

**Over big data in het onderwijs en de beperkingen die de privacywet daaraan stelt**



# **Over big data in het onderwijs en de beperkingen die de privacywet daaraan stelt**

Symposiumbundel 2017  
Nederlandse Vereniging  
voor Onderwijsrecht

Deel 37 in de serie Onderwijsrecht van de Nederlandse  
Vereniging voor Onderwijsrecht

Redactie:  
Prof. mr. M.T.A.B. Laemers

*Meer informatie over deze en andere uitgaven kunt u verkrijgen bij:*

Sdu Klantenservice  
Postbus 20014  
2500 EA Den Haag  
[www.sdu.nl/service](http://www.sdu.nl/service)

Secretariaat NVOR:  
mr. Pauline Demacker  
St. Canisiussingel 19f  
Postbus 1126  
6501 BC Nijmegen  
website: [www.nvor.nl](http://www.nvor.nl)

© NVOR

© 2017, Sdu Uitgevers bv, Den Haag, 2017

ISBN: 9789012401142

NUR: 840

Zetwerk: Studio Typeface, Lelystad

Alle rechten voorbehouden. Alle auteursrechten en databankrechten ten aanzien van deze uitgave worden uitdrukkelijk voorbehouden. Deze rechten berusten bij Sdu Uitgevers bv.

Behoudens de in of krachtens de Auteurswet gestelde uitzonderingen, mag niets uit deze uitgave worden veelevoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Voorzover het maken van reprografische veelevoudingen uit deze uitgave is toegestaan op grond van artikel 16 h Auteurswet, dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht (postbus 3051, 2130 KB Hoofddorp, [www.reprorecht.nl](http://www.reprorecht.nl)). Voor het overnemen van gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (artikel 16 Auteurswet) dient men zich te wenden tot de Stichting PRO (Stichting Publicatie- en Reproductierechten Organisatie, postbus 3060, 2130 KB Hoofddorp, [www.cedar.nl/pro](http://www.cedar.nl/pro)). Voor het overnemen van een gedeelte van deze uitgave ten behoeve van commerciële doeleinden dient men zich te wenden tot de uitgever.

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, kan voor de afwezigheid van eventuele (druk)fouten en onvolledigheden niet worden ingestaan en aanvaarden de auteur(s), redacteur(en) en uitgever deswege geen aansprakelijkheid voor de gevolgen van eventueel voorkomende fouten en onvolledigheden.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the publisher's prior consent.

While every effort has been made to ensure the reliability of the information presented in this publication, Sdu Uitgevers neither guarantees the accuracy of the data contained here in nor accepts responsibility for errors or omissions or their consequences.

# Inhoud

	blz.
<b>Voorwoord</b>	7
<i>Miek Laemers</i>	
<b>Over big data in het onderwijs en de beperkingen die de privacywet daaraan stelt</b>	11
<i>Arno Lodder en Gerrit-Jan Zwenne</i>	
<b>Woord vooraf (en leeswijzer)</b>	11
<b>1. Inleiding</b>	13
1.1 Bureaucratisering	14
1.2 Techniek, recht en ethiek	17
<b>2. Techniek en toekomstscenario's</b>	18
2.1 Vier scenario's	21
2.1.1 Robotisering – kleuters	21
2.1.2 Monitoring – basisschool groep 3-8	22
2.1.3 Augmented reality – middelbare school	22
2.1.4 Data-analyses en profilering – universiteit	23
<b>3. Privacy- en gegevensbeschermingsrecht</b>	23
3.1 Bijzondere gegevens (gezondheid, religie, etniciteit etc.)	25
3.2 Doelbinding	27
3.3 Profilering	29
3.4 Transparantie	30
3.5 Beveiliging, privacy-by-design en privacy-by-default	32
<b>4. Analyse van toekomstscenario's</b>	33
4.1 Robotisering	34
4.2 Monitoring	35
4.3 Augmented reality	36
4.4 Data-analyses en profilering	37
<b>5. Conclusie</b>	38
<b>6. Referenties</b>	39

**Het ethisch debat over big-data-analytics aan de hand van de beginselen uit de Algemene Verordening Gegevensbescherming** 41  
*Iris Hoen*

1.	Inleiding	41
2.	Reikwijdte verordening	41
3.	Beginsel van rechtmatigheid, behoorlijkheid en transparantie	42
4.	Beginsel van doelbinding	44
5.	Overige beginselen inzake de verwerking van persoonsgegevens	44
6.	Rechtmatigheid van de verwerking	45
7.	Verbod op verwerken van bijzondere persoonsgegevens, tenzij...	49
8.	Grondslag voor het verwerken van bijzondere gegevens	49
9.	Conclusie	50

**Big and small data – de praktijk van persoonsgegevens in het onderwijs** 53  
*Wouter Pors*

1.	Inleiding	53
2.	De onderwijscarrière van leerlingen en studenten	53
3.	Verwerking en overdracht van persoonsgegevens is essentieel voor onderwijs	54
4.	Praktijkvoorbeeld: invloed van big data op beoordeling in het onderwijs	54
5.	Leerlingen en studenten hebben zelf belang bij verwerking van persoonsgegevens	56
6.	Gebrekkige grondslag in de onderwijswetgeving	56
7.	Verwerking na beëindiging van de opleiding	58
8.	Verwerking van bijzondere gegevens	58
9.	Conclusie	59

**Verslag NVOR jaarsymposium 2016** 61  
*Ilona Bierkens*

## Voorwoord

Ruim een jaar geleden schreef prof. Corien Prins in het Nederlands Juristenblad (*NJB* 9 september 2016, afl. 30, p. 2161) een vooraf: ‘De (digitale) scholen zijn weer begonnen’. Daarin schetst zij de aanzienlijke veranderingen die onderwijsinstellingen de laatste jaren doormaken: de verandering van schoolbord en krijtje naar digibord, van zware met dikke boeken gevulde rugzak naar laptop, van vertrouwd rapport naar onlinesystemen die elk gewenst moment inzicht bieden in resultaten, aanwezigheid en voortgang. De vertrouwde schoolboekenleveranciers zijn verdrongen door een reeks, deels buitenlandse, informatie-aanbieders die alle hun graantje willen meepikken op de commerciële onderwijsmarkt. Maar nog belangrijker is het door Prins geconstateerde probleem van dataverzameling over leerlingen en studenten, de toekomstige beroepsbevolking. Ze noemt met name Basispoort, dat een onlineplatform aanbiedt voor educatief lesmateriaal. Dat ziet er op het eerste gezicht aantrekkelijk uit, maar: ‘Diverse gegevens over zowel leerlingen als leerkrachten (naam, geboortedatum, geslacht, naam van de school, groep en naam leerkrachten) komen via het systeem beschikbaar en worden daarmee gedeeld met uitgeverijen. Hiernaast faciliteert het systeem de combinatie van bovenstaande gegevens met toetsuitslagen voor rekenen en taal en biedt het dus inzicht in taalontwikkeling en rekenvaardigheid.’ De gevolgen van deze ontwikkeling voor de privacy van betrokkenen blijken dermate behartigenswaardig dat er Kamervragen over zijn gesteld en er in de zomer van 2016 een Privacyconvenant over is gesloten. Gesproken wordt over een ‘digitale tang’ waarin scholen terecht zijn gekomen, omdat ze door het aanleveren van gegevens zijn overgeleverd aan het systeem, in casu Basispoort. Een leerling uit het systeem verwijderen blijkt alleen te kunnen als de leerling wordt uitgeschreven van de school. De bekostigingsconsequentie daarvan is natuurlijk niet aantrekkelijk voor de school.

In het hoger onderwijs doen zich vergelijkbare ontwikkelingen voor: het gebruik van Black Board – en anno 2017 Canvas en soortgelijke systemen – herbergt dezelfde dataverzamelmogelijkheden waarmee met behulp van algoritmen op individueel niveau ‘toekomstvoorspellingen’ gemaakt kunnen worden.

Naast de privacykwesties voor leerlingen en studenten speelt de door Prins gesignaleerde kwestie van het ‘eigenaarschap’: wie is ‘eigenaar’ van de gegenereerde kennis, wie heeft toegang tot de data en wie mag deze gebruiken? De commerciële partijen die zich ‘ontfermen’ over het rijke materiaal en het vervolgens monopoliseren ten eigen nutte lijken in ieder geval niet de eerstgerechtigden. Aan Prins’ oproep om educatie als publiek belang, inclusief waarden als toegankelijkheid, gelijkheid, onderwijsvrijheid en privacy, onze noodzakelijke aandacht te geven, hopen we met de behandeling van dit thema tijdens het jaarlijkse symposium van de NVOR gehoor te geven.

Het bestuur van de NVOR prijst zich gelukkig dat twee op het terrein van privacywetgeving én van digitalisering deskundige hoogleraren bereid waren het preadvies voor het symposium 2017 te schrijven. Prof. mr. Arno Lodder en prof. mr. Gerrit-Jan Zwenne hebben een toekomstbeeld geschetst voor het onderwijs waarin de digitaletangconstruc-

tie zichtbaar en voelbaar wordt. Aan de hand van vier scenario's, die keurig gespreid zijn over de verschillende onderwijsfasen (kleuter-, basis- en middelbare school alsmede universiteit) laten ze zien hoe de digitalisering om zich heen grijpt en hoe zich daardoor een proces van dataficatie ontwikkelt. Die dataficatie maakt het mogelijk om te ontdekken welke patronen en correlaties daarin opgesloten zitten. Dat het daarbij gaat om vaak gevoelige informatie maakt de noodzaak om met privacy- en gegevensbeschermingsrecht tegenwicht te bieden alleen maar groter.

Voor veel onderwijsjuristen is de gehanteerde terminologie wellicht nog niet erg vertrouwd, maar het beeld dat geschetst wordt door de preadviseurs lijkt tot voortvarende bezinning over toelaatbaarheid en wenselijkheid van de gesignaleerde ontwikkelingen te nopen. Het preadvies en de toelichting daarop tijdens het symposium zullen er zeker aan bijdragen dat het bezinningsproces bij de aanwezige onderwijsjuristen (verder) op gang komt.

Mevrouw mr. Iris Hoen, advocaat bij Wille Donker in Alphen aan den Rijn, heeft al veel gepubliceerd over privacywet- en regelgeving, met name voor de onderwijssector. Zij draagt in haar coreferaat de nodige informatie aan over het huidige en toekomstige privacybeschermingsrecht en spitst dit toe op onderwijssituaties. Zij reageert ook op de in het preadvies opgeworpen vraag of we alles wat kan met digitalisering, dataficatie en analysering, ook moeten willen. Dat doet ook coreferent mr. Wouter Pors, advocaat bij Bird & Bird, die aan de hand van een fraaie casus, ontleend aan een rechterlijke uitspraak over de beoordeling van een examen Frans, de lezer meevoert in zijn ervaringen met digitalisering en gegevensbescherming in het onderwijs.

Naast de in dit boekje opgenomen teksten is er natuurlijk nog heel veel te lezen over het gekozen thema en nadere studie te verrichten over de praktische of juridische consequenties van de gaande en aanstaande ontwikkelingen. Een voorbeeld moge illustreren dat ook de wetgever zich dezer dagen niet onbetuigd laat op dit terrein. In februari van dit jaar stemde de ministerraad in met een wetsvoorstel van (toen nog) minister Bussemaker en staatssecretaris Dekker van Onderwijs, Cultuur en Wetenschap om de privacy van leerlingen beter te beschermen (zie *Kamerstukken II 2016/17, 34 741*). Het betreft het wetsvoorstel 'Pseudonimiseren van leerlinggegevens ten behoeve van de toegang tot en het gebruik van digitale leermiddelen.' Het inmiddels door de Tweede Kamer aangenomen wetsvoorstel beoogt te voorzien in bescherming van de privacy van leerlingen die digitale leermiddelen gebruiken. Het gebruiken van een pseudoniem voor leerlingen in de uitwisseling tussen de onderwijsinstelling en de leveranciers, gebaseerd op het persoonsgebonden nummer (PGN), maakt dat de leerlingen zonder gevaar van aantasting van hun privacy toegang hebben tot de juiste digitale leermiddelen en deze ook kunnen gebruiken. Om het pseudoniem te kunnen baseren op het PGN, was het noodzakelijk deze doelbepaling voor het gebruik van het PGN wettelijk te verankeren. De Raad van State adviseerde het voorstel aan de Tweede Kamer te zenden, maar achtte aanpassing van het voorstel aangewezen waar het gaat om het stellen van regels over de voorwaarden waaronder de pseudoniemen kunnen worden gebruikt: de bepalingen in het wetsvoorstel die zien op de regeling van de bewaartermijn, de aanvullende gegevens die mogen worden verstrekt en de categorieën ontvangers zouden op het niveau van een algemene maatregel van bestuur vastgesteld moeten worden. Tevens moest worden gemotiveerd



waarom het stellen van regels over de overige voorwaarden kon worden gedelegeerd naar het niveau van ministeriële regeling. Ten slotte moesten het voorstel en de toelichting op elkaar worden afgestemd op dit punt, aldus de Raad van State.

