Ministerie van Economische Zaken

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Binnenhof 4
2513 AA 's-GRAVENHAGE

**Directoraat-generaal Energie, Telecom & Mededinging**
Directie Telecommarkt

**Bezoekadres**
Bezuidenhoutseweg 73
2594 AC Den Haag

**Postadres**
Postbus 20401
2500 EK Den Haag

**Factuuradres**
Postbus 16180
2500 BD Den Haag

**Overheidsidentificatienr**
00000001003214369000

T 070 379 8911 (algemeen)
www.rijksoverheid.nl/ez

**Ons kenmerk**
DGETM-TM / 14179608

Datum 19 november 2014
Betreft Big data en privacy

Geachte Voorzitter,

Tijdens het Algemeen Overleg op 10 september 2013 over de Kabinetsvisie op e-privacy (kamerstuk 32761 nr. 49) heb ik toegezegd om uw Kamer nader te informeren over big data en profilering. Dat doe ik met deze brief, mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties en de staatssecretaris van Veiligheid en Justitie. Deze brief vormt een aanzet tot een kabinetsvisie op de fenomenen big data en profilering in de private sector, in relatie tot het recht op privacy en het recht op gelijk behandeling. Daarnaast geeft deze brief invulling aan de toezegging tijdens het Algemeen Overleg over de herziening van de Europese regels inzake gegevensbescherming op 24 april 2014 om nader in te gaan op het gebruik van big data door financiële instellingen.

De ontwikkeling van informatie- en communicatietechnologie en het internet zorgen voor een snelgroeiende stroom aan gegevens die vaak herleidbaar zijn tot personen. Deze grote hoeveelheid gegevens, vaak aangeduid met de term big data, kan steeds beter worden geanalyseerd en gebruikt voor tal van nieuwe toepassingen. Met het groeiend gebruik van data neemt ook de bezorgdheid bij de burger toe. Deze beseft weliswaar steeds beter dat zijn gegevens worden gebruikt, maar weet vaak niet waarvoor en door wie. Om de maatschappelijke en economische potentie van big data ten volle te benutten is het belangrijk dat de gebruiker met vertrouwen gebruik maakt van het internet en de daarmee verbonden apparatuur. Een van de pijlers voor het vertrouwen is de manier waarop met de gegevens wordt omgegaan. Gebruikers willen erop kunnen vertrouwen dat hun privacy daarbij wordt gerespecteerd en dat ze op grond van hun persoonsgegevens niet worden gediscrimineerd.

Deze brief gaat nader in op het economisch en maatschappelijk potentieel van big data en profilering en beschrijft tegelijkertijd hoe de wet daarbij bescherming biedt tegen een inbreuk op de persoonlijke levenssfeer en een ongelijke behandeling. Waar de wet niet altijd aansluit op de praktijk van big data en profilering zullen, bovenop het voldoen aan de formele eisen van de wet, andere manieren moeten worden gevonden om het vertrouwen van de burger te borgen, zodat hij zijn data beschikbaar kan blijven stellen voor innovatief gebruik van big data en profilering. Deze brief verkent welke mogelijkheden daartoe bestaan. Voor de brief is gebruik gemaakt van diverse rapporten en van diverse gesprekken en workshops met vertegenwoordigers van bedrijven, consumenten en wetenschap.

**Directoraat-generaal Energie, Telecom & Mededinging**
Directie Telecommarkt

**Ons kenmerk**
DGETM-TM / 14179608

Deze brief richt zich op het gebruik van big data en profilering in de private sector. Het gebruik van big data in de publieke sector, meer in het bijzonder in het domein van de veiligheid, zal aan bod komen in een advies van de Wetenschappelijke Raad voor het Regeringsbeleid over het thema "big data, veiligheid en privacy". Dit advies is gevraagd door de minister van Veiligheid en Justitie en de minister van Binnenlandse Zaken en Koninkrijksrelaties, en wordt medio 2015 verwacht.

**Kenmerken big data en profilering**

Big data kent vele definities, zo bleek ook uit gesprekken met belanghebbenden. Vaak worden er gegevensverzamelingen mee aangeduid die zo groot, complex en divers zijn dat ze niet in reguliere databasesystemen en met traditionele analysehulpmiddelen verwerkt en geanalyseerd kunnen worden. Verwerking is enkel mogelijk met dynamische systemen die over een grote rekenkracht en snelheid beschikken. De bigdata-waardeketen kan worden onderverdeeld in drie stadia, namelijk het verzamelen van data, het analyseren van data en het toepassen van data. Het verzamelen van data kan plaatsvinden door verstrekking door de betrokkene, door observatie of door gebruik van eerdere analyses. Het analyseren van data kan vele vormen aannemen. Het systematisch en automatisch zoeken naar verbanden in gegevensverzamelingen zonder hypothese vooraf (*data mining*) wordt daarbij steeds belangrijker. Bij het toepassen van data worden voorspellingen gedaan aan de hand van ontdekte patronen, worden nieuwe verbanden gelegd, worden data gerangschikt in categorieën en worden analyses gemaakt van gedrag of natuurverschijnselen.

