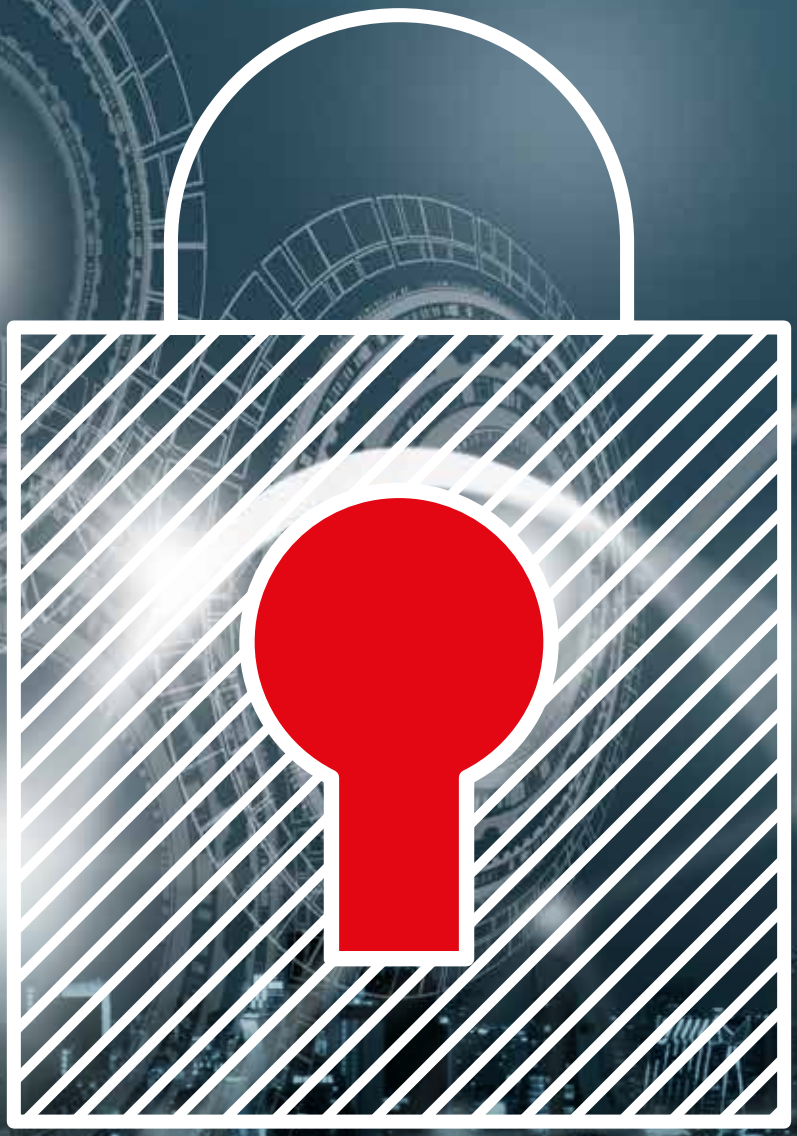
e-doc



PRIVACY
ONDER DE LOEP

onder de loep

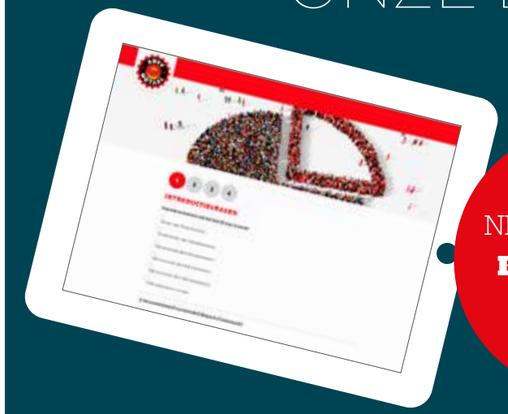
ABVV METAAL

december 2017

www.abvvmetaal.be

HOE ZIT HET OP JOUW WERK MET OPLEIDING, WERKBAAR WERK, PRIVACY ...?

DOE JE MEE AAN ONZE ENQUETES?



NEEM NU DEEL,
KLIK HIER.

Om meer inzicht te krijgen in onze congresthema's hebben wij evenwel jouw inbreng en ervaringen van op de vloer nodig. Daarom de 2 enquêtes. Met telkens vijf meerkeuzevragen en één open vraag. Het kost je hoogstens een kwartiertje om onze vragen te beantwoorden.

HARTELIJK DANK

Wil je nog meer lezen over **PRIVACY & BIG DATA**

De digitalisering heeft niet alleen een impact op de economie, maar brengt vergaande veranderingen teweeg voor alle aspecten van de samenleving.

DOWNLOAD
dan zeker onze fiches op de congressite via deze **link**.

INHOUD

6
DE OVERHEID IS WATCHING YOU

10
BELGIË IS NIET KLAAR VOOR DE NIEUWE PRIVACYWET

12
BIG DATA & PRIVACY

16
INTERNET OF THINGS

18
OP VRIJDAG 25 MEI 2018 VERANDERT DE WERELD

14
DIGITALISERING OP DE WERKVLOER

PRIVACY IS EEN COLLECTIEF RECHT

Van alle thema's die we op ons congres bespreken is 'Big Data & Privacy' het thema dat enerzijds het dichtbij ons staat en anderzijds het meest ver weg lijkt.

Dicht bij huis ...

... want 68 % van de Vlaamse huishoudens heeft minstens drie apparaten (pc/tablet/...) in huis; 3 op 4 Vlamingen (75,3 %) heeft een smartphone en 58 % van is in het bezit van een tablet.

Via al deze apparaten zijn we permanent en automatisch met het internet verbonden en wordt alles wat we doen geregistreerd. Via de gps wordt bijgehouden waar we ons bevinden en waar we gaan, via de sport-apps hoeveel stappen we zetten en hoeveel calorieën we verbruiken, via andere apps met wie we communiceren ...