Het wetsvoorstel is op 10 oktober 2017 met algemene stemmen aangenomen in de Tweede Kamer. De Kamer zal jaarlijks geïnformeerd worden over de voortgang van de invoering van het pseudoniem. De invoering van het pseudoniem binnen het onderwijs wordt samen met leveranciers en scholen vormgegeven. Alle betrokkenen moeten een zorgvuldige aanpak hanteren, zodat het onderwijs tijdens de invoering niet stil komt te liggen. Meer informatie over dit wetsvoorstel is te vinden op een speciale webpagina over nummervoorziening. Het wetsvoorstel ligt nu voor behandeling in de Eerste Kamer.

Eén recent verschenen boek, P.H. Blok (red.), *Big data en het recht; een overzicht van het juridisch kader voor big data-toepassingen in de private sector*, Sdu Uitgevers, Den Haag 2017 wil ik hier niet onvermeld laten. Een dozijn auteurs, waaronder preadviseur G.J. Zwenne, laten in deze uitgave in de reeks Monografieën Recht en Informatietechnologie de maatschappelijke impact van big data zien. Dat privacyrecht daarin een dominante rol vervult, zal u na lezing van dit preadvies en de coreferaten niet verwonderen.

Het bestuur van de NVOR is zich ervan bewust dat het volledige juridische kader dat geldt of binnenkort gaat gelden voor dataverzameling in het onderwijs en de bijbehorende bescherming van persoonsgegevens niet uitputtend aan de orde kan komen tijdens het jaarsymposium. Het bestuur vertrouwt er wel op dat de hier aangeboden teksten kunnen bijdragen aan de broodnodige bezinning van onderwijsjuristen op dit thema.

Miek Laemers

Voorzitter Nederlandse Vereniging voor Onderwijsrecht



# Over big data in het onderwijs en de beperkingen die de privacywet daaraan stelt

A.R. Lodder & G.J. Zwenne\*

## Woord vooraf (en leeswijzer)

In het preadvies dat u zo meteen gaat lezen, of wellicht al hebt gelezen, hebben wij verkend wat kan en wat mag als het gaat om de toepassing van *big data predictive analytics* in het onderwijs en de beperkingen of waarborgen waarin de privacy- en gegevensbeschermingswetgeving voorziet. Onze eerste gedachte was dat wij in deze verkenning zouden uitgaan van een denkbeeldig, niet heel onwaarschijnlijk maar wel verontrustend scenario, waaruit blijkt wat allemaal kan met de technologie die op dit moment beschikbaar is of op niet al te lange termijn waarschijnlijk beschikbaar komt. Aan de hand van dat scenario wilden wij eerst bekijken in hoeverre zo'n scenario zou passen binnen de kaders van ons huidige privacy- en gegevensbeschermingsrecht. Vervolgens wilden we in een beschouwing daarover normatieve uitspraken doen. Wat vinden we ervan? Waar moet het naartoe? Wat is acceptabel en wat niet? Welke randvoorwaarden zijn nodig?

In deze opzet liepen we enigszins vast. Het lukte ons niet om zo'n scenario te bedenken, althans niet één waarin alle door ons als relevant beoordeelde aspecten aan de orde kwamen. We hebben daarom besloten om dat over te laten aan romanschrijvers, zoals David Eggers of dichter bij huis Aglaia Bouma, en zijn uitgegaan van wat wij om ons heen zien gebeuren. We denken dat we daarvan misschien wel een betrouwbaar beeld hebben, omdat we zelf al enige tijd onderwijs verzorgen aan onze respectievelijke universiteiten en toch ook omdat we zo af en toe worden gevraagd om mee te denken over een aanvaardbaar gebruik van informatietechnologie bij andere onderwijsinstellingen. Ons beeld is dat onderwijsinstellingen op alle niveaus, van de eerste groep in het basisonderwijs tot en met de postdoctorale opleidingsprogramma's in hoog tempo bezig zijn om allerlei bedrijfsprocessen te *digitaliseren* – een begrip dat tegenwoordig probleemloos zonder toelichting kan worden gebruikt en waaronder wij het gebruik verstaan van moderne elektronische informatie- en communicatietechnologie om processen en procedures langs elektronische weg, en dus in digitale vorm, te laten verlopen. Als gevolg van die digitalisering komen veel meer gegevens over gebruikers en gebruik beschikbaar, een ontwikkeling die wel wordt aangeduid met het begrip *datafictie*. En deze ontwikkeling maakt het mogelijk om bigdata-analyses te doen, dat wil zeggen om te inventariseren welke patronen en correlaties in al deze gegevens zijn te vinden. En daarbij komt vervolgens betekenis toe aan zelflerende algoritmes, *machine learning* en *artificial intelligence*.

\* Arno Lodder is VU Professor of Internet Governance and Regulation, Department Transnational Legal Studies, Centre for Law and Internet, [www.lawandinternet.com](http://www.lawandinternet.com). Gerrit-Jan Zwenne is hoogleraar Recht en de Informatiemaatschappij aan de Universiteit Leiden.

We zien dat bijvoorbeeld bij de onlineplatforms waarmee leraren communiceren met leerlingen of hun ouders (bijvoorbeeld Mijnschoolinfo.nl) en docenten met studenten (zeg Blackboard). Ook als deze platforms alleen zouden worden gebruikt om papieren of mondelinge informatie te vervangen door digitale communicatie, dan nog komen er daardoor veel meer gebruiksgegevens beschikbaar. Van een digitaal verzuimbriefje (Matthijs moet morgen naar de tandarts) kan niet alleen op een later moment worden gezien hoe laat het werd verzonden, maar ook wie het op welk moment hebben gelezen. We denken tegelijkertijd ook aan de leersystemen waarbij de leraar op een dashboard een gedetailleerd inzicht kan hebben in de leerprestaties en de voortgang daarvan (Haru had vanochtend moeite met voorzetsels).

Ook zien we, in een heel andere fase van de opleiding, hoe papers en scripties, ingediend via digitale studentsystemen, volautomatisch van plagiaatscores worden voorzien. En *last but not least* zien we ook met enige regelmaat dat scholen ouders online surveys sturen waarin veel, heel veel en vaak ook nog eens heel gevoelige informatie wordt opgevraagd over leerlingen en hun thuissituatie, uiteenlopend van de vraag naar het opleidingsniveau van de ouders en hun geboorteland tot vragen naar de werk- en schuldensituatie en of er gezinsleden zijn met stemmingsstoornissen.

Als gevolg van digitalisering-dataficatie worden er dus, vermoeden wij, in het onderwijs meer gegevens dan ooit vastgelegd en bewaard. En, ook dat vermoeden wij, als deze gegevens niet nu al worden gebruikt voor analysedoeleinden, dan moeten we er op zijn minst rekening mee gaan houden dat dit op termijn gaat gebeuren, althans dat de technologie en de kosten daarvan weinig beperkingen opleggen. Vaststaat dat veel van de bij het onderwijs betrokken partijen een eigen, vaak goed te begrijpen belang hebben om met de beschikbare gegevens inzicht te verkrijgen in allerlei onderwijsprocessen:

- onderwijsinstellingen willen weten op welke wijze individuele leerlingen het beste, dat wil zeggen: gepersonaliseerd onderwijs kan worden aangeboden;
- het ministerie, de toezichthouders en ouders willen weten in hoeverre scholen voldoen aan de gestelde kwaliteits- en financieringsnormen;
- studenten willen weten wie de beste docenten zijn, en docenten wie de meest veelbelovende studenten zijn;
- aanbieders van online-leermiddelen willen hun dienstverlening verbeteren en beschikbaar stellen aan de leerlingen die daaraan behoefte hebben;
- internetdienstverleners willen nieuwe generaties van gebruikers vertrouwd maken met hun internet-ecosystemen;
- werkgevers en werving- en selectiebedrijven willen *high potentials* aan zich binden.

Andere voorbeelden kunt u wellicht zelf waarnemen of bedenken.

We zijn niet geneigd al deze analysedoeleinden op voorhand te verwerpen. Wel denken we dat het nuttig is om te inventariseren wat onder welke voorwaarden wordt toegelaten door de privacy- en gegevensbeschermingswetgeving, die op dit moment het belangrijkste kader biedt voor big data. Aan de hand daarvan kunnen we vervolgens

normatieve uitspraken doen over deze wetgeving. Zoals of deze wetgeving toereikend is, en zo niet, op welke wijze tekortkomingen moeten worden weggenomen.

Wij zijn ons ervan bewust dat dit preadvies soms een wat speculatief karakter heeft.

Amsterdam / Den Haag / Geneve  
september 2017

## 1. Inleiding

Niet iedereen ziet onderwijs als een belangrijk onderdeel van de samenleving, als een instituut dat een nuttige bijdrage levert aan de ontwikkeling van kinderen en volwassenen. Zo begon Paul Simon in 1973 het nummer *Kodachrome* met de constatering dat het voornamelijk onzin was die voorgeschoteld werd op de middelbare school:

*When I think back on all the crap I learned in high school  
It's a wonder I can think at all*

Bruce Springsteen onthulde in 1984 dat alles wat hij op school heeft opgestoken minder is dan wat hij leerde door naar een enkel muzieknummer te luisteren:

*We busted out of class had to get away from those fools  
We learned more from a three-minute record than we ever learned in school*

In 1980, ten slotte, werd *Another brick in the wall* de protestsong in de strijd tegen Apartheid in Zuid-Afrika:

*We don't need no education  
we don't need no thought control*

Het album *The Wall* van Pink Floyd gaat over hoe lastig het is om je als individu van de massa te onderscheiden. Tegenwoordig wordt steeds meer gebruik gemaakt van op de individuele student of leerling toegesneden methoden, adviezen, volgsystemen. Tegelijkertijd worden individuele gegevens gebruikt om algemene profielen op te stellen. Beide facetten roepen juridische vragen op vanuit privacy- en gegevensbeschermingsrecht. Een meer ethische vraag is hoe ver we het monitoren en controleren van de individuele student of leerling moeten laten gaan. Het controleren van gedachten is, voor zover het niet al mogelijk is, iets wat steeds dichterbij lijkt te komen. In deze bijdrage zullen wij op deze, en andere, verontrustende aspecten ingaan.

### 1.1 Bureaucratisering

Een ontwikkeling die al langer gaande is, betreft de toenemende protocollen en procedures binnen het onderwijs. Tevreden studenten die veel nieuwe inzichten verwerven, inspirerende docenten, is in de kern waar het bij onderwijs om moet gaan en een belangrijke reden voor mensen om in het onderwijs werkzaam te zijn. Een goede praktijk volstaat echter niet, op papier moet kunnen worden hard gemaakt dat het onderwijs (vermeend) op orde is. Zo moeten docenten niet alleen goede tentamens maken, maar zijn er toetsmatrizen die de kwaliteit van het tentamen beogen te garanderen; volstaat een tweede beoordelaar bij scripties niet, maar wordt het van belang geacht drie scriptieformulieren te produceren (van beide docenten apart en een gezamenlijke), en wordt de inhoud van de opleiding verwoord door middel van Dublin-descriptoren die kennis en inzicht operationaliseren tot:

“aantoonbare kennis van en inzicht in de kernelementen van de wetenschappelijke discipline verwerven en kennis maken met een aantal van de nieuwste ontwikkelingen binnen de discipline.”

Het toepassen van kennis en inzicht wordt verwoord als:

“vaardigheden verwerven die hen in staat stellen om verworven kennis en inzicht op een professionele, bij de discipline passende manier toe te passen, om standpunten te formuleren en die te onderbouwen met argumenten en om problemen op het gebied van de discipline op te lossen.”

Dergelijke omschrijvingen hebben een hoog opendeurgehalte. Universiteiten zijn niettemin verplicht hier prudent mee om te gaan. De descriptoren moeten terugkeren bij leerdoelen van vakken, eindtermen van de opleiding en uiteindelijk in uitgebreide rapporten bij visitaties worden toegelicht. Of iets in de praktijk ook goed werkt is van ondergeschikt belang, het moet er op papier, veel papier, nog steeds ook per se gedrukt, goed en overtuigend uitzien. Zo ontstaat een papieren werkelijkheid die niet noodzakelijkerwijze overeenstemt met de werkelijke wereld, meer algemeen bekend als bureaucratisering.

In het studiejaar 2013/14 organiseerde Andrew Murray aan de London School of Economics een boekenclub waarin de boeken *Brave New World* van Aldous Huxley, *Der Prozess* van Franz Kafka en *1984* van George Orwell werden besproken. Het doel van de boekenclub was niet primair het bespreken van de boeken, maar een alternatieve manier om internetrecht te doceren (Murray 2015). Veel van de thema's die in genoemde boeken aan de orde komen, zien we terug in het internetrecht en in meer algemene zin in de samenleving waar we in leven. Dat geldt zeker ook voor het onderwijs.

