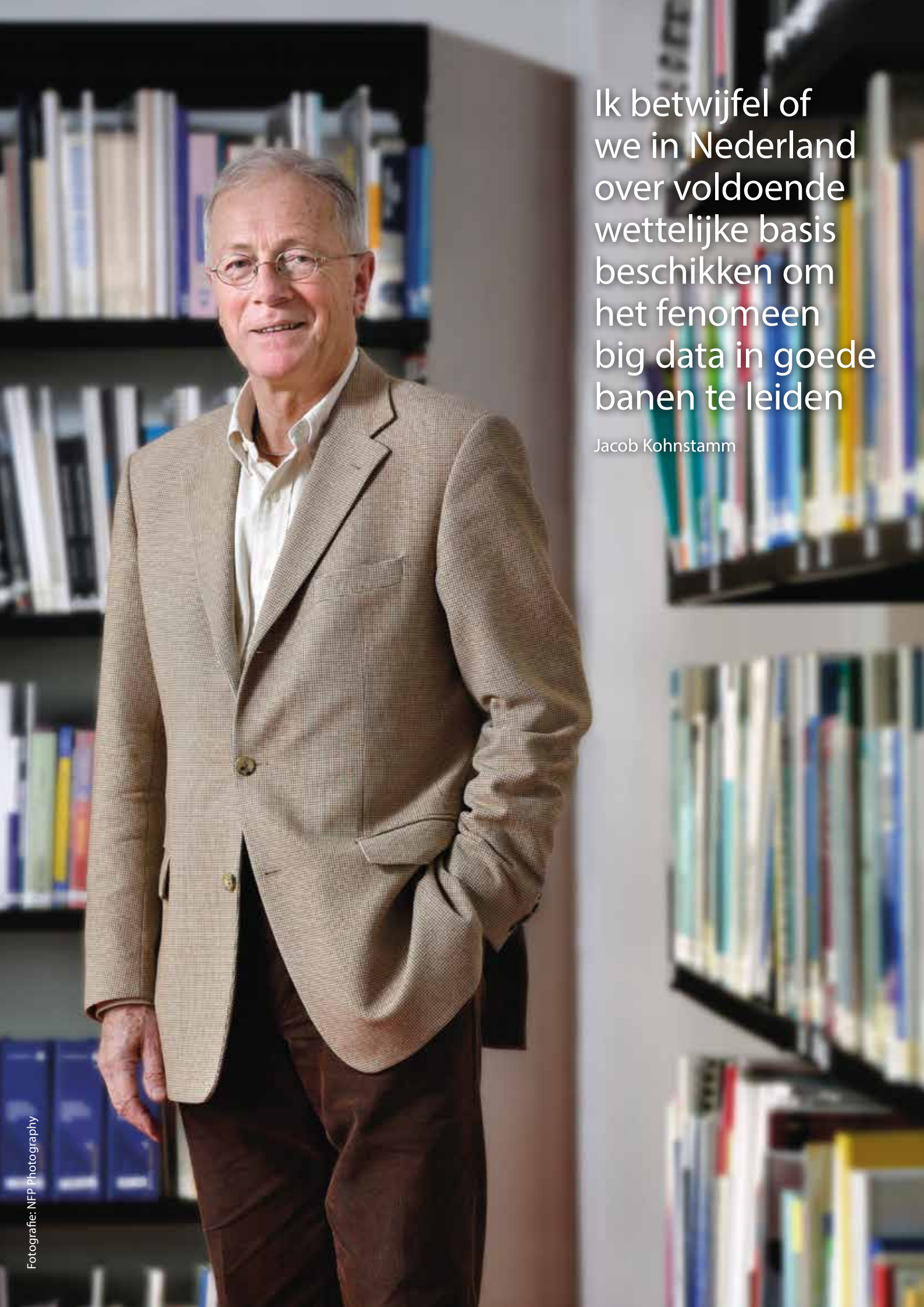

Ik betwijfel of we in Nederland over voldoende wettelijke basis beschikken om het fenomeen big data in goede banen te leiden

Jacob Kohnstamm

Fotografie: NFP Photography

Sander Diks CIA
Jip Olieroock MSc RO CIA

Audit Magazine sprak met Jacob Kohnstamm, voorzitter van de Autoriteit Persoonsgegevens, voorheen het College bescherming persoonsgegevens, over nut en noodzaak van het beschermen van persoonsgegevens, big data en over de veranderingen in het privacylandschap. Ook de rol van internal auditors kwam aan bod.

