Mr. R.P. Santifort[*]

Naar een meer genuanceerde benadering van 'pseudonimisering' in het privacyrecht

187

Trefwoorden:
pseudonimiseren, hashing, persoonsgegevens, anonimiseren, Breyer, AP, ICO, WP29

In deze bijdrage bespreek ik hoe de uitleg van de definitie 'pseudonimisering' uit de AVG naar mijn mening enige nuance verdient (§ 2), dat deze nuance in lijn is met overweging 26 van de AVG (§ 3) en het *Breyer*-arrest (§ 4). Vervolgens bespreek ik dat de mogelijkheid om iemand te individualiseren (single out) niet betekent dat iemand ook kan worden geïdentificeerd (§ 5). Ook (de huidige utopie van) artikel 11 AVG passeert de revue (§ 6). Ik kom tot de conclusie (§ 7) dat pseudonimisering niet doorslaggevend is voor de kwalificatie van gegevens als persoonsgegevens.

1 Inleiding

Pseudonimisering wordt gezien en veelvuldig toegepast als een adequate beveiligingsmaatregel om persoonsgegevens te beschermen. Zo wordt pseudonimisering expliciet genoemd als (technische) maatregel in artikel 32 lid 1 sub a AVG. Onze eigen Autoriteit Persoonsgegevens (AP) dicht pseudonimisering inmiddels ook niet meer waarde toe dan een loutere 'beveiligingsmaatregel'.[1] Het is echter verdedigbaar dat pseudonimisering onvoldoende is om per definitie identificeerbaarheid dan wel indirecte herleidbaarheid aan te nemen.

Er lijkt een hardnekkige misvatting te bestaan om gegevens die het *proces* van pseudonimisering hebben ondergaan *altijd* als persoonsgegevens te blijven beschouwen. Een dergelijke uitleg laat de daadwerkelijke toets om te bepalen of gegevens als persoonsgegevens kwalificeren compleet links liggen en is naar mijn mening niet alleen juridisch onjuist, maar wordt in de praktijk ook wel als belemmering voor innovatie en kwaliteitsonderzoek (in bijvoorbeeld de zorgsector) ervaren.[2] Immers, wanneer de *output* van het pseudonimiseringsproces altijd als persoonsgegevens moet worden beschouwd – voor welke partij dan ook – dan zal ook het (verder) verwerken van die gegevens moeten voldoen aan de AVG. Die verwerking loopt het risico te stranden vanwege het ontbreken van een passende verwerkingsgrondslag[3] of strijd met het doelbindingsvereiste[4]. Ook rechten van betrokkenen moeten dan in volle omvang worden gewaarborgd.[5]

Een onbedoeld effect daarvan lijkt dat de toepassing van artikel 11 AVG (verwerking waarvoor identificatie niet is vereist) onbereikbaar wordt. Op dit moment is het een artikel waar nagenoeg niemand in de praktijk gebruik van maakt. Dat kan in mijn ogen twee oorzaken hebben: of dit artikel is nog (te) onbekend of organisaties durven er simpelweg niet aan. De eerste organisatie die openlijk een beroep doet op artikel 11 AVG – en de uitoefening van bijvoorbeeld het vergeetrecht conform het tweede lid in beginsel uitsluit – moet ik in ieder geval nog tegenkomen. Dit terwijl organisaties die zich bezighouden met bijvoorbeeld direct marketing of wifitracking hier baat bij zouden kunnen hebben. Ik kom hierop terug.

Het is overigens niet mijn bedoeling om tot in detail de technische aspecten van het concept pseudonimisering (in zijn vele verschijningsvormen) volledig te bespreken in dit artikel. Wel doe ik een poging de belangrijkste juridische aspecten van pseudonimisering te benoemen en tegen anonimisering af te zetten in de volgende paragraaf. Wanneer dit artikel een eerste aanzet kan geven voor een hernieuwde discussie over een genuanceerdere opvatting inzake pseudonimisering, dan is mijn doel bereikt.

2 Pseudonimisering

Pseudonimisering wordt over het algemeen gezien als 'nuttige maatregel' voor beveiliging van persoonsgegevens.[6] Ook in geval van wetenschappelijk, historisch of statistisch onderzoek wordt pseudonimisering als adequate beveiligingsmaatregel gezien.[7] Privacyrisico's kunnen door toepassing van pseudonimisering onmiskenbaar in vergaande mate worden gemitigeerd. Door pseudonimisering wordt het immers moeilijker om ge-

---

* **Robbert Santifort is advocaat privacyrecht bij Houthoff. Dit artikel is geschreven op persoonlijke titel.**

1 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens#wat-is-pseudonimiseren-6129 en CBP Richtsnoeren, 'Beveiliging van persoonsgegevens', 1 maart 2013, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_beveiliging_van_persoonsgegevens.pdf.
2 Neem bijvoorbeeld in de geestelijke gezondheidszorg (GGZ): www.parool.nl/nederland/tientallen-miljoenen-later-is-dit-ggz-project-totaal-mislukt~b021ca273/.
3 Artikel 6 AVG.
4 Artikel 5 AVG.
5 Artikel 15-22 AVG.
6 Artikel 32 AVG. Zie ook overweging 26 en 28-29 AVG.
7 Artikel 89 en overweging 156 AVG.

gevens te herleiden tot een identificeerbare natuurlijke persoon.

Veelgebruikte pseudonimiseringstechnieken zijn: encryptie met een geheime sleutel, zogenoemde (salted) hashfuncties en key-hashfuncties met opgeslagen of verwijderde sleutel en tokeniseren.[8] Een voorbeeld is het hashen van klantnummers. Vaak wordt één attribuut (dat uniek is) in een record vervangen door een ander attribuut. Het is een cryptografische bewerking die omkeerbaar en herhaalbaar *kan* zijn.

'Salting' voegt extra beveiliging aan de hash toe. De salt zorgt er namelijk voor dat het niet mogelijk is om gehashte gegevens met behulp van een vooraf berekende tabel te kraken, omdat door een willekeurige salt toe te voegen de output hash voor dezelfde input alsnog anders is. Hashing werkt in principe maar één kant op. De input valt alleen te achterhalen door het uitproberen van alle mogelijkheden.[9] Wanneer er meer gegevens worden gehasht in een gegevensset met salting neemt de moeite om de hash te kraken exponentieel toe. Naar mijn mening is het met de huidige stand van de techniek niet altijd aannemelijk dat het lukt de originele gegevens te achterhalen, wanneer gebruik wordt gemaakt van de meest geavanceerde salted hashing algoritmes.[10]

De verwerkingsverantwoordelijke kan additioneel maatregelen treffen om de herleidbaarheid van persoonsgegevens verder te beperken, bijvoorbeeld door de salted hashing uit te laten voeren door een derde (Trusted Third Party) die als enige over het hashing algoritme beschikt. Het is dan de vraag of met dergelijke maatregelen het nog wel redelijkerwijs te verwachten is dat de betrokkene kan worden geïdentificeerd.[11] Bij deze vraag sta ik nader stil en geef ik een voorbeeldcasus in § 4.