Naast de protocollen en formulieren kent het onderwijs de laatste jaren een steeds grotere hoeveelheid regels die niet goed doordacht zijn en regelmatig tot contra-intuïtieve resultaten leiden. Zo is er een regel die bepaalt dat studenten zich voorafgaand aan het volgen van een vak voor dat vak moeten inschrijven. Op zichzelf is dit een begrijpelijke

regel. Het idee is dat dan zowel de docent als de onderwijsadministratie weet waar men aan toe is, namelijk hoeveel studenten het vak volgen. En dat is behulpzaam bij bijvoorbeeld het toewijzen van collegezalen en surveillanten bij schriftelijke tentamens. De regel bepaalt ook dat studenten die zich niet hebben ingeschreven, het vak niet mogen volgen. Er staat echter geen sanctie op het inschrijven en vervolgens het vak niet volgen. Het voorspelbare gevolg is dan dat 95 studenten zich inschrijven en er uiteindelijk maar 45 het vak daadwerkelijk volgen. Als een student heel graag een vak wil volgen, maar dat bedenkt nadat de inschrijftermijn is verlopen (veelal enkele weken voor aanvang van het vak), dan kan hij/zij het vak niet volgen. Er zijn dan 50 studenten die zich ingeschreven hebben en het vak niet volgen en een onbekend aantal studenten die het vak wel willen volgen, maar dat niet mogen. Een ergerlijke situatie voor de docent, die graag juist die gemotiveerde studenten erbij heeft. Er zijn soms U-bochten – gewoon op het eerste college aanschuiven en vervolgens als er wel degelijk nog plaats blijkt te zijn alsnog verzoeken om te worden toegelaten – maar de meeste studenten schrikken daarvoor terug en volgen het vak van hun keuze niet.<sup>1</sup>

Een ander voorbeeld is de *matching*, door het Ministerie van Onderwijs, Cultuur en Wetenschap ingevoerd om ervoor te zorgen dat studenten bewuster voor een bepaalde studie kiezen. Een interessant initiatief, dat door verschillende universiteiten verschillend wordt uitgevoerd. Een voorbeeld dat we in de praktijk hebben zien voorbijkomen is het volgende.

*Er zijn drie studenten die scheikunde willen studeren aan de Universiteit van Amsterdam (UvA) en die we gemakshalve aanduiden met fictieve namen:*

- *studente Ayaan doet aan de verplichte matching mee, maar krijgt het advies dat scheikunde voor haar niet geschikt is, dat wil zeggen dat zij niet geschikt is voor die studie;*
- *studente Babiche heeft een 9 voor scheikunde op haar eindlijst, heeft op NEMO en andere plekken vaak scheikundeproefjes gedaan, meegelopen op de UvA bij scheikunde en had slechts één fout bij de verplichte online wiskundematchingtoets;*
- *en studente Carola heeft een 6 voor scheikunde op haar lijst en heeft een positief matchingsadvies om rechten te studeren.*

Welke student kan zich voor scheikunde inschrijven? De inschrijving van Babiche wordt geweigerd omdat zij abusievelijk, vanwege een onduidelijke e-mail van de UvA, een matchingsbijeenkomst heeft gemist, studentes Ayaan en Carola kunnen zich wel inschrijven omdat ze wel een matchingsbijeenkomst hebben bijgewoond. Voor welke studie de matchingsbijeenkomst was, is niet relevant en ook een negatief advies speelt geen rol. In dit geval zijn Ayaan en Carola duidelijk niet of minder geschikt voor scheikunde, terwijl Babiche bijzonder geschikt is en gemotiveerd. Toch wordt zij niet toegelaten tot de studie. Dit lijkt vergezocht, maar het is echt gebeurd en illustreert dat het

---

1 Deze casus speelde bij het keuzevak telecommunicatierecht UL2015/16 en het vak e-commerce law aan de VU in 2016/17. In het laatste vak durfde slechts één student het risico te nemen het vak te volgen zonder ingeschreven te zijn en hij is handmatig toegevoegd aan de digitale leeromgeving. Hij sloot het vak af met een 8,5. Dit eindresultaat is tot de registratie toegelaten.

doel van regels in sommige gevallen volledig uit het oog verloren wordt.<sup>2</sup> Het idee is immers uitval te voorkomen door studenten een studie te laten volgen die bij hen past.

De studente Babiche kreeg begin juli te horen dat haar inschrijving geweigerd was. Bij de Universiteit Leiden kon ze toen nog online matchen en inschrijven. Gevolg is nu dat deze studente van Amsterdam naar Leiden moet reizen om een studie te volgen die zij het liefst aan de UvA gevolgd had, een merkwaardig gevolg van rigide optreden. In dit geval worden de regels op een geautomatiseerde wijze gevolgd. Er wordt niet gekeken naar het individuele geval, maar een eenvoudig algoritme toegepast:

*if <matchingsdag niet bijgewoond> then <niet toegelaten>.*

Er werd nog geprobeerd om door menselijke inbreng enige redelijkheid in het proces te brengen, maar tevergeefs. Het systeem voorzag niet in uitzonderingen of hardheidsclausules.

Bij de inzet van technologie en in het bijzonder data-analyse wordt het nog lastiger om een uitzondering te bepleiten: *how to prove yes if computer says no?* Dit lijkt een algemeen probleem te zijn bij data-analyses. De grootste gemene deler wordt leidend, voor afwijkende gevallen is minder of geen ruimte. Ook in die gevallen waarin ieder willekeurig, niet in het keurslijf van de universitaire bureaucratie gegoten persoon meteen doorziet dat de beslissing volkomen in strijd is met het doel waarvoor de maatregel is ingevoerd. Bij dergelijke willekeurige, al dan niet geautomatiseerde beslissingen is het van belang het individu te beschermen. Hierop richt zich, hoewel in onderhavig geval de betekenis beperkt is, het recht van de persoonlijke levenssfeer en gegevensbescherming.

Een andere tendens in het onderwijs is dat docenten steeds meer zelf moeten doen. Een professor van Queen Mary klaagde onlangs dat ze sinds kort zelf cijfers moet invoeren. In Nederland doen we dat al jaren. Cijfers voor de vakken in het onderwijssysteem, cijfers voor tussentoetsen en -opdrachten in de digitale leeromgeving etc. Aan de rechtenfaculteit bij de Vrije Universiteit Amsterdam moeten medewerkers sinds kort zelf facturen opstellen, de financiële ondersteuning is wegbezuinigd. In algemene zin heeft de digitale werkomgeving veel eenvoudige taken ondergebracht bij hoger personeel. Om excessen op dit terrein tegen te gaan is er op de VU sinds 2015 een 'Kafka-knop' ingevoerd, in de woorden van Jaap Winter:<sup>3</sup>

“We moeten zelf kritisch kijken naar de regels die we intern uitstorten over de universiteit. We implementeren dit jaar een *Kafka-knop* om overbodige bureaucratie te melden en aan te pakken.”

2 In werkelijkheid ging het overigens om de studie natuurkunde. De reactie van de UvA was o.a. “Dan neem je toch een tussenjaar.”

3 D. de Hoog, 'Jaap Winter: We gaan een Kafka-knop invoeren', *AdValvas* 28 april 2015, <http://www.advalvas.vu.nl/nieuws/jaap-winter-we-gaan-een-kafka-knop-invoeren>.



Een voorbeeld is het beëindigen van tijdelijke contracten. Het zou voor de hand liggen als die vanzelf aflopen, tenzij je ze verlengt. In het systeem moeten tijdelijke contracten echter actief worden beëindigd, anders lopen ze door. Hierin heeft een aanpassing plaatsgevonden naar aanleiding van een Kafka-melding. Er was een gastvrijheid verleend, die maakte het mogelijk dat een externe medewerker tijdelijk van de faciliteiten van de universiteit gebruik kon maken, en deze was verlopen maar liep dus door omdat er geen actieve beëindiging had plaatsgevonden. Toen de leidinggevende deze wilde beëindigen, kon dat niet met terugwerkende kracht, omdat er tussen het moment van beëindigen in het systeem en de beoogde einddatum niet meer dan een maand mag zitten. Het per heden beëindigen kon echter ook niet, omdat het einde van de gastvrijheidstermijn niet per heden was. De suggestie van de helpdesk om de gastvrijheid eerst te verlengen tot heden en vervolgens te beëindigen, bracht niet direct groot enthousiasme bij de leidinggevende teweeg. De melding middels de Kafka-knop van deze deadlocksituatie heeft ertoe geleid dat het inmiddels niet meer nodig is tijdelijke gastvrijheden actief te beëindigen.<sup>4</sup>

## 1.2 Techniek, recht en ethiek

De bovenstaande ontwikkelingen zijn exponenten van de digitalisering van het onderwijs, die veelal bureaucratiesering meebrengt of ondersteunt. Een achterliggende gedachte bij automatisering is dat het de werkzaamheden verlicht en dat bij intelligentere technologie ingewikkeldere taken door lager geschoold personeel gedaan kunnen worden. Ook de omgekeerde ontwikkeling manifesteert zich, namelijk dat er meer en regelmatig eenvoudig, nogal geestdodend werk op het bordje van docenten terechtkomt.

Wat de technologie in ieder geval in ruime mate oplevert is data. Gegevens over gedrag, kennis, inzicht en dergelijke, die door al dan niet zelflerende algoritmes worden geanalyseerd. De uitkomsten van deze analyses hebben veelal als doel om processen te optimaliseren. Een aspect dat hierbij bijzondere aandacht verdient is de leerling of student, omdat de uitkomsten van analyses betrekking op hen hebben en gevolgen voor hen hebben. Vanuit het recht is daarbij met name het privacy- en gegevensbeschermingsrecht relevant.

Alvorens daar nader op in te gaan zullen we enkele voorbeelden van bestaande techniek in het onderwijs geven en een viertal scenario's schetsen die zich in de toekomst zouden kunnen voordoen. Uitgangspunt daarbij zijn de mogelijkheden die de techniek biedt. Bij ontwikkelingen op het terrein van informatietechnologie en internet vormt de techniek steeds minder een belemmering. Er is veel mogelijk. Het feit dat iets kan, betekent nog niet dat hetgeen technisch mogelijk is ook juridisch toelaatbaar is. Dat vormt de tweede stap van de analyse. De randvoorwaarden binnen wat technisch mogelijk is worden bepaald door het recht, waarbij wij ons concentreren op privacy- en gegevensbeschermingsrecht. Na een algemene uiteenzetting over deze juridische invalshoek zullen de geschetste scenario's nader geduid worden. Hierbij komt naast de techniek en het

4 Een deadlock – van oorsprong gebruikt om routines in een softwarecode mee aan te duiden – is een situatie waarin een actie vastloopt door wederzijdse uitsluiting. Het tegenovergestelde is een livelock. In dat geval gaat de actie oneindig door.

recht ook een derde aspect aan de orde, dat zeker bij grootschalige dataverwerkingen niet onbelangrijk is: de ethiek. De ethiek richt zich op de wenselijkheid. In relatie tot de techniek en het recht is de rol van de ethiek ten minste tweeledig. Enerzijds kan de ethiek grenzen stellen aan de techniek en daarmee gebruikt worden voor het formuleren van het juridische kader. Anderzijds kan bij een bestaand juridisch kader worden aangegeven dat zelfs als bepaalde handelingen juridisch toelaatbaar zijn we mogelijk daar op ethische gronden van af moeten zien. Gezien onze achtergrond als jurist zal de nadruk in dit stuk liggen op het recht.

## 2. Techniek en toekomstscenario's

Als je vroeger de klas uitgestuurd werd, moest je je melden bij een (con)rector. Als je spijbelde, werd dat door de docent ergens genoteerd. Ouders werden geïnformeerd als er sprake was van structureel spijbelgedrag dan wel te regelmatige verwijdering uit de les. Cijfers werden op een rapport vermeld en twee of drie keer per jaar moest een kartonnen of papieren rapport door ouders en/of verzorgers ondertekend worden ter bevestiging dat zij van de cijfers hadden kennisgenomen.

Momenteel zien ouders bijna eerder dan de uit de les gestuurde leerling een aantekening over de verwijdering in de digitale leeromgeving verschijnen. Er wordt nog net geen whatsappje gestuurd, maar een ouder kan van iedere gemiste les op de hoogte zijn nog voordat de schooldag voorbij is.<sup>5</sup> Cijfers worden voor iedere gemaakte opdracht, toets en dergelijke ingevoerd en op ieder gewenst moment kunnen ouders per vak het gemiddelde alsmede alle individuele cijfers zien. Voor zover ze nog uitgedeeld worden, bevestigt een rapport wat al bekend was. De registratie in leerlingdossiers gaat verder. Als iemand zijn petje omgekeerd op zijn hoofd heeft, kan dit een aantekening opleveren van ongewenst gedrag. De zoekopdrachten en andere activiteiten op een leerlingaccount kunnen geanalyseerd worden, de voortgang kan nauwkeurig worden gedocumenteerd. Mobiel telefoongebruik van leerlingen kan door scholen nauwlettend in de gaten worden gehouden.<sup>6</sup>

“In a bid to protect students from pornography, predators and other online dangers, some schools are turning to technology that notifies teachers, parents and welfare staff when students access concerning material on their mobile phones.”

Al de gegevens die verzameld worden, blijven doorgaans niet beperkt tot de school. Op een elementair niveau speelt dit bij e-maildiensten. Vrij veel scholen en universiteiten outsourcen deze dienst naar Google. Er wordt gebruik gemaakt van een Gmail-account, maar dan onder de domeinnaam van de instelling. Het is dus voor gebruikers niet te zien, een mail van bijvoorbeeld een Groningse collega is verzonden via @rug.nl. Toch

5 Er zijn overigens wel aanbieders van 'gratis' apps voor communicatie met de ouders, zoals Klasbord, die volgens de aanbieder door duizenden klassen gebruikt wordt; <https://klasbord.nl/>.