Maar dat is niet alles: via zendmasten waarmee onze smartphones geconnecteerd zijn, weten ze waar we zijn, camera's in steden en op autostrades houden ons in de gaten, krediet- en bankkaarten houden onze aankopen bij, de tv waar we naar kijken houdt ons in het oog om ons dan gerichte films en series aan te bieden, de smart-tv kan meekijken en -luisteren in onze huiskamer, meer en meer van onze huis-, tuin- en keukenapparaten geraken met het internet verbonden en leggen ons reilen en zeilen vast ... Doordat we gelinkt zijn aan de vele databanken van de overheid tot de supermarkten wordt heel ons hebben en houden permanent vastgelegd. Als je het zo bekijkt, dan schrik je wel even.

Ver weg ...

... want is 'privacy' wel een syndicaal thema? Privacy op de werkvloer wel natuurlijk, maar daar hebben we (hopelijk) toch een cao voor of afspraken in het arbeidsreglement.

Digitale technologie heeft de burgers onmiskenbaar een grote vrijheid gegeven. Maar het heeft de overheid en het bedrijfsleven ook vergaande controlemogelijkheden gegeven. De bedoeling zijn steeds weer nobel: bestrijden fraude, garanderen veiligheid, betere dienstverlening, op jouw smaak afgestemde aanbiedingen ... Maar ondertussen komen door de vervagende grenzen tussen publieke, private en werkruimte de vrijheid en privacy van burgers steeds verder onder druk te staan.

Meer nog, de privacy-discussie is zelfs ontoereikend geworden om de problemen die gepaard gaan met de massale verwerking van persoonlijke data door bedrijven en door de overheid te behandelen. **De vraag is: in welke samenleving willen we leven?** Willen we dat overheden en bedrijven meer macht over ons hebben, door ons voortdurend te monitoren, te censureren en te controleren? De vraag is welke waarden we koesteren en welke waarden staan onder druk: burgerschap, solidariteit, autonomie en uiteindelijk democratie zelf. Want als we een open boek zijn dat door iedereen kan gelezen worden, dan houdt de vrijheid op. De vrije keuze om op elk moment te kunnen kiezen wie we willen zijn.

We moeten het idee loslaten om privacy te bezien als een individuele aangelegenheid: "het is allemaal toch niet erg als je niets te verbergen hebt". Integendeel we moeten de collectieve waarde van privacy opeisen. Of zoals het zo mooi gebald op een poster van Loesje stond te lezen "Ik heb niets te verbergen Maar dat hoeven ze niet te weten".

Herwig Jorissen
Voorzitter

SSSSSST...

DE OVERHEID IS WATCHING YOU

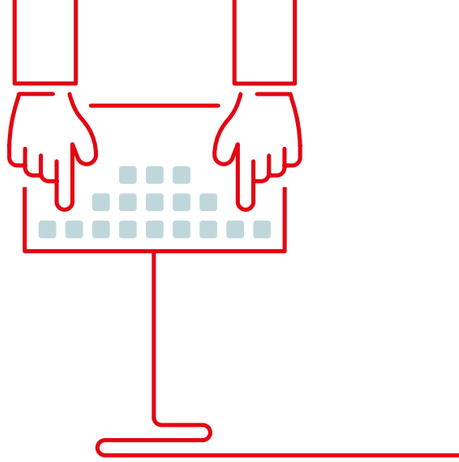
VDAB OMARMT DATAMINING

Steven Genbrugge
Adviseur Studiedienst
Vlaams ABVV

Niemand ontsnapt aan het **vangnet van Big Data**. Ons consumentengedrag wordt vastgelegd via onze e-commerce aankopen en digitale klantenkaarten, onze clicks en likes worden geregistreerd, en op basis van onze vriendenlijst, muziekvoorkeur en andere info bepaalt Facebook onze seksuele geaardheid. Op de werkvloer kan de nood aan onderhoud van de machine voorspeld worden, en worden onze prestaties en afwezigheden nauwgezet geregistreerd. We zijn ook vertrouwd met de Siri-stem die onze vragen met tal van persoonlijke suggesties beantwoordt en we schrikken er niet meer van als bol.com aangeeft dat een hippe zitbank ook wel interessant voor ons is net nadat we een forse grasmaaier kochten. Ons rechtvaardigheidsgevoel krijgt zelfs een opkikkertje als we lezen dat controlediensten Financiën data-analyse toepassen om fiscale fraude te detecteren. En in onze mailbox worden vervelende mails geweerd door hen het label spam te geven. Kortom we maken allemaal ongewild gebruik van technieken zoals datamining en dataprofiling.

Data verzamelen doen we natuurlijk al sinds mensenheugenis. Het analyseren van data is onderdeel van zowat elke wetenschap en bestaat er in om beschrijvend of diagnostisch om te gaan met bepaalde vraagstukken. Aan de hand van een salaris enquête zal men beschrijven hoeveel elke beroepscategorie verdient, en gaat men op zoek naar oorzaken en gevolgenfactoren die deze loonverschillen kunnen duiden, zoals een verhoogde vraag naar arbeidskrachten, gevaarlijk werk, hoge productiviteit.

> ***Met datamining zoeken we naar kennis, verbanden en dus eigenlijk verborgen patronen in grote databanken.***



Met **datamaning** en **profiling** gaan we echter een stapje verder. Als je weet waarom je in het verleden iets gebeurd is, kan je ook een poging doen om de toekomst te voorspellen. En dat kan bestaan uit een heel eenvoudige koppeling van gegevens. Als we weten dat 40% van de arbeiders metaal een reis gepland hebben naar Frankrijk dan kunnen we redelijk eenvoudig een voorspelling doen over het reisgedrag van deze groep in het volgend jaar. En dan kunnen we de marketing en inkoop van reizen hierop afstemmen. Een bekend voorbeeld hiervan is Amazon dat de pakjes die nog niet besteld zijn toch al op basis van deze predictive analyse opstuurt naar zijn verdeelcentra. Het voorspellen van het gedrag van mensen en ze indelen in groepen wordt als profiling benoemd. Met datamining zoeken we naar kennis, verbanden en dus eigenlijk verborgen patronen in grote databanken.

Digitalisering is al lang geen vooruitgangsgedachte meer, digitalisering is een werkelijkheid.