2.1 *De AVG*

De AVG geeft in artikel 4 sub 5 een definitie van het begrip 'pseudonimisering':

'(…) 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.'

Pseudonimisering betreft conform de hierboven weergegeven definitie een *proces* van gegevensverwerking. Een proces dat ertoe leidt dat gegevens niet meer *direct* aan een betrokkene kunnen worden gekoppeld. Daarvoor zijn aanvullende gegevens nodig. Die aanvullende gegevens moeten apart worden bewaard. Technische en organisatorische maatregelen moeten worden toegepast om te voorkomen dat de gegevens kunnen worden herleid naar een natuurlijke persoon. *Indirecte* identificatie is dus in beginsel nog wel mogelijk met behulp van die aanvullende gegevens. De definitie lijkt te suggereren dat de betreffende gegevens aan het begin en het einde van het pseudonimiseringsproces nog als persoonsgegevens te kwalificeren zijn.

In de AVG is geen definitie van 'anonimiseren' gegeven. In overweging 26 AVG wordt slechts genoemd dat gegevensbeschermingsbeginselen niet van toepassing te zijn op anonieme gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is. De AVG heeft derhalve geen betrekking op de verwerking van dergelijke anonieme gegevens.

2.2 *WP29: pseudonimiseren versus anonimiseren*

Hoewel beide technieken gelijkenissen vertonen, worden anonimisering en pseudonimisering benaderd als twee verschillende technieken waarmee gegevens onherleidbaar dan wel niet direct herleidbaar kunnen worden gemaakt. Geanonimiseerde gegevens vormen daarmee het tegenovergestelde van persoonsgegevens. Anonimisering is volgens de Europese Article 29 Working Party (WP29; nu European Data Protection Board (EDPB)) in beginsel onomkeerbaar.

WP29 heeft zich in 2014 (Advies 5/2014) over anonimiseringstechnieken vrij expliciet uitgesproken over pseudonimisering in de context van Richtlijn 95/46/EG:

'Pseudonimisering mag niet worden gezien als synoniem van anonimisering. Pseudonimisering beperkt louter de koppelbaarheid van een dataset aan de oorspronkelijke identiteit van een betrokkene, en is bijgevolg een nuttige maatregel om gegevens te beveiligen.'[12]

---

8 Artikel 29-werkgroep, Advies 5/2014 over anonimiseringstechnieken van 10 april 2014, WP216, p. 23-26 en Advies 4/2007 over het begrip 'persoonsgegevens' van 20 juni 2007, WP136, p. 18-19. Zie ook G-J. Zwenne, in: *Tekst & Commentaar Privacy- en telecommunicatierecht*, art. 4 AVG (Definities), aant. 5.

9 Zie ook: V.I. Laan & A. Rutjes, 'Privacy-issues bij blockchain: hoe voorkom of minimaliseer je die?', *Computerrecht* 2017/253, p. 368.

10 Anders: Artikel 29-werkgroep, Advies 5/2014 over anonimiseringstechnieken van 10 april 2014, WP216, p. 23: 'Hashfunctie: deze functie retourneert voor een invoer van willekeurige omvang (één enkel attribuut of een verzameling van attributen) een uitvoer met vaste grootte, en kan niet worden teruggedraaid. (…) Is het bereik van invoerwaarden van de hashfunctie echter bekend, dan bestaat de mogelijkheid de hashfunctie opnieuw daarop toe te passen (replay-aanval) om de juiste waarde voor een specifieke record af te leiden. (…) Door gebruik te maken van een salted-hashfunctie (…), verkleint de kans dat de invoerwaarde wordt herleid. Toch blijft het met redelijke middelen mogelijk de oorspronkelijke attribuutwaarde terug te rekenen die verborgen zit in het resultaat van de salted-hashfunctie (…).'

11 CBP Richtsnoeren, 'Beveiliging van persoonsgegevens', 1 maart 2013, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_beveiliging_van_persoonsgegevens.pdf.

12 Artikel 29-werkgroep, Advies 5/2014 over anonimiseringstechnieken van 10 april 2014, WP216, p. 23.

Pseudonimisering is – aldus WP29 – geen definitief onomkeerbare bewerking en het vergelijken van de gepseudonimiseerde persoonsgegevens met andere, niet in de pseudonimisering betrokken gegevens, kan onder omstandigheden leiden tot (her)identificatie. Volgens WP29 ontneemt pseudonimisering van persoonsgegevens aan die gegevens dan ook niet het karakter van persoonsgegevens.

Al in 2007 opperde WP29 in zijn advies over het begrip 'persoonsgegevens' dat de interpretatie van de definitie van persoonsgegevens niet onnodig moet worden beperkt en in het oog gehouden moet worden dat er aanzienlijke ruimte is voor een flexibele toepassing van de regels over gegevensbescherming op gegevens. Ook kenmerkte WP29 zogenaamde 'herleidbare gepseudonimiseerde gegevens' als informatie over 'indirect identificeerbare' personen en werd gesteld dat de regels uit de Richtlijn 95/46/EG weliswaar van toepassing zijn bij de verwerking van dergelijke informatie, maar 'soepeler [worden] toegepast dan bij de verwerking van informatie over direct identificeerbare personen'.[13] Aannemelijk is dat WP29 hier onder meer doelde op het nemen van minder vergaande additionele beveiligingsmaatregelen.

WP29 acht het dan ook allesbehalve een eenvoudige opgave een echt anonieme dataset te creëren met behoud van zo veel mogelijk onderliggende informatie als nodig is om het beoogde doel te verwezenlijken. Anonimisering zou volgens WP29 pas bewerkstelligd worden door persoonsgegevens zodanig te verwerken dat elke mogelijkheid tot identificatie van betrokkenen onherroepelijk wordt uitgesloten. Anonimisering moet anders gezegd even permanent zijn als uitwissing van de gegevens. Ik vraag mij af of de Uniewetgever het ook zo absoluut voor ogen zou staan.[14]

In genoemd Advies 5/2014 bespreekt WP29 voorts de belangrijkste anonimiseringstechnieken, zoals randomisatie, aggregatie en generalisatie. Daarbij moest de verwerkingsverantwoordelijke volgens WP29 rekening houden met diverse factoren en moet worden gekeken naar 'alle middelen waarvan mag worden aangenomen' dat zij 'redelijkerwijs' door de verwerkingsverantwoordelijke – dan wel door enige andere derde – in te zetten zijn om een persoon te identificeren. Anonimisering strekt, aldus WP29, tot verdere verwerking van persoonsgegevens en moet als zodanig beantwoorden aan het verenigbaarheidsvereiste door recht te doen aan de wettelijke grondslagen en omstandigheden van de verdere verwerking.