6 H. Cook, 'How schools are tracking students using their mobile phones', *The Age* 16 July 2017, [www.theage.com.au/victoria/](http://www.theage.com.au/victoria/).

maakt de Groningse universiteit ook voor medewerkers sinds 2014 gebruik van Gmail en deed dit voor studenten al langer. Technische afdelingen wilden graag op eigen kosten een ander e-mailsysteem in de lucht te houden, maar dit werd afgewezen. Ook meekijk-bezwaren werden niet als zwaarwegend gezien:<sup>7</sup>

“Volgens de wetenschappers wegen de voordelen van Gmail (grotere mailbox, goede beveiliging tegen hackers) niet op tegen de nadelen, zoals het mogelijke meekijken van de NSA en van Google zelf.”

Verdergaand dan faciliteren van de communicatie is het leerlingenportaal Basispoort. Het betreft een samenwerking van zeven uitgeverijen:

- Heutink Primair Onderwijs BV;
- de Rolf groep;
- L.C.G. Malmberg BV;
- Noordhoff Uitgevers;
- Reinders Oisterwijk BV;
- ThiemeMeulenhoff BV;
- Uitgeverij Zwijsen BV.

In Basispoort worden de leerlingen gelinkt aan hun school via BRIN, wat staat voor BasisRegistratie Instellingen. Iedere onderwijsinstelling heeft een dergelijk uniek nummer. Volgens de statuten van de Stichting Basispoort is het doel: “Het bieden van een centraal portaal voor de ontsluiting van digitaal lesmateriaal voor het basisonderwijs.” Noordhoff Uitgevers benadrukt in lijn hiermee dat het doel van de samenwerking tussen verschillende uitgeverijen is om het gebruik van online educatief materiaal voor leerkrachten en leerlingen in het Primair Onderwijs (PO) gemakkelijker te maken. Toch reikt het initiatief zeker verder dan enkel uitgeverijen:<sup>8</sup>

“Andere uitgeverijen, aanbieders van schooladministratiesoftware en schoolnetwerkleveranciers, met diensten gericht op het basisonderwijs, zijn welkom om aan te sluiten bij de samenwerking.”

Dat deze aansluiting al heeft plaatsgevonden blijkt uit onder meer uit de mededeling op de website van Basispoort in de zomer van 2017 over de administratie van scholen:

**“Maak uw schooladministratie gereed**

Scholen zijn in juni door Basispoort geadviseerd nog voor de zomervakantie de groepsindelingen voor 2017-2018 in orde te maken (ophogen, jaarovergang, migratie).”

---

7 Michael Persson, ‘Universiteit Groningen dwingt onderzoekers tot gebruik van Gmail’, *de Volkskrant* 13 juni 2014.

8 [Info.basispoort.nl](http://Info.basispoort.nl).

Hieruit blijkt dat de aanvankelijke samenwerking van uitgeverijen om onderwijsmateriaal online beschikbaar te maken, inmiddels onder andere ook de inmenging omvat over op welk moment door scholen groepsindelingen gemaakt moeten worden.

In 2014 ontstond ophef over de wijze waarop scholen met de gegevens van hun leerlingen omsprongen. Mede naar aanleiding daarvan werd dat jaar de *Big Brother Award*, een prijs voor personen of organisaties die uitblinken in het schenden van privacy, uitgereikt aan de Nederlandse scholen. Directe aanleiding was dat scholen op grote schaal gegevens van leerlingen doorspeelden naar uitgevers van leermiddelen, waarbij op zijn minst de suggestie werd gewekt dat deze uitgevers de leerlinggegevens voor eigen, commerciële doeleinden konden gebruiken. Toen RTL-nieuws daarover berichtte, leidde dat tot de nodige opwinding en verontwaardiging, en uiteraard Kamervragen. Volgens Prins (2016) is dit inmiddels verbeterd. Zo heeft Basispoort het ‘Convenant Digitale Onderwijsmiddelen en Privacy – Leermiddelen en Toetsen’ onderschreven. De mogelijke doelstellingen van deze producten en diensten zijn omschreven in het daarop betrekking hebbende onderdeel van artikel 5, lid 1, Convenant Digitale Onderwijsmiddelen en Privacy 2.0. Dit convenant voor het onderwijs is onder de generieke naam Privacyconvenant.nl op internet te vinden. Naast het convenant is er ook een door Kennisnet opgesteld 10-stappenplan dat ingaat op het creëren van bewustzijn, het informeren en wettelijke verplichtingen:

1. Weet waar privacy over gaat
2. Stel een beleidsdocument of privacyreglement op
3. Maak bewerkersafspraken
4. Informeer ouders
5. Wees transparant
6. Vraag altijd om toestemming
7. Maak afspraken over sociale media
8. Informeer leerlingen
9. Waarborg privacy bij overstapdossiers
10. Beveilig alle persoonsgegevens

In het volgende hoofdstuk gaan wij uitgebreider in op de hieraan gerelateerde wettelijke regels. Vooruitlopend kan de Autoriteit Persoonsgegevens (AP) worden aangehaald die, eveneens in 2014, het bedrijf Snappet op de vingers tikte voor de wijze waarop gegevens werden verwerkt die door het gebruik van Tablets in het onderwijs werden gegenereerd:<sup>9</sup>

“(...) [zes] verwerkingen [van Snappet] niet evident noodzakelijk zijn om onderwijs te kunnen geven met behulp van de tablets en omdat het om gevoelige gegevens gaat. De verwerkingen voldoen niet aan het proportioneelheidsvereiste. De verwerkingen voldoen ook niet aan het subsidiariteitsvereiste en door het ontbreken van andere waarborgen (zoals transparantie), maken de gegevensverwerkingen voor deze doeleinden (...) in verhouding een te grote inbreuk op de persoonlijke levenssfeer van de kinderen.”

<sup>9</sup> [https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn\\_privacy/rap\\_2013\\_snappet.pdf](https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013_snappet.pdf).

Het belang van Snappet weegt daarom niet op tegen het recht van de kinderen op eerbiediging van hun persoonlijke levenssfeer, aldus de AP. De verklaring van de GEU, de brancheorganisatie voor aanbieders van leermiddelen, toetsen en educatieve dienstverlening in Nederland, gaat vooral in op de belangen van de uitgevers en de leerkrachten. Zo is de persverklaring onduidelijk over de vraag hoe de belangen van de leerlingen – als zelfstandig gewicht in de schaal – zich verhouden tot het belang van de uitgevers.

## 2.1 Vier scenario's

Er wordt veel geschreven over hoe het onderwijs en de technologie zich de komende jaren gaan ontwikkelen. De toepassing van met name kunstmatige intelligentie leek in verhouding tot andere terreinen wat achter te blijven (Woolf *et al.* 2013), maar zelfs de werkzaamheden van de hoogleraar zijn inmiddels bijna binnen het bereik van de technische mogelijkheden aanbeland:<sup>10</sup>

“The current thinking about the automation of the workplace is that the jobs that require the most creativity will be those that are safest from the robot overlords when they come for our jobs. That might be true, but the erudite university professor with the rumpled corduroy jacket and scholarly spectacles might soon be headed for extinction as well.”

Niet iedereen is hiervan overtuigd. Zo geeft Daphne Koller, oprichter van het in MOOC (Massive Open Online Course) gespecialiseerde bedrijf Coursera, aan dat robots niet bijzonder inspirerend zijn en menselijke professoren wel over deze kwaliteiten kunnen beschikken.<sup>11</sup> Waar consensus over bestaat, is dat technologie binnen het onderwijs een grote rol zal spelen. Wij zullen ons hier beperken tot vier toepassingen:

1. robotisering;
2. augmented reality;
3. monitoren van personen;
4. data-analyse.

Aan de hand van de fases in het onderwijs (4-6-jarigen, 6-12-jarigen, 12-18-jarigen, 18+-jarigen) worden vier denkbeeldige scenario's geschetst, waar bij iedere fase wordt ingezoomd op ten minste één van de vier hierboven genoemde specifieke technologieën.

### 2.1.1 Robotisering – kleuters<sup>12</sup>

Het spelen en spelenderwijs leren in groep 1 en 2, de vroegere kleuterschool, is vanaf 2028 niet meer in handen van kleutermeesters en -juffen. De kinderen worden niet gebracht naar school, maar de zelfrijdende auto's, in sommige gevallen met GPS-onder-

10 D. Basulto, 'Watch out college professors, the robots are coming for your jobs', *Washington Post* 2 juni 2015.

11 E. Johnson, 'Robots won't replace teachers because they can't inspire us', *Recode* 22 juni 2016.

12 Zie recent bericht waarin Sir Anthony Sheldon van het Wellington College aangeeft dat binnen tien jaar leerkrachten door robots vervangen zijn: J. von Radowitz, 'Intelligent machines will replace teachers within 10 years, leading public school headteacher predicts', *Independent* 11 september 2017.

steunde fietsen en in een enkel geval schoenen, zorgen ervoor dat alle leerlingen om precies 8:30 binnen zijn. Onder begeleiding van de robot worden het eerste halfuur in een kring wetenswaardigheden uitgewisseld, waarbij de robotonderwijzer soms aanvult vanuit de informatie over het reilen en zeilen van de leerlingen waar deze over beschikt. Ook worden er regelmatig uitstapjes gemaakt naar meer algemene aspecten die samenhangen met de individuele avonturen. Gedurende de dag wordt er veel gespeeld, in verschillende samenstellingen (groepen van 2, 3, 6 en 10 leerlingen). De robotonderwijzer begeleidt het proces. Individuele en gezamenlijke leermomenten worden naadloos ingevlochten in de overige activiteiten.

### 2.1.2 *Monitoring – basisschool groep 3-8*

Na de robots van groep 1-2, is er in 2028 in groep 3-8 weer ruimte voor menselijke leerkrachten. Deze zijn 'enhanced', ze worden op allerlei manieren ondersteund door de technologie. Ook lopen er allerlei assistenten rond, dit zijn voornamelijk robots. Deze robots assisteren ook in de observatie. Er worden veel data verzameld tijdens de leerprocessen, onder andere:

- hoe lang doet een leerling over een taak;
- hoe snel wordt een som gemaakt en hoe vaak klopt de uitkomst;
- hoeveel tijd wordt er besteed aan het lezen van een tekst en begrijpt de leerling ook wat er staat;
- wordt er naar de juiste onderwerpen gezocht op internet.

De bovenstaande informatie wordt aangevuld met wat de robots in de klas en op het schoolplein opvangen en waarnemen. Uiteindelijk komt al deze informatie, al dan niet nader geïnterpreteerd, in het leerlingendossier terecht. Het leerlingendossier faciliteert het aanbod van het op de individuele leerling toegesneden onderwijs. Herhaling voor wie herhaling nodig heeft, versnelling voor wie versnelling nodig heeft.

### 2.1.3 *Augmented reality – middelbare school*

Boeken zijn in 2028 enkel nog digitaal beschikbaar. Op de middelbare school wordt lesstof in veel gevallen via augmented reality aangeboden. In plaats van fysieke, gevaarlijke scheikundige proeven wordt gewerkt in een virtueel laboratorium, waar de leerlingen stoffen kunnen mengen die zelfs nog veel gevaarlijker zijn dan de stoffen die de leraar vroeger op school gebruikte in zijn experimenten voor de klas. In de geschiedenisles wordt rondgelopen in het tijdvak waar de betreffende lessen over gaan: de oertijd, de Romeinse tijd, de middeleeuwen, maar ook modernere ervaringen als Auschwitz, Politonele acties, Srebrenica. Hierbij kunnen de leerlingen soms een rol kiezen en andere keren moeten ze een bepaalde rol spelen. Ook in allerlei andere vakken, zoals biologie, natuurkunde, talen, en dergelijke wordt gebruik gemaakt van augmented reality. Zo kunnen dieren van nabij geobserveerd worden en kan er rondgelopen worden in lichamen van allerhande levende wezens, kan de impact van een met een bepaalde snelheid botsend object worden gevolgd en is spreken met bijvoorbeeld Franses, desgewenst in Parijs gesitueerd, mogelijk. Alle activiteiten die plaatsvinden binnen de augmentedrealityomgeving worden gelogd en geanalyseerd.

#### 2.1.4 *Data-analyses en profilering – universiteit*

De overheid bepaalt op basis van de tijdens de eerdere drie onderwijsperiodes (de zojuist beschreven 4-6-jarigen, 6-12-jarigen en 12-18-jarigen) verzamelde, geprofileerde en geanalyseerde informatie welke vervolgopleiding het beste past, of dat wellicht direct gaan werken de voorkeur heeft. Hierbij wordt ook een specifieke onderwijsinstelling voorgesteld, die – op grond van de beschikbare informatie van de leerling alsmede analyses van vergelijkbare studiecarières – het beste past. Deze onderwijsinstelling biedt aan de student vervolgens een top 3 van voor de student meest geschikte studies, wederom naar aanleiding van analyses van relevante karakteristieken van de leerling en van het succes van eerdere leerlingen met de studie. Het collegegeld is afhankelijk van de keuze die de student maakt. De eerste keuze is gratis, bij de tweede keuze is het collegegeld 5.000 euro per jaar, bij de derde keuze 10.000 euro per jaar. Het is niet toegestaan studies buiten de voorgestelde top 3 te volgen. Als een student ten minste gemiddeld een 7 staat, dan valt deze terug in het gratis-segment. Behaalt de student gemiddeld minder dan een 7 dan moet 5.000 euro per jaar betaald worden. Nog slechter presterende studenten hoeven niet op een bindend studieadvies te wachten, maar krijgen maandelijkse scores die een indicatie geven van hoe de zaken ervoor staan.