Het gaat bij big data vaak om persoons- of persoonsgerelateerde gegevens. In dat geval kunnen er gevolgen zijn voor de privacy. Vooral analyses die gericht zijn op het categoriseren van gegevens over personen en groepen en het toepassen van deze categorieën op een persoon (profilering) kunnen privacygevolgen hebben. Deze analyses kunnen namelijk leiden tot uitspraken en conclusies over individuen en specifieke groepen. Ook kan profilering leiden tot het in- en uitsluiten van (groepen van) personen. Overigens is profilering geen nieuw fenomeen. Al veel langer worden diverse gegevens verzameld om personen of groepen in te kaderen met als doel deze gericht te kunnen benaderen of behandelen. Wel nieuw zijn de omvang en diversiteit van de gebruikte data en de analysetechnieken die worden toegepast.

Big data analyses en toepassingen zullen lang niet altijd betrekking hebben op persoons- of persoonsgerelateerde gegevens. Bijvoorbeeld wanneer data over objecten en complexe processen worden verzameld en verwerkt. Een groot deel van de kansen voor bedrijven om met big data te innoveren ligt hierin verscholen, bijvoorbeeld door productinnovatie, effectief beheer van wegen, bruggen en energienetwerken, het simuleren en bouwen van complexe machines en het analyseren van radioastronomische gegevens.

Big data is nog sterk in ontwikkeling. De hoeveelheid data groeit snel door een steeds wijdverbreider gebruik van internet, sensoren en ingebouwde chips. Doordat steeds meer apparaten met sensoren aan elkaar zullen worden gekoppeld

via het internet (het zogenaamde *internet of things*) zal de verzameling van kwalitatief hoogwaardige data een nog hogere vlucht nemen. Door technologische vooruitgang daalt de prijs van opslag en analyse van data, waardoor big data ook door kleine bedrijven benut kan worden. Er is bovendien sprake van een ontkoppeling van de verschillende stadia van de bigdata-waardeketen, die mede mogelijk wordt gemaakt door clouddiensten. Een bedrijf dat data verzamelt hoeft deze bijvoorbeeld niet zelf op te slaan of te analyseren, maar kan dit aan andere bedrijven uitbesteden. Dit stelt bedrijven in staat zich te specialiseren, waardoor de complexiteit van de waardeketen sterk is toegenomen. Voor de buitenwereld, waaronder de betrokkene, is het hierdoor lastig om de (juridische) rollen in de waardeketen te onderscheiden, en te weten welke marktpartij(en) voor het verwerken van de persoonsgegevens verantwoordelijk zijn en daarop kunnen worden aangesproken.

**Maatschappelijke en economische relevantie**
De toepassing van big data leidt tot nieuwe kansen door de hele samenleving heen. Niet alleen de ICT- sector, de dienstensector en de industrie profiteren. Ook de overheid, het onderwijs en de gezondheidszorg kunnen veel baat hebben bij de toepassing van big data. Volgens de OESO kan door-data-gedreven innovatie zorgen voor een stijging in de productiviteit van gemiddeld 5 tot 10 procent[1], met uitschieters naar boven in specifieke sectoren. Naast de toepassing van data is ook de dienstverlening rondom big data een belangrijke bron van economische activiteit, zoals data-analyse, het beschikbaar stellen van reken- en opslagcapaciteit of juridisch advies.

De toepassingsmogelijkheden van big data laten zich onderverdelen in efficiencyverbetering, strategische kennisopbouw, profilering en wetenschappelijk onderzoek. Bij efficiencyverbetering zorgt het gebruik van data bijvoorbeeld voor verbetering van werkprocessen in de zorg, van productieprocessen in de industrie of van logistiek in de transportsector. Bij strategische kennisopbouw nemen bedrijven strategische beslissingen op basis van verkoopcijfers en transacties. Profilering maakt het mogelijk om vraag en aanbod beter op elkaar af te stemmen, potentiële klanten te identificeren, gerichte aanbiedingen te doen en nieuwe producten te ontwikkelen. Hierbij kan gedacht worden aan commerciële toepassingen maar bijvoorbeeld ook aan nieuwe en gerichte onderwijs- en behandelmethoden. Ook kan profilering risico's beperken, bijvoorbeeld dat van wanbetaling. Wetenschappelijk onderzoek op basis van grote dataverzamelingen heeft tal van toepassingen, onder andere in de medische wereld. Stuwende krachten achter al deze innovaties zijn een voortdurende zoektocht naar meer efficiëntie, een grotere effectiviteit en een beperking van risico's.