Bescherming van persoonsgegevens begint aan de **tekentafel**

Over...

Jacob Kohnstamm is sinds 2004 voorzitter van de Autoriteit Persoonsgegevens. Van 2010 tot 2014 was hij ook voorzitter van de Artikel 29-werkgroep. Dit onafhankelijke en raadgevende orgaan bestaat uit de verzamelde Europese privacytoezichthouders. Daarnaast was hij van 2011 tot 2014 voorzitter van het executive committee van de International Data Protection and Privacy Commissioners Conference. Na diverse jaren als advocaat trad hij in 1981 namens D66 toe tot de Tweede Kamer en in de periode 1982-1986 bekleedde hij tevens het partijvoorzitterschap van D66. Hij was staatssecretaris van Binnenlandse Zaken van 1994 tot 1998. Van 1999 tot 2004 was hij lid van de Eerste Kamer.

Als introductie voor de lezers van Audit Magazine: wat doet de Autoriteit Persoonsgegevens?

"De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor de bescherming van persoonsgegevens, waaronder de Wet bescherming persoonsgegevens (Wbp) en adviseert over nieuwe regelgeving. Sinds 1 januari van dit jaar heeft het College bescherming persoonsgegevens een andere naam: Autoriteit Persoonsgegevens.
Met betrekking tot het houden van toezicht maakt de Autoriteit Persoonsgegevens een onderscheid in het realiseren van zogenoemde alternatieve interventies en het uitvoeren van meer diepgaande onderzoeken. Een alternatieve interventie is het bellen of aanschrijven van een bedrijf of organisatie wanneer de Autoriteit Persoonsgegevens een tip ontvangt over een (mogelijke) overtreding van de privacyregelgeving. De diepgaande onderzoeken ter plaatse vinden met name bij de meer ernstige overtredingen plaats en dienen volgens de regels van de Algemene Wet Bestuursrecht te worden uitgevoerd."

Kunt u een paar voorbeelden noemen van wapenfeiten van de Autoriteit Persoonsgegevens?

"De Autoriteit Persoonsgegevens heeft in samenwerking met de zusterorganisatie in Canada onderzoek gedaan naar WhatsApp. Het onderzoek richtte zich op het gegeven dat wanneer iemand de app downloadt, WhatsApp voor de dienstverlening ook toegang kreeg tot de mobiele telefoonnummers van niet-gebruikers in het elektronisch adresboek van de gebruiker. WhatsApp heeft inmiddels een aantal maatregelen genomen die waarborgen dat WhatsApp de telefoonnummers van niet-gebruikers alleen verwerkt om gebruikers met elkaar in contact te brengen en niet voor andere doelen.

Soms kunnen interventies van de Autoriteit Persoonsgegevens zeer snel effect hebben. Een voorbeeld hiervan betreft de ING die enige tijd geleden het plan lanceerde om de betalingsgegevens van klanten te vermarkten. Hierbij heeft de Autoriteit Persoonsgegevens, evenals de minister van Financiën, De Nederlandsche Bank en enkele Tweede Kamerleden, snel laten weten tenminste grote vraagtekens te zetten bij dit plan, met als gevolg dat het plan vooralsnog niet tot uitvoering is gebracht."

Hebben we met ons ongebreideld gebruik van social media, het op allerlei plekken achterlaten van onze persoonsgegevens op internet en het klakkeloos accepteren van gebruikersvoorwaarden, ons recht op privacy niet een beetje verspeeld?

"De gedachte dat men enkel vrijwillig informatie afstaat klopt niet. Het achterlaten van digitale voetsporen is bijna inherent aan het moderne leven, ook zonder dat je daar een keuze in kunt maken. Wanneer een medewerker met zijn OV-chipkaart naar kantoor gaat, voor het werk websites bezoekt en communiceert via zijn smartphone, worden tal van databases van nieuwe informatie voorzien. Dit gaat doorgaans ongemerkt. Dit kan een individu eigenlijk niet tegengaan. De enige mogelijkheid om dit te voorkomen is te kiezen voor een kluizenaarsbestaan. Dit laatste is natuurlijk een absurde gedachte, zeker omdat de bescherming van jouw persoonsgegevens een grondrecht is.
Microsoft heeft ooit eens aan enkele medewerkers gevraagd de tijd in kaart te brengen die zij nodig hadden om de verschillende privacyvoorwaarden waar zij als gebruiker mee werden geconfronteerd woord voor woord te lezen. Dit kwam uiteindelijk neer op ongeveer 76 dagen per jaar! Dat kun je in redelijkheid van niemand vergen. Daarom heeft de samenleving voor het doen naleven van het grondrecht ook goede wetgeving, een goede consumentenorganisatie en een sterke toezichthouder nodig."