### 3. **Privacy- en gegevensbeschermingsrecht**

In de voorgaande paragrafen hebben wij met grove penseelstreken geschetst wat er allemaal kan als het gaat om digitalisering in het onderwijs en de toepassing van nieuwe technologieën, die vrijwel alle als gemeenschappelijk kenmerk hebben dat daarmee meer persoonsgegevens over leerlingen, scholieren en studenten beschikbaar komen. En trouwens ook over leraren en docenten, en ouders, en alle anderen die bij het onderwijs betrokken zijn. We voorzien dan dat, behoudens de voorwaarden die daaraan door wet- en regelgeving worden opgelegd, de stap naar *big data predictive analytics* haast vanzelfsprekend is. In elk geval lijken de technische beperkingen niet of nauwelijks daaraan in de weg te staan.

We veronderstellen dat, eufemistisch uitgedrukt, niet iedereen direct heel enthousiast wordt van dit beeld. Er zijn zorgen over wat dit betekent in termen van privacybescherming of zelfontplooiing. Vragen die dan opkomen zijn in hoeverre de privacy- en gegevensbeschermingswetgeving voorziet in beperkingen en waarborgen, of ten minste randvoorwaarden ter bescherming van de persoonlijke levenssfeer van de betrokkenen, dat wil zeggen: de leerlingen, scholieren en studenten, leraren en docenten, ouders etc.

Afhankelijk van de specifieke situatie zijn er allerlei regels en normen waaraan leerlingen en studenten rechtsbescherming kunnen ontlenen tegen de geschetste privacyrisico's. Het gaat dan niet alleen om privacy- en gegevensbeschermingsrechten, maar ook om maatschappelijke betamelijkheids- en zorgvuldigheidsnormen, over goede trouw en wat in redelijkheid over en weer van elkaar mag worden verwacht in de verhoudingen tussen leerlingen, scholieren en studenten of hun ouders tegenover scholen en onderwijsinstellingen. Ook gaat het over het discriminatieverbod en de Wet gelijke behandeling,

en mogelijk ook over het verdedigingsbeginsel of de onschuldpresumptie in den brede, dus niet in strafrechtelijke zin.<sup>13</sup>

Toch ligt het voor de hand om vooral uit te gaan van de regels en voorschriften, rechten en waarborgen die zijn vastgelegd in de privacy- en gegevensbeschermingsregels. In elk geval vinden we daar de meest uitvoerige en gedetailleerde regelingen, zijnde op dit moment nog de Wet bescherming persoonsgegevens (Wbp) en straks, vanaf 25 mei 2018, de Algemene Verordening Gegevensbescherming (AVG) in combinatie met de Uitvoeringswet AVG (UAVG). Daaruit komt dan, is onze inschatting, overwegend betekenis toe aan die regels en uitgangspunten die het meest direct beperkingen opleggen aan het verzamelen en verder verwerken van leerling- en studentgegevens, zijnde:

1. de regels voor de verwerking van bijzondere gegevens, zoals betreffende gezondheid, geloofsovertuiging en etniciteit;
2. de vereisten met betrekking tot de verwerking van gegevens voor andere doelen dan waarvoor deze zijn verzameld (doelbinding);
3. de regels voor geautomatiseerde besluitvorming en profilering;
4. de verplichtingen met betrekking tot transparantie van gegevensverwerkingen, dat wil zeggen de verplichtingen om degenen over wie gegevens worden verwerkt (de zogenoemde betrokkenen) daarover op begrijpelijke wijze te informeren;
5. het beveiligen van informatie en uitgangspunten met betrekking tot privacy-by-design en privacy-by-default of 'gegevensbescherming door ontwerp' en 'gegevensbescherming door standaardinstellingen'.

In aanvulling op bovenstaande kan nog genoemd worden de functionaris gegevensbescherming die voor sommige organisaties, zoals overheidsinstanties, verplicht wordt (artikel 37-39 AVG). De functionaris gegevensbescherming krijgt een centrale rol en moet worden betrokken bij alle aangelegenheden betreffende de verwerking van persoonsgegevens en daarover adviseren en informeren alsmede toezien op de naleving van de AVG. Verder zal in het onderwijs en zeker bij de door ons geschetste toekomstscenario's een privacy impact assessment (of 'gegevensbeschermingseffectbeoordeling', de Nederlandse vertaling van Data Protection Impact Assessment) verplicht worden: "een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, [en die] gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen" (artikel 35 AVG). Ten slotte kunnen worden vermeld gedragscodes en certificeringen (artikel 40-43 AVG) die op een sector, zoals het onderwijs, toegespitste nadere uitwerkingen van gegevensbeschermingsrecht bevatten en daarmee organisaties binnen die sector concrete handvatten bieden over hoe de informatiehuishouding van per-

---

13 Deze paragraaf betreft een bewerking van een onderdeel van een preadvies over een vergelijkbaar thema, dat werd geschreven voor de jaarvergadering van de Vereniging voor Gezondheidsrecht, G.J. Zwenne & W.A.M. Steenbruggen, 'Privacyrisico's en -waarborgen bij het gebruik van big data tegen zorgfraude: een verkenning', *Big Data in de zorg*, Sdu 2017, p. 73-99.



soonsgegevens dient te worden ingericht.<sup>14</sup> Het ontbreekt ons aan ruimte om op deze en andere aspecten van de AVG in te gaan, maar de daarin geïnteresseerde lezer verwijzen wij naar de alleen al in Nederland verschenen uitgebreide literatuur.<sup>15</sup> Voordat we komen tot een duiding van de toekomstscenario's en enkele afsluitende woorden richten we ons, bij wijze van vingeroefening, op de voor de vijf thema's gestelde regels en de daaruit voortvloeiende waarborgen en randvoorwaarden.

### 3.1 Bijzondere gegevens (gezondheid, religie, etniciteit etc.)

Om voor de meesten van ons goed begrijpelijke redenen gelden er extra strenge regels voor het verzamelen en verder verwerken van gegevens betreffende achtereenvolgens:

- ras of etnische afkomst;
- politieke opvattingen en vakbondslidmaatschap;
- religieuze of levensbeschouwelijke overtuigingen;
- genetische gegevens en gezondheidsgegevens;
- biometrische gegevens die worden gebruikt met het oog op de unieke identificatie van iemand (zoals vingerafdruk, irisscan, stemgeluid etc.);
- gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid of oriëntatie;
- gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten.

We moeten daarbij bedenken dat de wetgever van oudsher uitgaat van een ruime opvatting over deze onderscheiden categorieën van bijzondere gegevens. Zo vallen onder gezondheidsgegevens niet alleen gegevens over ziektes, aandoeningen en stoornissen en de behandeling daarvan, maar ook het gegeven dat iemand ziek is zonder dat bekend is wat eraan mankeert.<sup>16</sup> Dit betekent dat een enkele ziekmelding of een ongespecificeerd verzuimbrieffje ('Niels is vanochtend naar de tandarts') al onder het begrip kan vallen. En, hoewel vergezocht, het is ook voorstelbaar dat onschuldige gegevens over geboortjaar of leeftijd, of woonplaats, kunnen worden opgevat als gezondheidsgegevens, aangezien ook dergelijke gegevens inzicht kunnen geven in de gezondheidstoestand van de betrokkene.<sup>17</sup> Onder etniciteitsgegevens vallen ook het geboorteland van iemand, alsook dat van zijn of haar ouders en grootouders, en volgens toezichthouders ook wel de nationaliteit van betrokkenen. En onder gegevens over geloofsovertuiging kunnen ook gegevens over eetgewoonten of dieet vallen. Voor de hand ligt dat als het gaat om varkensvlees of schaaldieren. Ook de gevierde feestdagen geven natuurlijk inzicht in geloofsovertuiging.

<sup>14</sup> Aansluiten bij certificaten en gedragscodes kan zelfs worden aangevoerd "als element om aan te tonen dat de verplichtingen van de verwerkingsverantwoordelijke zijn nagekomen" (artikel 24, lid 3, AVG).

<sup>15</sup> Zie onder andere De Vries & Goudsmit (2015), Verdoodt & Lievens (2017), Schermer (2017), Comijs (2017), Oude Elferink & Reus (2017).

<sup>16</sup> *Kamerstukken II 1997/98*, 25 892, nr. 3, p. 109; Autoriteit persoonsgegevens, De zieke werknemer: beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers, z2015-00774, 23 februari 2016, p. 10; zie ook overweging 35 Preambule AVG.

<sup>17</sup> Een hoge of lage leeftijd zegt immers iets over de kans om last te krijgen van bepaalde kinder- of ouderdomsziektes. En wie woont in Amsterdam of Utrecht heeft veel meer dan een inwoner van Zeeland of Drenthe een risico om klachten te krijgen over fijnstof.

In het onderwijs worden om uiteenlopende redenen bijzondere gegevens verwerkt. Om passend taalonderwijs aan te bieden, bijvoorbeeld, is van belang dat bekend is dat een leerling dyslexie heeft (gezondheidsgegevens) of dat er thuis vooral Frans of Berbers wordt gesproken (mogelijk een etniciteitsgegevens).<sup>18</sup> Een aantekening dat een kind bepaald voedsel niet mag, kan duiden op een allergie (gezondheidsgegevens) of op een geloofsovertuiging of etniciteit, zoals op een herkenbare foto de huidskleur, een hoofddoek of een bril kan blijken (respectievelijk etniciteit, geloofsovertuiging en gezondheidsgegevens).

U kunt zelf ongetwijfeld andere, betere of interessantere voorbeelden bedenken.

Voor dergelijke categorieën van bijzondere gegevens geldt een verwerkingsverbod. Op grond van artikel 9, lid 1, AVG (artikel 16 Wbp) mogen dergelijke gegevens niet worden verwerkt (verzameld, vastgelegd, gebruikt etc.), tenzij sprake is van een *lex specialis* die dit wel uitdrukkelijk toestaat of als er gebruik kan worden gemaakt van een in de verordening of de wet genoemde uitzondering. Deze uitzonderingen vinden we artikel 9, lid 2, onderdeel a t/m j, AVG en in artikel 22 t/m 31 oUAVG (artikel 17 t/m 23 Wbp).

De vraag is dan in hoeverre deze wetgeving toestaat dat onderwijsinstellingen dergelijke bijzondere gegevens mogen vastleggen en verder verwerken. Een eerste inventarisatie levert een gemengd beeld op. In artikel 23, lid 1, onderdeel c, oUAVG (artikel 21, lid 1, onderdeel c, Wbp) vinden we een bepaling op grond waarvan het scholen is toegestaan om gezondheidsgegevens te verwerken voor zover dat met het oog op de speciale begeleiding van leerlingen of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand noodzakelijk is.

Voor gegevens over etniciteit kunnen scholen mogelijk gebruik maken van een uitzondering die de verwerking van dergelijke gegevens toestaat, met het oog op toekennen van een bevoorrechte positie aan personen van een bepaalde etnische of culturele minderheidsgroep teneinde feitelijke nadelen verband houdende met de grond ras of etnische afkomst op te heffen of te verminderen. Daarbij wordt wel als voorwaarde gesteld dat (1) dit voor dat doel noodzakelijk is, (2) de gegevens slechts betrekking hebben op het geboorteland van de betrokkene, van diens ouders of grootouders, dan wel op andere, bij wet vastgestelde criteria, op grond waarvan op objectieve wijze vastgesteld kan worden of iemand tot een minderheidsgroep behoort, en (3) de betrokkene, of zijn of haar ouders, daartegen geen schriftelijk bezwaar heeft gemaakt.

Voor gegevens betreffende geloofsovertuiging biedt artikel 29, lid 1, oUAVG de mogelijkheid om deze te verwerken als dat noodzakelijk is met het oog op de geestelijke verzorging van de betrokkene, tenzij de betrokkene daartegen schriftelijk bezwaar heeft gemaakt.

---

18 College bescherming persoonsgegevens, Rapport definitieve bevindingen inzake onderzoek naar de verwerking van persoonsgegevens door Snappet, 14 juli 2014 met corrigendum van 27 augustus 2014 (z2013-00795).

In andere gevallen kan de verwerking op grond van artikel 9, lid 2, onderdeel a, AVG zijn toegestaan als de uitdrukkelijke toestemming van de betrokken leerling of student is verkregen of, als deze jonger is dan 16 jaar, van zijn of haar ouders. Verwerking kan eventueel ook zijn toegestaan als het desbetreffende bijzondere gegeven door de scholier of student zelf openbaar is gemaakt, bijvoorbeeld via een sociaal netwerk waarmee een student een herkenbare foto van zichzelf verspreidt. Voor de verwerking van die gegevens kan dan gebruik worden gemaakt van de uitzondering van artikel 9, lid 1, onderdeel e, AVG (artikel 23, lid 1, onderdeel b, Wbp).