De door WP29 besproken anonimiseringstechnieken worden telkens getoetst aan drie criteria:

i. de herleidbaarheid, dat wil zeggen de mogelijkheid om een persoon te individualiseren;
ii. de koppelbaarheid, dat wil zeggen de mogelijkheid om records in verband te brengen met een persoon; en
iii. de deduceerbaarheid, dat wil zeggen de mogelijkheid om persoonsgebonden informatie af te leiden.

De lat voor anonimisering wordt door WP29 daarmee behoorlijk hoog gelegd. Een door WP29 geaccepteerde anonimiseringstechniek moet alle drie de bovenstaande voorwaarden doorstaan. Hoewel WP29 in zijn advies open lijkt te staan voor een '*risk-based approach*' en technische issues en risico's inherent aan anonimisering bespreekt, suggereert WP29 ook dat het risico op re-identificatie nagenoeg nul moet zijn.[15] In een advies over ontwikkelingen inzake *internet of things*, stelt WP29 dat gegevens mogelijk zelfs na anonimisering als persoonsgegevens moeten worden beschouwd.[16] De opvatting van WP29 is dus behoorlijk verstrekkend. Hier slaat de flexibele toepassing van de regels inzake gegevensbescherming naar mijn mening toch wel wat door.[17]

Het gaat buiten het bereik van dit artikel om het concept 'anonimisering' in het huidige bigdatatijdperk nader te analyseren, ook al lijkt ook op dit vlak herijking gewenst. Immers, op basis van de vrij rigide (zwart-wit)benadering van WP29 kan men met de huidige eindeloze stroom van nieuwe technologische mogelijkheden nagenoeg alles als persoonsgegevens kwalificeren en dus bijna niks meer als strikt anoniem. Dit lijkt mij ongewenst. De AVG krijgt dan een onbegrensd toepassingsbereik, met allerlei onbedoelde neveneffecten – inclusief overbelaste toezichthouders – van dien.

Het is interessant om te bezien hoe nationale toezichthouders omgaan met het concept pseudonimisering. Ik heb ervoor gekozen om de huidige opvatting van de AP, af te zetten tegen die van de Britse toezichthouder, de Information Commissioner's Office (ICO), een van oudsher actieve(re) toezichthouder met een flink trackrecord. Het is opvallend dat de AP sinds 2015 ineens geheel ongenuanceerd meent dat pseudonimisering slechts een beveiligingsmaatregel is, daar waar de ICO zichtbaar een meer liberale opvatting heeft over pseudonimisering.

2.3 *De AP*

Het College bescherming persoonsgegevens (tot 1 januari 2016 de naam van de Autoriteit Persoonsgegevens) ging er tot eind 2015 van uit dat persoonsgegevens na pseudonimisering geen persoonsgegevens meer vormden.[18] Dit hield in dat de toenmalige Wet bescherming persoonsgegevens niet van toepassing was na pseudonimisering,

13 Artikel 29-werkgroep, Advies 4/2007 over het begrip 'persoonsgegevens' van 20 juni 2007, WP136, p. 19.
14 Vgl. de Nederlandse wetgever in het Wbp-tijdperk: '[Er is niet] vereist dat iedere mogelijkheid de gegevens met betrekking tot personen te gebruiken, is uitgesloten.' *Kamerstukken II* 1997/98, 25892, nr. 3, p. 48.
15 Artikel 29-werkgroep, Advies 5/2014 over anonimiseringstechnieken van 10 april 2014, WP216, p. 23.
16 Artikel 29-werkgroep, Advies 8/2014 over de recente ontwikkelingen op het gebied van internet of things, WP223, p. 12.
17 Artikel 29-werkgroep, Advies 4/2007 over het begrip persoonsgegevens van 20 juni 2007, WP136, p. 5-6.
18 Zie bijvoorbeeld *Kamerstukken II* 2015/16, 32761, nr. 103, p. 3.

althans wanneer aan de volgende vier (4) voorwaarden werd voldaan:

– er wordt vakkundig gebruikgemaakt van pseudonimisering, waarbij de eerste van de twee uitgevoerde versleutelingen van gegevens plaatsvindt bij de aanbieder van de gegevens;
– er zijn technische en organisatorische maatregelen getroffen om herhaalbaarheid van de versleuteling te voorkomen;
– de verwerkte gegevens zijn niet indirect identificerend;
– deze drie voorwaarden worden onderworpen aan periodiek te houden audits.[19]

Toen kwam echter WP29 met zijn genoemde Advies 5/2014. De AP heeft eind 2015 de visie van WP29 in zijn beslissingen en toezichtspraktijk overgenomen.[20] Volgens de AP is pseudonimiseren sindsdien slechts een beveiligingsmaatregel, waarbij persoonsgegevens worden verwerkt zonder dat daarbij duidelijk wordt over welke personen de gegevens gaan. Bij pseudonimiseren van persoonsgegevens kunnen gegevens alleen nog herleidbaar zijn tot een specifieke persoon als er gebruik wordt gemaakt van aanvullende gegevens. De AP adviseert bij pseudonimisering onder meer rekening te houden met informatie uit externe bronnen zoals de Basisregistratie Personen, de Kamer van Koophandel, het Kadaster, de Telefoongids, Facebook en Twitter. En met de ontwikkeling van nieuwe databronnen en -methoden.[21]

Wanneer gegevens volgens de AP 'volledig geanonimiseerd' zijn, is de AVG niet meer van toepassing. Voorts zijn geanonimiseerde gegevens volgens de AP 'gegevens die helemaal geen betrekking meer hebben op individuen. Er mogen bij anonimisering dus géén aanvullende gegevens beschikbaar zijn waarmee iemand alsnog een koppeling kan maken met een specifiek persoon'. Dat gegevens helemaal geen betrekking meer mogen hebben op individuen is naar mijn mening te kort door de bocht en dus onjuist. Hier lijkt de AP haar visie in *Bluetrace* gewoon door te trekken.[22]

Bovengenoemde inkeer van de AP ten aanzien van pseudonimisering is overigens niet de eerste. Zo was de AP in 2001 nog van mening dat een IP-adres niet altijd een persoonsgegeven is.[23] Zwenne beschrijft op lezenswaardige wijze dat het CBP er zes jaar later ineens van uitging dat een IP-adres hoe dan ook kwalificeert als persoonsgegeven, omdat wordt verondersteld dat daarmee een individuele internetgebruiker kan worden onderscheiden van andere gebruikers. Voor het CBP maakte het daarbij niet uit dat onbekend is wie deze internetgebruiker is.[24] Gelet op bovengenoemd statement lijkt de AP nog niet om wat betreft de singling-out-discussie (§ 5). Dat de inkeer van de AP ten aanzien van pseudonimisering best wat nuance verdient bespreek ik hierna.

