgegevens;
- eisen die worden gesteld aan de toestemming voor het gebruik van de persoonsgegevens;
- de mogelijkheid tot intrekking van de toestemming voor het gebruik van de persoonsgegevens;
- informatie/transparantie over de finaliteit van het gebruik van de persoonsgegevens;
- uitlegbaarheid: een individu heeft recht op logische uitleg van iedere algoritmische besluitvorming;
- verwijdering van persoonsgegevens *(the right to be forgotten)*;
- bescherming van de persoonsgegevens ingebed in het ontwerp van de computersystemen *(privacy by design and default*: *privacy*verhogende maatregelen moeten waar mogelijk ingebouwd worden en datadiensten mogen niet meer persoonsgegevens verwerken dan noodzakelijk is) (6);
- persoonsgegevens mogen standaard niet gebruikt worden, tenzij voor de specifiek in het ontwerp van de computersystemen aangegeven doelstellingen (doelbinding);
- grenzen van de profilering: beperking van de verwerking van persoonsgegevens met als doel persoonskenmerken te evalueren;
- meldingsplicht van datalekken aan de gegevensbeschermingsautoriteit.

De aanstelling van een DPO (*data protection officer*) is verplicht in de openbare sector (behalve in rechtbanken als het gaat om de uitoefening van hun rechterlijke taken). In de privésector is de hoofdtaak van een DPO de bescherming van persoonsgegevens indien de betrokken onderneming persoonsgegevens verzamelt.

De maximale boetes voor het niet naleven van de GDPR zijn vergelijkbaar met boetes uit de mededingingswetgeving. Ze kunnen oplopen tot 4% van de mondiale omzet van een bedrijf. Dat lijkt veel, maar schandalen als dieselgate hebben aangetoond dat zonder een proportionele sanctionering verordeningen van overheden bijzonder weinig effect hebben.

We benadrukken hier nog dat de GDPR enkel slaat op persoonsgegevens (gegevens van natuurlijke personen, niet van rechtspersonen): data die via allerlei bronnen (sensoren, camera's...) in het Internet der Dingen verzameld worden, vallen niet onder de GDPR.

III.2. Andere internationale initiatieven

Naast de Europese initiatieven voor de juridische omkadering van het gebruik van persoonsgegevens zijn er ook belangrijke bewegingen in het onderzoeksveld, zoals de recente *Barcelona Declaration for Proper Development and Usage of Artificial Intelligence* van het *B-debate International Centre for Scientific Debate* en de IEEE *Principles of Ethically Aligned Design*. In de IEEE *Principles* wordt ervoor gepleit de bescherming van persoonsgegevens verplicht te integreren in het ontwerp van AI-systemen. In de Verenigde Staten zijn ook de oprichting van het *Future of Life Institute* in Boston en het AI-NOW-instituut van New York University voor het onderzoek van sociale implicaties van AI signalen dat de wetenschappelijke wereld de potentiële risico's van AI wel degelijk onderkent.

De *World Wide Web Foundation* werd in 2009 opgericht door Sir Tim Berners-Lee – samen met de Belg Robert Cailliau, de bedenker en grondlegger van het world wide web – om het internet te laten uitgroeien tot een openbaar nut en een basisrecht voor iedereen. De *Foundation* publiceerde een *Contract for the Web* (35), waarin de basisprincipes van het internet en de rol daarin van overheden, bedrijven en gebruikers heel helder geformuleerd worden:

Overheden moeten ervoor zorgen dat:

- het internet voor iedereen toegankelijk is, zodat iedereen, wie hij ook is of waar hij zich ook bevindt, actief online kan participeren;
- het internet bovendien in zijn geheel en te allen tijde steeds beschikbaar is, zodat niemand het recht op een volledige internettoegang wordt ontzegd;
- dat het fundamenteel recht op *privacy* gerespecteerd wordt, zodat elkeen vrijuit, veilig en zonder vrees het internet kan gebruiken.

Bedrijven moeten ervoor zorgen dat:

- het internet voor elkeen betaalbaar en toegankelijk is;
- **de persoonsgegevens en de *privacy* van gebruikers gerespecteerd worden**;
- technologieën ontwikkeld worden die het beste voor ogen hebben en het kwaad aan het licht brengen, zodat het internet een openbare nutsvoorziening wordt die mensen op de eerste plaats stelt.

Gebruikers moeten:

- creatief meewerken om het internet voor iedereen relevante en rijke informatie te laten aanreiken;
- beschaafd en op menselijk waardige wijze met elkaar op het internet omgaan, zodat iedereen er zich veilig en welkom voelt;
- vechten voor het behoud van het internet als een open en wereldwijde openbare informatiebron voor mensen waar ook ter wereld, nu en in de toekomst.

III.3. De GDPR oogst zowel kritiek als waardering

De GDPR wordt door bedrijven vaak als een hindernis voor digitale ontwikkelingen aanzien, zeker in vergelijking met regio's die minder streng zijn bij de bescherming van persoonsgegevens. De GDPR levert echter een unieke gelegenheid om in een eengemaakte EU-markt digitale producten en diensten te ontwikkelen die de persoonsgegevens respecteren. Dergelijke producten en diensten kunnen dan ook aantrekkelijk zijn voor landen buiten de Europese Unie die zelf ook meer zorg wensen te dragen voor persoonsgegevens.

Het Europees Parlement wil een voortrekkersrol spelen door het auteursrecht aan te passen aan de hierboven vermelde uitdagingen van het digitale tijdperk. Lobbyisten van de internetgiganten, zoals Google, Facebook e.a., kijken gespannen toe.

Er wordt nagedacht over een soort belasting op internetlinks waardoor uitgevers kunnen onderhandelen met de internetreuzen over een vergoeding voor het gebruik van hun nieuwsberichten. Het uploaden van muziek of video op websites zou streng gefilterd worden om geen boetes te riskeren: *memes* zouden de facto van het internet moeten verdwijnen. (Memetica is een samentrekking van *memory* en *mime* [imitatie]. Het gaat om gefotoshopte of anders gewijzigde foto's of video's.)

Tegen deze plannen van het Europees Parlement bestaat ook heel wat kritiek: het uitgeversrecht zou een laagdrempelige toegang tot nieuwsartikels niet in de weg mogen staan. De filters die muziek- of video-uploads zouden moeten controleren worden door velen als 'censuurmachines' beschouwd en zouden niet toegepast mogen worden bij kleine of opstartende internetbedrijven.

Het mag duidelijk zijn dat de overheden zich hierover moeten buigen, maar ook het grote publiek draagt een verantwoordelijkheid als men de integere bedrijven wil scheiden van wie het niet zo nauw neemt met persoonsgegevens.

Tim Cook, CEO van Apple, sprak tijdens een recent debat in het Europees Parlement in Brussel zijn lof over de Europese GDPR uit: '*We see vividly – painfully – how technology can harm rather than help: regulations are needed to protect user privacy.'* Enkele opmerkelijke citaten uit zijn toespraak:

- informatieasymmetrie door een 'data-industrieel complex': bedrijven die persoonsgegevens verzamelen en verwerken kennen ons beter dan wij onszelf kennen;
- criminele actoren en zelfs regeringen misbruiken het vertrouwen van de gebruiker om te polariseren, aan te stoken tot geweld en nepnieuws te verspreiden;
- AI mag geen opoffering betekenen van de menselijke creativiteit en vindingrijkheid;
- Apple stelt zich onafhankelijk op van internetreuzen als Google en Facebook, en incasseert zelf jaarlijks grote bedragen van deze giganten, bijvoorbeeld omdat zij als *default* zoekmachine op iPhones, iPads and Macs willen figureren.

IV. Impact van de digitalisering op het bedrijfsleven

IV.1. Gericht adverteren zonder inbreuk tegen de GDPR: het Bisnode-model

Bisnode (6) is gespecialiseerd in het analyseren van data. Ze doen dit in onderaanneming voor bedrijven die voor belangrijke beleidsbeslissingen professionele hulp wensen bij het interpreteren van gegevens uit hun klantenbestanden. Op die manier hopen die bedrijven dat – bijvoorbeeld – hun marketing over accuratere informatie zal beschikken. Bisnode 'verhuurt' persoonsgegevens aan adverteerders, hanteert daarbij een strenge deontologische code en respecteert de *privacy*regels. Gegevensbronnen en klanten van Bisnode blijven geheim.

Toepassingen ervaren we allemaal, bijvoorbeeld zodra we in het vooruitzicht van een aankoop van een product of dienst online gaan prospecteren wie mogelijke leveranciers kunnen zijn, of wanneer we onlineaankopen gedaan hebben bij de Amazon's of bol.com's van deze wereld: vervolgens krijgen we naderhand van diverse zijden aanbiedingen voor gelijkaardige producten (*retargeting*).

