

De botte bijl van het privacytoezicht

Over de strengere uitleg van de drie belangrijkste rechtmatigheidsgrondslagen onder de AVG

Quinten Kroes¹

Sinds de vroege jaren tachtig van de vorige eeuw is een van de basisbeginselen van het Europese gegevensbeschermingsrecht dat de verzameling en verdere verwerking van persoonsgegevens ‘rechtmatig’ moet zijn. Richtlijn 95/46/EG gaf daartoe een limitatieve opsomming van zes alternatieve voorwaarden waarop deze rechtmatigheid kon worden gebaseerd. Deze voorwaarden zijn min of meer woordelijk gehandhaafd in de opvolger van de richtlijn, de AVG. Het uitputtende karakter van deze opsomming brengt mee dat het lidstaten niet vrijstaat om nieuwe voorwaarden toe te voegen, en evenmin om bijkomende vereisten te stellen aan de vervulling van die voorwaarden. Europese toezichthouders leggen deze voorwaarden echter steeds beperkter uit. Het fenomeen dat toezichthouders met – soms niet evidente – interpretaties hele categorieën van verwerkingen taboe verklaren, is niet nieuw, maar lijkt onder de AVG vleugels te hebben gekregen. De Autoriteit Persoonsgegevens loopt daarbij internationaal voorop. De AVG heeft privacy-toezichthouders vergaande handhavingsbevoegdheden gegeven maar die moeten daarbij niet op de stoel van de wetgever gaan zitten.

De Algemene Verordening Gegevensbescherming (AVG) is inmiddels ruim drie jaar van toepassing. Deze Europese privacywet had niet alleen ten doel om een hoog niveau van gegevensbescherming tot stand te brengen, maar ook om dat op eenvormige wijze te doen.² Een uniforme Europese wet had moeten bijdragen aan uniformiteit en rechtszekerheid.³ Tussen deze doelstelling en de realiteit is echter een hiaat waarneembaar. Daarbij gaat het niet alleen om onduidelijkheid over nieuwe regels, maar ook om basale uitgangspunten van het gegevensbeschermingsrecht die al meer dan 25 jaar bestaan. Een pregnant voorbeeld daarvan vormen de zogeheten voorwaarden (ook wel: grondslagen) voor rechtmatigheid van gegevensverwerking, die in de AVG vrijwel ongewijzigd zijn overgenomen uit haar voorganger, Richtlijn 95/46/EG. Waar die onder de richtlijn een tamelijk rustig bezit vormden, staat inmiddels de inhoud van zo'n beetje elke voor de praktijk relevante voorwaarde ter discussie. Er is sprake van een tendens bij toezichthouders om deze deels open normen aan te grijpen om hier een strengere koers in te zetten dan voorheen. De Autoriteit Persoonsgegevens (AP) loopt daarbij internationaal voor-

op. Ik zal dat in deze bijdrage illustreren aan de hand van de drie voor de rechtspraktijk belangrijkste grondslagen voor rechtmatige verwerking van persoonsgegevens, namelijk toestemming, uitvoering van de overeenkomst en het zogeheten gerechtvaardigd belang. Ook zal ik toelichten waarom die ontwikkeling – hoewel vanuit de beschermingsgedachte op het eerste gezicht aansprekend – onwenselijk is.

1. De voorwaarden voor rechtmatigheid van gegevensverwerking: waar gaat het om?

Sinds de vroege jaren tachtig van de vorige eeuw⁴ is één van de basisbeginselen van het Europese gegevensbeschermingsrecht dat de verzameling en verdere verwerking van persoonsgegevens ‘rechtmatig’ moet zijn. In Richtlijn 95/46/EG was dit uitgewerkt in artikel 7, dat een limitatieve opsomming gaf van zes alternatieve voorwaarden waarop deze rechtmatigheid kon worden gebaseerd. Deze zelfde voorwaarden zijn min of meer woordelijk gehandhaafd in artikel 6 lid 1 AVG. Het gaat hier om één van de belangrijkste voorvragen bij de naleving van de AVG voordat tot een meer gedetailleerde toetsing kan wor-

den overgegaan of alle andere gedragsnormen uit de AVG worden nageleefd.