Nederland is uitstekend toegerust om te profiteren van de potentie van big data. De telecominfrastructuur in Nederland – een van de basisvoorwaarden voor het transport van data – is van wereldklasse. Nederland kent goedlopende bedrijven die actief zijn op gebied van big data en er vindt veel en hoogstaand ICT- en wetenschappelijk onderzoek plaats. Het kabinet onderneemt diverse activiteiten

[1] OESO, 2014, Data-driven Innovation for Growth and Well-being

om de kansen van big data verder te benutten. Een van de negen publiek-private doorbraakprojecten met ICT is gericht op big data, waarbij het MKB bewust zal worden gemaakt van de mogelijkheden van het analyseren van big data voor nieuwe producten en nieuwe diensten. In het nationale open-data-beleid zet het kabinet zich in voor het vergroten van het aanbod van data en het gebruik daarvan, samen met het bedrijfsleven en andere relevante partijen. Door middel van de Roadmap ICT voor topsectoren wordt het ICT-onderzoek op het gebied van big data in PPS-verband gebundeld. Tot slot zijn er diverse activiteiten op het gebied van cyber security en privacy gericht op bewustwording, het toepassen van open standaarden en het bundelen van kennis.

Ook op Europees niveau is er aandacht voor big data. De Europese Commissie publiceerde op 2 juli haar mededeling "naar een bloeiende data economie". Uw Kamer is hierover separaat geïnformeerd (Kamerstuk 22 112, nr. 1898). Deze mededeling bundelt diverse, vaak al in gang gezette, initiatieven zoals publiek-private samenwerking bij onderzoek naar nieuwe technologieën en diensten, het opzetten van een Europees netwerk van kenniscentra om het aantal dataspecialisten met de nodige vaardigheden te vergroten, het stimuleren van open data en open standaarden en het beschikbaar stellen van infrastructuur voor onderzoek. Nederland steunt dit actieplan.

**De markt voor persoonsgegevens**
Zoals hiervoor is toegelicht, vertegenwoordigen persoonsgegevens economische waarde. In theorie zou iedere burger zelf op elk moment volledig geïnformeerd kunnen beslissen of hij deze waarde verzilvert en zijn gegevens afstaat in ruil voor voldoende baten. Die baten kunnen bijvoorbeeld bestaan uit het verkrijgen van een gratis dienst, een financiële vergoeding of een bijdrage aan de oplossing van een maatschappelijk probleem. Zo zou een markt ontstaan voor het gebruik van persoonsgegevens waarin vraag en aanbod elkaar vinden op basis van de individuele waarde die burgers en bedrijven toekennen aan data[2].

Maar in de praktijk werkt deze markt vaak niet goed of komt hij niet van de grond. De volgende factoren zijn daarop van invloed:

- *Transactiekosten* maken het te kostbaar en tijdrovend om een op de persoon en de situatie toegesneden overeenkomst op te stellen.
- *Moral hazard* zorgt ervoor dat de consument niet weet of de verantwoordelijke voor de verwerking van persoonsgegevens zich zal houden aan de afspraken en aan de toepasselijke regelgeving op dit terrein. Hij is aangewezen op de reputatie van een bedrijf en op goed toezicht door de toezichthouder (een sectorspecifieke toezichthouder of het College bescherming persoonsgegevens (Cbp)).
- *Informatie-asymmetrie* zet de burger vaak op een grote achterstand ten opzichte van een verantwoordelijke voor verwerking van persoonsgegevens zodat van een eerlijke afweging en uitruil geen sprake is. Vaak is de burger zich er niet eens van bewust dat zijn gegevens

[2] Centraal Plan Bureau, 2014, Kiezen voor privacy, CPB Policy Brief.

worden verzameld en verwerkt in het kader van big data en profilering, en weet hij niet welk effect dat op hem heeft.
- *Irrationeel gedrag* tenslotte, zorgt ervoor dat de burger zelf niet altijd een rationele afweging maakt, onder andere als gevolg van haast, een korte-termijn horizon of onvoldoende kennis. De lange en veelal complexe privacy-overeenkomsten waarmee gebruikers van diensten vaak instemmen zonder ze te lezen vormen een voorbeeld.

Bovenstaande marktimperfecties legitimeren een rol voor de overheid om voorwaarden te scheppen en waarborgen te bieden voor een verantwoorde en zorgvuldige omgang met gegevens. Deze voorwaarden en waarborgen zijn voor een belangrijk deel vastgelegd in de Wet bescherming persoonsgegevens (Wbp), de Telecommunicatiewet (Tw), het consumentenrecht en de Algemene wet gelijke behandeling (Awgb). De desbetreffende wetten bevatten algemene verplichtingen voor private en publieke organisaties en rechten voor burgers. Ook regelen ze toezicht en handhaving, respectievelijk monitoring en klachtbehandeling, door van de regering onafhankelijke organen, namelijk het College bescherming persoonsgegevens (Cbp), de Autoriteit Consument en Markt (ACM) en het College voor de Rechten van de Mens.