Ook hier bestaat het gevaar dat de algoritmes stereotypen gaan versterken: we krijgen wat deze sites denken dat we willen. Dit soort praktijken is dus niet neutraal en kan bij misbruik democratische principes in het gedrang brengen. Zo willen sommige Chinese steden op alle burgers een soort score kleven op basis van kredietgegevens, veroordelingen, koop- en zoekgedrag, onlineberichten enzovoort. Algoritmes kunnen dus door autoritaire regimes als instrument voor sociale controle ingezet worden en dan is Orwells *big brother* natuurlijk niet meer veraf. Bedrijven zijn soms bereid heel ver te gaan om een markt te bereiken. Denk aan de bereidheid van Facebook om gebruikersdata in China aan de overheid ter beschikking te stellen.

De overheid loopt voortdurend achterop op de technische ontwikkelingen. Wie kon in 1990 voorspellen wat in 2018 de mogelijkheden en risico's van het internet zouden zijn? Evenmin kan men nu voorspellen wat in 2025 de toepassingen van AI zullen zijn om daarvoor nu al een regelgevend kader te scheppen. De traditionele instellingen van de democratie (parlementen, verkiezingen, politieke partijen enzovoort) zijn ontstaan toen de politiek nog sneller ageerde dan de technologische evolutie. Dat dit niet langer het geval is, kan de democratie zoals we die kennen onder druk zetten; denk aan het boek *Homo Deus* van Harari (17). Daarom spelen klokkenluiders een steeds belangrijkere rol: er zullen immers steeds wel weer *free riders* zijn die zullen pogen de regels te omzeilen.

IV.2. Impact van de digitalisering op arbeid

De digitalisering heeft onmiskenbaar invloed op zowel de werkgelegenheid (het aantal jobs) als op de aard van het werk. Om de impact van de digitalisering

op arbeid te begrijpen moet men een onderscheid maken tussen manuele en cognitieve taken, en binnen deze twee groepen tussen repetitieve (routineuze) en niet-routineuze taken. De impact op de routineuze taken is al geruime tijd voelbaar: denk aan manuele taken in de maakindustrie die worden vervangen door robots en aan repetitieve administratieve taken die worden vervangen door ICT-systemen. Toch is de weerslag op de routinematige cognitieve taken nog relatief beperkt.

Beroepen zullen ook veranderingen ondergaan: zo zullen boekhouders in de toekomst wellicht meer een adviserende rol krijgen en minder tijd moeten besteden aan het verzamelen en verwerken van financiële data. (18)

Technologieondernemer en auteur Peter Hinssen (19) ziet vooral een impact op jobs van mensen die met gegevens omgaan: routinematige activiteiten zullen meer en meer door algoritmes uitgevoerd kunnen worden. Maar ook handenarbeid kan ermee geconfronteerd worden. Denk aan robotica, zoals de *bricklaying robot* die het overneemt van de klassieke metselaar, of aan toepassingen van 3D-printing in de bouw of bij het flexibel produceren van complexe producten waarvoor de manuele weg heel veel meer tijd en mankracht zou vergen.

Belangrijke toepassingen van AI zijn vooral te verwachten in de domeinen van de mobiliteit (*smart cities*), de gezondheidszorg, het onderwijs, defensie, robotica, cultuur en de bestrijding van kansarmoede. Een voorbeeld is de terbeschikkingstelling van MOOCS, computergebaseerd onderwijs, voor studenten in ontwikkelingslanden) (5).

Peter Hinssen: 'Mensen zitten vandaag te diep in de comfortzone van hun job en durven zich niet meer afvragen of wat ze doen nog wel een meerwaarde heeft. Maar zo kunnen ze misschien wel meer ruimte krijgen om na te denken over waar hun passie ligt. Nu zit hun creativiteit en meerwaarde soms vooral in wat ze na hun werkuren doen. Eerder dan een bedreiging kan dit een unieke kans zijn.' (19) De impact van AI en *blockchain* vergelijkt Hinssen met de Industriële Revolutie van het eind van de 18de eeuw en met de opkomst van het internet eind 20ste eeuw. Wat het www betekent voor de *business-to-consumer* handel zal *blockchain* betekenen voor *business-to-business* en transacties.

De echte doelstelling moet zijn om mensen met behulp van AI beter, slimmer en duurzamer te laten functioneren. Paul Daugherty, *chief technology and innovation officer* bij Accenture (20), vindt de benaming *artificial intelligence* daarom fout en verkiest *collaborative intelligence*. In het debat over de impact van AI op tewerkstelling is dit het ontbrekende middelpunt: het effectiever laten samenwerken van mens en machine zal het menselijke werk interessanter maken, wat bevorderlijk zal zijn voor de gezondheid en het welbevinden.

Naast de puur professionele vaardigheden zullen de menselijke vaardigheden (*soft skills*) aan belang winnen: een kritische geest, empathie, samenwerken met anderen, blijven leren... Dat zijn facetten die niet door een machine overgenomen kunnen worden. Ook het onderwijs zal zich aan deze ontwikkelingen moeten aanpassen: dankzij AI kan men beter rekening houden met de kennis, het niveau en het tempo van een individuele student. *Soft skills* overbrengen vraagt topleerkrachten: Vlaanderen moet er naar het voorbeeld van de Scandinavische landen voor zorgen dat het onderwijs ook in de toekomst getalenteerde jongeren blijft aantrekken. (18)

IV.3. Digital divide?

Monopolies en oligopolies zijn zeer klassiek in de IT-wereld. Denk aan de dominante positie van bedrijven als IBM bij de opkomst van de *mainframes* in de jaren 1960. Nu zijn er nieuwe giganten, zoals Facebook, Apple, Microsoft, Google, Amazon (ook afgekort als 'FAMGA').

Antitrustwetten moeten oligo- en monopolievorming onder controle houden, om een minimum aan concurrentie op de markt te behouden. Dat is voordelig voor de eindgebruikers. Overheden kunnen belastingen en heffingen als wapens inzetten om grote spelers ervan te weerhouden hun commerciële macht te misbruiken. Europa heeft dit recent gedaan door het opleggen van zware boetes aan wereldspelers zoals Apple (13 miljard euro wegens het betalen van te weinig belasting op grond van fiscale afspraken van de Apple-zetel in Ierland) en Google (4,3 miljard euro wegens het 'verplicht' installeren van Google-apps op Android *smartphones*).

Naast de ongelijkheid op bedrijfsniveau is er ook een risico op ongelijkheid op individueel menselijk niveau: digitale ongeletterdheid kan in een geavanceerde economie tot een duale samenleving leiden, waarin een deel van de bevolking structureel achterop zal hinken. Op mondiaal niveau kan hierdoor de kloof tussen de postindustriële ontwikkelde landen en de ontwikkelingslanden nog verbreden.

IV.4. Het argument van het hellend vlak (26)

Volgens Jochanan Eynikel, businessfilosoof bij ETION, zijn heel wat van de hierboven aangehaalde bezorgdheden over AI en aanverwante nieuwe technologieën gebaseerd op het argument van het hellend vlak: iets is niet goed omdat het de deur openzet voor nieuwe acties met onaanvaardbare gevolgen. De bezwaren tegen de zelfrijdende auto zijn wellicht het meest sprekende voorbeeld. Niet de (zeldzame) ongevallen die zouden kunnen gebeuren, maar het feit dat we beslissingen met zware menselijke risico's aan machines en zelflerende software zouden overlaten, veroorzaakt angst. Bij autonome technologie zoals zelfrijdende wagens is het immers niet langer de IT-specialist die elke actie van een machine

programmeert. Het is de machine die door observatie en verwerking van massale hoeveelheden data zichzelf autonoom aanstuurt. Hierdoor zijn de 'handelwijze' en het beslissingsproces van autonome technologie soms onvoorspelbaar. Dat is het (reeds eerder genoemde) 'zwarte doos-probleem'.

Eynikel keert het argument om: precies omdat machines geen morele of ethische overwegingen (moeten) (kunnen) in acht nemen om een beslissing te nemen, zal de rol van de mens in de toekomst eerder toe- dan afnemen. Rekenkracht volstaat niet voor ethische besluitvorming. Ethiek vraagt een afweging van waarden en vormen van inleving.

V. Aan de gang zijnde en toekomstige (r)evoluties

V.1. Het einde van het digitaal tijdperk in zicht?

Greg Satell, ex-topondernemer en nu auteur en veelgevraagd spreker, schreef een geruchtmakend artikel in *Harvard Business Review* (21) waarin hij stelt dat genetica, materiaalkunde en robotica de digitalisering aan het verdringen zijn als motor voor innovatie.

Daar staat tegenover dat de toepassing van digitale technologie in domeinen als de genetica en de materiaalkunde in de maakindustrie, de energiesector en de gezondheidszorg eigenlijk aan de basis liggen van alle recente ontwikkelingen in die disciplines. Satell formuleert dit als 'bits gebruiken om atomen aan te sturen'. Voorbeelden zijn:

- de atlas van kankergenomen of het materiaalgenoom-initiatief,
- de ontwikkeling van nieuwe materialen voor batterijen, die essentieel zal zijn voor een economie die draait op hernieuwbare 'schone' energie,
- supercomputers waardoor het uittesten van nieuwe materialen grootteorden sneller is geworden.