Het uitputtende karakter van deze opsomming brengt mee dat het lidstaten niet vrijstaat om nieuwe voorwaarden toe te voegen, en evenmin om bijkomende vereisten te stellen aan de vervulling van die voorwaarden.⁵

Zoals hierna zal blijken, leggen Europese toezicht-houders deze voorwaarden echter steeds beperkter uit. Het fenomeen dat toezichthouders met – soms niet evi-dente – interpretaties hele categorieën van verwerkingen taboe verklaren, is niet nieuw, maar lijkt onder de AVG een verdere vlucht te nemen. De Nieuwetgever werkt dit soms in de hand met onduidelijke wetgeving. Het eindresultaat is een ondoorgrondeijk stelsel dat inmiddels Byzantijns genoemd mag worden. Dat maakt het steeds moeilijker voor diegenen die persoonsgegevens verwerken om de belangrijkste (voor)vraag uit de AVG te beantwoorden: is hun verwerking toelaatbaar?

Artikel 6 AVG

Rechtmatigheid van de verwerking

1. De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:

- a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
- b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op zoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
- (....)
- f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

2. De eerste voorwaarde: toestemming voor de verwerking van persoonsgegevens

2.1. Betekenis

Toestemming wordt in de AVG genoemd als eerste mogelijkheid voor een toelaatbare gegevensverwerking. Het betreft een autonoom begrip met een eigen betekenis binnen het Europese gegevensbeschermingsrecht. Toestemming is namelijk gedefinieerd als een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een

ondubbelzinnige actieve handeling een verwerking van persoonsgegevens aanvaardt.⁶ De toestemming kan op elk moment weer worden ingetrokken.⁷ Met name het vereiste dat toestemming vrijelijk moet zijn gegeven, is aan een steeds strengere interpretatie onderhevig geweest.

2.2. Het vereiste van vrije toestemming

Dat toestemming een andere betekenis heeft dan een civi-list wellicht zou verwachten, wordt duidelijk als we kijken naar de inmiddels gangbare opvatting over toestemming in de arbeidsrelatie. Al in 2001 schreef de werkgroep van Europese privacy-toezichthouders dat toestemming in de arbeidsrelatie problematisch is, vanwege het vereiste dat die toestemming vrijelijk gegeven moet zijn.⁸ Dat is op het eerste gezicht best een opmerkelijk standpunt. Geen Nederlandse arbeidsrechtjurist zou opperen dat er vanwege de hiërarchische verhouding tussen werkgever en werknemer in de regel sprake is van een wilsgebrek als die contractuele afspraken maken, of als de werknemer uitdrukkelijk afstand doet van een recht. En ook de hoogste Europese rechter acht het wel degelijk mogelijk dat werknemers vrijelijk instemmen met bijvoorbeeld de overschrijding van een wettelijk maximum van hun arbeidstijden.⁹ Als gevolg van deze uiteenlopende opvattingen wordt een werknemer wel bekwaam geacht om een vergaand concurrentiebeding met een boete te aanvaarden, maar niet om wel of niet in te stemmen met een foto op intranet. Niettemin is de opvatting dat vrije toestemming in de arbeidsverhouding problematisch is, inmiddels gemeengoed in het gegevensbeschermingsrecht. Zij vormt daarmee een vroeg voorbeeld hoe toezichthouders met hun uitleg van rechtmatigheidsgrondslagen de koers van het gegevensbeschermingsrecht ingrijpend hebben bepaald. Een uitleg die overigens sinds 2001 nooit met zoveel woorden aan het Hof van Justitie is voorgelegd, maar sindsdien bij de AP wel veelvuldig toepassing heeft gevonden.