Ook de overheid ontdekte dat er met de gigantische stroom informatie waarover ze beschikken heel wat toepassingen binnen het bereik liggen om hun dienstverlening of opdracht te kunnen verbeteren en dit vooral binnen een context van **besparingen**. De fiscus bepaalt op basis van datamining de risicoprofielen die vatbaar zijn voor controle. Een aanpak die als vorm van efficiëntie in de behandeling van de onderzoeken in elk geval ook aangeeft dat de overheid al lang niet meer in staat is om alle belastingplichtige personen en vennootschapen te controleren. En bij gebrek aan voldoende personeel dus risico's op ongelijke en oneerlijke benadering installeert. Om te vermijden dat (dezelfde groep) bedrijven en personen steeds opnieuw de dataminingsradar kunnen ontlopen moeten voldoende menselijke factoren worden ingebouwd. Voldoende inspecteurs die hun terreinkennis kunnen inzetten aanvullend op deze digitale selecties en hen de mogelijkheid blijven bieden om open, doelgerichte controles te laten uitvoeren zijn essentieel om deze gevaren te kunnen corrigeren.

Verbeteren van kennis, manipuleren van gedrag

Maar ook in andere bevoegdheidsterreinen graaft men naarstig naar en in de dataschatten. Een van de instellingen die fel inzet op digitale processen is de Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding (VDAB), vooral door het ontwikkelen van nieuwe toepassingen die heel wat voorspellende informatie aanleveren. VDAB beschikt niet alleen over honderdduizenden digitale dossiers van werkzoekenden maar ze ontvangen jaarlijks ook tienduizenden nieuwe vacatures. VDAB zorgt voor een **automatisch vacatureaanbod** door in enkele milliseconden honderdduizenden werkzoekenden te matchen met de tienduizenden vacatures.

Daarnaast beheert de overheid in tal van andere levensdomeinen databanken die de burgers en diensten toelaten dezelfde informatie niet altijd opnieuw te moeten opgeven. Door het koppelen van deze databanken kan de VDAB ook andere parameters uit de loopbanen kruisen met hun bemiddelingsgegevens. En nog meer tot de verbeelding spreekt de registratie van het **clickgedrag** van diezelfde mensen wanneer ze gebruik maken van de tools die VDAB beschikbaar stelt. Bij het navigeren wordt het gedrag van de surfer nauwgezet bijgehouden: welke vacatures klikt men aan, hoeveel bekijkt men er op de website, hoeveel tijd besteed hij aan een kijkje nemen… Deze gigantische berg aan dossier- en arbeidsmarktinformatie vormen samen met de matchings-, navigatie- en historische gegevens, de Big Data van de VDAB. De VDAB heeft nu in samenwerking met de KU Leuven en de Vlerick Business School algoritmes ontwikkeld die een inzicht in het **zoekgedrag** van de werkzoekende genereren. Via een statistische benadering kunnen er aanbevelingen worden geformuleerd die de klant moet vooruithelpen in zijn zoektocht. Zo kunnen er vacatures worden aangereikt die in het verleden een grote matchbaarheid hadden bij soortgelijke profielen of kunnen er suggesties op maat worden voorgesteld om andere acties te ondernemen in functie van het gekozen jobdoelwit. Hetzelfde systeem van data-analyse kan ook gebruikt worden om onpopulaire vacatures bij de juiste werkzoekenden aan te bevelen. Het opent ook de mogelijkheid om de huidige onevenwichten in vacaturebereik bij te stellen. Uit interne audits blijken namelijk heel wat vacatures momenteel quasi (+ 70%) niet bekeken, en slechts een beperkt deel van

dit aanbod wordt veelvuldig aangeklikt. De data-analyse opent de deur om commerciele vacatures waar de werkgever expliciet een VDAB-tussenkomst vraagt naar werkzoekende te pushen. Al deze hulpmiddelen hebben één ding gemeen: ze voorspellen ons gedrag. Ze doen dit door data te verzamelen in **grote datasets**, deze te analyseren en vervolgens patronen en verbanden voor te stellen die een voorspellende uitspraak doen over het gedrag van de klant/gebruiker. Het opgraven van deze informatieschat heet **Datamining**, het proces om via deze algoritmes voorspellende modellen te creeren die door een voortdurende stroom aan nieuwe data gevoed en aangepast worden, omschrijft men als **Machine Learning**.

Een dam opwerpen tegen deze ontwikkelingen is niet mogelijk noch wenselijk. De vloedstroom aan data zijn belangrijke bouwstenen in de ontwikkeling van nieuwe technologieën. Maar innovaties worden geboren vanuit een rationaliteit. Het is aan de beleidsmakers om er ook een laagje moraliteit op aan te brengen. Anders kunnen het disruptieve mechanismen worden die de rechten en vrijheden van de burgers, werkzoekenden bruuskeren. Een kritische lezing is op zijn plaats om de onderhuidse gevaren van die wonderbaarlijke technologieën goed te kunnen inschatten.

Is de dataverstrekker op de hoogte?

De databergen zijn ondertussen zo immens dat het onmogelijk is deze te onderwerpen aan een menselijke controle. Het gevolg hiervan is dat we veroordeeld zijn om slaafs de correctheid van de algoritmes te volgen.

Volgens professor Max Welling, hoogleraar Machine Learning aan de Universiteit van Amsterdam is het naïef om naast de comfortopportuniteiten blind te blijven voor de gevaren van de dataficatie: privacy schendingen, misbruik van gegevens, het trekken van verkeerde conclusies, de ontmenselijking van de dienstverlening, de verdringing van arbeidsplaatsen door automatische systemen.

VDAB legt de werkzoekende conform de wet op de privacy wel voor dat de gegevens door hen worden verwerkt en dat de ze op elk moment kunnen worden bekeken en aangepast. Maar het geeft de werkzoekende geen inzicht in de wijze waarop VDAB de registraties uitvoert en op welke manier de verwerking van de gegevens verlopen. Nog minder zijn ze er zich van bewust dat het klikgedrag gecapteerd wordt in databronnen.