2.4 *De ICO*

Opvallend is dat de definitie van pseudonimisering in de AVG afwijkt van andere in het veld gebruikte definities. Zo bezigde de ICO al in 2012 in zijn *Anonymisation: managing data protection risk code of practice* de volgende definitie van pseudonimisering:

'The process of distinguishing individuals in a dataset by using a unique identifier which does not reveal their "real world" identity.'[25]

De ICO stelt zich op het standpunt dat het proces van pseudonimisering wel tot anonieme gegevens kan leiden op individueel niveau van de betrokkene.[26] Hoewel de ICO erkent dat gepseudonimiseerde gegevens een groter privacyrisico met zich brengen dan strikt anonieme gegevens, overwoog zij namelijk:

'This does not mean though. That effective anonymization through pseudonymisation becomes impossible.'[27]

Met de komst van de AVG is de ICO niet van dit standpunt afgeweken.[28] De vraag of er sprake is van persoonsgegevens hangt af van hoe moeilijk het is om een pseudoniem naar een natuurlijke persoon te herleiden:

'Personal data that has been pseudonymized – e.g. key-coded – can fall within the scope of the GDPR depending

19 CBP, Advies pseudonimisering risicoverevening, 6 maart 2007.
20 Zie bijvoorbeeld de brief van het CBP aan de NZa van 26 november 2015 over de gepseudonimiseerde persoonsgegevens uit het Diagnose Behandelcombinatie(DBC)-informatiesysteem.
21 *Kamerstukken II* 1998/99, 25892, nr. 13, p. 2. Zie ook CBP, Onderzoeksrapport KPN en XS4ALL, Openbare versie Rapport definitieve bevindingen, 20 juni 2016, https://autoriteitpersoonsgegevens.nl/sites/default/files/01_onderzoek_kpn_xs4all.pdf.
22 Zie: CBP, 13 oktober 2015, z2014-00944, 'Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace', waarin het CBP stelt dat slechts vereist is dat de gegevens 'ervoor zorgen dat een bepaald persoon kan worden onderscheiden van anderen wanneer gegevens' en dat wanneer gegevens 'in verband kunnen worden gebracht met een bepaalde persoon', het indirect identificerende persoonsgegevens betreffen, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapport_db_bluetrace.pdf.
23 https://autoriteitpersoonsgegevens.nl/nl/nieuws/een-ip-adres-niet-altijd-een-persoonsgegeven-%C2%A0.
24 G-J. Zwenne, 'Nog enkele opmerkingen over IP-adressen en persoonsgegevens, identificeerbaarheid en "single-out"', *P&I* 2015, afl. 6, p. 219.
25 Information Commissioner's Office, 'Anonymisation: managing data protection risk code of practice' (Wilmslow, November 2012), https://ico.org.uk/media/1061/anomymisation-code.pdf. Idem: the Anonymisation Decision-Making Framwork: 'A technique where direct identifiers are replaced with a fictitious name or code that is unique to an individual but not itself directly identify them'.
26 Information Commissioner's Office, 'Anonymisation: managing data protection risk code of practice' (Wilmslow, November 2012), https://ico.org.uk/media/1061/anonymisation-code.pdf, p. 7.
27 ICO, Anonymisation: managing data protection risk code of practice (Wilmslow, November 2012), https://ico.org.uk/media/1061/anonymisation-code.pdf, p. 21.
28 ICO, 'Overview of the General Data Protection Regulation (GDPR)', https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/.

on how difficult it is to attribute the pseudonym to a particular individual.'[29]

Als herleidbaarheid door bijvoorbeeld key-coding of onomkeerbare hashing te ingewikkeld is of – met andere woorden – redelijkerwijs niet te verwachten is, dan zouden de betreffende gegevens ook buiten de scope van de AVG kunnen vallen. Een en ander is vanzelfsprekend altijd afhankelijk van de specifieke omstandigheden van het geval.

2.5 *Anonymisation Decision-Making Framework/ISO*

Ook de Anonymisation Decision-Making Framework geeft een meer liberale definitie van pseudonimiseren, nu deze definitie in het midden laat of een individu identificeerbaar is:

'A technique where direct identifiers are replaced with a fictitious name or code that is unique to an individual but does not itself directly identify them.'[30]

En zo zijn er nog meer definities die in het veld worden gebruikt om het proces van pseudonimiseren te duiden. Neem bijvoorbeeld de definitie uit de recente ISO 25237:2017-standaard voor 'Pseudonymization in Health Informatics':

'(…) particular type of de-identification that both removes the association with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms.'

De AVG specificeert niet welke technieken moeten worden gebruikt, zolang er maar een proces van pseudonimisering wordt toegepast. Het verschil in de definities van de AVG en de ICO bestaat eruit dat de definitie van de ICO neutraal is over de uitkomst van het proces van pseudonimisering. Is het echter in dit verband de bedoeling geweest van de Europese wetgever om wel iets over de uitkomst van dit proces te zeggen? Ook verdedigbaar is dat het standpunt van de ICO niet per se in conflict is met de definitie van pseudonimisering in de AVG. Uitleg door de hoogste Europese rechter zou hier zeker welkom zijn.

In dit bigdatatijdperk komt de benadering van de ICO meer toekomstbestendig voor. Anders zal met de alsmaar voortschrijdende technologische mogelijkheden het persoonsgegevensbegrip blijven uitdijen. Dat er gebruik wordt gemaakt van een proces van pseudonimisering hoeft nog niets te zeggen over het resultaat van dat proces. Daarvoor blijft de toets van overweging 26 AVG relevant.

3 Overweging 26 AVG

Overweging 26 van de AVG luidt als volgt:

'De beginselen van gegevensbescherming moeten voor elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon gelden. Gepseudonimiseerde persoonsgegevens die door het gebruik van aanvullende gegevens aan een natuurlijke persoon kunnen worden gekoppeld, moeten als gegevens over een identificeerbare natuurlijke persoon worden beschouwd. Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken. Om uit te maken of van middelen redelijkerwijs valt te verwachten dat zij zullen worden gebruikt om de natuurlijke persoon te identificeren, moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen. De gegevensbeschermingsbeginselen dienen derhalve niet van toepassing te zijn op anonieme gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is. Deze verordening heeft derhalve geen betrekking op de verwerking van dergelijke anonieme gegevens, onder meer voor statistische of onderzoeksdoeleinden.'

Deze Nederlandse vertaling van overweging 26 AVG spreekt (naar mijn mening ten onrechte) in de tweede volzin van 'gepseudonimiseerde persoonsgegevens' in plaats van 'persoonsgegevens die pseudonimisering hebben ondergaan'. Dat is niet zo in de Engelse versie van overweging 26 AVG, waar slechts wordt gesproken over 'persoonsgegevens' ('personal data'). Het kan niet de bedoeling zijn om 'gepseudonimiseerde persoonsgegevens' als aparte categorie persoonsgegevens te behandelen. Daar is geen enkele juridische basis voor.[31]

Uit overweging 26 AVG volgt de doorslaggevende test om te bepalen of een natuurlijke persoon identificeerbaar is en dus of een bepaalde dataset wel of niet als persoonsgegevens is te kwalificeren. Tijdens de ontwerpfase van de AVG heeft (ook hier) de ICO zich kritisch over deze overweging uitgelaten (toen nog overweging 23):

'In our view there should be a single definition of "personal data". Therefore it is welcome that "pseudonymous data" is no longer treated as a separate category of per-

29 Zie vorige noot.
30 Mark Elliot e.a., 'The Anonymisation Decision-Making Framework' (UKAN, 2016), p. 15, https://ukanon.net/wp-content/uploads/2015/05/The-Anonymisation-Decision-making-Framework.pdf.
31 Mourby e.a., 'Are "pseudonymised" data always personal data? Implications of the GDPR for administrative data research in the UK', *Computer Law & Security Review*, Vol. 34, Issue 2, p. 222-233, www.sciencedirect.com/science/article/pii/S0267364918300153.

sonal data. However, pseudonymisation should only be relevant as a privacy enhancing technique – for example in relation to data minimisation or security. It would be better not to try to define pseudonymisation in the context of the definition of personal data.