In andere gevallen biedt de wetgeving welbeschouwd maar één goed bruikbare mogelijkheid om bijzondere gegevens, ondanks het verwerkingsverbod van artikel 9, lid 1, AVG, wel te mogen verwerken. Dat is de uitzondering van artikel 9, lid 1, onderdeel g, AVG (artikel 23, lid 1, onderdeel g, Wbp), die ziet op de gevallen waarin de gegevensverwerking nodig is met het oog op een zwaarwegend algemeen belang, waarbij er passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en ofwel dit bij wet wordt bepaald ofwel door de Autoriteit Persoonsgegevens ontheffing is verleend. Deze door de toezichthouder te verlenen ontheffing is overigens problematisch doordat deze tegenwoordig de eis stelt dat er reeds een wetsvoorstel aanhangig is waarin wordt voorzien in een wettelijke regeling die de verwerking mogelijk maakt.<sup>19</sup>

De verordening biedt daarbij in artikel 89, lid 1 en 2 en artikel 9, lid 2, onderdeel j, AVG (artikel 23, lid 1, onderdeel j, Wbp) de mogelijkheid dat de nationale wetgever of de Uniewetgever voorziet in een uitzondering op het verwerkingsverbod voor wetenschappelijk onderzoek of statistische doeleinden. Daarbij is vereist dat de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de belangen van de betrokkene.<sup>20</sup>

In het licht van het voorgaande lijkt de verwerking van bijzondere gegevens in het onderwijs, en in het bijzonder het gebruik van bigdata-analyses daarbij, behoudens enkele specifieke situaties, eigenlijk alleen goed mogelijk als er sprake is van een wettelijke regeling, waarbij passende waarborgen zijn getroffen.

### 3.2 Doelbinding

Een belangrijk uitgangspunt uit de privacy- en gegevensbeschermingswetgeving is het doelbindings- of doelverenigbaarheidsvereiste. Dit stelt eisen aan de verwerking van alle persoonsgegevens en dus niet alleen aan de verwerking van de bijzondere gegevens die

---

19 Het beleid van de Autoriteit Persoonsgegevens daarover lijkt niet heel consistent. Opvallend is dat in de zaak die uiteindelijk leidde tot ABRvS 3 september 2008, ECLI:NL:RVS:2008:BE9698, AB 2008, 335, door de toezichthouder zelf werd beargumenteerd dat een ontheffing ook kan worden verleend om een pilot mogelijk te maken, zodat aan de hand van de uitkomsten daarvan kan worden besloten om al dan niet een dergelijk wetsvoorstel voor te bereiden. In latere besluiten lijkt de toezichthouder daarvan afstand te hebben genomen, maar zonder uit te leggen waarom.

20 Overweging 52 Preambule AVG.

wij hierboven behandelden. Het verlangt enerzijds in artikel 5, lid 1, onderdeel b, AVG (artikel 7 Wbp) dat persoonsgegevens alleen worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde verzameldoelen en anderzijds, in artikel 5, lid 1, onderdeel b, AVG (artikel 9, lid 2, Wbp), dat deze gegevens, nadat ze zijn verzameld, alleen verder mogen worden verwerkt voor doeleinden die niet onverenigbaar zijn met de doeleinden waarvoor ze zijn verzameld.

Of er sprake is van ‘niet onverenigbaarheid’ wordt bepaald aan de hand van de verwantschap tussen de onderscheiden doeleinden, de gevoeligheid van de gegevens, de gevolgen voor de betrokkenen en of de gegevens al dan niet van de betrokkenen zelf zijn verkregen, en de overige waarborgen die zijn getroffen ter bescherming van de betrokkenen. Daarbij komt, zo blijkt uit artikel 6, lid 4, AVG (artikel 9, lid 2, Wbp), veel gewicht toe aan de redelijke verwachtingen die de betrokkenen hebben met betrekking tot de verdere verwerking van hun gegevens.<sup>21</sup> Voor verwerking voor wetenschappelijke of statistische doeleinden bepaalt de verordening in artikel 5, lid 1, onderdeel b, AVG dat de verdere verwerking met het oog op overeenkomstig artikel 89, lid 1, AVG niet als onverenigbaar met de oorspronkelijke doeleinden wordt beschouwd.

Deze doelverenigbaarheidsvereisten komen in verschillende andere gedaanten terug in de wetgeving. We zien het onder andere in het zogenoemde opslagbeperkingsvereiste van artikel 5, lid 1, onderdeel e, AVG (artikel 10 Wbp) dat verlangt dat gegevens niet langer worden bewaard dan nodig voor het doel waarvoor deze zijn verzameld en in het gegevensminimalisatiebeginsel van artikel 5, lid 1, onderdeel a, AVG (artikel 11 Wbp), op grond waarvan niet meer gegevens mogen worden verzameld en verwerkt dan nodig voor het doel waarvoor deze zijn verzameld.

Voor het doelbindingsvereiste in het algemeen, en voor het opslagbeperkings- en gegevensminimalisatievereiste in het bijzonder, is wel duidelijk dat er op zijn minst sprake is van een gespannen verhouding met de toepassing van bigdata-analyses. Vanuit het perspectief van big data ligt voor de hand om zo veel mogelijk gegevens zo lang mogelijk te bewaren – wie weet levert het nog bruikbare correlaties, patronen en trends op – terwijl deze gegevensbeschermingsvereisten juist erop zijn gericht om over zo min mogelijk gegevens te beschikken. Als zodanig lijken deze vereisten dus vergaande beperkingen op te leggen. Wel voorziet de wet, zoals dat gaat, in een aantal uitzonderingen, maar die lijken in het onderwijs niet heel relevant. Zo kan voorbij worden gegaan aan het doelbindingsvereiste als dat nodig is voor, onder andere, de voorkoming, opsporing en vervolging van strafbare feiten, of gewichtige economische en financiële belangen van de Staat en andere openbare lichamen, of het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van deze gewichtige economische en financiële belangen (artikel 23, lid 1, onderdeel d, e, g en h, AVG). Ook de bescherming van de belangen van de betrokkenen (scholieren, studenten) of de onderwijsinstelling zelf kan een reden zijn om voorbij te gaan aan het doelbindingsvereiste (artikel 23, lid 1, onderdeel i, AVG).

21 Zie overweging 50 Preambule AVG.

Een en ander biedt dus weinig mogelijkheden om in het onderwijs voorbij te gaan aan het doelbindingsvereiste. Voor onderwijsinstellingen die gebruik willen gaan maken van bijvoorbeeld *big data analytics* is dan ook van groot belang dat zij verzamel- en verwerkingsdoeleinden vastleggen die voorzien in dergelijke analyses. Er moet daarbij wel worden voldaan aan de voorwaarden die de wet stelt. Deze verzamel- en verwerkingsdoelen moeten gerechtvaardigd zijn, uitdrukkelijk omschreven én wel bepaald. Het laatste vereiste, het welbepaaldbaarheidsvereiste, verlangt dat de uitdrukkelijk omschreven en gerechtvaardigde verzameldoelen een kader bieden waaraan getoetst kan worden of de gegevens nodig zijn voor die doeleinden of niet. En als we moeten vaststellen dat de verzameldoelen wat dat betreft geen onderscheidend vermogen hebben en eigenlijk alles toelaten, betekent dat dat die onvoldoende welbepaald zijn. Een onderwijsinstelling kan dus niet volstaan met het verzamel- en verwerkingsdoel van ‘analyse doeleinden’, maar zal dat moeten specificeren.<sup>22</sup> Bijvoorbeeld door uiteen te zetten wat men beoogt te bereiken met deze analyse, welke organisaties daarbij nog meer over de gegevens kunnen beschikken etc. Waar het gaat om gegevens die in een heel andere context worden verzameld, zoals wellicht de voor opdrachten of examens behaalde cijfers of een CITO-toets, zal het gebruik ervan niet snel te verenigen zijn met het doelbindingsvereiste. Er zal dan dus gebruik moeten worden gemaakt van een van de uitzonderingen waarin de wet voorziet.

### 3.3 Profilering

Voor bigdata-analyses zijn verder ook de regels voor profilering van belang. We vinden deze regels met zoveel woorden in artikel 22, lid 1 en 2, AVG, die wat dit betreft evenwel voortbouwen op regels die in de daaraan voorafgaande wetgeving werden gesteld voor zogeheten geautomatiseerde besluitvorming (artikel 42 Wbp). Het begrip ‘profilering’ is ruim en omvat, zo blijkt uit artikel 4, onderdeel 4, AVG, elke vorm van geautomatiseerde gegevensverwerking waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd. Het gaat daarbij met name om het analyseren of voorspellen van de beroepsprestaties van de betrokkene, diens economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen.

Een betrokkene heeft op grond van artikel 22, lid 1, AVG, het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem of haar anderszins in aanmerkelijke mate treft. In drie gevallen voorziet artikel 22, lid 2, AVG, in uitzonderingen. Een uitzondering geldt in de volgende gevallen:

- a) Een betrokkene heeft dit recht niet (meer) als de profilering nodig is voor de uitvoering van een overeenkomst met de betrokkene: we kunnen daarbij denken aan de situatie waarin een aanbieder van streaming video-on-demand-diensten op basis van profilering, en met gebruikmaking van bigdata-analyses, aan zijn abonnees bepaalde programma’s of series aanbeveelt.

<sup>22</sup> *Kamerstukken II 1997/98, 25 982, nr. 3, p. 79.*

- b) Als er een wettelijke regeling is die de profilering mogelijk maakt en die voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene. Een voorbeeld zou hier het SyRI-besluit<sup>23</sup> kunnen zijn dat data-analyse ten behoeve van de aanpak van fraude in het sociale domein mogelijk maakt.
- c) En ten slotte, als restcategorie, als de gegevensverwerking voor profileringsdoeleinden gebeurt op basis van de uitdrukkelijke toestemming van de betrokkene, de scholier of student of zijn of haar ouders als deze nog niet 16 jaar is.

Verder is nog relevant dat de verordening bepaalt dat er bij de gegevensverwerking voor profileringsdoeleinden alleen gebruik mag worden gemaakt van bijzondere gegevens, zoals gezondheids- of etniciteitsgegevens, als de betrokken scholier of student of eventueel zijn of haar ouders, daarvoor uitdrukkelijke toestemming heeft gegeven of als er passende maatregelen zijn getroffen ter bescherming van de gerechtvaardigde belangen van die betrokkene. Dit staat in artikel 22, lid 4, jo. artikel 9, lid 2, onderdeel a of g, AVG.

Deze regels zijn streng en zoals we ook al zagen bij de bespreking van de doelbindingsvereisten, voorziet de wetgever dan wel in een aantal uitzonderingen. In dezelfde bepaling als die voorziet in uitzonderingen op het doelbindingsvereiste, artikel 23, lid 1, AVG, is er ook in voorzien dat de nationale wetgever het mogelijk maakt dat wordt voorbijgegaan aan de beperkingen die de wet stelt met betrekking tot profilering. In de oUAVG zien we dat de wetgever voornemens is van deze uitzonderingsmogelijkheid gebruik te maken, maar alleen voor de gevallen waarin er sprake is van geautomatiseerde individuele besluitvorming, anders dan op basis van profilering, die noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of ter uitvoering van een taak van algemeen belang. We moeten dan denken aan besluiten die worden genomen op grond van regelingen die eigenlijk geen enkele beoordelingsruimte kennen, zoals bijvoorbeeld bij het toekennen van toelagen of uitkeringen.<sup>24</sup>

Wat betekent dit voor het gebruik van big- data-analyses in het onderwijs? Het komt ons voor dat er, als het gaat om beslissingen over de afstudeerrichting of opleidingsvariant waarvoor een scholier of betrokkene in aanmerking komt, in vrijwel alle gevallen sprake is van rechtsgevolgen of gevolgen die hem of haar in aanmerkelijke mate treffen. Er is dan, menen wij, geen sprake van uitdrukkelijke toestemming en evenmin van uitvoering van, zeg, een onderwijsovereenkomst, zodat in dat geval alleen een wet een grondslag kan bieden voor het gebruik van bigdata-analyses in het onderwijs.

### 3.4 Transparantie

De privacy- en gegevensbeschermingswetgeving verlangt verder dat de betrokkenen worden geïnformeerd over de verwerking van de hen betreffende persoonsgegevens. Onder de Wbp moeten betrokkenen worden geïnformeerd over de identiteit van degene

<sup>23</sup> Besluit van 1 september 2014 tot wijziging van het Besluit SUWI in verband met regels voor fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens met inzet van SyRI, *Stb.* 2014, 320; zie daarover Zwenne & Schmidt 2016, p. 310 en 339-341.

<sup>24</sup> Zie artikel 30, lid 1, oUAVG en de MvT daarbij, p. 53.

die verantwoordelijk is voor de gegevensverwerking (zgn. ‘verantwoordelijke’) en de doeleinden waarvoor de gegevens worden verwerkt, alsmede ‘nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen (artikel 33, lid 1 t/m 3 en artikel 34, lid 1 t/m 3, Wbp). In het geval de gegevens bij iemand anders dan de betrokkene zelf worden verkregen, behoeft er evenwel niet te worden geïnformeerd, als dat onmogelijk blijkt of een onevenredige inspanning kost (artikel 34, lid 4, Wbp). Evenmin behoeft de betrokkene te worden geïnformeerd als de vastlegging of verstrekking van de gegevens bij of krachtens wet is voorgeschreven. In dat geval moeten betrokkenen desgevraagd wel worden geïnformeerd over dat wettelijk voorschrift (artikel 34, lid 5, Wbp).

Onder de AVG is de regeling niet heel anders. Wel vereisen de nieuwe regels dat betrokkenen uitgebreider en gedetailleerder worden geïnformeerd. Zo moet op grond van artikel 13, lid 2, en artikel 14, lid 2, AVG ook mededeling worden gedaan van de contactgegevens van degene die verantwoordelijk is voor de verwerking, en over klachtmogelijkheden, ontvangers van de gegevens, eventuele doorgiften van gegevens naar landen buiten de EU etc.