Voorbeeld 1: toestemming in de arbeidsrelatie

Een werkgever wil op basis van vrijwilligheid de COVID-vaccinatiestatus van medewerkers vastleggen en moedigt medewerkers aan besmetting te melden zodat directe collega's gewaarschuwd kunnen worden.

De verwerking van persoonsgegevens is niet toegestaan op grond van de toestemming van de medewerkers, omdat de toestemming geacht wordt niet vrijelijk te zijn gegeven.¹⁰

Niet alleen raakt het gegevensbeschermingsrecht hiermee losgezongen van de opvattingen zoals die in de rest van

Auteur

1. Mr. Q. Kroes is advocaat te Amsterdam (Brinkhof). Hij staat verschillende partijen bij in handhavingdossiers van de AP over de hier beschreven onderwerpen. Hij bedankt Manon Oostveen, Leonie van Sloten, Rik Lambers en Gerrit-Jan Zwenne voor hun commentaar.

Noten

2. Overweging (3), (6) en (7) AVG.
3. Overweging (9) AVG.
4. De 'Privacy Principles' uit 1980 van de Europese Organisatie voor Economische Samenwerking en Ontwikkeling, Conventie 108 van de Raad van Europa.
5. HvJ EU 24 november 2011, C-468/10 en

C-469/10, ECLI:EU:C:2011:777 (ASNEF, FECEMD), r.o. 36, 39.

6. Art. 4 onderdeel 11 AVG.

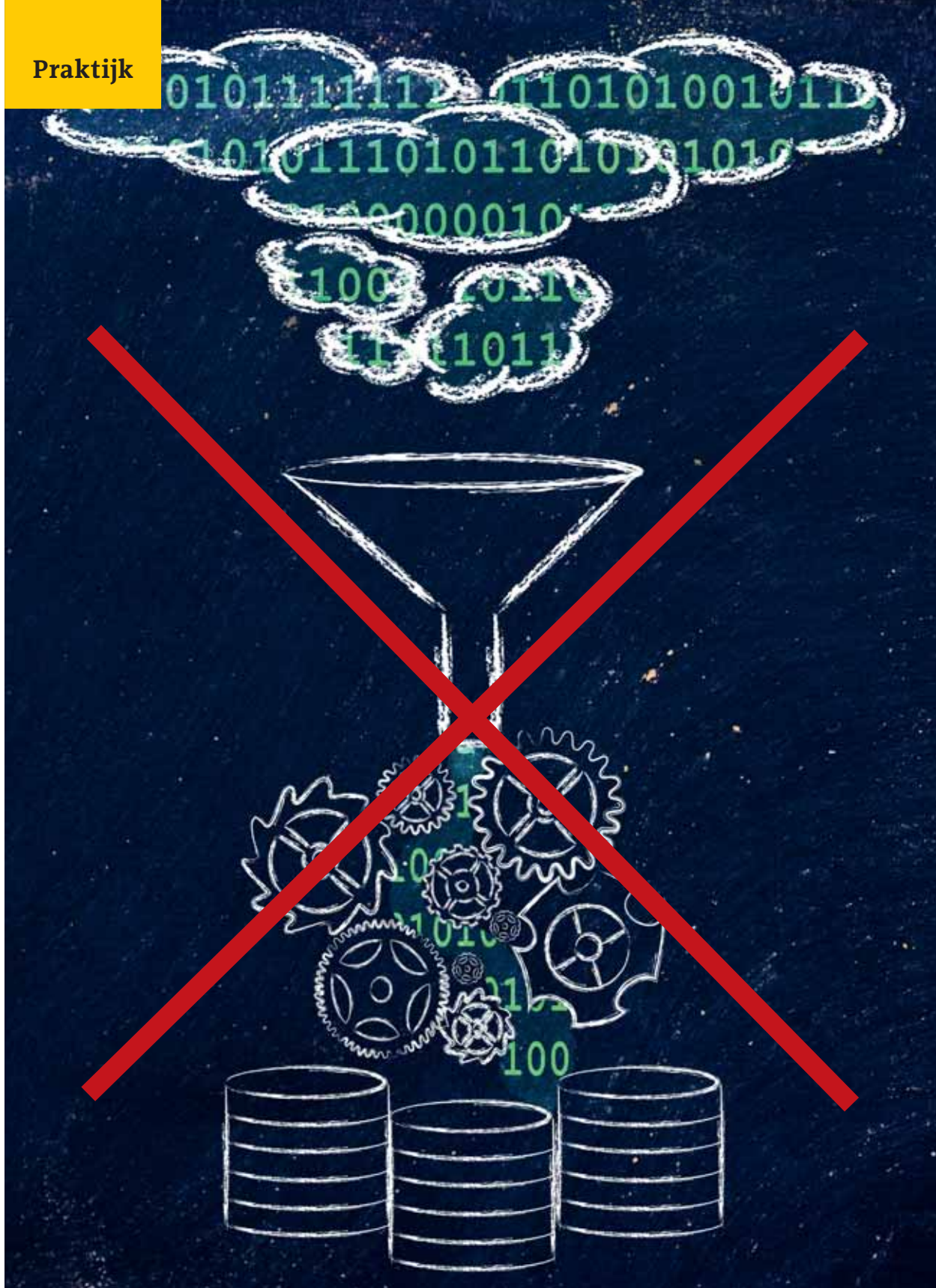
7. Art. 7 lid 3 AVG.