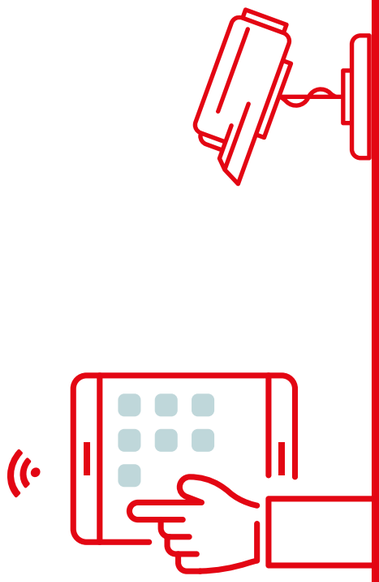
Relativiteit van de data

Om een goede datamining te kunnen uitvoeren heb je een goede grondstof nodig, wat zich digitaal vertaald in betrouwbare, correcte geordende en geregistreerde data. Nadat het basismateriaal uitgezuiverd is worden algoritmes op de databases afgevuurd om op zoek te gaan naar statistische verbanden. Het gevaar van een algoritme is dat het de indruk wekt dat het patroon een objectief gegeven is. Maar de voorspelling is in werkelijkheid afhankelijk van het invoeren van correcte data. En laat dit nou net mensenwerk zijn. Enerzijds kunnen menselijke inschattingen, misplaatste vooringenomenheid blindelings over het hoofd worden gezien wat dan uiteindelijk uitmondt in een slecht instrument. Slecht maar net omwille van zijn immense dataomvang nog moeilijk controleerbaar en herstelbaar. Voldoende mensen en middelen moeten vrijgemaakt worden om een open controle en toepassing van democratische spelregels op deze processen te kunnen blijven uitvoeren.

De grootste struikelblok in deze analyse zit in de begripsverwarring tussen 'een correlatie' en 'causaal verband'. Je kan vaststellen dat een bepaald profiel meer kans op werk heeft als hij zou solliciteren naar een job in een andere sector omdat er een correlatie is vastgesteld tussen dat profiel en een bepaalde beroepscategorie. Maar een causaal verband kunnen we er nooit aan vastknopen. Dit zou namelijk betekenen dat je het switchen naar andere job doelwitten op basis van die analyse resulteert in het bemachtigen van die job. We hoeven geen wetenschappelijke expert te zijn om te beseffen dat toeval, omstandigheden, motivationele, inhoudelijke en ook wel subjectieve elementen de cruciale rol spelen in het aanwervingsproces. De data analyse schiet te kort in het overbruggen van die subjectieve elementen maar draagt wel het gevaar in zich ten minste de suggestie op te wekken dat er een causaal verband is tussen zich heroriënteren naar andere jobs en het aangeworven worden.

Vertrouwen

Een belangrijke bedenking met een brede maatschappelijke dekking is het gevaar dat burgers, sociaal verzekerden en dus ook werkzoekenden zich afkeren van een overheid die zich steeds dieper ingraaft



> ***De digitalisering is een realiteit en het graven en exploiteren van dit nieuwe goud zal nog exponentieel toenemen.***

in onze **persoonsgebonden data**. Zo dreigt het gevaar dat de overheidsdiensten het vertrouwen verliezen, noodzakelijk om een goede klantenbinding met het doelpubliek te kunnen realiseren. Zoals de VDAB die met zijn determinerende zoekpatronen, het gevoel stimuleert dat de overheid via uitdijende dossiervorming, clicks en andere data steeds alwetender wordt en steeds minutieuzer het zoekgedrag onder de loep kan houden. Maar anderzijds krijgt die werkzoekenden het alsmaar moeilijker om de structuur, doelstellingen en informatiestromen van de VDAB te kunnen begrijpen. Die mentale twist vormt zo een voedingsbodem die het vertrouwen ondermijnt. Transparantie en duidelijke meerwaarden zullen in een communicatielijn moeten geplaatst worden om het vertrouwen van de burgers te kunnen behouden. Zoniet riskeert men processen waarbij men doelbewust dataregistratie probeert te manipuleren om te ontsnappen aan deze autonomiebeperking.

Controle

VDAB geeft aan dat de persoonlijke data van die werkzoekende in de analyse enkel als statistisch materiaal worden aangewend. Bedrijven, werknemers en werkzoekenden krijgen wel gepersonaliseerde suggesties maar zonder de bescherming van de privacy te schenden.

Maar de VDAB wil een stapje verder gaan dan enkel suggesties te lanceren die het bemiddelen faciliteert. Het zal ook een tool worden die de mate van beschikbaarheid in kaart kan brengt. En het zal een mogelijkheid bieden om moeilijke vacatures dwingender aan te bieden bij de werkzoekenden.
Als de nieuwe technologie een draagvlak verdient, zal ze er moeten voor zorgen dat niet alleen de plichten maar ook de rechten worden gevrijwaard en dat de aangereikte tools op een evenwichtige en wederkerige wijze kunnen worden ingezet voor de noden van zowel de vraag- als aanbodzijde van de arbeidsmarkt. De verleiding is dan ook groot om dergelijke digitale systemen in te zetten **ter vervanging van een menselijke tussenkomst** en dit volop in te zetten om besparingsoperaties te organiseren. We verwachten van de overheid dat de werkzoekenden kwalitatief worden opgevolgd en dat personen die niet beschikbaar zijn geresponsabiliseerd worden. Maar niet door algoritmes, wel door **motiverende gespreksvoering en empathische ondersteuning en adequate begeleiding**.
En wiens keuzevrijheid staat hier ter discussie? **Datamining versterkt de macht van het getal**. Keuzes die niet kunnen buigen op de topnoteringen via de artificiële intelligentie zullen richting exit worden geleid.

Het lijkt het ons ook redelijk dat vacaturematching niet alleen vanuit het werkzoekendenperspectief wordt bekeken maar dat ook de data-analyse losgelaten wordt op de impact van de werkgeverszijde. Zichtbare onevenwichten in het niet weerhouden van bepaalde groepen (leeftijd, geslacht, afkomst,...) verdienen evenzeer een sturend beleid met bijvoorbeeld quota.