As it stand, the relevant Recital 23 is confusing. It says that pseudonymous data should be considered as information on an identifiable natural person – this implies all pseudonymous data whoever it is held by. However, the relevant Recital's new reference to the likelihood of identification presumably means that some pseudonymous data would be personal data whilst other pseudonymous data would not be, depending on the likelihood of the relevant identifying information being added to the pseudonymous information.'[32]

De ICO is in lijn met haar eerdergenoemde standpunten dus van mening dat gegevens die pseudonimisering hebben ondergaan, niet als persoonsgegevens hoeven te kwalificeren. Ook andere schrijvers hebben zich over de formulering van overweging 26 negatief uitgelaten.[33] Het feit dat de Europese wetgever de in 2013 voorgestelde terminologie 'gepseudonimiseerde gegevens' niet in de definitieve Engelse versie van de AVG heeft opgenomen, wijst erop dat besloten is om een dergelijke categorie niet in te voeren.[34] De definitie van persoonsgegevens uit artikel 4 lid 1 AVG wordt met overweging 26 AVG dan ook niet verbreed, laat staan dat er een aparte categorie persoonsgegevens wordt geïntroduceerd. De discussie over pseudonimisering is in de finale versie van overweging 26 AVG niet beslecht en wellicht heeft de Nederlandse tekst van de overweging het daarom abusievelijk over 'gepseudonimiseerde persoonsgegevens'. Pseudonimisering is echter onvoldoende om aan te nemen dat per definitie sprake is van identificeerbaarheid dan wel indirecte herleidbaarheid van gegevens.

Een dergelijke opvatting doet afbreuk aan de doorslaggevende test van overweging 26 AVG. Om te bepalen of een natuurlijke persoon identificeerbaar is, moet conform overweging 26 AVG rekening worden gehouden met 'alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren'. Selectietechnieken (singling out) worden hierbij als voorbeeld genoemd.

Relevant is hier de discussie over de vraag of voor de kwalificatie van persoonsgegevens onder de AVG de zogenoemde 'absolute' (of 'objectieve') dan wel 'relatieve' leer moet worden toegepast. De absolute leer beschouwt gegevens als identificeerbaar wanneer een partij (of dit nu de verwerkingsverantwoordelijke of een willekeurige, onbekende derde is) in staat is om de betrokkene te identificeren. Onder deze leer kwalificeren gegevens veel sneller dat persoonsgegevens. De relatieve leer beschouwt de middelen die de verwerkingsverantwoordelijke redelijkerwijs ter beschikking staan als juridisch relevant, waarbij wel de mogelijkheid wordt opengelaten dat de gegevens eerst zijn opgevraagd bij een derde.[35] Bij de bespreking van het *Breyer*-arrest sta ik nader stil bij de absolute versus de relatieve leer.

Wat zijn dan de middelen redelijkerwijs waarvan te verwachten valt dat zij zullen worden gebruikt om de natuurlijke persoon te identificeren? Hiervan zegt overweging 26 dat rekening moet worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen. Naar mijn mening geeft deze opsomming van objectieve factoren echter geen uitsluitsel over de toepassing van de absolute dan wel relatieve leer.[36] Er hoeft geen sprake te zijn van persoonsgegevens als de betrokken personen niet of slechts met disproportionele aanwending van geld, mankracht of middelen kunnen worden achterhaald. In zulke gevallen is identificatie niet te verwachten en is de AVG derhalve niet van toepassing.[37]

Context kan dus een cruciale rol spelen, zoals ik zal bespreken in het kader van het *Breyer*-arrest. Het blijft ook de vraag hoe de test van overweging 26 AVG zich verhoudt tot de ogenschijnlijk zeer rigide benadering van WP29 over anonimiseringstechnieken uit het tijdperk van Richtlijn 95/46/EG. Is deze dan met het *Breyer*-arrest dan wel de AVG achterhaald en moet de strikte uitleg van anonimiseren worden losgelaten? Hier kan een taak voor de EDPB zijn weggelegd om tot herijking te komen.

4 Breyer

Het belang van de doorslaggevende test van overweging 26 is benadrukt door het Europees Hof van Justitie in het *Breyer*-arrest.[38] Dit arrest werd gewezen toen Richtlijn 95/46/EG nog van toepassing was. Over IP-adressen had het Hof zich al eerder uitgelaten, zo ook in zijn arrest *Scarlet/Sabam*.[39] De internetserviceprovider (ISP) in die zaak had zich erop beroepen dat de regels over de bescherming van persoonsgegevens in de weg staan aan het vastleggen van IP-adressen, omdat IP-adressen voor

32 'ICO analysis of the Council of the European Union text of the General Data Protection Regulation', https://ico.org.uk/media/1432420/ico-analysis-of-the-council-of-the-european-union-text.pdf.
33 Leslie Stevens, 'The proposed Data Protection Regulation and its Potential Impact on Social Sciences Research in the UK', [2015] *EDPL* 107.
34 Zie noot 32.
35 V.I. Laan & A. Rutjes, 'Privacy-issues bij blockchain: hoe voorkom of minimaliseer je die?', *Computerrecht* 2017/253.
36 In tegenstelling tot wat Laan en Rutjes lijken te schrijven in hun artikel (zie vorige noot).
37 G-J. Zwenne, in: *Tekst & Commentaar Privacy- en telecommunicatierecht*, art. 4 AVG (Definities), aant. 1.
38 HvJ EU 19 oktober 2016, C-582/14, ECLI:EU:C:2016:779.
39 HvJ EU 2 november 2011, C-70/10, ECLI:EU:C:2011:771.

hem persoonsgegevens zijn. Het Hof gaf de ISP daarin gelijk. Hoewel IP-adressen feitelijk geen pseudoniemen zijn, kunnen deze naar analogie wel zo worden beschouwd.

In het *Breyer*-arrest lag de vraag voor of een websitehouder die dynamische IP-adressen van bezoekers van zijn website vastlegt, terwijl hij zelf niet over het register van de ISP beschikt waarmee hij bezoekers kan identificeren, persoonsgegevens verwerkt. Aanleiding voor deze vraag was de vordering van Breyer, die websites van de Duitse overheid had bezocht en vond dat de overheid niet gerechtigd was zijn IP-adres te bewaren in het kader van *denial-of-service* cyberaanvallen.