Toch maant Satell ook aan tot voorzichtigheid: over toepassingen van de genetica en AI zijn er belangrijke ethische vragen. De ontwikkeling van een quantumcomputer, een nieuw kankermedicijn of nieuwe materialen zal hierdoor trager gaan dan we gewend waren in het digitale tijdperk.

V.2. Het einde van de homo sapiens in zicht?

Historicus en (sceptisch) transhumanist[4] Yuval Noah Harari van de Hebreeuwse Universiteit Jeruzalem publiceerde in 2014 met *Sapiens* (22) een wereldwijde bestseller waarin hij een boeiende schets maakt van de evolutie van de aarde en het leven op onze planeet. In het slothoofdstuk heeft hij het over het potentieel (en de risico's) van de koppeling tussen het menselijk brein en computers.

---

[4] De aanhangers van deze filosofie noemen zich 'transhumanisten' en beweren dat de mens is beland in het post-Darwintijdperk en dat hij zijn evolutie in eigen hand kan gaan nemen. Transhumanisten onderschrijven over het algemeen de standpunten van het traditionele humanisme, maar willen dat ook tot het uiterste verkennen en zelfs overstijgen. Zij propageren dat de mens zich fysiek zal en moet *verbeteren* of, naar analogie met computers en software, *upgraden* met technieken als nanotechnologie, genetische manipulatie en de verregaande integratie van computertechniek in het menselijk lichaam. Het doel waar transhumanisten naar streven is *posthumanist* te worden.
Raymond Kurzweil is een uitgesproken voorstander van het transhumanisme: hij voorspelt dat tegen 2050 de intelligentie van computers bovenmenselijk zal zijn. Yuval Harari is een scepticus: hij toetst mogelijke toekomstbeelden aan gebeurtenissen uit het verleden (als historicus).

Vanuit een optimistische kijk kan men ervan uitgaan dat zo'n koppeling de mens van de toekomst sterker, intelligenter, beter bestand tegen ziektes, ecologisch bewuster enzovoort zal maken, en dat dit voor onze planeet misschien wel dé redding zal zijn. Alleen stoot ook Harari op het argument van het hellend vlak. Hij geeft het voorbeeld van computervirussen en antivirussoftware: zij vormen het eerste duidelijke voorbeeld van hoe zelflerende programma's niet langer controleerbaar zijn door hun oorspronkelijke ontwerpers. Antivirusalgoritmes worden zo geconcipieerd dat zij op grond van voorbije aanvallen zelf een strategie ontwikkelen om nieuwe virussen te onderscheppen: op die manier gaan zij autonoom evolueren, zonder dat daar nog een programmeur bij te pas komt. *Cyborgs*, wezens die een geïntegreerde combinatie zijn van een mens en een machine, lijken niet langer tot het domein van de sciencefiction te behoren. Nu al slaagt men erin mensen kunstmatige ('bionische') ledematen te geven die door de hersenen kunnen worden aangestuurd, net zoals de gewone biologische of organische ledematen.

Het KVAB-Standpunt over AI (5) staat heel kritisch tegenover de vrees voor de teloorgang van de menselijke intelligentie als gevolg van AI en *machine learning*. AI in de medische sector moet beschouwd worden als een hulpmiddel voor de zorgverstrekkers, waardoor zij meer kunnen focussen op empathie, ethische vraagstukken en de emotionele ondersteuning van patiënten.

Kennisgebaseerde AI berust op kennis en inzicht van menselijke experts en datagestuurde AI op menselijk gedrag. Uiteraard zal het absoluut noodzakelijk zijn dat het onderwijs hierop inspeelt: een grondige basiskennis van computerwetenschappen en wiskunde gekoppeld aan kennis van humane wetenschappen zoals logica, psychologie en taalkunde zijn meer dan ooit nodig om jongeren te laten begrijpen waarover AI precies gaat en om ze te motiveren voor het wetenschappelijk onderzoek. Zie hierover Standpunt 27 uit 2014 van de KVAB: *Informaticawetenschappen in het leerplichtonderwijs* (23).

V.3. Homo Deus? (17)

In zijn boek *Homo Deus* voorspelt Harari dat de exponentiële groei van de dataverwerkingscapaciteit van machines (en het daaruit ontwikkelen van het Internet der Dingen) een (r)evolutie zal teweegbrengen die hij vergelijkt met de opkomst van de Verlichting in de 18de eeuw. Managementgoeroe McAfee van MIT Sloan School of Management – Center for Digital Business formuleerde het als volgt (24): digitale technologieën zullen voor de capaciteit van het menselijk brein hetzelfde effect hebben als de stoommachine en aanverwante technologie voor de menselijke spierkracht tijdens de Eerste Industriële Revolutie.

De mensheid (althans een deel ervan) evolueerde van een theocentrisch naar een homocentrisch wereldbeeld. Met het Internet der Dingen zijn we volop aan

het evolueren naar een datacentrisch wereldbeeld. Dit zou wel eens onverwachte consequenties kunnen hebben, ook politiek. Klassieke democratische structuren zullen de ultrasnelle *dataflows* niet kunnen verwerken: eerbiedwaardige 'instituten' als verkiezingen, politieke partijen en parlementen zouden wel eens in onbruik kunnen raken, niet omdat ze als onethisch beschouwd worden, maar omdat ze niet efficiënt genoeg zijn in het verwerken van gegevens. Ze zijn ontstaan in een tijdperk waarin de politiek sneller ageerde dan de technologie. In de 19de en 20ste eeuw verliep de Industriële Revolutie nog zo langzaam dat politici en kiezers haar altijd een stap voor konden blijven en de loop ervan konden reguleren en manipuleren. Als gevolg van de datacentrische revolutie zullen andere structuren ontstaan, waarin de rol van de *homo sapiens sapiens* wel eens veel beperkter zou kunnen worden, als hij al niet, net als zijn voorgangers uit het Neandertal, volledig van de kaart zal worden geveegd.

Is het einde van de homo sapiens in zicht? Visie(s) in de workshops

AI: eerder praxis dan poiesis

De Griekse filosoof Aristoteles onderscheidde twee vormen om iets te doen: *poiesis* en *praxis*:

- *poiesis* betekent: 'iets verrichten' of 'produceren'. Het doel van de handeling ligt buiten de handeling. Het doel van het bakken van een taart is niet het bakproces, maar de taart die er straks zal zijn. Het gaat om een doel in de toekomst;
- praxis betekent: 'doen'. Er is geen andere doel dan de handeling zelf: de voldoening van de handeling ligt in de handeling zelf. In het geval van de taart: ook al komt die mislukt uit de oven, het maakt niets uit. Het ging om het proces van het bakken.

Robots, zoals een poetsrobot, zijn doeners waarvan een resultaat wordt verwacht. Hun waarde zit in de handeling. Creatieve *poiesis* is een zaak van het menselijk vernuft.

Vooralsnog staat de menselijke expertise ver boven AI: je kan een heel goede schaakcomputer maken, maar als er een brandalarm afgaat zal die superslimme computer rustig doorspelen, terwijl de mens, dankzij zijn capaciteit om diverse informatie te integreren, het gebouw snel zal verlaten. Maar als een computersysteem iets beter kan dan een mens (bijvoorbeeld bandwerk), zou het onverantwoord zijn hiervan geen gebruik te maken. Ook moet men de keuze behouden om dingen niet te doen die technologie zou kunnen doen, door afweging van de meerwaarde ervan, bijvoorbeeld inzake het gebruik van militaire *drones*.

Hype cycle

Verwachting en vrees worden vaak uitvergroot wanneer zich nieuwe ontwikkelingen voordoen. Volgens de Gartner-cyclus gaat men meestal eerst door een *hype*-fase (zeer hoge verwachtingen), vervolgens door een dal van ontgoocheling om tot slot naar een stijgende productiviteit te gaan wanneer het grote publiek de technologie echt begint te gebruiken en de technologie stabiel is geworden.

Zullen robots jobs vernietigen?

Men voorspelt dat zowat 20% van de huidige jobs zal verdwijnen door robotisering en digitalisering. Door *reskilling* kan dit jobverlies opgevangen worden.

#SociaalsteSchool-initiatiefneemster Katja Schipperheijn geeft harde cijfers (37): 65% van de toekomstige jobs bestaat vandaag nog niet (bron *World Economic Forum*). Dit betekent zeker niet dat er 65% van de bestaande jobs zouden verdwijnen: ze zullen er gewoon anders uitzien (*jobs shift* vooral richting *soft skills*). We moeten jongeren dan ook begeleiden om hen voldoende kansen te geven op de arbeidsmarkt en hun vaardigheden te laten aansluiten op de beschikbare jobs.

Het jobaanbod van de toekomst zal veelal inspelen op menselijke eigenschappen die een computer of robot onmogelijk kunnen nabootsen. Zo heeft de markt nood aan profielen die analytisch en kritisch kunnen denken. Mensen die beseffen dat je niet zomaar alles moet geloven wat online staat. Ook hebben we professionals nodig die nieuwe businessmodellen kunnen uitdenken op basis van de digitalisering.