Win-win voor iedereen

De digitalisering is een realiteit en het graven en exploiteren van dit nieuwe goud zal nog exponentieel toenemen. De overheid moet gebruik maken van de merites van deze technologieën om wins voor haar burgers te realiseren. Maar ze moet ook maatstaven ontwikkelen zodat deze platformen betrouwbaar zijn in analyse, rechtvaardig in hun output, evenredig in gebruik en transparant in hun opzet. Pas dan zal de nieuwe technologie bij de overheid een breed maatschappelijk draagvlak verdienen waar alle burgers beter van worden.

Steven Genbrugge
Adviseur Studiedienst Vlaams ABVV

BELGIË IS NIET KLAAR VOOR DE NIEUWE PRIVACYWET

Telenet experimenteert momenteel met gepersonaliseerde reclame. 1 miljoen kijkers krijgen nu al reclame te zien, aangepast aan hun kijk- en surfgedrag. De kans is groot dat ook jij onbewust je goedkeuring gaf en dus in die testgroep zit. Vlaams sp.a-parlementslid Katia Segers: "Big Data helpen ons op veel vlakken vooruit. Maar mensen zijn zich vaak niet bewust van alle gegevens die ze te grabbel gooien van bedrijven. De nieuwe Europese privacywet, de GDPR, is een belangrijke stap in de goede richting om mensen te beschermen."

Wie is Katia Segers?

- Vlaams parlementslid en deelstaatsenator voor sp.a
- Hoofddocent aan de vakgroep Communicatiewetenschappen van de VUB
- Codirecteur van het onderzoekscentrum Centre for Studies on Media and Culture
- Voorzitter van het Brussels Arts Platform van de Universitaire Associatie Brussel

Waar gaan big data en privacy precies over?
Katia Segers: "Vandaag zijn alles en iedereen met elkaar verbonden. Via onze smartphone, smartwatch en fitnesstrackers delen we waar we zijn met wie en wat we doen. Ook thuis zijn al heel wat apparaten met het internet verbonden: de televisie, koelkast, printer, verwarming en verlichting. Die registreren voortdurend ons gedrag en onze voorkeuren. De digitalisering maakt ons leven op vele vlakken makkelijker, denk aan de verkeersapps die je locatie gebruiken om je langs de files te loodsen. Maar bedrijven gebruiken die gegevens ook voor minder koosjere doelen. De targeted advertising van Telenet is dan nog redelijk onschuldig."

Hoe misbruiken bedrijven en organisaties onze gegevens?
"Het gaat bijvoorbeeld over prijsdiscriminatie. Taxidienst Uber prikt zijn tarieven per passagier. De Uber-app meet het percentage van de batterij van je smartphone. Is die bijna plat, dan zal je meer betalen. Ook als je met een iPhone een vliegreis boekt vanaf een locatie in de stad, dan tel je wellicht hogere bedragen neer dan iemand met een goedkopere smartphone op het platteland. Een ander voorbeeld: een Amerikaans bedrijf uit de medische sector aast momenteel op patiëntengegevens van Belgische ziekenhuizen om die door te verkopen aan farmabedrijven. En de privacy speelt ook een rol op de werkvloer: wat met camera's in je bedrijf of tracking via je prikkaart? De grote uitdaging is om het evenwicht te vinden tussen gemak en privacy."

Op 25 mei 2018 treedt de General Data Protection Regulation (GDPR) in werking. Gaan die regels ver genoeg om onze privacy te beschermen?
"De nieuwe privacywet is heel streng. Willen bedrijven persoonlijke gegevens bewaren, zoals je adres en aankoop- of surfgedrag, dan moet je daar voortaan uitdrukkelijk toestemming voor geven. Bedrijven moeten ook precies zeggen wat ze met je informatie gaan doen en ze mogen je gegevens alleen voor dat doel gebruiken. Doen ze dat niet, dan riskeren ze een boete tot maar liefst 4% van hun jaaromzet."

Is België klaar voor de privacywet?
"Ik vrees van niet. Grote bedrijven zijn er al een tijdje mee bezig. Maar veel kmo's, zelfstandigen en kleinere organisaties zijn nog niet in orde. Ik heb recent de Vlaamse ministers bevraagd om hen te wijzen op het belang van de privacywet, maar ze liggen er niet bepaald van wakker. Vlaams minister van Cultuur Sven Gatz gaat ervan uit dat er uitzonderingen komen voor de kunst- en cultuurorganisaties, maar dat is dus absoluut niet het geval. Niet alleen bedrijven, maar iedereen die data verzamelt, valt onder de GDPR."

"De wetgeving toepassen is één zaak, handhaving een andere. Die taak is in handen van de privacycommissie, een Belgische overheidsinstelling die toeziet op de bescherming van onze privacy bij de verwerking van persoonsgegevens. Zij zullen bijvoorbeeld ook beslissen over de boetes. Maar die commissie heeft daar op dit moment niet genoeg mankracht voor. De vraag is bovendien of de privacycommissie in haar nieuwe vorm wel voldoende slagkracht zal hebben om de strikte Europese spelregels ook echt af te dwingen. "

> **Voor mij zijn er twee cruciale aandachtspunten: mensen leren omgaan met wat er online gebeurt en meer inzetten op open data**

Hoe kunnen we onze privacy beschermen in een digitaal en geconnecteerd tijdperk?
"Voor mij zijn er twee cruciale aandachtspunten. Mediawijsheid is het eerste. Mensen moeten zich veel bewuster zijn van het digitale informatiespoor dat ze achterlaten en ze moeten weten wie hun gegevens gebruikt. We moeten op diezelfde nagel blijven kloppen, zodat we in de toekomst niet meer blind vinkjes aanklikken. Ten tweede pleit ik voor meer open data. Big data staan al te vaak alleen ten dienste van de big business: bedrijven tellen grof geld neer voor die datasets om ze voor commerciële doeleinden aan te wenden. Ik pleit voor meer open data: gegevens die conform de privacywetgeving verzameld, verwerkt en bewaard worden, en ter beschikking staan van onderzoekscentra, het middenveld en overheden. Dat betekent ook dat we meer moeten inzetten op cyberveiligheid en cryptografie, de techniek om informatie te verbergen of te beschermen, zodat open data ook geanonimiseerde data zijn."