In de Duitse rechtsdoctrine was de rechtsvraag al langer onderwerp van discussie, waarbij voorstanders van de absolute leer van mening waren dat uitsluitend relevant is dat er ergens iemand beschikt over identificerende informatie waarmee een betrokkene kan worden geïdentificeerd. Zo ja, dan zijn die gegevens te kwalificeren als persoonsgegevens, ongeacht wie erover beschikt en of diegene toegang heeft tot de identificerende gegevens. Terwijl voorstanders van de relatieve leer het wel degelijk van belang achtten of de verwerkingsverantwoordelijke zelf in staat is de betrokkene te identificeren. Anders gezegd: gegevens die voor de ene partij als persoonsgegeven kwalificeren, hoeven dat voor een andere partij niet te zijn.

De A-G concludeerde in deze zaak tot toepassing van de relatieve leer, aangezien de objectieve leer ertoe zou leiden dat elk soort informatie als persoonsgegeven wordt aangemerkt, hetgeen praktisch niet werkbaar is. Voorts stelde hij dat overweging 26 van Richtlijn 95/46/EC zo moet worden begrepen dat de wetgever met derden enkel diegenen bedoelt van wie, eveneens redelijkerwijs, mag worden aangenomen dat zij degenen zijn tot wie de verantwoordelijke zich voor aanvullende gegevens voor de identificatie zal wenden.

In de overwegingen 42 en 43 van het arrest verwijst het Hof naar de doorslaggevende toets uit overweging 26 Richtlijn 95/46/EC, welke doorslaggevend is voor de kwalificatie van persoonsgegevens. Naar mijn mening kan uit rechtsoverweging 44 van het Hof worden opgemaakt dat het voor deze kwalificatie van persoonsgegevens relevant is welke partij de beschikking krijgt over aanvullende gegevens:

'Dat de extra informatie die nodig is om de gebruiker van een website te identificeren, niet berust bij de aanbieder van onlinemediadiensten, maar bij de internetprovider van deze gebruiker, lijkt dan ook niet uit te sluiten dat dynamische IP-adressen die worden geregistreerd door deze aanbieder, *voor hem* persoonsgegevens vormen in de zin van artikel 2, onder a), van richtlijn 95/46' (cursivering toegevoegd).

Uiteindelijk koos het Hof voor een redelijke middenweg, zonder expliciet een keuze te maken voor de absolute dan wel de relatieve leer. Het Hof oordeelde dat een dynamisch IP-adres een persoonsgegeven is voor een websitehouder als die de juridische middelen heeft om toegang te verkrijgen tot de identificerende gegevens van de ISP. Voor de Duitse overheid bestonden immers juridische middelen om bij de ISP identificerende informatie te verkrijgen in het geval van cyberaanvallen.[40]

Verdedigbaar is dus dat het Hof – zonder zich uit te spreken voor een relatieve uitleg – het toch relevant vindt wie de beschikking kan krijgen over de aanvullende informatie en de betrokkene vervolgens kan identificeren. Althans, de woorden 'voor hem' uit bovengenoemde overweging kunnen impliceren dat daarmee willekeurige derden worden uitgesloten. Daarmee zou een strikt absolute leer – waarbij de gegevens vervolgens voor elke partij als persoonsgegevens kwalificeren – toch buitenspel kunnen zijn gezet door het Hof.

Het *Breyer*-arrest blijft hoe dan ook belangrijk voor de uitleg van overweging 26 AVG. Als de benadering van het Hof in *Breyer* wordt toegepast op gegevens die pseudonimisering hebben ondergaan, is het naar mijn mening onder omstandigheden mogelijk de gegevens als *de facto* anoniem aan te merken. Een voorbeeld ter illustratie (zie p. 202).[41]

Opmerkelijk genoeg is dit voorbeeld vergelijkbaar met het voorbeeld uit Advies 4/2007 van WP29, waarin WP29 stelt dat een andere dan de oorspronkelijke verwerkingsverantwoordelijke niet noodzakelijk persoonsgegevens verwerkt, door de verwerking zodanig te organiseren dat re-identificatie uitdrukkelijk is uitgesloten en ter voorkoming daarvan passende technische maatregelen zijn genomen.[42] Ik moet bekennen dat dit voorbeeld in schril contrast staat met de besproken strenge uitleg van WP29.

In het op p. 202 aangehaalde voorbeeld bevat de dataset die door Instelling A aan Onderzoekscentrum B wordt verstrekt persoonsgegevens. Na de pseudonimisering door Onderzoekscentrum B is het echter uiterst onwaarschijnlijk dat Onderzoeker C toegang kan of zou hebben tot informatie die haar in staat zou stellen natuurlijke personen te identificeren. De onderzoeksdata die Onderzoeker C verwerkt voor onderzoek kan onder deze omstandigheden niet als persoonsgegevens worden gekwalificeerd. Hetzelfde geldt in beginsel voor de onderzoeksresultaten.

Als de test van 'redelijkerwijs beschikbare middelen' van overweging 26 en *Breyer* wordt toegepast op gegevens

40 HvJ EU 19 oktober 2016, C-582/14, ECLI:EU:C:2016:779, r.o. 47.

41 Een variant op het voorbeeld gegeven in Mourby e.a., 'Are "pseudonymised" data always personal data? Implications of the GDPR for administrative data research in the UK', *Computer Law & Security Review*, Vol. 34, Issue 2, p. 222-233, www.sciencedirect.com/science/article/pii/S0267364918300153.

42 Artikel 29-werkgroep, Advies 4/2007 over het begrip 'persoonsgegevens' van 20 juni 2007, WP136, p. 20-21.

Instelling A verstrekt persoonsgegevens in een dataset aan Onderzoekscentrum B, voor gebruik voor onderzoeksdoeleinden. Onderzoekscentrum B wil onderzoeksdata verstrekken aan Onderzoeker C, maar wil geen persoonsgegevens delen.

Onderzoekscentrum B laat bepaalde 'unieke identifiers' pseudonimiseren door middel van salted hashing door een *Trusted Third Party* (TTP) en aggregeert andere (niet-noodzakelijke) data in de dataset. Het algoritme tot deze unieke identifiers wordt beheerd door de TTP. Technische en organisatorische maatregelen worden toegepast om te voorkomen dat het algoritme voor een derde beschikbaar is en de unieke identifiers weer aan de dataset (output) worden gekoppeld.

Onderzoeker C heeft toegang tot de output dataset met onderzoeksdata in een beveiligd lab van Onderzoekscentrum B. Onderzoeker C heeft een accreditatieopleiding bij Onderzoekscentrum B afgerond, geen telefoon of tablet mee in de ruimte waar C met de dataset werkt en de pc waarop C werkt is niet aan een netwerk gekoppeld. Daarnaast is een geheimhoudingsovereenkomst van toepassing. Onderzoeksresultaten worden gecontroleerd voordat deze Onderzoekscentrum B verlaten.