8. Advies 2/2017 over gegevensverwerking op het werk, Artikel 29 Werkgroep, WP48.

9. HvJ EU 5 oktober 2004, gevoegde zaken C-397/01 tot en met C-403/01,

ECLI:EU:C:2004:584, (Pfeiffer e.a./Deutsches Rotes Kreuz, Kreisverband Waldshut eV), r.o. 84.

10. Op haar website op autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/vaccinatie-tegen-corona stelt de AP dat de AVG geen grondslag biedt om vaccinatiestatus te registreren.



ons rechtssysteem bestaan, maar – zoals hierna blijkt – zo'n categorische en fundamentele koersbepaling kan bovendien gevolgen hebben die destijds waarschijnlijk niet zijn voorzien.

2.3. Nuancering van het vereiste van vrije toestemming onder de AVG

Hoewel de rechtmatigheidsgronden grotendeels ongewijzigd in de AVG zijn overgenomen vanuit de richtlijn, geldt voor de grondslag van toestemming dat de Uniewetgever

daarin enkele nuancerings heeft aangebracht, waarvan de strekking helaas niet geheel eenduidig is. In de overwegingen bij de AVG is gesteld dat toestemming niet geacht mag worden vrijelijk te zijn gegeven als de toestemming niet kan worden geweigerd zonder nadelige gevolgen.¹¹ Deze eis komt echter als zodanig niet terug in de bepalingen van de AVG zelf. Wel stelt artikel 7 een aantal nieuwe voorwaarden aan de geldigheid van toestemming. Eén van die voorwaarden is dat bij de vraag of toestemming vrijelijk gegeven kan worden, ten sterkste rekening wordt

gehouden met de vraag of de toestemming als voorwaarde wordt gesteld voor het aangaan van een overeenkomst, terwijl de verwerking waarvoor toestemming wordt gevraagd niet noodzakelijk is voor de uitvoering van die overeenkomst. Het verschil tussen de overweging en de bepaling zelf (waarbij de laatste prevaleert)¹² draagt alle tekenen van een moeizaam bereikt compromis. Aldus is het aan de praktijk gelaten om te bepalen wat het betekent om 'ten sterkste rekening' te houden met genoemde omstandigheid, en wanneer een verwerking wel of niet noodzakelijk wordt geacht voor de uitvoering van een overeenkomst.

2.4. Toepassing door de AP

Duidelijk is wel dat toezichthouders, en zeker de AP, hier hebben gekozen voor een vlucht naar voren.