Initiatieven zoals de #SociaalsteSchool zetten die beweging mee in gang. Er zijn duidelijke gedragscodes nodig om jongeren aan te leren hoe ze nu in een onlinewereld moeten leven (Katja Schipperheijn vond daarvoor het woord "netiquette" uit). Maar leerkrachten en andere groepen staan dikwijls weigerachtig tegenover veranderingen. We boeken dus vooruitgang, maar het gaat nog te traag. De reden is dat mensen te veel met de korte termijn voor ogen denken. Het onderwijs geraakt niet getransformeerd in één jaar tijd: we hebben een duurzame pedagogische visie nodig, een structurele aanpak.

Sommige analisten verwachten dat we evolueren naar een maatschappij met meer vrije tijd, en men denkt na over een basisinkomen voor iedereen, ook wie niet werkt. Mensen moeten echter voor meerwaarde blijven zorgen. En meerwaarde wordt bepaald door de klant, niet door de producent.

Er zijn heel wat technische en onderhoudstaken waarvoor robots en AI onvoldoende handig of veelzijdig zijn en het ziet er ook naar uit dat dit nog lang zo zal blijven (zie hiervoor Standpunt 46 van de KVAB: *Naar een inclusieve robotsamenleving. Robotisering, automatisering en werkgelegenheid* (25)). Wel zullen veel routinematige jobs van laag- en middengeschoolden door automatisering en robotisering onder druk komen te staan. Ook van hooggeschoolden zal veel meer flexibiliteit verwacht worden: dit zal een doorgedreven aanpassing van het klassieke carrièrepad vergen, gebaseerd op levenslang leren. Door *blockchain* komen ook administratieve functies onder druk. Overheden lopen achter op die evolutie.

VI. Verantwoord omgaan met digitalisering

VI.1. Basisprincipes van verantwoord omgaan met de digitalisering volgens Accenture (2)

Management consulting firm Accenture (*Accent on the Future*) publiceerde in 2016 een toekomstvisie over CDR (*Corporate Digital Responsibility*). Hierin worden vijf CDR-principes naar voren geschoven die bedrijven kunnen wapenen tegen een onverantwoordelijk gebruik van dataontginning (*datamining)* en die hen in staat stellen om zich van andere bedrijven te onderscheiden in duurzaamheids- en groeipotentieel.

Digitale beveiliging (stewardship)

a) doelstelling

Bedrijven die persoonsgegevens verzamelen en gebruiken moeten die veilig bewaren en op een verantwoorde en verantwoordelijke manier gebruiken. In het bijzonder het doorspelen van data van klanten of medewerkers aan derden vormt daarbij een heel gevoelig thema.

Negentig procent van de internetgebruikers beweert dat ze niet meer bij bedrijven zouden aankopen die niet op een veilige en correcte manier met hun persoonsgegevens omgaan. (2)
Wie data aanlevert gaat ervan uit dat die enkel gebruikt zullen worden voor datgene waarvoor ze nodig waren, bijvoorbeeld het betalen van een factuur.

Standaard zouden persoonsgegevens enkel met derden uitgewisseld mogen worden mits een uitdrukkelijke toestemming van wie de data heeft aangeleverd (gedeeld eigenaarschap). Wie data aanlevert zou altijd de mogelijkheid moeten krijgen al dan niet toelating te verlenen voor de aanwending ervan voor niet-oorspronkelijk bedoelde zaken (*opting-in* of *opting-out*). Dit wordt het best ook op Europees niveau legaal bekrachtigd.

Ook de gebruiker draagt een verantwoordelijkheid.

Dit Standpunt focust weliswaar op CDR, maar ook PDR (*personal data responsibility*) is belangrijk.

Bij het bezoeken van een website op het internet wordt heel vaak het akkoord van de bezoeker gevraagd met het plaatsen van *cookies* (en er zijn vergelijkbare technieken zoals pixels, webbakens enzovoort) telkens als de website bezocht wordt. Soms vraagt men ook een *privacy*verklaring van het bedrijf te lezen en voor akkoord goed te keuren. Onlineklanten van webwinkels of lezers van sites van kranten of tijdschriften vinken vaak vlug '*I agree*' of 'Akkoord' aan, omdat ze nu eenmaal geen keuze denken te hebben om het product of de dienst te verkrijgen waarnaar ze op zoek zijn.

Voor de gebruiker is het niet altijd duidelijk wat de gevolgen zijn van het al dan niet aanvinken van zo'n akkoord. De ervaring leert ook dat potentiële klanten die '*I do not agree*' aanvinken toch toegang krijgen tot de site die ze willen bezoeken. Wat er dan met hun persoonsgegevens precies gebeurt is onduidelijk.

In de workshops werd ervoor gepleit:

- dat website-eigenaars duidelijk aangeven wat er met de persoonsgegevens gebeurt als de onlinebezoeker niet akkoord gaat met *cookies* of met de privacyverklaring;
- dat website-eigenaars uitleggen wat er met de *cookies* beoogd wordt of hoe persoonsgegevens van onlinebezoekers gebruikt zullen worden als de bezoeker 'Akkoord' heeft aangevinkt;
- dat gebruikers de mogelijkheid krijgen om *cookies* te accepteren die nodig zijn voor een vlot werkende site, maar dat ze ook *cookies* voor *tracking* en vergelijkbaar gebruik kunnen weigeren;
- dat op Europees niveau wordt aangegeven wat een aanvaardbaar gebruik van persoonsgegevens kan zijn: een aanwending voor openbaar nut (*public good*) zal voor de meeste gebruikers geen probleem vormen;
- dat consumentenverenigingen toekijken op de *privacy*verklaringen van bedrijven: ze moeten helder zijn, beknopt, vrij van juridisch jargon en zo veel mogelijk gestandaardiseerd.

Zorg dragen voor persoonsgegevens en ze alleen op een verantwoorde manier gebruiken lijkt een grotere uitdaging voor consumentgerichte bedrijven dan voor B2B[5]-gerichte bedrijven. In de B2B-bedrijven is het personeelsdepartement hier uiteraard mee bezig, met het oog op het beschermen van de data van de eigen werknemers.

Voor B2B-bedrijven is de grootste uitdaging eerder het beschermen van de eigen intellectuele eigendom. Grote bedrijven worden vrijwel dagelijks *gehackt*. (Sinds het uitlekken van de praktijken van de Amerikaanse NSA weten we dat ook politici een doelwit zijn van *hacking*. Denk aan het afluisteren van het telefoonverkeer van de Duitse bondskanselier Angela Merkel.) Heel wat gegevens worden bewaard in de *cloud* en zijn dus de facto in handen van giganten als Microsoft. De GDPR komt voor de B2B-bedrijven daarom vaak over als een vorm van *window dressing* door de Europese autoriteiten; het geeft een vals gevoel van veiligheid. Het recente verhaal over de Chinese microchip in de servers van Amazon en Google is niet van aard om de angst voor bedrijfsspionage weg te nemen.

Bij consumentgerichte bedrijven liggen de kaarten iets anders: *big data* wordt door hen onder meer aangewend voor de profilering van hun klanten. Dat kan leiden

[5] B2B = *business to business* = bedrijven die producten of diensten produceren bestemd voor andere bedrijven, niet voor het brede consumentenpubliek.

tot een gedifferentieerde prijszetting, naargelang van het profiel of de locatie van de klant. Zo krijgt dit fenomeen ook een ethische dimensie, zeker wanneer het gaat om data in de persoonlijke sfeer. Denk aan gezondheidsdata die gekoppeld zouden worden aan ziekteverzekeringspremies. Deels krijgen we hierdoor een aanval op de vrije wil: via allerlei kanalen (*chatboxen* enzovoort) probeert men de consument te benaderen en hem ervan te overtuigen dat algoritmen beter weten wat goed voor hem is dan de consument zelf. Denk ook aan het begrip 'informatieasymmetrie'.

b) Technische aspecten van de digitale beveiliging van persoonsgegevens

Er bestaan heel wat technieken om gevoelige data te beschermen, meer specifiek om het onmogelijk te maken na te gaan van welke individuele persoon data afkomstig zijn. Dit is bijvoorbeeld heel belangrijk als het om medische data gaat. Tegelijk moet het perfect mogelijk blijven de data te analyseren. Men maakt daarbij een onderscheid tussen het anonimiseren en het pseudonimiseren van data (6):

- anonimiseren (*randomised response*): het wordt onmogelijk gemaakt de data aan een individu te koppelen. Dit betekent dat de data in feite geen persoonsgegevens meer bevat en dat de GDPR dus niet van toepassing is;
- pseudonimiseren: het wordt lastig gemaakt individuen te traceren, maar het is in wezen niet onmogelijk. Hier is de GDPR wel van toepassing.