Onderzoeker C heeft verder geen enkele relatie met instelling A dan wel Onderzoekscentrum B. Tot unieke identifiers heeft C dus geen toegang. C beschikt dus niet over middelen waarmee zij redelijkerwijs de onderzoeksdata kan herleiden en natuurlijke personen kan identificeren. De unieke identifiers bestaan echter wel en in theorie is herleiding niet onmogelijk. De ontkoppeling van unieke identifiers is technisch niet per definitie onomkeerbaar.

die het proces van pseudonimisering hebben ondergaan, zou het dus onder omstandigheden mogelijk moeten zijn om van *de facto* anonieme gegevens te spreken wanneer deze gegevens worden verstrekt (of ter beschikking worden gesteld) aan een derde partij. Uit *Breyer* volgt immers dat relevant blijft wie redelijkerwijs de beschikking heeft over de (juridische) middelen waarvan te verwachten is dat ze worden ingezet, om te bepalen of gegevens herleidbaar zijn tot individuen.

5 Singling out

Een aan pseudonimisering (en anonimisering) relaterend begrip is het gebruikmaken van selectietechnieken oftewel het kunnen *individualiseren* van een persoon (*singling out*). Immers, bepaalde vormen van pseudonimisering maken het mogelijk om een individu in een database te onderscheiden (en te volgen). Individualiseren is het tegenovergestelde van generaliseren en betreft het kunnen aanwijzen, van anderen onderscheiden en afzonderen van een bepaalde persoon. Dit kan bijvoorbeeld aan de hand van een pseudoniem (als unieke identifier).

Voor bepaalde vormen van onderzoek is het vaak zelfs noodzakelijk om een individu door een database te kunnen volgen. Zodoende kunnen bepaalde patronen worden herkend, wat weer maakt dat resultaten van onderzoek bepaalde zeggenschap krijgen. Om zulke valide gegevens over patronen te verkrijgen is het dan ook noodzakelijk om individuen te kunnen onderscheiden.

Er is veel discussie geweest of singling out als zodanig zou leiden tot identificatie. Dit in verband met verschillende adviezen, richtsnoeren en oordelen van WP29 en (toen) het CBP.[43] Volgens WP29 was namelijk de mogelijkheid om iemand te onderscheiden van anderen (single out) voldoende om te kunnen spreken van identificatie.[44] WP29 doelde daarbij echter in het bijzonder op IP-adressen of MAC-adressen, waarmee apparaten op internet worden aangeduid. Met dergelijke 'device identifiers' kunnen internetgebruikers worden gevolgd en vervolgens worden ingedeeld aan de hand van sociaaleconomische, psychologische, filosofische of andere criteria en kunnen bepaalde beslissingen aan hun worden toegeschreven. Daarop zou volgens WP29 bij uitstek het privacyrecht van toepassing moeten zijn.

In de overwegingen van de Engelse tekst van de AVG wordt eenmaal de term 'singling out' gebruikt. Zoals hierboven benoemd is dit in de Nederlandse versie vertaald als 'selectietechnieken'. Het wordt echter *alleen* als voorbeeld genoemd van een middel dat *kan* bijdragen aan het identificeren van een natuurlijke persoon. Het is onjuist om de mogelijkheid van *singling out* te beschou-

43 Artikel 29-werkgroep, Advies 4/2007 over het begrip 'persoonsgegevens' van 20 juni 2007, WP136. Vgl. ook HvJ EU 24 november 2011, C-70/10 (*Scarlet/Sabam*), waaruit de conclusie dat IP-adressen als unieke identifiers altijd persoonsgegevens zijn zou volgen. En CBP, 'GeenStijl IP-checker op Geen-Commentaar', 27 oktober 2008 (z2008-01174). Zie ook CBP Richtsnoeren, 'Publicatie van persoonsgegevens op het internet', 11 december 2007, p. 19.

44 Artikel 29-werkgroep, Advies 4/2007 over het begrip 'persoonsgegevens' van 20 juni 2007, WP136, p. 17.

wen als zelfstandig element leidend tot identificatie. Een natuurlijke persoon individualiseren is niet hetzelfde als identificeren. In deze zin pleit bijvoorbeeld Zwenne tegen oprekking van het persoonsgegevensbegrip.[45]

Het uitgangspunt dat singling out zelfstandig tot identificeerbaarheid zou leiden, is terug te vinden in een amendement bij de AVG.[46] Ten tijde van de behandeling in het Europees Parlement van de AVG werd namelijk voorgesteld om de betrokkene te definiëren als 'a natural person who can be identified or singled out'.[47] Uiteindelijk zijn de woorden 'or singled out' als aparte voorwaarde naast identificeerbaarheid in de definitie van de betrokkene geschrapt in de AVG. In de General Approach van de Raad van 15 juni 2015 komt de term dan ook niet meer voor.[48]

Zelfs in de Tweede Kamer was fel verzet tegen dit uitgangspunt, blijkens de opmerking van de bewindspersoon dat 'er geen enkele steun [is] voor het verder verfijnen van het begrip "persoonsgegevens" met categorieën als "singling out"'.[49] Daarmee lijkt zowel de Uniewetgever als de Nederlandse wetgever afstand te hebben willen nemen van de gelijkstelling van identificatie en singling out als zelfstandig constitutief element voor identificeerbaarheid.

Een en ander sluit aan bij het genoemde *Breyer*-arrest. Hoewel dit arrest niet direct ingaat op het fenomeen singling out en is uitgesproken onder Richtlijn 95/46/EG, kan er nog steeds uit worden afgeleid dat (de aanwezigheid van) een unieke identifier (het dynamische IP-adres) op zichzelf niet maakt dat er sprake is van persoonsgegevens in de zin van de AVG. Het dynamische IP-adres kon immers worden gebruikt om een individu te volgen over het internet, maar dat maakte voor de kwalificatie van persoonsgegevens als zodanig niet uit.

(Dynamische) IP-adressen zouden dus niet zonder meer, maar mogelijk wel in combinatie met andere gegevens, ertoe kunnen leiden dat een natuurlijke persoon wordt geïdentificeerd. Het is daarbij niet relevant of de identificatie daadwerkelijk plaatsvindt. Een slechts hypothetische mogelijkheid om iemand te identificeren is evenwel niet voldoende om die persoon als identificeerbaar te beschouwen. Als die mogelijkheid niet bestaat of verwaarloosbaar is, kan de persoon niet als identificeerbaar worden beschouwd en is er geen sprake van persoonsgegevens.[50]

Ook de Nederlandse rechter lijkt zich hierbij aan te sluiten in een meer recent kort geding over de vraag of ROM-gegevens als persoonsgegevens moesten worden aangemerkt.[51] Met verwijzing naar een rapport van de Autoriteit Persoonsgegevens van 13 april 2016 over de herleidbaarheid van zogenaamde DIS-gegevens overwoog de voorzieningenrechter van de Rechtbank Midden-Nederland:

'(…) zij [de Autoriteit Persoonsgegevens] heeft daarbij niet met zoveel woorden uitgesproken dat gegevens waarbij enkel van "singling out" sprake is, zonder dat de betrokken persoon door directe of indirecte herleiding kan worden geïdentificeerd, onder het begrip persoonsgegevens van de Richtlijn en de Wbp vallen.'