**Het recht op de eerbiediging van de persoonlijke levenssfeer (privacy)**
Indien bij big data persoonsgegevens worden verwerkt is het recht op bescherming van persoonsgegevens van kracht, zoals geregeld in de Wet bescherming persoonsgegevens (Wbp). Deze implementeert de Europese Privacy richtlijn uit 1995. In de Wbp zijn twee principes het meest relevant voor het gebruik van big data, namelijk *rechtmatigheid* van de verwerking en *informatieverstrekking* aan degenen van wie de persoonsgegevens worden verwerkt.

Met het principe van *rechtmatigheid* van de verwerking wordt bedoeld dat persoonsgegevens alleen mogen worden verwerkt in overeenstemming met de toepasselijk wetgeving (waar onder de algemene regels van de Wbp) en met het contract dat tussen partijen is gesloten. Verder moeten persoonsgegevens op behoorlijke en zorgvuldige wijze worden verwerkt. Dit betekent dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld; de verwerking niet onverenigbaar mag zijn met de doeleinden waarvoor de gegevens oorspronkelijk zijn verzameld; en er een wettelijke grondslag moet bestaan voor de verwerking, zoals toestemming van de betrokkene of het bestaan van een "gerechtvaardigd belang van de verantwoordelijke". Het betekent ook dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is en er niet meer persoonsgegevens mogen worden verwerkt dan noodzakelijk is voor het doeleinde.

Het principe van *informatieverstrekking* betekent onder andere dat de verantwoordelijke voor de gegevensverwerking degene van wie de persoonsgegevens worden verwerkt op een voor hem begrijpelijke wijze moet informeren over de verzameling en doeleinden van de (verdere) verwerking van

zijn gegevens (transparantie). Ook heeft de betrokkene het recht om op eigen initiatief te informeren welke gegevens over hem worden verwerkt. Indien de verantwoordelijke de verwerking baseert op het bestaan van een eigen "gerechtvaardigd belang" dan beschikt de betrokkene bovendien over het recht om zich tegen de verwerking van zijn persoonsgegevens te verzetten.

Deze principes en hun invulling zullen naar verwachting van kracht blijven en op onderdelen worden versterkt in de Algemene verordening gegevensbescherming, waarover momenteel wordt onderhandeld in Brussel. Over de voortgang van deze onderhandelingen wordt uw Kamer periodiek geïnformeerd door de staatssecretaris van Veiligheid en Justitie[3].

Dit kader biedt niet alleen bij klassieke gegevensverwerking, maar ook bij het gebruik van big data een bescherming tegen een ongerechtvaardigde inbreuk op privacy. Het eigen karakter van big data en profilering kan wel zorgen voor een spanning met deze principes[4]. Spanning met het principe van rechtmatigheid, omdat het interessant en winstgevend is data voor een ander doel en context te gebruiken dan waarvoor ze zijn verzameld, ze langer vast te houden met oog op toekomstige analyses en zoveel mogelijk data te verwerken met oog op een betere analyse. Spanning met het principe van informatieverstrekking, omdat het lastig is de betrokkene op een begrijpelijke wijze te informeren over de vele ingewikkelde analyses in de complexe waardeketen en de grote hoeveelheid gegevens die daarbij wordt gebruikt. Daarbij is het wel belangrijk om op te merken dat het wettelijk kader de nodige flexibiliteit biedt. Zo betekent verdere verwerking van gegevens voor nieuwe doeleinden niet automatisch dat deze verwerking onverenigbaar is met het oorspronkelijke doeleinde[5]. Ook maakt de al genoemde grondslag "gerechtvaardigd belang van de verantwoordelijke" het mogelijk om gegevens te verwerken zonder toestemming van de betrokkene, waarbij bedrijven hun eigen legitieme belang wel goed moeten afwegen tegen het privacybelang van de betrokkene. Ook hebben bedrijven meer vrijheden wanneer ze gegevens louter gebruiken voor (markt)onderzoek, zolang dit niet leidt tot automatische beslissingen over individuen.

Voor de bescherming van de persoonlijke levenssfeer op het internet is eveneens hoofdstuk 11 van de Telecommunicatiewet (Tw) relevant. Deze vormt een vertaling van de Europese e-Privacyrichtlijn. Zo houdt art 11.7a Tw in dat gegevens op randapparatuur van de gebruiker – zoals cookies – alleen mogen worden opgeslagen (en uitgelezen) met toestemming van de desbetreffende gebruiker en nadat deze daarover volledig en duidelijk is geïnformeerd. Het instemmen met gebruikersvoorwaarden waarin alle manieren worden beschreven waarop gegevens worden opgeslagen en/of toegang wordt verkregen, kan niet worden beschouwd als toestemming. Hier kan spanning ontstaan met de wens

[3] Kamerstukken 32761.
[4] International Working Group on Data Protection in Telecommunications, 2014, Working Paper on Big Data and Privacy.
[5] Information Commissioner's Office (ICO), 2014, Big data and data protection. Zie ook het afwegingskader van artikel 9, tweede lid, Wbp.

van commerciële partijen om zoveel mogelijk gegevens binnen te halen voor zoveel mogelijk doelen. De ACM ziet toe op de naleving van deze regels.