Andere methodes focussen op de verwerking van de gegevens, bijvoorbeeld door AI-modellen in *machine learning*. Dit is vooral handig wanneer meerdere organisaties bij de verwerking van de data betrokken zijn; men spreekt in het vakjargon over *federated learning*. De individuele algoritmes van elke deelnemende organisatie kunnen de afkomst van de data niet traceren, maar door een slimme combinatie van de modellen krijgt men toch betrouwbare resultaten.

Het beveiligen van digitale informatie door cryptografie is niet nieuw: gegevens worden van zender naar ontvanger gestuurd in versleutelde vorm. Alleen met behulp van de geheime sleutel kunnen de data gelezen worden. Terwijl aanvankelijk de geheimhouding van de communicatie primeerde (enkel een gespecificeerde ontvanger kan de informatie lezen), moet er meer en meer voor gezorgd worden dat de data zelf niet door malafide derden gewijzigd kunnen worden (bescherming van de integriteit) en dat zender en ontvanger correct geïdentificeerd kunnen worden. (3)

Daarenboven moet men ook de metadata (*aggregated* data) beschermen, bijvoorbeeld de identiteit en locatie van zender en ontvanger, en moet men de data beschermen wanneer er berekeningen mee worden uitgevoerd. Met behulp

van homomorfische[6] cryptografische algoritmes kan men gevoelige data in versleutelde vorm in de *cloud* opladen om een dienstverlener in staat te stellen er berekeningen op uit te voeren, bijvoorbeeld in de medische sfeer, zonder dat die data ontcijferd hoeven te worden. Vervolgens kan enkel de opdrachtgever de resultaten *downloaden* en ontcijferen. (3)

Een toetsing van de effectiviteit van de anonimiseringstechnieken is belangrijk: bekende methodes zijn *k-anonymity* – combinaties van identificeerbare gegevens moeten meerdere (k) keren voorkomen – en *differential privacy* – data van een enkel individu mogen de uitkomst van een analyse niet te sterk beïnvloeden.

Men botst hierbij vaak op het spanningsveld tussen databescherming en analysekwaliteit (34): een te strikte databescherming kan algauw de kwaliteit van de analyse verlagen.

Digitale transparantie

Transparantie slaat op drie belangrijke deelgebieden:

- de klanten,
- het platform waarop de data terechtkomen,
- de applicatie die de data verwerkt.

Data die de klant zelf geeft zijn zogeheten *delivered* of aangevoerde data. Daarnaast zijn er ook *inferred* of afgeleide data en *observed* of getraceerde data (hoe beweegt de klant in het netwerk?). Vooral die laatste nemen toe door de aangroei van toestellen en software die data genereren, zoals het Internet der Dingen en de miljoenen apps. Bij getraceerde data is de transparantie het vaagst, omdat de gebruiker ze vaak niet bewust vrijgeeft maar ze wel uit zijn gedrag kunnen worden gehaald. Denk aan het bijhouden van verplaatsingen of medische data bij het gebruik van sportapps. De getraceerde data worden aangewend voor de optimalisatie van de netwerken. Hiervoor wordt gebruik gemaakt van AI.

Er moet hier een onderscheid gemaakt worden tussen het gebruik van geanonimiseerde data en van identificeerbare persoonsgegevens. Vooral bij persoonlijke gezondheidsdata moeten bedrijven aantonen hoe ze deze individuele data beschermen.

Digitale transparantie houdt in dat internetgebruikers ervoor kunnen opteren dat hun persoonsgegevens aan derden beschikbaar gesteld worden, al dan niet in ruil voor extra diensten van het bedrijf dat de data verzamelt en aan derden doorgeeft (‘geïnformeerde toestemming’). Transparantie over wat een bedrijf met

[6] Homomorfisch wil zeggen dat de data niet (door derden) ontsleuteld hoeven te worden om ze te kunnen verwerken.

de persoonsgegevens doet blijkt bovendien een commerciële troef te zijn voor die bedrijven.

In een recent gepubliceerde *whitepaper* van TNO (6) wordt doelbinding als expliciete voorwaarde naar voren geschoven om persoonsgegevens te mogen verwerken: de dataverzameling moet plaatsvinden met een specifiek, expliciet en legaal doel. Hieraan zijn twee randvoorwaarden gekoppeld: 'noodzakelijkheid' (is de dataverwerking noodzakelijk om het doel te bereiken?) en 'proportionaliteit' (zijn de data allemaal nodig om dit doel te bereiken?).

Digitale ondersteuning (empowerment)

Door klanten in staat te stellen hun persoonsgegevens zelf te beheren, bijvoorbeeld om ze bij te werken, en analytische instrumenten aan te reiken om juistere beslissingen te treffen (bijvoorbeeld inzake hun gezondheid, vorming, financiën enzovoort) stijgt de klanttevredenheid en -loyaliteit. Zo kunnen bedrijven groeien omdat hun reputatie verbetert.

Maar ook hier stoot men op paradoxen en moeilijke evenwichten. Een klassiek voorbeeld is het gebruik van *big data* in de gezondheidszorg.(27) Met *big data* kan de onderzoeker ongeziene hoeveelheden data verwerken en onvoorziene patronen ontdekken. Men maakt zich sterk dat men hierdoor de uitdagingen zal aankunnen waar chronische aandoeningen zoals hart- en vaatziekten ons voor plaatsen, net als voorlopig nog ongeneeslijke ziekten, zoals dementie en kanker. Voor zorgverleners en -verzekeraars biedt dit de mogelijkheid om de almaar toenemende kosten voor de gezondheidszorg in te dijken. Het *Electronic Health Record* (EHR) van het individu kan nieuwe inzichten bieden, zoals een beter begrip van het effect van medische interventies en de doeltreffendheid van de zorgpaden.

Beschikbaarheid, juistheid, betrouwbaarheid en veiligheid zijn essentiële voorwaarden opdat datawetenschappen in de gezondheidszorg een grote toegevoegde waarde kunnen hebben. Data moeten geanonimiseerd beschikbaar gesteld kunnen worden ten behoeve van onderzoek, op zo'n wijze dat de identiteit van de patiënt niet te achterhalen is.

Digitale wederkerigheid (equity)

Klanten worden zich meer en meer bewust van de waarde van hun persoonsgegevens en verwachten dat bedrijven die van persoonsgegevens gebruik maken ook iets teruggeven. Dataverzameling wordt een tweerichtingsverkeer op basis van een faire wisselwerking. De beloning voor het aanleveren van persoonsgegevens kan financieel zijn, maar kan ook de vorm aannemen van extra dienstverlening. Banken kunnen bijvoorbeeld in ruil leningen toestaan tegen betere voorwaarden voor de klant.

Er is ook zoiets als het *fair value*-principe: *data for money*. Dit is gerelateerd aan het reeds aangehaalde probleem van de informatieasymmetrie: de internetbedrijven weten 'alles' (of toch heel veel) over hun klanten, maar de klanten weten 'niets' (of toch weinig) over de internetbedrijven.

Digitale inclusie

Persoonsgegevens kunnen ook gebruikt worden voor maatschappelijke doelen: zo stelt Johnson & Johnson klinische testgegevens ter beschikking van Yale University voor academisch onderzoek. Klanten, onderzoekers en artsen kregen daardoor een meer positief beeld van Johnson & Johnson. De Franse telecomoperator Orange wisselt gegevens over mobiel telefoongebruik in Ivoorkust uit met een onderzoeksinstituut dat de economische ontwikkeling van het land bestudeert.

Deze vijf principes ogen mooi, maar de realiteit staat daar vaak nog ver vanaf. Net zoals ondernemingen CSR aanvankelijk louter toepasten voor risicobeheersing en niet als een instrument voor duurzame groei (28), is dit ook het geval met CDR. Ondernemingen passen CDR in de eerste plaats toe om klanten gerust te stellen over het gebruik dat ze maken van hun persoonsgegevens (het versterken van hun *license to operate*), niet als een middel voor waardecreatie.

VI.2. Datacultuur volgens McKinsey

Consultant McKinsey heeft aan de hand van een reeks diepte-interviews met CEO's een aantal kernelementen voor een goede datacultuur geformuleerd: (29)

- Dataverzameling en -analyse mogen geen doel op zichzelf zijn: ze moeten bedrijven helpen om betere beslissingen te nemen. Kijk eerst naar je bedrijfsdoelen of -problemen en ga dan pas na over welke data je zou moeten beschikken om correcte beslissingen te nemen. Zie ook het begrip 'doelbinding' in de GDPR (6).
- De betrokkenheid en het akkoord van de CEO en de raad van bestuur bij en met dataverzameling en -analyse zijn noodzakelijk: zij moeten rechtstreeks en continu in dialoog gaan met de verantwoordelijke personen voor data-initiatieven in hun organisatie.
- De toegang tot data mag niet beperkt blijven tot de top van een organisatie: stimuleer de vraag naar data bij alle medewerkers. Data moeten gedemocratiseerd worden.
- Een effectieve datacultuur moet een delicaat evenwicht vinden tussen regels (wat mag je zeker niet doen met data?) en creativiteit (hoe kan ik met mijn datacultuur mijn organisatie laten groeien?). Combineer de vrijheid van denken en de innovatiekracht van een Silicon Valley-bedrijf met de extreme veiligheidsrestricties van de luchtvaartindustrie.