Van belang is dat zowel de Wbp als straks de AVG ook verlangen dat, in het geval er sprake is van profilering, de betrokkenen ook mededeling wordt gedaan van ‘de logica die ten grondslag ligt aan de geautomatiseerde verwerking van de hen betreffende gegevens’ (artikel 42, lid 4, Wbp). Wat daaronder precies moet worden verstaan is onduidelijk. Uit de parlementaire geschiedenis van de Wbp kan het voorbeeld worden ontleend van het geval waarbij aan een naam bepaalde gegevens worden toegevoegd op basis van ‘postcodesegmentatie of statistisch onderzoek’ (zeg ‘verhoogd incassorisico’). In zo’n geval kan de betrokkene er aanspraak op maken dat hem wordt medegedeeld welke methoden zijn gebruikt om daartoe te komen. Als het gaat om algemeen toegankelijke kennis geldt dit echter niet. Zo is algemeen bekend dat een levensverzekeraar het overlijdensrisico op kortere termijn van een tachtigjarige hoger inschat dan dat van een veertigjarige. De verzekeraar is niet gehouden daarover nadere uitleg te geven. Dat is anders als het gaat om minder voor de hand liggende verbanden, bijvoorbeeld op grond van eigen ongepubliceerde statistische recherches.<sup>25</sup>

Met een en ander wordt beoogd de betrokkene, over wie persoonsgegevens worden verwerkt, in staat te stellen kennis te hebben van wat er over hem bekend is en wat daarvan de gevolgen kunnen zijn. Evenals bij het doelbindingsvereiste voorziet de wet (artikel 43, onderdeel a t/m e, Wbp) en de verordening (artikel 23, lid 1, onderdeel d, e, g t/m i, AVG), ook hier in uitzonderingen. Het is de vraag echter in hoeverre daarvan gebruik kan worden gemaakt in het onderwijs. Het is misschien niet onvoorstelbaar dat de rechten en vrijheden van onderwijsinstellingen in het geding zijn als bepaalde analyses van leerlingegegevens *niet* mogelijk zijn. Maar erg waarschijnlijk lijkt ons dat niet.

25 *Kamerstukken I 1999/2000*, 25 892, nr. 92c, p. 13.

### 3.5 Beveiliging, privacy-by-design en privacy-by-default

De beschikbaarheid van persoonsgegevens brengt verplichtingen met zich mee. Van degenen die over de gegevens beschikken wordt verlangd dat zij ervoor zorgdragen dat er passende technische en organisatorische maatregelen worden genomen om een op het risico afgestemd beveiligingsniveau te waarborgen. Om te bepalen of deze maatregelen passend zijn wordt onder andere rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig. In de verordening (artikel 32, lid 1, onderdeel a t/m d, AVG) wordt een aantal mogelijke maatregelen genoemd:

- de pseudonimisering en versleuteling van persoonsgegevens;
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingsystemen en diensten te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Enigszins verwant aan deze beveiligingsverplichting zijn de uitgangspunten van privacy-by-design en privacy-by-default, in het Nederlands vertaald als gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen (artikel 25, resp. lid 1 en lid 2, AVG). Het uitgangspunt van privacy-by-design verlangt dat technische en organisatorische maatregelen worden genomen om op doeltreffende wijze uitvoering te geven aan de in de wetgeving vastgelegde beginselen, zoals het gegevensminimalisatiebeginsel, alsmede om de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften en ter bescherming van de rechten van de betrokkenen. Het uitgangspunt van privacy-by-default verlangt dat passende technische en organisatorische maatregelen worden getroffen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Bij privacy-by-default gaat het dan om de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid ervan. De te nemen maatregelen moeten onder andere ervoor zorgen dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

Waar het gaat om het onderwijs besteedt de wetgever nadrukkelijk aandacht aan een ander. De aanleiding was de ophef en verontwaardiging die ontstond toen er sprake van was dat educatieve uitgeverij via Basispoort konden beschikken over gegevens betreffende onder andere leerprestaties van leerlingen op de lagere school (zie ook hoofdstuk 2



van dit preadvies). Het wetsvoorstel *Pseudonimisering*<sup>26</sup> *leerlinggegevens*<sup>27</sup> heeft tot doel, aldus blijkt uit de memorie van toelichting, om een veiliger, betrouwbaarder en meer efficiënte digitale uitwisseling van gegevens door onderwijsinstellingen mogelijk te maken, waarbij zo min mogelijk persoonsgegevens worden gebruikt van leerlingen, deelnemers of studenten (gegevensminimalisatie).<sup>28</sup>

#### 4. Analyse van toekomstscenario's

De in hoofdstuk 2 geschetste scenario's belichten verschillende technologieën, zoals robotica en augmented reality, en trends of ontwikkelingen die daarmee verband houden, zoals datafication en big data. Een rode draad daarin is dat het gebruik van deze toepassingen met zich brengt dat er persoonsgegevens over leerlingen, scholieren en studenten worden vastgelegd en beschikbaar worden gemaakt. Tegenwoordig verwerken vrijwel alle systemen gegevens, veelal zijn deze aangeduid met de prefix 'smart'. Zowel wat aantal gebruikers en frequentie van het gebruik betreft, als de hoeveelheid data die verwerkt worden is de smartphone in dat opzicht prominent. Maar ook iets onschuldigs als een tandenborstel verzamelt informatie over poetstijden, zowel over het moment waarop er gepoetst wordt als de duur van de poetsbeurt. Dit soort gegevens worden dan doorgaans doorgespeeld naar de fabrikant, lang niet altijd met medeweten van de gebruiker ervan. Gevoeliger gegevens betroffen het geval waar de gebruiker van een vibrator ontstemd was over het buiten haar om verzenden van allerlei data over het gebruik. Zij spande een procedure aan, niet zonder succes.<sup>29</sup>

In 2013 waren in Nederland om vergelijkbare redenen slimme tv's in het nieuws, de Autoriteit Persoonsgegevens (toen nog: College bescherming persoonsgegevens) stelde onder andere vast:<sup>30</sup>

“TPVision heeft naar aanleiding van het onderzoek een toestemmingsvraag ingevoerd voor cookies die het kijkgedrag vastleggen, om persoonlijke kijk-aanbiedingen te kunnen doen. Door het ontbreken van volledige en duidelijke informatie is deze toestemming echter niet rechtsgeldig. Voor advertentie-

26 In de AVG wordt in artikel 4, onderdeel 5 pseudonimisering gedefinieerd als “het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;”.

27 Voluit: *Kamerstukken II 2016/17*, 34 741, nrs. 1 t/m 5, Wijziging van diverse onderwijswetten in verband met het pseudonimiseren van het persoonsgebonden nummer van een onderwijsdeelnemer ten behoeve van het bieden van voorzieningen in het kader van het onderwijs en de begeleiding van onderwijsdeelnemers.

28 *Kamerstukken II 2016/17*, 34 741, nr. 3, p. 2.

29 <https://www.forbes.com/sites/janetwburns/2017/03/15/we-vibe-settles-for-3-7m-in-spying-vibrator-data-lawsuit/>. *We-Vibe Settles For \$3.7M In 'Spying Vibrator' Data Suit*.

30 <https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-persoonsgegevens-smart-tv's-verzameld-strijd-met-wet>.

cookies en de cookies waarmee TP Vision het appgebruik en websitebezoek vastlegt, vraagt het bedrijf helemaal geen toestemming.”

Ook in het onderwijs worden data volop geanalyseerd. Aan de Vrije Universiteit wordt bijvoorbeeld geëxperimenteerd met *student analytics*, om studievertraging te signaleren nog voordat die plaatsvindt en de marketingactiviteiten een zekere richting te geven. Zo is geconstateerd dat dames uit het Gooi het best goed doen bij rechten. Voor zover juist, is het de vraag wat je met dergelijke informatie moet. Je moet in ieder geval heel zorgvuldig te werk gaan bij de uitvoering van dergelijke verwerkingen. Die zorgvuldigheid is nu precies ook wat wij als uitgangspunt nemen bij het analyseren van de scenario's.

#### 4.1 Robotisering

Robots zijn tot steeds meer in staat en beperken zich al lang niet meer tot het aan de lopende band indraaien van een schroefje, plaatsen van een autoportier of het betrekkelijk zombie-achtig huizen stofzuigen of gazons maaien. Een sprekend voorbeeld is Alice, de zorgrobot. Deze heeft mensachtige, enigszins kinderlijke, trekjes. Qua communicatie doet ze enigszins denken aan de klassieker Eliza, in de jaren zestig ontwikkeld aan MIT; Eliza maakte furore als therapeut. Het was een AI-programma, dat voor veel informaticastudenten een van de eerste oefeningen is geweest (en mogelijk nog) in het programmeren van (vermeende) intelligentie. De natuurlijke taalverwerking was simpel, maar redelijk doeltreffend.

```
I am the psychotherapist. Please, describe your problems.
Each time
you are finished talking, type RET twice.

I have a terrible headache.

Maybe you should consult a doctor of medicine, I am a psychiatrist.

Okay, I'll do that then.

Can you elaborate on that?

What are you talking about? No I cannot elaborate. See you later.

Why do you say that?

Now you're just talking nonsense!

What makes you believe now I am just talking nonsense?

You are not making any sense.

Perhaps your plans have something to do with this.
```

De zorgrobot Alice is tot veel meer in staat dan het eenvoudige scriptje van Eliza:

Alice: de postcode is 1057 BA

Mevrouw: Dirk Anton

Alice: Niet Dirk, maar Bernard.

Ze kijkt ook mee in fotoboeken en geeft commentaar op de foto's. Vanuit die achtergrond is ons scenario van de kleuterklas in 2028 niet direct onrealistisch.<sup>31</sup> De vraag is natuurlijk of we het willen. Persoonlijk hebben wij onze bedenkingen, maar die beperken we nu tot gegevensverwerking.

Wat doet de robot met de informatie die deze verzamelt? Hij is in staat om tijdens gesprekken eerdere gebeurtenissen, algemene kennis of in andere systemen aanwezige informatie in te vlechten. Dit is een nogal ingrijpende verwerking van gegevens. Het is ook de vraag of combinaties van informatie die een dergelijke robot maakt, altijd even gelukkig zullen zijn in de kleutergroep. Zeker bij zelflerende algoritmes is niet ondenkbaar dat er kennis gedeeld wordt die mogelijk juridisch gedeeld mag worden, maar ethisch, of zo u wilt pedagogisch, beter niet gedeeld had kunnen worden. Bovendien is de vraag of uitgangspunten als doelbinding bij zelflerende algoritmes tot gewenste resultaten leiden.

Verder is een vraag wat de robot met al die informatie doet. Aan welke partijen wordt deze doorgespeeld? Bij een bewerkers- of verwerkersovereenkomst met het bedrijf dat de robots levert, zal het niet altijd eenvoudig zijn de grenzen aan te geven.

Behalve van tevoren nadenken over toelaatbare verwerkingen is het noodzakelijk dat regelmatig de communicatie van de robot en het delen van informatie geëvalueerd worden. Dit geldt bijvoorbeeld ook voor in vertrouwen met de 'leerkracht' (robot) gedeelde informatie. Wie mag dergelijke informatie verkrijgen en onder welke voorwaarden?

## 4.2 Monitoring

Ons scenario van de lagere school ligt het meest dicht aan tegen hoe het op dit moment gaat. Er zijn scholen waar prestaties gelogd worden en resultaten daarvan bijgehouden. Digitalisering in het onderwijs als manier om te oefenen met de stof, is al zo oud als dat er computers zijn. Begin jaren negentig beperkte het Computer Ondersteund Onderwijs (COO) zich nog voornamelijk tot onderzoek, onder andere door de ontwikkeling van Intelligent Tutoring Systems (ITS). De onvermoeibaarheid van dergelijke systemen,

---

31 In werkelijkheid was het niet de zorgrobot Alice die communiceerde, maar een mens die door de ogen van de robot keek. Een moderne variant van de 18e-eeuwse *The Turk*, ook bekend als the *Mechanical Turk* en *Automaton Chess Player*. Bij *The Turk* was het ook niet de machine die schaakte, maar een mens, verborgen voor de toeschouwers. Dat wij het voorbeeld van Alice toch geven is omdat het aanvankelijk wel de bedoeling was de robot automatisch te laten communiceren. De ontwikkeling van *Sophia* komt al erg in de richting van wat met Alice beoogd was, haar ontwikkeling is te volgen via <http://www.hansonrobotics.com/robot/sophia/>: "Sophia is an evolving genius machine. Her incredible human likeness, expressiveness, and remarkable story as an awakening robot. Over time, her increasing intelligence and remarkable story will enchant the world and connect with people regardless of age, gender, and culture."

eindeloos herhalen waar nodig, het analyseren van waar het fout gaat en daar het aanbod op aanpassen, zien we tegenwoordig in geavanceerde toepassingen. Deze worden deels door ouders privé afgenomen, maar ook binnen scholen worden online educatieve pakketten ingezet. Er zijn ook universiteiten waar gemonitord wordt op welke wijze kennis genomen wordt van digitaal ter beschikking gestelde literatuur. Het verhaal gaat dat er studenten in het café zitten met hun tablet en regelmatig pagina's omslaan zonder deze te lezen, de onderwijsinstelling zo de indruk gevend dat er actief gewerkt wordt.