Voor zover het om informatie aan consumenten gaat, kunnen ook regels uit het generieke consumentenrecht relevant zijn voor het gebruik van big data en profilering. Aanbieders dienen consumenten onder meer op een niet misleidende, eerlijke manier te informeren over de voornaamste kenmerken en de prijs van een product. Ook mag niet op een oneerlijke manier gebruik worden gemaakt van het begrip 'gratis' of bewoordingen van gelijke strekking. Hiervan zou sprake kunnen zijn als apps of diensten als gratis worden geadverteerd terwijl in wezen sprake is van een uitruil doordat de gegevens van de consument worden uitgelezen. Ook moet de aanbieder van een digitale dienst de consument informeren of de digitale inhoud gebruikt wordt voor het in kaart brengen van consumentengedrag (ook wel bekend als tracking). De ACM ziet toe op de naleving van deze regels.

**De impact van big data op het recht op gelijke behandeling**
Voor het gebruik van big data, en profilering in het bijzonder is ook het recht op gelijke behandeling bij de toegang tot het aanbod van goederen en diensten van belang van belang, zoals dat is vastgelegd in de Algemene wet gelijke behandeling (art 7. Awgb) en in de Wet gelijke behandeling op grond van handicap en chronische ziekte (artikelen 6b en 8 WgbH/CZ). Onderscheid op grond van godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht, nationaliteit, hetero- of homoseksuele gerichtheid of burgerlijke staat is niet toegestaan. Dit verbod kan soms op gespannen voet staan met de gevolgen die zijn verbonden aan besluitvorming op basis van bigdata-analyse. Marktpartijen zullen er in beginsel voor waken om opzettelijk te discrimineren; een goed of dienst zal niet gauw aan alleen mannen of mensen met een bepaalde politieke gezindheid worden aangeboden. *Direct* onderscheid tussen groepen zal zich waarschijnlijk dan ook niet snel voordoen. Wel dient voorkomen te worden dat als gevolg van het bigdata-proces *indirect* onderscheid tussen groepen optreedt. Dan is het weliswaar niet de bedoeling om de toegang tot een goed of dienst aan een bepaalde groep onmogelijk te maken, maar leidt een besluit of handeling van het bedrijf (op basis van big data) er in de uitwerking wel toe dat een bepaalde groep op grond van een of meer kenmerken uit de wet, wordt uitgesloten. Wanneer een bigdata-analyse tot een concrete uitkomst leidt, zal binnen een bedrijf een vertaalslag naar een bepaalde marketingstrategie plaatsvinden. Mogelijk richt een bedrijf zijn aanbod – op basis van de uitkomsten van de bigdata-analyse – vooral op bepaalde groepen gebruikers, maar dat mag niet leiden tot uitsluiting van individuele of groepen gebruikers die net als de doelgroep van het bedrijf ook toegang tot de aangeboden dienst of goed willen.

De wet laat evenwel ruimte voor het maken van uitzonderingen. Het nastreven van winstmaximalisatie en andere commerciële doelen door het bedrijfsleven is op zichzelf legitiem, en het inzetten van bigdata-processen ten behoeve van die winstmaximalisatie eveneens. Als het middel om het nagestreefde doel (winstmaximalisatie) te bereiken passend en noodzakelijk is, kan indirect onderscheid, mits deugdelijk gemotiveerd, met objectiveerbare feiten worden

gerechtvaardigd. Zo kunnen verzekeraars niemand uitsluiten op grond van geslacht of godsdienst, ook al lijkt de uitkomst van een bigdata-analyse daartoe aanleiding te geven. Wel kunnen zij als gevolg van besluitvorming op grond van bigdata-uitkomsten premies differentiëren aan de hand van bepaalde gedragskenmerken die iets zeggen over het risico van een verzekerde. Als dat besluit vervolgens in de uitwerking leidt tot indirect onderscheid op grond van één van de in de wet genoemde kenmerken, moeten de verzekeraars daarvoor een objectiveerbare rechtvaardiging aanvoeren.