– Vroeger werden dataverzameling en -analyse door ondernemingen vaak in onderaanneming uitbesteed aan gespecialiseerde databedrijven. Nu lijkt er een trend naar *insourcing* te zijn, omdat datawetenschap meer en meer als een concurrentievoordeel op prijs wordt gesteld.

VI.3. Ethische aspecten (30)

Nu AI steeds vaker wordt ingezet voor belangrijke beslissingen, bijvoorbeeld bij de aanwerving van personeel of in medische diagnoses, worden ethische overwegingen steeds belangrijker: welk soort beslissingen mag je overlaten aan AI? Wie draagt verantwoordelijkheid voor de kwaliteit van de AI-besluiten? Is AI van aard dat zij uiteindelijk de menselijke zelfbeschikking in het gedrang zal brengen?

Robuuste procedures zijn noodzakelijk om ongewenste gevolgen en oneerlijke beslissingen van AI te voorkomen. AI zou voorspelbaar en uitlegbaar moeten zijn: hiertoe werden reeds programma's ontwikkeld, zoals DARPA (*Defense Advanced Research Project Agency*), die de beslissingsprocessen van AI moeten verklaren. Deze programma's moeten echter ook de ethische impact van de AI-besluiten analyseren. De moeilijkheid hierbij is dat AI het resultaat is van de interactie van talrijke spelers: ontwikkelaars van software, gebruikers, hardware... Er is sprake van een gedeelde verantwoordelijkheid. Tot hiertoe was een ethische toetsing erop gericht de verantwoordelijkheid voor een beslissing toe te wijzen aan een individu, dat daarop afgerekend werd. In het geval van een gedeelde verantwoordelijkheid, zoals bij AI, zijn nieuwe ethische beoordelingsprogramma's nodig.

Maar er is meer: AI heeft ook een 'onzichtbare' invloed op het menselijk gedrag. AI heeft een voorspellend karakter en kan worden gebruikt om menselijke gedragingen op subtiele wijze te beïnvloeden, bijvoorbeeld met zoekmachines, gerichte advertenties... Dit hoeft uiteraard niet altijd negatief te zijn, maar inherent bestaat er een risico dat AI ongemerkt onze privékeuzes gaat beïnvloeden zonder dat we ons daarvan bewust zijn. Dit raakt opnieuw aan de menselijke zelfbeschikking. Het *IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems* (33) wil daarom het publieke debat over de waarden en principes van een ethisch gebruik van AI aanmoedigen.

Het Europees Parlement lanceerde in februari 2018 het project *AI4People* (34). Dat moet ervoor zorgen dat AI ontwikkeld en gebruikt wordt voor het welzijn van de maatschappij en van elk individu. Bij dit initiatief zijn een wetenschappelijk comité van internationale experts en een forum van belanghebbenden betrokken, in nauw overleg met de *High-Level Expert Group on AI* van de Europese Commissie.

VII. Aanbevelingen en conclusies

VII.1. Persoonsgegevens

- Doelbinding: bedrijven en organisaties die persoonsgegevens gebruiken en verwerken moeten goed toezien op de aspecten 'noodzakelijkheid' en 'proportionaliteit': zijn die persoonsgegevens absoluut nodig om een bepaald doel te bereiken? Staat het volume van de verzamelde gegevens in verhouding tot het doel?
- Persoonsgegevens doorgeven aan derden of gebruiken voor doelen die de eigenaar van de gegevens niet bekend zijn, mag uitsluitend na het expliciete akkoord van de eigenaar van de data.
- Registreer alle verwerkingsactiviteiten inzake de persoonsgegevens (GDPR art. 22: *data protection impact assessment*): 'verwerking' betekent ordenen, opslaan, bijwerken, wijzigen, doorzenden, combineren of aligneren, afschermen, wissen, vernietigen (conform EU-verordening GDPR). Onderzoek kritisch de bescherming van de data die uw instelling/bedrijf beheert: wie heeft er toegang toe?
- Analyseer de data waarover uw instelling/bedrijf beschikt: over welke soorten data gaat het: klantengegevens, personeelsdata, facturatiegegevens enzovoort? Hoe en waar worden ze bewaard? Wie heeft de data aangeleverd? Zijn de betrokkenen voldoende geïnformeerd? Zijn de databanken voldoende beveiligd, bijvoorbeeld tegen *hacking*?
- Bij gebruik van zelflerende algoritmes voor de dataverwerking is het belangrijk een maximale uitlegbaarheid van de resultaten na te streven (in de GDPR: *explainable artificial intelligence*).
- Zorg voor een procedure in geval van datalekken.
- Het *privacy*beleid van een bedrijf of organisatie moet in het arbeidsreglement worden opgenomen: het is belangrijk dat op alle niveaus in het bedrijf de restricties inzake de verzameling en verwerking van persoonsgegevens bekend zijn: alle werknemers moeten hierover een passende opleiding krijgen.
- Consumentenorganisaties zoals Test Aankoop zouden inzake onlineverkoop moeten toezien op het *privacy*beleid van een webwinkel. Het moet duidelijk zijn wat een webwinkel doet met persoonsgegevens of waartoe men *cookies* (en aanverwante technieken) aanwendt.
- Bedrijven hebben er uiteindelijk zelf belang bij persoonsgegevens te beschermen, want anders zal de overheid 'overreguleren'. Bedrijven moeten het liefst gaan inzien dat CDR ook voor henzelf goed is: net zoals dat in het verleden het geval is geweest met IKZ (integrale kwaliteitszorg) en CSR (*corporate social responsibility*), moet men gaan van een formalistische houding (meedoen omdat het 'moet') naar het 'authentieke' inzicht dat deze ontwikkelingen ook goed zijn voor het ondernemerschap.
- Zorg ervoor dat iemand in de organisatie het aanspreekpunt is voor databeheer: in de GDPR heeft men het over een 'DPO': *data protection officer*.

– Zorgvuldig omgaan met data gebeurt overigens beter *bottom-up* dan door een *top-down*-hiërarchie te creëren: het is efficiënter de uitvoerende niveaus van een organisatie goed op te leiden, zodat zij bij twijfel zelf aan hun hiërarchie de toelating vragen om persoonsgegevens te gebruiken, dan alles met loodzware procedures van bovenaf te willen beschermen. In kleinere bedrijven zal de functie van dataverantwoordelijke wellicht eerder door de CTO (*chief technical officer*) en zijn medewerkers zelf waargenomen worden dan dat hiervoor een aparte hiërarchische lijn wordt gecreëerd. In grote bedrijven zal de DPO wellicht in de ICT-sfeer actief zijn.

VII.2. Good practices binnen de bedrijven zelf

– De bedrijfscultuur inzake connectiviteit van werknemers: communiceer duidelijk over de verwachte omgang met e-mailverkeer, bijvoorbeeld over het vermijden van nutteloze *broadcasting* e-mails: 'allen beantwoorden' is zelden noodzakelijk.
– Vermijd informatieoverbelasting: probeer bij de interne informatieverspreiding een onderscheid te maken tussen wat iedereen 'moet weten' en wat 'interessant kan zijn'.
– Vermijd het gebruik van *smartphones* en *laptops* tijdens vergaderingen.
– Bescherm klokkenluiders. Die bescherming is noodzakelijk op drie niveaus:
  • maatschappij: onethische of illegale activiteiten aan het licht brengen is altijd positief. De klokkenluiders moeten goed beschermd worden om ze aan te moedigen activiteiten openbaar te maken die in conflict zijn met het maatschappelijk belang;
  • bedrijf: moet zich het liefst proactief zodanig organiseren dat klokkenluiders de mogelijkheid hebben twijfelachtige activiteiten te melden (bijvoorbeeld *hotline* voor klokkenluiders, *Messenger*, SMS enzovoort). Werknemers die zulke toestanden openbaar maken zouden nooit het risico mogen lopen ontslagen te worden of hun carrièremogelijkheden gefnuikt te zien;
  • persoonlijk: feiten gekoppeld aan individuele personen moeten discreet behandeld kunnen worden, tenzij de organisatie het gevaar zou lopen het openbaar belang te schaden.
– De aanduiding van een DPO ontslaat bedrijven uiteraard niet van hun verplichting om in meldpunten te voorzien waar medewerkers misbruiken kunnen aankaarten (vertrouwenspersoon). Vertrouwenspersonen treden vooral naar voren wanneer het gaat om gevallen van seksueel ongewenst gedrag en pestgedrag. Voor internationaal opererende bedrijven is ook fraudebestrijding een thema.

VII.3. Onderwijs

– De bedrijven en het onderwijs moeten ervoor zorgen dat Vlaanderen tot de leidende regio's gaat behoren inzake toepassingen van AI, zodat het potentiële

jobverlies door het verdwijnen van routineuze manuele en cognitieve taken gecompenseerd wordt door de creatie van banen in AI-gerelateerde toepassingen.
- Bedrijven zullen nood hebben aan specialisten die competenties op het vlak van algemene ondernemingsstrategie, cyberpsychologie, interactie tussen mens en computer en cyberantropologie in zich zullen moeten verenigen.