Niet valt in te zien waarom deze overweging onder de AVG anders zou zijn. Toch lijkt de AP nog (te) strak in de leer te zitten door zoals eerdergenoemd te stellen: 'Geanonimiseerde gegevens zijn gegevens die helemaal geen betrekking meer hebben op individuen.' Dat gegevens zien op een individu, wil echter niet zeggen dat dat individu ook kan worden geïdentificeerd. Naar mijn mening is een dergelijke opvatting ook niet in lijn met de definitieve tekst van de AVG. Het feit dat singling out mogelijk is, doet geen afbreuk aan de doorslaggevende test van overweging 26 AVG.

6 Artikel 11 AVG

Wanneer dan toch redelijkerwijs te verwachten is dat (juridische) middelen door een partij kunnen worden gebruikt om de natuurlijke persoon te identificeren, maar identificatie door de verwerkingsverantwoordelijke zelf in beginsel niet kan, dan biedt artikel 11 AVG een mogelijk wenselijk alternatief. Het probleem is echter waarschijnlijk dat organisaties door de huidige ongenuanceerde benadering van pseudonimisering er nog niet aan durven. Zolang niet wordt erkend dat pseudonimisering niet per definitie iets zegt over de kwalificatie van gegevens als persoonsgegevens zie ik geen voortvarende adoptie van het lichtere regime van artikel 11 AVG voor me.

Waarom is artikel 11 AVG dan een interessant alternatief? Artikel 11 AVG regelt dat wanneer een verwerkingsverantwoordelijke aan de hand van de door hem verwerkte persoonsgegevens geen natuurlijke persoon kan identificeren, hij niet mag worden verplicht om (uitsluitend om aan de AVG te voldoen) aanvullende gegevens te verkrijgen ter identificatie. Hier doemt de vraag op onder welke omstandigheden sprake is het 'niet kunnen identificeren'. Is in het lichtere regime van artikel 11 dan alleen de verwerkingsverantwoordelijke relevant en niet de aanvullende gegevens die zich eventueel bij der-

45 G-J. Zwenne, 'Over IP-adressen en persoonsgegevens, en het verschil tussen individualiseren en identificeren'. *TvIR* 2011, afl. 1, p. 4-9 en G-J. Zwenne, 'De verwaterde privacywet' (oratie Leiden), 12 april 2013.
46 Albrecht amend. nr. 15. De bijbehorende argumentatie in het kader van intelligenter wordende zoek- en profileringstechnieken: Ms. Reding, speech Brussels d.d. 19 March 2013, MEMO/13/233.
47 Albrecht, Draft Report, 17 december 2012, (COM(2012)0011), nr. 84.
48 G-J. Zwenne, 'Nog enkele opmerkingen over IP-adressen en persoonsgegevens, identificeerbaarheid en "single-out"', *P&I* 2015, afl. 6, p. 216-221.
49 *Kamerstukken II* 2012/13, 32671, nr. 51, p. 2.
50 Zie ook G-J. Zwenne, in: *Tekst & Commentaar Privacy- en telecommunicatierecht*, art. 4 AVG (Definities).
51 Rb. Midden-Nederland 2 augustus 2017, ECLI:NL:RBMNE:2017:4011, r.o. 4.20.

den kunnen bevinden? Daarvan kan sprake zijn na pseudonimisering, wanneer een derde de sleutel onder zich houdt. Maar hoe verhoudt zich dit dan tot de besproken relatieve leer?

De verwerkingsverantwoordelijke mag evenwel niet weigeren de door de betrokkene tot uitoefening van zijn rechten verstrekte aanvullende gegevens aan te nemen, aldus het tweede lid. De identiteit van de betrokkene dient ook digitaal te worden geverifieerd, bijvoorbeeld aan de hand van persoonlijke beveiligingsgegevens. Als voorbeeld wordt genoemd gegevens die worden gebruikt voor het aanmelden van een onlinedienst.[52] De verwerkingsverantwoordelijke heeft dus wel de plicht de identiteit van de betrokkene te verifiëren. In geval van login credentials gebruikt voor onlinediensten, hoeft dit de verwerkingsverantwoordelijke nog steeds niet in staat te stellen de betrokkene te kunnen identificeren.

Verdedigbaar is dan ook dat artikel 11 lid 1 AVG een lichter AVG-regime beoogd op het moment dat identificeerbaarheid voor de verwerkingsverantwoordelijke niet (meer) nodig is.[53] Zo kan men denken aan verwerkingen voor directmarketingdoeleinden of aan wifitracking. Verwerkingen voor op zichzelf nuttige doeleinden, die gebaat zijn bij nadere uitleg van toezichthouders op dit vlak. Wat mij betreft kan een herijking van de opvattingen over pseudonimisering haar vruchten afwerpen voor de toepassing van artikel 11 AVG.

7 Conclusie

Het is verdedigbaar dat pseudonimisering onvoldoende is om per definitie identificeerbaarheid dan wel indirecte herleidbaarheid van gegevens aan te nemen. Voor de kwalificatie van persoonsgegevens is en blijft overweging 26 AVG doorslaggevend. De besproken meer liberale opvatting van de ICO – kort gezegd inhoudende dat gegevens na pseudonimisering ook buiten de scope van de AVG kunnen vallen – lijkt beter te passen in het bigdatatijdperk. Een meer genuanceerde, risicogebaseerde benadering, van pseudonimisering is wat mij betreft in ieder geval zeer welkom.

Al is het maar om bijvoorbeeld de adoptie van artikel 11 AVG te bevorderen. Wanneer pseudonimisering is toegepast kan immers sprake zijn van een situatie waarin de verwerkingsverantwoordelijke de betrokkene niet kan identificeren, omdat de sleutel zich bij een derde bevindt. Zolang echter niet wordt erkend dat pseudonimisering niet per definitie iets zegt over de kwalificatie van gegevens als persoonsgegevens, zie ik geen voortvarende adoptie van het lichtere regime van artikel 11 AVG voor me.

In dit artikel heb ik betoogd dat herijking van het concept pseudonimisering door de EPDB en in navolging door de nationale toezichthouders meer dan welkom is. Een alternatief is dat het Europees Hof meer rechtszekerheid schept. Het is dan wachten op een casus, waarbij het Hof in meer algemene bewoordingen richting wil geven.

52 Zie ook overweging 57 AVG.
53 Anders: M. Jansen, 'AVG en beveiliging: passende maatregelen voortaan proactiever nemen en monitoren', *Computerrecht* 2017/152, p. 213.