Het proces van profilering kan ook zorgen voor onterechte conclusies over een individu of groep, bijvoorbeeld doordat aan onbetrouwbare informatie onjuiste gevolgtrekkingen worden verbonden, of door gebruik van correlatie zonder het bestaan van een oorzakelijk verband. Dit kan leiden tot onterecht onderscheid op basis van profielen en leiden tot onjuiste voorspellingen, en kan er langs die weg ook voor zorgen dat bepaalde groepen onterecht een beperktere toegang tot goederen en diensten wordt geboden op basis van dit profiel. Wanneer consumenten of gebruikers menen dat in hun geval onterecht onderscheid is gemaakt bij de toegang tot het aanbod van een goed of dienst, bestaat de mogelijkheid om de casus te laten toetsen aan de Awgb of de WgbH/CZ door het College voor de Rechten van de Mens. Dat spreekt een niet-bindend oordeel uit, dat vervolgens indien gewenst kan worden voorgelegd aan de civiele rechter.

Het is van belang de onwenselijke neveneffecten van profilering zoveel mogelijk te beperken om het vertrouwen in onlinetoepassingen te borgen en te voorkomen dat mensen zich niet langer vrij gedragen in hun meningsuiting, in vertrouwelijke communicatie of in groepsvorming omdat ze bang zijn digitale sporen na te laten (het zogenaamde *chilling effect*). De Wbp probeert de meest verstrekkende gevolgen van profilering te ondervangen, door voor te schrijven dat iemand niet onderworpen mag worden aan een besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem in aanmerkelijke mate treft, indien dat besluit alleen wordt genomen op grond van geautomatiseerde verwerking van persoonsgegevens bestemd om een beeld te krijgen van bepaalde aspecten van zijn persoonlijkheid. Er moet dan sprake zijn van menselijke tussenkomst. Op dit verbod zijn echter wel uitzonderingen mogelijk.

**Volstaat een juridische benadering?**
Het mag duidelijk zijn dat het wettelijk kader niet altijd goed aansluit op de praktijk van big data en profilering. Daarom zal het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties inventariseren welke impact big data heeft op de uitoefening van diverse grondrechten zoals het recht op bescherming van de persoonlijke levenssfeer, het recht op gelijke behandeling, de vrijheid van meningsuiting en de vrijheid van vereniging. In 2015 zal onderzoek worden geïnitieerd met als doel de kennis en bewustwording van de Rijksoverheid op dit terrein te vergroten. Dat de wet moet worden gerespecteerd, zodat er sprake is van een rechtmatige verwerking van data en een goede naleving van de rechten van burgers, staat buiten kijf. Bedrijven zullen zelf doorgaans ook voldoende prikkels ervaren om te wet na te leven. Voltooiing van de hiervoor al genoemde Algemene verordening gegevensbescherming zal kunnen bijdragen aan meer

duidelijkheid over de – op onderdelen versterkte – Europese regels die de komende jaren van kracht zullen zijn. Een formeel-juridische benadering volstaat echter niet waar het doel is om burgers met vertrouwen hun data te laten delen, op basis van een eerlijke afweging van kosten en baten. Het kabinet zoekt de oplossing in de invulling van drie randvoorwaarden voor vertrouwen die al werden genoemd in de e-privacybrief, namelijk controle van de burger over zijn eigen gegevens, transparantie en verantwoordelijkheid van bedrijven. Dat de verantwoordelijkheid van bedrijven van belang is, kan worden geïllustreerd aan de hand van een recent voorbeeld (zie kader).

**Het gebruik van big data door financiële instellingen**
Enige tijd geleden ontstond ophef over een plan van een bank om betaalgegevens van klanten in te zetten voor een nieuwe vorm van dienstverlening, namelijk het onder de aandacht brengen van gepersonaliseerde aanbiedingen van andere commerciële partijen. Hoewel volgens de desbetreffende bank aan alle juridische vereisten zou worden voldaan, ontstond de vraag of juist de bancaire sector zich wel met nieuwe vormen van dienstverlening moet inlaten, gezien de privacygevoeligheid van financiële gegevens. De maatschappelijke ophef die ontstond, illustreert dat de bereidheid van consumenten om data te delen sterk verschilt per sector en laat zien dat een strikt juridische benadering niet altijd volstaat. Ook als een datatoepassing voldoet aan de voorwaarden zoals opgenomen in de Wet bescherming persoonsgegevens, zullen bedrijven rekening moeten houden met eventuele gevoeligheden rondom privacy, met het oog op behoud van het vertrouwen van hun klanten. Hierbij zij opgemerkt dat de Nederlandse overheid staat voor een goed functionerende, integere bankensector, die dienstbaar is aan de Nederlandse economie en waarin de klant centraal staat. De commerciële activiteiten van de banken dienen deze uitgangspunten niet te ondermijnen.