> **Privacy speelt ook op de werkvloer: wat met camera's of tracking via je prikkaart?"**

8 BELANGRIJKE SPELREGELS VAN DE NIEUWE PRIVACYWETGEVING

1. Verzamel je als organisatie, overheid of bedrijf gegevens van mensen? Dan moet je hun expliciet toestemming vragen, duidelijk vertellen waarom je die verzamelt en waarvoor je ze gebruikt.
2. De persoonsgegevens moeten altijd juist en up-to-date zijn.
3. Gegevens aan derden doorgeven of verkopen, is verboden.
4. Je mag persoonlijke gegevens alleen voor specifieke en duidelijk omschreven doelen verzamelen.
5. Die gegevens moeten relevant zijn voor het doel van de verwerking.
6. Je mag de gegevens niet langer bewaren dan nodig is om je doel te bereiken.
7. Je moet alle persoonsgegevens beschermen tegen verlies, diefstal en hacking.
8. Datalek? Meld dat binnen de 72 uur aan de Privacycommissie en je klanten. Tenzij je kunt bewijzen dat de persoonlijke gegevens niet in gevaar zijn.

Nog niet in orde met de GDPR? De tijd dringt!
Download het stappenplan op www.privacycommission.be/nl/algemene-verordening-gegevensbescherming-0.

Big data & Privacy

We leven niet in een informatiemaatschappij, maar in een data-maatschappij. Steeds meer van wat we doen, waar we zijn, waar we geld uitgeven … wordt gezien en gemeten. We worden in de gaten gehouden (gesurveilleerd) door bedrijven en overheid. We houden ook onszelf (de stappen die we zetten, hoeveel we slapen, waar we reizen …) en elkaar in de gaten. En zo voegen we aan de data over ons en over elkaar nog data toe. Door de nieuwe technologieën kan men nu enorme hoeveelheden opslaan, verzamelen, bewaren en analyseren. En door netwerken kunnen nu vooral verschillende databestanden met elkaar gecombineerd worden.

Het verzamelen en opslaan gebeurt zowel door de overheid als door privébedrijven. Wat de overheden en bedrijven doen, is op basis van data en algoritmes ons een score geven. Om de goeden van de slechten te onderscheiden: hoe herkennen we terroristen of fraudeurs, welke klant levert winst op …? We worden gecategoriseerd en meer en meer bepalen de scores of we van rechten of diensten gebruik zullen kunnen maken: een job, een verzekering, een woning. Allemaal zijn ze op zoek naar (meer) data over ons: burgers, werknemers, klanten, consumenten …

De bedoeling is om op een rationele(re) manier beslissingen te kunnen nemen waarvan we allemaal kunnen profiteren: betere aanbiedingen, minder fraude … Het gevaar is echter dat de privacy in het gedrang komt.

Onder het mom van 'brave burgers hebben niets te verbergen', worden fundamentele rechten aangetast en wordt de waarde van publieke privacy kleiner en kleiner. Het onderscheid tussen privé en publiek verdwijnt. Wie met zijn smartphone op stap is, heeft dikwijls meer privégegevens bij de hand (foto's, adressen …) dan er in zijn huis te vinden zijn. Zowel in ons huis als in de publieke ruimte worden we constant gevolgd (door apps, door trackers op websites, door wifi-tracking, door camera's …). "Er zijn twee groepen die in de samenleving gevolgd worden. De eerste groep door een rechterlijke beslissing om een enkelband te dragen, de tweede groep zijn al de anderen." Op basis van onze digitale voetafdruk kunnen computerprogramma's je persoonlijkheid beter inschatten dan je vrienden, collega's of familie. Op basis van 70 likes doet de computer het beter dan een vriend. De grootste digitale spionnen zijn Google en Facebook. Hoe beter ze ons kennen, hoe beter ze ons kunnen verkopen. We mogen van hun diensten gebruikmaken door ons door hen te laten kennen, dat is de ongeschreven afspraak. Die kennis verkopen ze in de vorm van advertenties.

Digitale technologie geeft burgers grote vrijheid, maar geeft de overheid en het bedrijfsleven ook vergaande controlemogelijkheden. Door de vervagende grenzen tussen publieke, private en werkruimte staat de vrijheid en privacy van burgers steeds verder onder druk. We moeten het idee loslaten om privacy te bezien als een individuele aangelegenheid, we moeten daarentegen de collectieve waarde van privacy opeisen.

Bron: Wereld Economisch forum @LoriLewis @OfficiallyChadd

68%
van de Vlaamse huishoudens heeft minstens drie **apparaten** (pc/tablet/…) in huis.

9/10
Vlamingen heeft een **pc** (de meeste een **laptop**).

58%
van de Vlamingen heeft een **tablet**, iets meer dan de helft heeft een iPad. Amper 12 % heeft een mobiel abonnement om op internet te gaan.

2/3
gebuikt elke dag **e-mail**.

64% koopt **online**.

44%
gebruikt de smartphone om naar **nieuws** te zoeken.
3 op 10 leest de krant digitaal.
6 op 10 zoekt naar nieuws via zoekmachines zoals Google.

3%
heeft een **smart wearable** (sportwatch/smartwatch).

4/5
logt minstens eens per maand in op **sociale media**.

47%
gebruikt de smartphone **dagelijks** gedurende meer dan drie uur.
40 % gebruikt de tablet elke dag (27 % tussen 1 en 3 uur).

DIGITALISEREN & PRIVACY OP DE WERKVLOER

Usewils Bruno,
Engie Fabricom

Net zoals bij de meeste bedrijven doet ook bij Engie Fabricom de digitalisatie bijna geruisloos zijn intrede. Maar geruisloos is het niet gepasseerd bij de ABVV-fractie. Eerst kwam de vraag om onze voertuigen met een 'Track & Trace-geolocatiesysteem' uit te rusten, niet om onze mensen te controleren verzekerde de directie ons. Maar we wisten wel beter.