'Privacy by design' is nodig om naleving van de Wbp te waarborgen

Is de Autoriteit Persoonsgegevens voldoende uitgerust om deze toezichthoudersrol te kunnen vervullen?

"De omvang van de Autoriteit Persoonsgegevens is zeker veel te beperkt. Een positieve ontwikkeling is wel dat de Autoriteit Persoonsgegevens per 1 januari 2016 een boetebevoegdheid heeft gekregen. Omdat wij sinds die datum boetes mogen uitschrijven is de naam dan ook veranderd in Autoriteit Persoonsgegevens. De boetebevoegdheid is echt nodig omdat een bedrijf nu nog weinig (financieel) risico loopt bij mogelijke overtreding van de Wbp. De prikkel ontbreekt om als bedrijf zelf toe te zien op strikte naleving. Ik verwacht dat met het verkrijgen van de nieuwe bevoegdheid de Wbp meer serieus zal worden genomen en beter zal worden nageleefd."

Wat zijn de grootste risico's van big data? En biedt big data ook kansen?

"Big data biedt zeker ook kansen. Denk bijvoorbeeld aan het inzetten van big data voor detectie en bestrijding van epidemieën. De mogelijkheden zijn enorm, maar eigenlijk staat het fenomeen big data nog in de kinderschoenen. Het probleem is dat de kern van de wetgeving en het doel van big data strijdig met elkaar lijken te zijn. De Wbp mikt op 'surprise minimalization' terwijl 'surprise maximalization' juist inherent is aan het inzetten van big data. De Wbp stelt onder meer dat er bij gebruik van gegevens altijd een duidelijk vooraf overeengekomen doel moet zijn vastgesteld (ofwel geen verrassingen waar de data voor wordt gebruikt). Bij big data is juist sprake van een zoektocht naar nieuwe mogelijkheden en toepassingen, die lang niet altijd vooraf zijn bepaald. Hierbij speelt natuurlijk de vraag in hoeverre individuen nog in staat zijn om vooraf 'explicit and informed consent' te geven wanneer zij hun data afstaan: het is immers niet te overzien waarvoor en op welk moment hun data gebruikt gaat worden. Overigens betwijfel ik of we in Nederland momenteel over voldoende wettelijke basis beschikken om het fenomeen big data in goede banen te leiden."

U sprak en schreef al eerder over digitale predestinatie. Wat houdt dit in en waarom is het onwenselijk?

"Met digitale predestinatie doel ik op de ontwikkeling dat mensen op basis van hun doen en laten online bepaalde profielen krijgen toebedeeld, die vervolgens bepalend zijn voor de wijze waarop zij worden gezien en behandeld. Het zogenoemde 'profiling'. Mensen worden ingedeeld in profielen zonder dat ze daarvan op de hoogte zijn, zonder dat zij weten wat de consequenties van de profielen voor hen zijn, laat staan hoe zij daar verandering in kunnen brengen. Dit blijkt in de praktijk niet alleen effecten te hebben op de reclameboodschappen die mensen ontvangen, maar bijvoorbeeld ook op de aard van de informatie die zoekmachines opleveren. Mensen kunnen zich daardoor minder vrij ontplooien en worden belemmerd in hun keuzevrijheid. Ik ben daar een sterk tegenstander van."

Wat zijn de grootste dilemma's en uitdagingen voor organisaties als het gaat om bescherming van persoonsgegevens en privacy?

"Voor bedrijven bestaat het risico dat bij het ontwikkelen van nieuwe producten en diensten er onvoldoende rekening wordt gehouden met de Wbp. Er ontbreekt dan iemand met gedegen kennis van de Wbp aan de ontwerptafel, met het risico dat achteraf moet worden vastgesteld dat een eerste release niet voldoet. De vervolgens noodzakelijk door te voeren aanpassingen pakken altijd duur uit. Bedrijven doen er dus goed aan om waarborgen in te bouwen dat de Wbp bij de ontwikkeling van nieuwe producten of diensten voldoende serieus wordt genomen. 'Privacy by design' is nodig om naleving van de Wbp te waarborgen.