**Naar meer transparantie en controle**
Bedrijven kunnen de nodige acties ondernemen om burgers meer transparantie en controle te bieden over de verzameling en verwerking van gegevens. Deze acties zullen moeten inspelen op de hierboven genoemde onvolkomenheden in de markt voor persoonsgegevens, waarvan informatie-asymmetrie en irrationeel gedrag de belangrijkste zijn. Sommige van deze maatregelen kunnen er toe leiden dat een individu ervoor kiest minder data te delen in een specifieke situatie, maar alle individuen gezamenlijk op termijn bereid zijn meer data beschikbaar te stellen[6]. Het kabinet roept bedrijven op tot:

- *Het beter en handzamer informeren van betrokkenen over het doel waarvoor gegevens worden verzameld*, vooral wanneer dat doel ruimer is dan de dienst doet vermoeden. Een gebruiker van sociale media moet bijvoorbeeld vooraf worden uitgelegd dat zijn data ook worden gebruikt voor marktonderzoek. Bedrijven zullen betere en innovatieve manieren moeten vinden om dit te communiceren, zodat burgers niet langer lange privacy-overeenkomsten ondertekenen zonder de inhoud daarvan te lezen. Daarbij kan ook worden

[6] Boston Consulting Group, 2012, The value of our digital identity, Liberty Global Policy series.

bezien in hoeverre bij deze communicatie aanduidingen van de mate van privacyvriendelijkheid kunnen worden gebruikt.
- *Het ontwikkelen van keurmerken*, om te laten zien dat ze data gebruiken conform de regelgeving, of zelfs boven de wettelijk gestelde eisen uitgaan. Certificering kan plaatsvinden door een onafhankelijke organisatie. Vooral voor kleine of beginnende bedrijven die nog geen reputatie hebben ontwikkeld, is een keurmerk een nuttig instrument om een signaal af te geven over hun betrouwbaarheid.
- *Het opstellen van gedragscodes,* waarin zij laten zien hoe zij data gebruiken conform de regelgeving. Gedragscodes kunnen ter goedkeuring aan het College bescherming persoonsgegevens worden voorgelegd.
- *Het bieden van meer en eenvoudiger te gebruiken controlemogelijkheden*. Daarbij valt te denken aan eenvoudig aan te passen privacy-instellingen en de mogelijkheid bepaald gebruik van data uit te sluiten (een zogenaamde *opt-out*). Bedrijven moeten handige manieren vinden om betrokkenen opnieuw toestemming te vragen wanneer gegevens worden gebruikt voor andere doelen, of door andere partijen dan de oorspronkelijke. Betrokkenen zouden ook de mogelijkheid moeten hebben om hun data mee te nemen naar een andere aanbieder, zodat ze kunnen uitwijken als ze niet tevreden zijn.
- *Het duidelijk maken dat gepersonaliseerde diensten, producten en informatie worden aangeboden*. Bedrijven zouden de keuze kunnen bieden deze personalisering uit te zetten.

**Naar een zorgvuldige omgang met gegevens**
Naast het bieden van meer transparantie en controle kunnen bedrijven in hun eigen bedrijfsvoering veel doen om zorgvuldig met gegevens om te gaan. Het kabinet denkt aan:
- *Het beperken van het gebruik van persoonsgegevens* door deze bijvoorbeeld zoveel mogelijk te anonimiseren. Voor veel doeleinden waarvoor big data wordt ingezet, zijn tot de persoon herleidbare gegevens immers helemaal niet nodig. Ook kan de bewaartijd van data worden beperkt tot het nodige.
- *Het gebruiken van Privacy by design en Privacy by default oplossingen* bij het ontwerpen van hun datagebruik, zodat de bescherming van gebruikers zit opgesloten in de techniek en de standaardinstellingen. Dit beschermt de betrokkene tegen ongewenst gebruik van zijn data (moreel gevaar) en tegen zijn eigen onwetendheid of onoplettendheid (irrationaliteit).
- *Het uitvoeren van Privacy Impact Assessments,* zodat ze grip houden op de verzameling en verwerking van data en de privacygevolgen voor betrokkenen. Uit deze assessments kan volgen dat een bedrijf kiest voor een slimme *privacy by design* oplossing.
- *Het beperken van het gebruik van zelflerende systemen* (met ongewisse uitkomst zonder menselijke tussenkomst) tot maatschappelijk toelaatbare toepassingen door middel van zelfregulering.

Diverse van deze oplossingsrichtingen komen, al dan niet als verplichting, terug in het al eerder genoemde Commissievoorstel voor de Algemene verordening gegevensbescherming, dat onder meer beoogt om de burger meer controle te geven over zijn data en de gebruiker van data aan te zetten tot meer

zorgvuldigheid. Deze onderdelen kunnen in de onderhandelingen rekenen op steun van Nederland.