VII.4. Weg met het doemdenken over digitalisering!

Mensen kunnen een pessimistische of een optimistische visie hebben op nieuwe technologie. Pessimisten zien vooral de bedreigingen van de digitalisering: het verdwijnen van jobs, cyberpestgedrag, nepnieuws, teloorgang van de *privacy* enzovoort. Dit leidt tot een rigide houding: minder neiging tot experimenteren, minder openstaan voor creatieve ideeën.

Een derde optie, het 'technorealisme', gaat ervan uit dat technologie altijd ontworpen is met bepaalde bedoelingen. Of we optimistisch dan wel pessimistisch moeten zijn is dan niet van tel. Het hangt af van wat wij met die technologie willen bereiken.

Opportuniteitsdenkers grijpen de nieuwe kansen die zich aandienen en die de pessimisten laten liggen. Zo neemt e-commerce een hoge vlucht in Nederland, terwijl Vlaanderen achterop hinkt en zo banen in de *retail* verloren ziet gaan. AI is bezig een nieuwe industrie te creëren die de leiding zal nemen. Als Vlaanderen niet tot de leiders gaat behoren, dan zullen hier banen vernietigd worden en elders banen gecreëerd worden. (18)

Uiteraard raakt AI aan basisprincipes van de democratie, zoals transparantie en verantwoordelijkheid. De dataverzameling en de werking van modellen en algoritmes moeten op een begrijpelijke manier zichtbaar gemaakt worden, zeker voor toepassingen in het financiële, juridische of medische domein.

Het gebruik van *chatbots* (*chat*-robot: geautomatiseerde gesprekspartner) voor de manipulatie van de publieke opinie, bijvoorbeeld op het vlak van de politieke actualiteit, moet aan banden gelegd worden.

Technologie is moreel geladen (26): de grootste ontwrichting van de nieuwe datagebaseerde technologie is haar autonomie. De morele verantwoordelijkheid over het gebruik ervan verschuift meer en meer van de gebruiker naar de ontwerper. Er zal dus meer dan ooit morele verbeeldingskracht nodig zijn vanwege de mens die de (semi)autonome systemen ontwerpt. Machines of computers hebben nu reeds een veel hogere rekenkracht dan mensen, maar ze hebben geen enkele verbeeldingskracht of inlevingsvermogen. Ethiek overstijgt rekenkundige afwegingen, waardoor er dus meer dan ooit nood aan menselijke expertise zal zijn in het innovatieproces dat we volop aan het beleven zijn.

Hoewel machines nu al in staat zijn autonoom te functioneren, blijft de mens over een unieke combinatie van intelligentie én autonomie beschikken, die buiten het bereik van AI ligt: een computer kan geprogrammeerd worden om de sterkste menselijke schaakspelers te verslaan, maar diezelfde computer zal niet zomaar kunnen overschakelen op het spelen van het Japanse Go. Een zelfrijdende auto beslist niet over zijn bestemming, dat doen zijn menselijke gebruikers. (31)

Oren Erzioni verwijst hierbij naar het begrip *'AI savants*': gerichte (*narrow*) systemen die buitengewoon sterk zijn in één specifieke taak, maar die niet in staat zijn over te schakelen naar een andere activiteit. Hun intelligentie overstijgt in één domein de menselijke intelligentie, omdat zij gigantische hoeveelheden data kunnen verwerken dankzij door mensen geprogrammeerde algoritmes. Hun autonomie blijft vooralsnog zeer beperkt. (31)

Bronnen

(1) Martin Giles – *Four questions Silicon Valley should expect from Capitol Hill* – MITTechnology Review (4 september 2018)

(2) Tim Cooper, Jade Siu, Kuangyi Wei – *Corporate digital responsibility: Accenture Outlook* (2016)

(3) Yolande Berbers e.a.– *Privacy in tijden van internet, sociale netwerken en big data* – KVAB-Standpunt 49 (mei 2017)

(4) Andy Van Yperen, Geert Verhenne – *Big Data: opportuniteiten en uitdagingen* – ArcelorMittal Gent Magazine "1" (september 2017)

(5) Luc Steels, Bettina Berendt, Aleksandra Oizurica, Dirk Van Dyck, Joos Vandewalle e.a. – *Artificiële Intelligentie: naar een vierde industriële revolutie* – KVAB-Standpunten 53 (2018)

(6) Thymen Wabeke, Victor Klos, Tjerk Timan – *Tijd voor implementatie van verantwoorde datadiensten. De trias analytica voor 'responsible data science'* – TNO Whitepaper (september 2018)

(7) Frederic Petitjean – *Blockchain, een ketting naar de toekomst* - Fokus (Smart Media) (december 2017)

(8) Jon Berkeley – *The promise of the blockchain: the trust machine* – The Economist (oktober 2015)

(9) Cathy O'Neil – *Weapons of math destruction / Goed dat we eindelijk bang zijn van algoritmes* – Crown Publishing Group (2016) – Interview in De Standaard (maart 2018)

(10) Annelien De Greef – *De macht van big data* – De Standaard Weekblad 2017 (februari 2017)

(11) Gaea Schoeters – *Het internet als matrix* – De Standaard Weekblad 2017 (september 2017)

(12) Keith Weed – *Unilever dreigt te stoppen met adverteren op Google en Facebook* – USA Today (12 februari 2018)

(13) Christopher Wylie – *Sociale media zijn nutsbedrijven en daarom zijn regels nodig* – The Guardian/De Standaard (maart 2018)

(14) Arwa Mahdawi – *Facebook: is it time we all deleted our accounts?* – The Guardian (maart 2018)

(15) Katrien Martens – *GDPR – Lezing Legal Counsel BARCO NV* – Gent (mei 2018)

(16) BISNODE website www.bisnode.be

(17) Noah Harari Yuval – *Homo Deus: een kleine geschiedenis van de toekomst* – Thomas Rap (2017)

(18) Piet Desmet (KU Leuven) – *Zorg dat je bij de winnaars hoort* – Trends Summer University (juli 2018)

(19) Peter Hinssen – *AI maakt menselijk contact alleen maar belangrijker*- Fokus (Smart Media) (december 2017)

(20) Paul R. Daugherty, H. James Wilson – *Human + Machine: reimagining work in the age of AI* – Harvard Business Review Press (juni 2018)

(21) Greg Satell – *The industrial era ended, and so will the digital era* – Harvard Business Review (11 juli 2018)

(22) Noah Harari Yuval – *Sapiens: een kleine geschiedenis van de mensheid* – Thomas Rap (2014)

(23) Giovanni Samaey, Jacques Van Remortel e.a. – *Informaticawetenschappen in het Leerplichtonderwijs* – KVAB-Standpunt 27 (2014)

(24) Erik Brynjolfsson, Andrew McAfee – *Het tweede machinetijdperk* – Lannoo (2014)

(25) Hendrik Van Brussel, Joris De Schutter, e.a. – *Naar een inclusieve robotsamenleving. Robotisering, automatisering en werkgelegenheid* – KVAB-Standpunt 46 (2016)

(26) Jochanan Eynikel – *Robot aan het stuur* – Lannoo Campus (2017)

(27) Marc Van Hulle, Pascal Verdonck e.a. – *Datawetenschappen en gezondheidszorg* – KVAB-Standpunt 48 (maart 2017)

(28) Luc Bonte, Paul Verstraeten e.a. – *Maatschappelijk Verantwoord Ondernemen – Meedoen omdat het moet of echt engagement?* – KVAB-Standpunt 29 (november 2014)

(29) Alejandro Diaz, Kayvaun Rowshankish, Tamim Saleh – *Why data culture matters* – McKinsey Quarterly (September 2018)

(30) Mariarosaria Taddeo, Luciano Floridi – *How AI can be a force for good* – Sciencemag.org vol. 361 issue 6404 (Augustus 2018)

(31) Oren Etzioni (Allen Institute for AI) - *Artificial Intelligence and Machine Learning to Accelerate Translational Research: Proceedings of a workshop* – National Academy of Sciences/Washington (juli 2018)

(32) Tim Cook (Apple) – *Debating Ethics (Europees Parlement)* – Forbes (oktober 2018)

(33) Lloyd Greene, Jeff Pane – *IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems* – IEEE Standards Association (november 2017)

(34) *AI4People: A roadmap for Europe's first global forum on the social impacts of Artificial intelligence* – Atomium European Institute (november 2017)

(35) *Contract for the Web* – https://fortheweb.webfoundation.org/principles-1/

(36) Els Bellens – *Bitcoin verbruikt per jaar meer energie dan Ierland* – Datanews (November 2017)

(37) Katja Schipperheijn – Het onderwijs kampt vooral met een imagoprobleem: daar wil ik verandering in brengen – Bloovi.nl: Innoveren (Augustus 2017)