Voorbeeld 2: toestemming en cookiemuren

Voor het plaatsen van cookies waarmee surfgedrag van bezoekers in kaart wordt gebracht (tracking-cookies) moet op grond van de e-Privacy Richtlijn¹³ toestemming in de zin van de AVG worden gevraagd. Websites die content bieden waarvoor de bezoeker niet hoeft te betalen, en die met advertentie-inkomsten wordt gefinancierd, doen dat soms met een cookiemuur: voordat een bezoeker toegang krijgt tot bepaalde content, krijgt die de keuze om wel of niet in te stemmen met het plaatsen van cookies. Bij weigering van toestemming, verkrijgt de bezoeker geen toegang tot de content.

Op 7 maart 2019 publiceerde de AP haar 'normuitleg cookiemuren'.¹⁴ Daarin betreft de AP het standpunt dat een cookiemuur neerkomt op 'take it or leave it' en niet als 'vrije' keuze kwalificeert. Weigering heeft volgens de AP nadelige gevolgen, omdat de content dan überhaupt niet kan worden bekeken. De AP concludeert daarom dat het gebruik van een cookiemuur ontoelaatbaar is.

Deze normuitleg roept de nodige onbeantwoorde vragen op en heeft vergaande implicaties. Zo kan over cookiemuren zeer wel gesteld worden dat de bezoeker niet zozeer 'nadelige gevolgen' (in de zin van overweging 42 AVG) ondervindt van een weigering, maar alleen het aangeboden voordeel misloopt van toegang tot content waarvoor niet hoeft te worden betaald. De juridische en economische positie van de websitebezoeker blijft bij weigering van toestemming zoals die was. Het is ook maar de vraag of hier toestemming wordt gevraagd voor een verwerking die niet noodzakelijk is voor het contract dat de bezoeker hier wordt voorgehouden. Die kan namelijk zonder betaling toegang krijgen, maar moet daarvoor accepteren dat de exploi-

tant een alternatieve bron van inkomsten aanboort door gerichte advertenties. Deze benadering ligt in lijn met de opvatting van A-G Szpunar, die het Hof van Justitie adviseerde in de zaak *Planet 49*.¹⁵ Het ging daar om een propositie aan website-bezoekers waarbij zij hun e-mailadres opgaven om mee te dingen naar prijzen in een gratis loterij. Wel moesten deelnemers instemmen met het gebruik van hun e-mailadres voor ongevroegde aanbiedingen van een lijst bedrijven. A-G Szpunar achtte dit niet in strijd met de AVG, nu deze instemming in wezen de tegenprestatie vormde van de gebruiker voor deelname aan de loterij, en die toestemming dus inderdaad noodzakelijk kon worden geacht voor deelname aan de loterij. Helaas heeft het Hof zich niet over deze kwestie uitgelaten.¹⁶

De casus van de loterij toont aan dat het standpunt van de AP problematisch is. Moet een aanbieder van zo'n loterij consumenten de mogelijkheid bieden deel te nemen zonder in te stemmen met het gebruik van hun e-mailadres voor bepaalde marketingacties? Het laat zich raden dat de consument liever die optie zal kiezen als dat verder geen consequenties heeft voor deelname, en dat dan de commerciële basis wegvalt voor de aanbieder om een *sweepstake* te houden. Of mag in dat geval betaling worden verlangd? Maar dan zou in de opvatting van de AP net zozeer kunnen worden gesteld dat de weigering van toestemming 'nadelige gevolgen' heeft. En hoe verhoudt een eventuele verplichting om een alternatief te moeten bieden dat niet wordt gefinancierd met marketingacties zich tot de vrijheid van ondernemerschap, die ook door het Handvest beschermd wordt als fundamenteel recht?¹⁷ Is dit een evenredige en proportionele beperking van de contractsvrijheid, het basisbeginsel uit ons contractenrecht dat partijen in beginsel zelf de inhoud van hun aanbod mogen bepalen en met wie zij wel of niet een overeenkomst willen aangaan?