**De rol van de overheid**
Bovengenoemde acties vragen om een extra inspanning van bedrijven die data willen verzamelen en verwerken. De overheid is hier op de volgende wijze bij betrokken:

- De overheid geeft een impuls aan *privacy by design* oplossingen door middel van het actieplan Privacy, in 2013 en 2014 uitgevoerd door het Privacy & Identity Lab (PI.lab) en TNO in opdracht van het Ministerie van Economische Zaken. Het actieplan Privacy beoogt privacy-vriendelijke innovatie te stimuleren door de beste technologieën en praktijken te verzamelen en deze beschikbaar te stellen.
- De overheid is betrokken bij Qiy, een afsprakenstelsel dat beoogt de internetgebruiker controle en overzicht over, en inzicht in, de eigen data te geven[7].
- De overheid geeft voorlichting over datagebruik en technologie. Het ministerie van Economische Zaken heeft samen met het NCSC en ECP, platform voor de informatiesamenleving, gewerkt aan een nieuwe informatiebron voor burgers en bedrijven: www.veiliginternetten.nl. Deze is onlangs gelanceerd. Op de website worden eindgebruikers geïnformeerd over de risico's van internetgebruik en wordt handelingsperspectief geboden. De privacy-implicaties van internetgebruik vormen daarbij een van de aandachtsgebieden.
- De overheid overlegt met de sector over de wijze waarop zij informatie verstrekt over het gebruik van data. Tijdens de plenaire behandeling van het wetsvoorstel tot wijziging van de Telecommunicatiewet op 2 oktober 2014 heb ik uw Kamer toegezegd om met aanbieders van websites te gaan overleggen over een eenduidige informatievoorziening over het gebruik van cookies – die veel worden ingezet voor het maken van profielen. De gebruiker moet eenduidig en overzichtelijk duidelijk worden gemaakt of zijn surfgedrag wordt gebruikt voor het opstellen van een profiel, of informatie wordt gedeeld met derden, en wat die derden met die informatie doen. Het overleg hierover met de sector is inmiddels gestart.

**Conclusie**
De ontwikkeling van big data en profilering biedt volop kansen. Kansen op onder andere efficiëntiewinst, ontwikkeling van nieuwe producten, dienstverlening op maat en het vinden van oplossingen voor maatschappelijke problemen. De toepassing van big data en profilering vindt plaats buiten het zicht van de betrokkene, wat de ongerustheid over de verwerking van zijn gegevens voedt. De burger weet zich beschermd door waarborgen in de wet, maar deze sluiten niet altijd op een voor hem begrijpelijke wijze aan op de praktijken van big data en profilering. Behoud van vertrouwen van de burger in het gebruik van zijn gegevens is niet alleen een maatschappelijk belang, het is ook een voorwaarde

[7] www.qiyfoundation.org

**Directoraat-generaal**
**Energie, Telecom &**
**Mededinging**
Directie Telecommarkt

**Ons kenmerk**
DGETM-TM / 14179608

om de stroom van data niet te laten opdrogen en de kansen die big data en profilering bieden optimaal te benutten.

Meer vertrouwen van de burger vraagt allereerst om meer transparantie en controle over de verzameling en verwerking. Een goed geïnformeerde burger die meer de touwtjes in handen heeft zal eerder zijn data afstaan als hem duidelijk is dat de kosten daarvan worden overtroffen door de baten, zoals een gratis dienst of vergoeding. Meer vertrouwen vraagt in de tweede plaats om een zorgvuldige omgang met data door bedrijven die ze verwerken, en een zorgvuldige benadering van de burger van wie de data worden verwerkt. In deze brief zijn langs deze twee sporen enkele mogelijke maatregelen voorgesteld die bedrijven zelf kunnen nemen. Naarmate het bewustzijn en de keuzemogelijkheden van de burger groeien, zullen bedrijven de manier waarop ze omgaan met data steeds meer kunnen inzetten als concurrentiemiddel. Dit is de wens en verwachting van het kabinet.

Het is duidelijk dat dit thema en de oplossingsrichtingen vragen om verdere verkenning en uitwerking. De overheid kan dit niet alleen. Het onderwerp is sterk in ontwikkeling en de belangen zijn groot en divers. Het kabinet wil zijn gesprekken met belanghebbenden over dit thema op meer gestructureerde wijze voortzetten. Hiertoe zal een high level expertgroep worden opgericht met deelname uit de wetenschap, consumentenorganisaties, bedrijven en het maatschappelijk middenveld. Deze high level expertgroep krijgt als opdracht de relatie tussen big data en profilering en de bescherming van grondrechten verder te verkennen en oplossingsrichtingen uit te werken voor het verenigen van twee doelen: het benutten van de mogelijkheden van big data enerzijds en het behoud van vertrouwen van de samenleving in het internet anderzijds. Ook de rol die de overheid daarbij speelt zal aan bod komen. Deze brief vormt daartoe het startpunt. Uw Kamer zal voor eind 2015 worden geïnformeerd over de resultaten van de high level expert groep.

(w.g.) H.G.J. Kamp
Minister van Economische Zaken