De werkgever was eigenlijk van plan om individueel met elke chauffeur van een bedrijfswagen een overeenkomst te ondertekenen. Hier konden wij natuurlijk niet mee akkoord gaan, want dit was gewoon om de syndicale afvaardiging te omzeilen en buiten spel te zetten

Wij waren van mening dat voor de introductie van elke nieuwe technologie in ons bedrijf een Cao diende afgesloten te worden. Dankzij onze volharding kwam die er dan ook. Een compromis, maar waar wel meer rechten voor de werknemers in stonden dan plichten.

De doeleinden van 'Track & Trace' waren:

- de naleving van de reglementering in verband met de CO_2-bijdrage
- het vervangen van de papieren reisboekjes;
- het facturatiesysteem aan de klanten (en aldus van de registratie van de geleverde prestaties) optimaliseren
- de dispatching en spoedoproepen vergemakkelijken
- het preventief onderhoud van de voertuigen vergemakkelijken
- opvolging van de gepresteerde uren van de betrokken werknemers ter staving voor facturatie
- bij koppeling van prestatie- en tijdsregistratiesystemen (vb. Esperanza) met Track & Trace verbinden partijen zich ertoe in overleg te treden.

> ***We zijn ten alle tijden zichtbaar voor de werkgever, ook buiten de werkuren.***

De werkgever verbond er zich toe de regelgeving met betrekking tot de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer te respecteren. Overeenkomstig de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer, is de registratie, de controle en het bijhouden van de verplaatsingsgegevens via Track-and-Trace enkel toegelaten voor zover voldaan is aan de principes van finaliteit, proportionaliteit en transparantie.

Later kwam er dan 'check-in@work' bij en wel de RSZ tegemoet te komen ter bestrijding van het zwartwerk op werven. Met dezelfde 'Track & Trace'-badges dienden al de mensen zich in te badgen op de werf zodat de aanwezigen automatisch aangemeld waren bij de RSZ op desbetreffende werf.

Nu anno 2018 wil onze Engie België al zijn werknemers de digitale weg doen inslaan.

Niet alleen om de elektronische loonbrieven verder en uitgebreider toe te passen. Want zeg nu zelf maandelijks 20.000 loonbrieven verzenden per post (en andere communicatie per post) kost nu fortuinen. Geld dat beter kan besteed worden aan nuttiger zaken. Ook tal van andere apps zouden onze werknemers positief kunnen helpen in ons complex bedrijf met al zijn werven. Bijvoorbeeld verlofaanvragen, ziektebriefjes, mails... kan hun leven vereenvoudigen.

Maar het is natuurlijk niet alleen rozengeur en maneschijn. De privacy van iedere werknemer komt in gevaar als degelijke procedures en afspraken ontbreken. Op elke smartphone of iPad staat er een gps met locatievoorziening, dus zijn we ten alle tijden zichtbaar voor de werkgever, ook buiten de uren en tijdens de weekends of verlof. Misschien loopt het allemaal niet zo'n vaart. Maar we moeten waakzaam zijn. Nu verkoopt de werkgever de digitalisering vooral als een vereenvoudiging voor de werknemers en een kostenbesparing voor hen. En het is nog goed waarschijnlijk voor het milieu ook, want geen gekapte bomen meer om onze verslagen van het Comitee, de Ondernemingsraad of Syndicale Afvaardiging meer op af te printen. Maar hoe zit dat morgen of overmorgen?

Gaan we met de directie digitaal vergaderen via onze iPad of smartphone?

We zitten natuurlijk met 1.000 vragen. Wat gaat het ons kosten of is het gratis? Is het gratis dan zijn wij waarschijnlijk het product. Wat bij diefstal? Wat bij verlies, wat en wanneer kan en wil de werkgever controleren... Hoe pak je dit nu het doeltreffendste aan voor ons bedrijf met werven en vaste werkplaatsen met +2.000 arbeiders, ook wetende dat je deze evolutie toch niet kunt tegenhouden?

Veel vragen waar we een syndicaal antwoord op moeten (en zullen) vinden.

Usewils Bruno,
Engie Fabricom

INTERNET of THINGS

The Internet of Things (IoT) verbindt machines en apparaten met elkaar. IoT kan de industrie efficiënter, productiever en veiliger maken.

Evolutie of revolutie?

De Smart Industrie doet zijn intrede in onze bedrijven en in ons leven. We staan aan de vooravond van de vierde Industriële Revolutie, waarin ondernemingen nog meer gebruik maken van informatie-, communicatie- (zoals artificiële intelligentie, nanotechnologie, machine-learning, internet of things, big data ...) **en operationele technologieën** (robotica, automatisering, 3D-printing)**. Alle toestellen worden in de toekomst (en nu ook een groot deel) met elkaar verbonden door het internet: Internet of Things.**

Dit schept opnieuw mogelijkheden voor onze industrie, zoals het aantrekken van nieuwe hoogtechnologische productie. De fabrieken zullen een digitalisering ondergaan waardoor ze kostenefficiënter, flexibeler en productiever worden.

We zetten voor jullie eens wat specifieke cijfers rond IoT op een rijtje!

IoT RISICO'S

privacy

cyber veiligheid

aansprakelijkheid

IoT VOORDELEN

IOT brengt ook vele voordelen en mogelijkheden met zich mee als bedrijven ten volle het potentieel van IOT benutten. Bedrijven zich voorbereiden op de toekomstige uitdagingen. Wij als vakbond hebben ook de taak om daar een prioriteit van te maken.

2003 - 2010
10 - 20 MILJARD
dingen zijn vandaag **verbonden met het internet**.

Om verbinding te kunnen maken, moet het object **data** kunnen **opvangen** en **doorgeven**.

Tegen 2020 zal naar schatting dit aantal stijgen naar
40 -50 MILJARD

Wat overeenkomt met
5 VERBONDEN APPARATEN
per persoon wereldwijd.