3. De tweede voorwaarde: noodzaak voor een contract of een precontractuele handeling

3.1. Betekenis

Daarmee zijn we aanbeld bij de voorwaarde dat verwerking mag plaatsvinden als die noodzakelijk is voor de uitvoering van een overeenkomst met de betrokkene. Net als bij toestemming is hier de geoorloofdheid van de verwerking afhankelijk van een wilsuiting van de betrokkene, degene om wiens persoonsgegevens het gaat. In het eerste geval is de wilsuiting gericht op een specifieke verwerking; in het tweede geval op de totstandkoming van een overeenkomst en wat daarvoor nodig is. Dat laatste omvat uitdrukkelijk precontractuele handelingen op verzoek van betrokkene die aan de contractsluiting noodzakelijkerwijs voorafgaan. Noodzaak impliceert daarbij een subsidiariteitstoets (kan het doel met minder vergaande middelen gerealiseerd worden?).¹⁸

11. Overweging 42 AVG.

12. HvJ EG 15 mei 1997, C-355/95, ECLI:EU:C:1998:554, r.o. 54.

13. Richtlijn 2002/58/EG.

14. autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_ap_

[cookiewalls.pdf](#).

15. Conclusie van A-G M. Szpunar van 21 maart 2019, C-673/17,

ECLI:EU:C:2019:246 (*Planet49 GmbH*).

16. HvJ EU 1 oktober 2019, ECLI:EU:C:2019:801.

17. Zie voor een recent voorbeeld waarbij

de ondernemersvrijheid zwaarder mocht

wegen dan het fundamentele recht op

godsdienstvrijheid het arrest van het HvJ EU

van 15 juli 2021 in C-804/18 en C-341/19,

ECLI:EU:C:2021:594.

18. Zie bijvoorbeeld HvJ EU 9 november

2010, C-92/09, C-93/09, ECLI:EU:C:2010,

r.o. 76 e.v.; HvJ EU 4 mei 2017, C-13/16,

ECLI:EU:C:2017:336, r.o. 30.

Profilering gebeurt niet alleen bij reclame, maar ook om de inhoud van de dienst zelf af te stemmen op de individuele gebruiker

3.2. Wie bepaalt wat noodzakelijk is voor de uitvoering van de overeenkomst?

In 2014 heeft de werkgroep van Europese privacy-toezichthouders zich uitgesproken over deze rechtmatigheidsgrondslag, en het standpunt betrokken dat daaronder geen verwerkingen mogen worden geschaard die niet strikt noodzakelijk zijn voor de uitvoering van de overeenkomst, maar door de verantwoordelijke eenzijdig aan de betrokkene worden opgelegd.¹⁹ Om deze noodzaak te kunnen beoordelen, moet eerst het doel van de overeenkomst bepaald worden. De noodzaak van de verwerking dient vervolgens tegen dat doel getoetst te worden. Dat klinkt eenvoudiger dan het is, en verhult de kernvraag waarom het hier draait: in welke mate staat het de aanbieder van een dienst waarop het contract ziet, vrij om zelf de randvoorwaarden van diens propositie te bepalen, inclusief de doeleinden waarvoor hij persoonsgegevens wenst te verwerken? Enkele jaren later formuleerden de Europese toezichthouders, inmiddels onder de AVG verenigd in het zogeheten Europese Comité voor Gegevensbescherming, een antwoord: de doelstelling van het contract dient 'objectief' bepaald te worden en staat dus niet geheel ter vrije bepaling van de aanbieder.²⁰ Daarbij dient volgens het Comité gekeken te worden naar onder meer de aard van de dienstverlening en de verwachtingen van partijen over en weer. Hoe wordt de dienst gepromoot? Zou een doorsnee gebruiker redelijkerwijs verwachten dat de verwerking plaatsvindt bij de uitvoering van het contract, gelet op de aard van de dienstverlening?