Samenstelling van de werkgroep

Yolande Berbers	KU Leuven, departement Computerwetenschappen – lid van KTW
Luc Bonte	KTW (covoorzitter van de werkgroep)
Hugo De Man	KU Leuven, emeritus-hoogleraar – medeoprichter IMEC
Jochanan Eynikel	ETION, businessfilosoof
Aimé Heene	UGent, ere-buitengewoon hoogleraar faculteit Economie en Bedrijfskunde
Joos Vandewalle	KU Leuven, departement ESAT-STADIUS – voorzitter KVAB
Willy Van Overschée	ASEM Europe, vicepresident – lid van KTW
Paul Verstraeten	KTW (covoorzitter van de werkgroep)

Experten workshops

De conclusies en aanbevelingen van dit Standpunt werden getoetst aan de visies en ervaringen van experts uit het bedrijfsleven, de academische wereld en onderzoeksinstituten. Daartoe werd een reeks workshops georganiseerd waarin aan een panel telkens eenzelfde reeks vragen werd voorgelegd. Met enkele experts werden Skype-interviews afgenomen. Hier volgt de lijst van de deelnemers aan de workshops:

Yolande Berbers	KU Leuven, departement Computerwetenschappen
Luc Blyaert	Technologie- en telecomjournalist, Vlaamse Vereniging van Journalisten
Luc Bonte	KVAB, lid KTW (covoorzitter werkgroep CDR)
Filip Bogaert	Ernst & Young, partner EMEIA Financial Services
Jochanan Eynikel	ETION, businessfilosoof
Aimé Heene	UGent, ere-buitengewoon hoogleraar faculteit Economie en Bedrijfskunde
Philip Hermans	Dredging International, general manager
Marius Hovens	NOKIA (OSS Assurance Lead-PM)
Tim Huygh	UAntwerpen, dept. Management Information Systems/IT governance research group
Patrick Vandenberghe	ArcelorMittal Europe, head of HR
Joos Vandewalle	KU Leuven, departement ESAT-STADIUS – voorzitter KVAB
Saskia Van Uffelen	Ericsson BeLux, CEO
Paul Verstraeten	KVAB, bestuurder KTW (covoorzitter werkgroep CDR)
Wayne Visser	Chair in Sustainable Transformation, Professor of Integrated Value / Academic Director of the Sustainable Transformation Lab (Antwerp Management School)

KTW = Klasse van de Technische Wetenschappen

RECENTE STANDPUNTEN (vanaf 2015)

36. Marnix Van Damme – *Financiële vorming*, KVAB/Klasse Menswetenschappen, 2015.

37. Els Witte – *Het debat rond de federale culturele en wetenschappelijke instellingen (2010-2015)*, KVAB/Klasse Menswetenschappen, 2015.

38. Irina Veretennicoff, Joos Vandewalle e.a. – *De STEM-leerkracht*, KVAB/Klasse Natuurwetenschappen en Klasse Technische wetenschappen, 2015.

39. Johan Martens e.a. – *De chemische weg naar een CO_2-neutrale wereld*, KVAB/Klasse Natuurwetenschappen, 2015.

40. Herman De Dijn, Irina Veretennicoff, Dominique Willems e.a. – *Het professoraat anno 2016*, KVAB/Klasse Natuurwetenschappen, Klasse Menswetenschappen, Klasse Kunsten en Klasse Technische wetenschappen, 2016.

41. Anne-Mie Van Kerckhoven, Francis Strauven – *Een bloementapijt voor Antwerpen*, KVAB/Klasse Kunsten, 2016.

42. Erik Mathijs, Willy Verstraete (e.a.), *Vlaanderen wijs met water: waterbeleid in transitie*, KVAB/Klasse Technische wetenschappen, 2016.

43. Erik Schokkaert - *De gezondheidszorg in evolutie: uitdagingen en keuzes*, KVAB/Klasse Menswetenschappen, 2016.

44. Ronnie Belmans, Pieter Vingerhoets, Ivo Van Vaerenbergh e.a. – *De eindgebruiker centraal in de energietransitie*, KVAB/Klasse Technische Wetenschappen, 2016.

45. Willem Elias, Tom De Mette – *Doctoraat in de kunsten*, KVAB/Klasse Kunsten, 2016.

46. Hendrik Van Brussel, Joris De Schutter e.a., *Naar een inclusieve robotsamenleving*, KVAB/Klasse Technische Wetenschappen, 2016.

47. Bart Verschaffel, Marc Ruyters e.a., *Elementen van een duurzaam kunstenbeleid*, KVAB/Klasse Kunsten, 2016.

48. Pascal Verdonck, Marc Van Hulle (e.a.) - *Datawetenschappen en gezondheidszorg*, KVAB/Klasse Technische wetenschappen, 2017.

49. Yolande Berbers, Mireille Hildebrandt, Joos Vandewalle (e.a.) - *Privacy in tijden van internet, sociale netwerken en big data*, KVAB/Klasse Technische wetenschappen, 2017.

50. Barbara Baert (e.a.), *Iconologie of 'La science sans nom'*, KVAB/Klasse Kunsten, 2017.

51. Tariq Modood, Frank Bovenkerk – *Multiculturalism. How can Society deal with it?* KVAB/Klasse Menswetenschappen, 2017.

52. Mark Eyskens – *Europa in de problemen.* KVAB/Klasse Menswetenschappen, 2017.

53. Luc Steels – *Artificiële intelligentie. Naar een vierde industriële revolutie?.* KVAB/Klasse Natuurwetenschappen, 2017.

54. Godelieve Gheysen, René Custers, Dominique Van Der Straeten, Dirk Inzé*, Ggo's anno 2018. Tijd voor een grondige herziening*. KVAB/Klasse Natuurwetenschappen, 2017.

55. Christoffel Waelkens (e.a.) – *Deelname van Vlaanderen aan grote internationale onderzoeksinfrastructuren: uitdagingen en aanbevelingen*, KVAB/Klasse Natuurwetenschappen, 2017.

55. Addendum. Jean-Pierre Henriet. – *Mijlpalen in internationale wetenschappelijke samenwerking*, KVAB/Klassen Natuurwetenschappen, 2017.

56. Piet Swerts, Piet Chielens, Lucien Posman – *A Symphony of Trees. Wereldcreatie naar aanleiding van de herdenking van de Derde Slag bij Ieper, 1917*, KVAB/Klasse Kunsten, 2017.

57. Willy Van Overschée e.a. – *De mobiliteit van morgen: zijn we klaar voor een paradigmawissel*?, KVAB/Klasse Technische Wetenschappen, 2018.

59. Dirk Van Dyck, Elisabeth Monard, Sylvia Wenmackers e.a. – *Onderzoeker-gedreven wetenschap. Analyse van de situatie in Vlaanderen*, KVAB/Klasse Natuurwetenschappen, 2018.

De volledige lijst met standpunten en alle pdf's kunnen worden geraadpleegd op
www.kvab.be/standpunten

Decennialang was artificiële intelligentie (AI) veeleer een academisch onderzoeksthema, maar nu lijkt AI in tal van sectoren echt door te breken. Dat dit nu gebeurt, is het gevolg van de fenomenale toename van de rekencapaciteit van computers: zelflerende algoritmes zijn in staat om massale hoeveelheden data, in uiteenlopende verschijningsvormen (beeld, tekst, geluid) en afkomstig van diverse bronnen, te verzamelen en te verwerken.

Een aanzienlijk deel van deze data zijn persoonsgegevens die de gebruikers van diverse toepassingen op het internet al dan niet bewust hebben vrijgegeven. Het recente verhaal van Cambridge Analytica heeft de potentiële risico's van deze datagebaseerde ontwikkelingen onder de aandacht van de media en het grote publiek gebracht. Op 25 mei 2018 werd in de Europese Unie de *Algemene Verordening Gegevensbescherming* van kracht, die een betere bescherming van persoonsgegevens moet waarborgen en de regelgeving in alle lidstaten op één lijn brengt.

Voor de totstandkoming van dit Standpunt werd een reeks workshops georganiseerd met experts en ervaringsdeskundigen uit het onderzoeksveld en het bedrijfsleven. Er worden aanbevelingen geformuleerd voor een verantwoordelijke omgang met persoonsgegevens door bedrijven en instellingen, maar ook de rol van de consument wordt belicht. Datagestuurde technologie is bezig productieprocessen en diensten grondig te veranderen. Het bedrijfsleven, de overheden en het onderwijs moeten ervoor zorgen dat Vlaanderen de boot van deze nieuwe Industriële Revolutie niet mist.

De reeks Standpunten van de Academie is een bijdrage tot het wetenschappelijk onderbouwd debat over actuele maatschappelijke en artistieke thema's. De auteurs, leden en werkgroepen van de Academie schrijven in eigen naam, onafhankelijk en met volledige intellectuele vrijheid. De goedkeuring voor publicatie door een of meerdere Klassen van de Academie waarborgt de kwaliteit van de gepubliceerde studies.

Vlaamse overheid

RICHTING MORGEN