Een van de grootste problemen bij de Wbp is dat de gevolgen van het niet naleven van deze wet voor gewone mensen vaak totaal onzichtbaar zijn. Als je in een auto rijdt met slechte remmen en het gaat mis dan zijn de gevolgen en de ernst direct duidelijk. Schort het in de naleving van de Wbp dan is het nog maar de vraag of een consument of burger kan zien of weten dat zijn grondrecht op bescherming van persoonsgegevens is geschonden."

Is er momenteel niet sprake van een overkill aan wet- en regelgeving op privacygebied? En werkt dit niet verlammend of is het juist bittere noodzaak?

"In beginsel hebben we goede wetgeving die de tand des tijds redelijk heeft doorstaan. De nieuwe Europese verordening over gegevensverwerking is bovendien een stap in de goede richting die er daarenboven voor zorgt dat er gelijke regels zullen komen in alle EU-lidstaten. De principes uit de thans geldende wetgeving zijn overigens per saldo in de nieuwe EU-wetgeving overeind gebleven.
Wij horen wel eens de kritiek dat de wetgeving te abstract is. Wettelijke formuleringen moeten echter altijd 'techniekonafhankelijk' blijven. Je kunt immers niet continu de wetgeving aan technologische ontwikkelingen blijven aanpassen. Wel is de verwachting dat de toekenning van de boetebevoegdheid ertoe gaat leiden dat er meer tegen de Autoriteit Persoonsgegevens geprocedeerd zal gaan worden. Dit leidt dan tot toenemende jurisprudentie en daar is in de rechtspraktijk dringend behoefte aan. Jurisprudentie maakt de wetgeving meer concreet en dit geeft bedrijven en consumenten handvatten."

Kijken jongere generaties anders tegen privacy aan? Is er in dat opzicht sprake van een generatiekloof?

"Ik kom nog wel eens op middelbare scholen en daar is er altijd wel iemand die roept dat-ie niets te verbergen heeft. Wanneer ik vervolgens vraag of zijn of haar ouders ook lid zijn van hun Facebook-vriendenclub is het antwoord van diegene 'daar niet aan te moeten denken'. De informationele zelfbeschikking speelt voor iedereen en lijkt redelijk los te staan van leeftijd. Ongetwijfeld zijn er verschillen per generatie maar in de kern heeft iedereen behoefte om een bepaalde controle te hebben en te houden over de informatie die wordt gedeeld met anderen."

Welke rol hebben internal auditors als het gaat om privacy en bescherming van persoonsgegevens binnen organisaties?

"Per 1 januari 2016 is de meldplicht datalekken van kracht. Dit houdt in dat zodra sprake is van een datalek, dit door betreffende organisatie moet worden gemeld bij de Autoriteit Persoonsgegevens en in bepaalde gevallen ook aan burgers en consumenten. Internal auditors doen er goed aan om zich inhoudelijk te verdiepen in de meldplicht datalekken om vervolgens te toetsen of de eigen organisatie voldoende waarborgen heeft ingebouwd om succesvol aan deze meldplicht te kunnen voldoen. De aanwezigheid van een plan om datalekken te voorkomen en om adequaat te reageren op een datalek zou in organisaties aanwezig moeten zijn en auditors zouden hier op kunnen toetsen. Het geven van invulling aan de meldplicht zou voor de bedrijven een vanzelfsprekendheid moeten worden.
Verder zouden internal auditors erop toe kunnen zien dat bij de ontwikkeling van nieuwe producten en diensten voldoende rekening met de Wbp wordt gehouden. Dit vergt enerzijds de aanwezigheid van voldoende kennis aan de tekentafel en anderzijds het voldoende serieus nemen van de wet in de dagelijkse praktijk van de organisatie."

Hebt u ten slotte nog een advies aan de beroepsgroep als het gaat om privacy en bescherming van persoonsgegevens?

"In algemene zin wil ik wijzen op het gezegde 'denkt aleer gij doende zijt en doende denkt dan nog'. Zorg er nu voor dat er voldoende kennis van de Wbp is en voorkom dat vertrouwen wordt geschaad. Internal auditors zouden deze uitgangspunten, mits relevant voor het auditobject, heel goed een plek kunnen geven in hun audits." <<