Zoals al gezegd en overigens bekend, is het doel van onderwijs leerlingen kennis en vaardigheden bij te brengen. Het monitoren en analyseren moet daartoe beperkt blijven. Data-analisten zullen ongetwijfeld allerhande niet direct relevante analyses aanbieden, maar de scholen moeten zich beperken tot wat binnen hun taak ligt. Een belangrijke kwestie is ook om na te denken over welke informatie opgeslagen wordt en hoe lang. De neiging bestaat nog al eens om lang nadat, in dit geval vanuit onderwijsperspectief, de relevantie van informatie niet meer aanwezig is toch de informatie te bewaren. Dit staat op gespannen voet met gegevensbeschermingsrecht, gegevens moeten immers slechts zolang bewaard worden als voor het realiseren van het doel waarvoor ze verzameld zijn nodig is. Doelen kunnen natuurlijk creatief worden geformuleerd om een langere tijd over gegevens te kunnen beschikken, maar ook daaraan stelt de wet beperkingen. En ook als rekening wordt gehouden met de ruimere mogelijkheden die er wellicht zijn voor het verwerken van persoonsgegevens voor wetenschappelijke doeleinden, dan nog moet heel kritisch gekeken worden naar in hoeverre het doel ook het belang dient van het leveren van (goed) onderwijs.

### **4.3 Augmented reality**

Computers zijn in staat om nauwgezet en uitgebreid informatie te registreren. Wanneer een docent in bijvoorbeeld een spelsituatie bepaalde voorkeuren, handelingen of anderszins opvallende gedragingen van leerlingen kan vaststellen, is dit redelijk beperkt tot het volgen van tegelijkertijd één of hooguit enkele leerlingen. Anders dan docenten zijn computers in staat om continu van iedere leerling afzonderlijk veel informatie te verzamelen en deze vervolgens te analyseren. De impact bij monitoren door geautomatiseerde systemen is alleen al vanwege de alomvattendheid veel groter. Daar komt bij dat de analyses veel dieper kunnen gaan dan waar mensen toe in staat zijn. Wat moet er met al die bevindingen gebeuren? Opslaan in het leerlingendossier?

Binnen augmented reality van bijvoorbeeld historische gebeurtenissen kan van alles afgeleid worden over de eigenschappen van de leerling. Deze analyses hoeven niet eens juist te zijn, maar zelfs als het klopt, moet een duidelijk onderscheid gemaakt worden tussen welke informatie relevant is en welke informatie niet. We hebben te maken met een leeromgeving en hoewel het technisch mogelijk is iedere leerling binnenstebuiten te keren en tot in detail op allerhande aspecten te scoren, is dat vrijwel zeker niet in lijn met het doel waarvoor informatie verzameld wordt. Althans, dat doel zou in beginsel niet verder moeten strekken dan educatie. Het onderwijs moet zich primair bezighouden met leerlingen kennis en vaardigheden bijbrengen. In het geval er psychoanalyse wordt uitgevoerd is dat voor zover het relevant is voor pedagogische ondersteuning

mogelijk verdedigbaar, maar op het moment dat je dergelijke verwerkingen toelaat, is de kans dat er grenzen overschreden worden die je liever niet over gaat, niet onaannemelijk. Wordt een vinkje gezet bij potentieel crimineel indien geconstateerd gedrag minder normconform is dan gemiddeld? En wie krijgt vervolgens toegang tot die informatie? Alle hulpverleners en docenten, en voor hoe lang, jaren later nog?

Niet uit het oog verloren mag worden dat het bij augmented reality gaat om een gecreëerde wereld. Dat iemand graag wil begrijpen hoe kampbewaarders in concentratiekampen hun rol beleefden, hoeft geenszins te betekenen dat deze leerling verkeerde sympathieën heeft. Dit klinkt vanzelfsprekend, maar het moet niet onderschat worden hoe snel dergelijke analytische vervuiling de systemen binnen kan dringen. De rijkheid aan informatie over al het gedrag binnen augmented reality reikt mogelijk dieper dan het inzicht dat een leerling zelf in zijn functioneren heeft, maar zal lang niet altijd het doel dienen dat beoogd zou moeten worden. Strikte controle op wat bedrijven precies doen met de verzamelde informatie, welke informatie het is en wat voor analyses er plaatsvinden, is daarbij noodzakelijk.

#### 4.4 Data-analyses en profilering

In het voorbeeld van de universiteit komen ten minste twee zaken aan bod. Ten eerste dat er een dossier is van een leerling met veel informatie over zijn schoolloopbaan. Een dergelijk leerlingendossier moet niet uitdijen tot een veelomvattend en allesbeheersend document met daarin allerhande niet direct voor het onderwijs relevante zaken. Er dient kritisch gekeken te worden naar de aanwezige informatie en worden nagegaan in hoeverre de verzamelde informatie ook past binnen het doel waarvoor dergelijke gegevens verwerkt worden. Wat verder in ons voorbeeld naar voren komt, is het op basis van profielen nemen van besluiten.

Er worden in ons 2028-scenario zelfs financiële consequenties verbonden aan studiekeuze. Het lijkt nogal verstrekkend dat de autonomie van personen in zo een sterke mate wordt aangetast. Toch zijn we wel al langzaam op weg daarnaar toe. We schetsten al een voorbeeld van matching, wat in een minder geavanceerde vorm, en niet altijd juist uitgevoerd, al een voorportaal is van de ontwikkeling die zou kunnen uitmonden in het – op basis van profielen – studenten nogal dwingend een bepaalde richting op sturen. Het bindend studieadvies is – anders dan de matching bijvoorbeeld – niet vrijblijvend. Indien je binnen een daarvoor gestelde tijd niet de vastgestelde minimale hoeveelheid studiepunten hebt behaald, moet je in beginsel stoppen met de studie aan de instelling waar je die volgt. Merkwaardig aan dergelijk adviezen is dan weer dat je weliswaar weg moet bij de studie aan de universiteit die je dat advies geeft, maar vervolgens op een andere universiteit weer vrolijk verder kan gaan met dezelfde studie.

Zowel matching als bindend studieadvies zijn maatregelen die ver verwijderd zijn van de zeker tot in de jaren tachtig regelmatig voorkomende eeuwige student. Sinds die tijd zijn uiteenlopende maatregelen betreffende financiering er mede op gericht om studenten hun studies zo snel mogelijk te laten afronden. Resultaten van onderwijs in de vorm van een afgestudeerde student kan een samenleving veel opleveren, maar als studenten

niet afstuderen kost het de samenleving geld zonder dat het wat oplevert. Tegen deze achtergrond worden de genoemde maatregelen vastgesteld. Mogelijk zonder het ons te realiseren zijn wij niet heel ver verwijderd van dwingende studieadviezen en daarmee corresponderende collegegelden, zoals in het door ons geschetste scenario.

Wij zijn hier geen voorstander van, maar mocht het zover komen, dan wordt de zorgvuldige verwerking van gegevens nog belangrijker dan dat nu al is. Het huidige regelgevend kader biedt enige bescherming tegen algoritmes op grond waarvan profielen worden gecreëerd, alsmede algoritmes die vervolgens gebruikt worden om op grond van de profielen op het individu toegesneden besluiten te nemen. Maar als we terugkijken naar de geschetste toekomstscenario's vragen wij ons af of die bescherming voldoende is. Al was het maar omdat er onvoldoende zicht is op wat algoritmes nu precies doen en waarom ze dat doen. Zelfs als dat inzicht er is en de uitkomsten een grote mate van betrouwbaarheid hebben, is het belangrijk dat er uitzonderingen mogelijk blijven. De ervaring leert dat onze samenleving niet goed in staat is om afwijkingen van de algemene regel toe te laten.

In het licht van de te verwachten technologische ontwikkelingen moet hierover nog heel goed worden nagedacht.

## 5. Conclusie

In het inleidende hoofdstuk noemden wij de triade techniek, recht en ethiek. Er zijn mensen die denken dat de mogelijkheden van de techniek grenzeloos zijn en die daarom de vraag naar de technische mogelijkheden (Kan het?) niet echt relevant vinden. Wij zijn minder stellig en denken niet dat alles technisch mogelijk is, ook niet op termijn. Er kan wel veel. Binnen de technische mogelijkheden is het noodzakelijk goed na te denken over het recht (Is het toelaatbaar?) en de ethiek (Is het wenselijk?). Als juristen houden wij ons primair bezig met juridische vragen, maar bij ontwikkelingen zoals wij hier schetsen ontkomen wij er niet aan om ook over de wenselijkheid na te denken. De ethiek kan daarbij zowel een richtsnoer zijn voor de ontwikkeling van toekomstige regulering, als een standaard om bestaande regels kritisch tegen het licht te houden. Meer praktisch is het – zeker gezien de traagheid waarmee juridische regels tot stand komen – niet mogelijk enkel naar het recht te kijken. In voorkomende gevallen zal ook als het recht bepaalde activiteiten toestaat, daar mogelijk toch van afgezien moeten worden vanwege de onwenselijkheid daarvan.

Het doel van onze bijdrage is om het kritisch nadenken over de huidige en toekomstige ontwikkelingen in het onderwijs te stimuleren. Het is van belang daar niet mee te wachten. De ervaring leert dat als de technologie eenmaal is ingevoerd, het lastig is om er niet gebruik van te blijven maken. Wij moeten zien te voorkomen dat we aanbelden in scenario's zoals door ons geschetst of die u mogelijk zelf voor ogen ziet, zonder

zorgvuldig nagedacht te hebben over de toelaatbaarheid (het recht) en de wenselijkheid (de ethiek).<sup>32</sup>

Wij hebben een bijzondere affiniteit met technologie. Echter, hoe mooi de technologie ook is en hoe sprookjesachtig de beloftes van data-analisten kunnen zijn, wij moeten belangrijke menselijke waarden voorop blijven stellen. Het is niet zonder reden dat privacy, en binnen de Europese Unie zelfs gegevensbeschermingsrecht (respectievelijk artikel 7 en 8 Handvest van de Europese Unie), een fundamenteel recht is. Onze menselijke waardigheid bepaalt wie we zijn en we moeten voorkomen dat de praktijk afbreuk doet aan artikel 1 van de Universele verklaring van de Rechten van de Mens: “All human beings are born free and equal in dignity and rights.” Wij worden geboren met rechten en waardigheid en die moeten wij niet uit het oog verliezen. Laten we profiteren van de zegeningen van de techniek, maar binnen de grenzen van het recht en de ethiek.

## 6. Referenties

- Comijs, D. (2017), De bescherming van bijzondere persoonsgegevens in de Uitvoeringswet AVG, *NJB* 3027/1281.
- Cortesi, S. et al. (2014), *Youth Perspectives on Tech in Schools: From Mobile Devices to Restrictions and Monitoring*, Berkman Center Research Publication No. 2014-3.
- Hoen, I.A. & B.A.J. van Lammeren (2016), ‘Privacy van leerlingen in het digitale onderwijs’, *School en Wet* 2016/1, p. 5-11.
- Haduong, P. et al. (2015), *Student Privacy: The Next Frontier - Emerging & Future Privacy Issues in K-12 Learning Environments*, Berkman Center Research Publication No. 2015-12.
- Murray, A. (2015), ‘The value of analogue educational tools in a digital educational environment’, *European Journal of Law and Technology*, Vol. 6, No. 1, 2015.
- Oude Elferink, E. & J.G. Reus, ‘Handhaving van de Algemene Verordening Gegevensbescherming vanuit Nederlands perspectief’, *NTER* 2017/06.
- Pardo, A. & G. Siemens (2014). ‘Ethical and privacy principles for learning analytics’, *British Journal of Educational Technology* 45(3), p. 438-450.
- Prins, C. (2016), ‘De (digitale) scholen zijn weer begonnen’, *NJB* 2016/1560, afl. 30.
- Richards, N.M. & J.H. King (2014), ‘Big Data Ethics’, *Wake Forest Law Review*, 2014.
- Schermer, B.W. (2017), ‘Van meldplicht naar registerplicht: de registratie van verwerkingen onder de AVG’, *Computerrecht* 2017/151.
- Stulpin, A.A. (2015), *Reclaiming ‘The Right to Be Let Alone’: Seeking Transparency & Uniformity in the Unchartered Territory of Student Data Mining*, <https://ssrn.com/abstract=2772619>.
- Verdoodt, V. & E. Lievens (2017), ‘De AVG bekeken vanuit een kinderrechtenperspectief: pluspunten, knelpunten & vraagstukken’, *Computerrecht* 2017/155.

32 Richards & King (2014) geven in de context van big data mooi weer waar het om gaat: “We are building a new digital society, and the values we build or fail to build into our new digital structures will define us. Critically, if we fail to balance the human values that we care about, like privacy, confidentiality, transparency, identity and free choice with the compelling uses of Big Data, our Big Data Society risks abandoning these values for the sake of innovation and expediency.”

- Vos, J. *et al.* (2015), *Privacy in 10 stappen. Een praktische handleiding voor privacy op school*, Zoetermeer: Kennisnet.
- Vries, H. de & M. Goudsmit (2015), 'Voorsorteren op de Algemene Verordening Gegevensbescherming', *NJB* 2016/1077.
- Wolf, B.P. *et al.* (2013), 'AI Grand Challenges for Education', *AI Magazine* (Special issue on Intelligent Learning Technologies), 34(4), p. 66-84.
- Zeide, E. (2016), 'Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs', 8 *Drexel Law Review* 339.