DE OPKOMST VAN SENSOREN
Sensoren maken IoT mogelijk. Elk object, zelfs het menselijk lichaam.

Alles dat moeilijk te controleren is, kan **gemakkelijk** worden.

Tegenwoordig hebben **alle apparaten**
6-9 SENSOREN

SFEER LICHT · ACCELEROMETER · MAGENTOMETER · M7 MOTION COPROCESSOR · SFEER GELUID · GYROSCOPIC · NABIJHEID · TEMPERATUUR & VOCHTIGHEID · BAROMETER

Goedkope sensoren nemen toe door de groei van IoT.

De daling van de kosten van sensoren heeft het **aantal aangesloten apparaten** doen **stijgen**.

KOSTPRIJS ACCELEROMETER

2007 - 1 AXIS
$ 7

VANDAAG - 6 AXIS
$ 0,5

EEN NIEUWE ECONOMISCHE TIJD
Het jaarlijkse wereldwijde economische potentieel van 2020 in alle sectoren wordt geschat op
14,4 BILJOEN
Dat is het huidige bbp van de Europese unie.

DEZE INDUSTRIEËN PROFITEREN MOMENTEEL VAN IoT:

AUTOMOBIEL · BANKEN · SCHEEPVAART · VASTGOED · ENERGIE · LUCHTVAART · GEZONDHEIDSZORG · FABRICAGE · VOEDSEL

Bron: AIG

OP VRIJDAG 25 MEI 2018 VERANDERT DE WERELD...

“DIE DAG WORDT DE NIEUWE EUROPESE PRIVACYWETGEVING VAN TOEPASSING. EN DAT ZOU WEL EENS TOT GROTE VERANDERINGEN KUNNEN LEIDEN.”

In gesprek met ...
Willem Debeuckelaere

Dan toch die van de privacybescherming. Die dag wordt de nieuwe Europese privacywetgeving van toepassing. En dat zou wel eens tot grote veranderingen kunnen leiden.

Vooreerst toch **even de verwachtingen bijstellen**: die nieuwe wetten zijn eigenlijk vooral het herhalen van de vroegere principes die al sinds de jaren tachtig van kracht zijn. En geleidelijk in onze wet- en regelgeving zijn opgenomen geworden, ook in ons Belgisch recht en ook in de sociale wetgeving. Er zijn belangrijke voorbeelden te vermelden: in de sociale-zekerheid is er de Kruispuntenbank voor de uitwisseling en de verwerking van de persoonsgegevens van alle Belgen en meer gekomen met de wet van 15 januari 1990: een instituut dat niet meer weg te denken is en de informationele ruggegraat vormt van de sociale zekerheid én gezondheid in ons land. Overigens een uniek systeem dat al als voorbeeld geldt voor tal van andere landen en door de Verenigde Naties werd vereremerkt.

Maar die oudere wetgeving hield geen rekening met nieuwe fenomen zoals het internet, de cloud, smartphones en sociale netwerken. In de jaren tachtig en negentig was de informatica nog iets voor grote administraties en bedrijven, de wereld van de mainframes. Sindsdien is er de pc gekomen, de netwerken, het internet en vooral een onwaarschijnlijke doorbraak van allerlei informatica naar de gewone gebruiker zoals jij en ik: bijna iedereen is tegenwoordig doende met ICT of toch minstens elektronische communicatie. En daaraan probeert die nieuwe Europese wetgeving een antwoord te bieden.

En is dat gelukt ?
Eigenlijk maar zeer ten dele. Maar om nu reeds een negatief bilan te trekken is het nog veel te vroeg. Laten we eerst zien wat het allemaal met zich zal meebrengen.

Twee testcases dringen zich wel op.
Vooreerst voorziet het artikel 88 dat de arbeids- en sociale zekerheidswetgeving nationaal blijft, Belgisch dus, maar dat deze zal moeten aangepast worden aan die nieuwe Europese regels. Moeilijk zal dat niet echt zijn : onze sociale regels zijn grosso modo in overeenstemming met die regels. Overigens hebben we nog wel ruim de tijd om her en der aanpassingen door te voeren. En dat zal nodig zijn. Eén voorbeeld: de cao 81 (Arbeidsovereenkomst nr. 81 van 26 april 2002 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische on-linecommunicatiegegevens) is op vandaag meer dan vijftien jaar oud en eigenlijk toe aan een serieuze herziening: het was toen onderhandeld zonder dat we konden rekening houden met nieuwe fenomenen zoals sociale netwerken, cloud, smartphones, de tablets en laptops, geolocalisatie, skype, big data en artificiële intelligentie. En bij die onderhandelingen in de nationale arbeidsraad zal moeten gezocht worden naar een fragiel evenwicht tussen controle en autonomie, transparantie en duidelijke informatie van de werkgever aan de werknemer en ook omgekeerd ... Het belooft een boeiende onderhandelingsronde te worden.

Een tweede toetssteen wordt zeker de doorwerking van één van de nieuwe principes van de nieuwe wetgeving: privacy by default, bij standaardzetting betekent dat **producten en diensten die worden aangeboden een goede graad van privacybescherming moeten hebben**. Je zou er dus meteen een goede privacybescherming te hebben vanaf de eerste minuut dat je het product of dienst gaat gebruiken (zonder dat je allerlei foefjes en technologie moet bovenhalen). Als je vanaf 15 mei 2018 een sociaal netwerk zoals Facebook gaat gebruiken dan zou die dienst meteen zo moeten ingericht zijn dat jouw privacy niet meer openbaar open staat (en iedereen, zowel overheid, werknemer als familie kan meekijken) maar eigenlijk afgeschermd, afgebakend is, tot de kring van medegebruikers die je kan en mag verwachten en die je kan controleren ... Zal dat zo zijn? Afwachten en alert blijven uiteraard. De wereld zal niet veranderen op 25 mei maar misschien jouw facebookaccount wel.
Tot dan.

Willem Debeuckelaere
Voorzitter Federale Privacy Commissie

Lees ook het volledige interview met **Willem De Beuckelaar** in de **M@gMetal-editie** van oktober 2017.

www.abvvmetaal.be