Volgens het Comité sluiten de rechtmatigheidsgrondslagen van toestemming en uitvoering van de overeenkomst elkaar uit: als een verwerking noodzakelijk is voor de uitvoering van de overeenkomst, dan dient de aanbieder er geen toestemming voor vragen, en omgekeerd geldt dat als de verwerking niet strikt nodig is voor de overeenkomst, deze alleen op de grondslag van toestemming zal kunnen worden gebaseerd (die in dat geval ook geweigerd moet kunnen worden zonder negatieve consequenties voor het mogen aangaan van de overeenkomst; zie de vorige paragraaf).

3.3. Kan klantprofilering nodig zijn voor de uitvoering van de overeenkomst?

Een ander standpunt van het Comité over deze rechtmatigheidsgrondslag, is dat profilering door een online retailer nooit noodzakelijk kan zijn voor de uitvoering van de overeenkomst. Zelfs als dit uitdrukkelijk in het contract wordt benoemd, kan dat niet meebrengen dat dit noodzakelijk is voor de uitvoering van de overeenkomst, en dient de retailer op zoek te gaan naar een andere grondslag.²¹

Over dit thema zijn inmiddels vragen gesteld aan het Hof van Justitie. In een zaak over de gebruiksvoor-

waarden van Facebook, oordeelde de Oostenrijkse rechter in twee instanties dat verwerking van persoonsgegevens van Facebook-gebruikers voor gerichte advertenties gebaseerd mocht worden op de noodzaak van de uitvoering van de gebruikersovereenkomst. Die gebruikersovereenkomst van Facebook voorzag namelijk sinds de inwerking-treding van de AVG uitdrukkelijk in het door Facebook kunnen tonen van op de persoon afgestemde advertenties. Voorheen vroeg Facebook daarvoor toestemming. Omdat die toestemming een voorwaarde was voor de inschrijving op het sociale netwerk, had Facebook kennelijk de afweging gemaakt dat de verwerking onder de AVG beter op de noodzaak van de uitvoering van overeenkomst kon worden gebaseerd. Inmiddels buigt het Hof van Justitie zich over de vraag of voor de verwerking van persoonsgegevens met het oog op gepersonaliseerde reclame, altijd toestemming moet worden gevraagd of dat dit in plaats daarvan mag worden opgenomen in het contract.²²

Profilering gebeurt niet alleen bij reclame, maar ook om de inhoud van de dienst zelf af te stemmen op de individuele gebruiker. Die trend is vooral waarneembaar bij online dienstverlening.

Voorbeeld 3: gepersonaliseerde diensten

Streaming diensten doen aanbevelingen op basis van eerder kijk- of luistergedrag, sociale apps zoeken soortgenoten op basis van het profiel van de gebruiker, een online persoonlijke assistent geeft tips over de verwachte reistijd voor dagelijks woon/werkverkeer.

Volgens het Comité kan personalisatie alleen worden gebaseerd op de uitvoering van de overeenkomst als dit objectief gerechtvaardigd is. Het mag niet slechts dienen om de betrokkenheid van de gebruiker bij de dienst te vergroten: bijvoorbeeld een reissite die hotels aanraadt op basis van eerdere reserveringen. Doorslaggevend is of de dienst zonder personalisatie geleverd kan worden.

Het verschil tussen de eerste en de laatstgenoemde voorbeelden is subtiel. Dat vormt een dilemma voor aanbieders van gepersonaliseerde diensten die niet zeker zijn van een beroep op de uitvoering van de overeenkomst: moeten zij toestemming vragen? Zo ja, dan moet de consument de dienst ook kunnen afnemen zonder toestemming te geven. Daardoor zouden zulke aanbieders gedwongen worden een variant van hun dienst te bieden die – in elk geval in hun ogen – suboptimaal of zelfs zinloos is, zoals een persoonlijke assistent of online datingservice die zonder informatie over de klant aanbevelingen moet doen.

Het voorgaande voorbeeld illustreert hoe toezichhouders op de stoel van de ondernemer gaan zitten door voor hen 'objectief' te bepalen wat wel en niet voor hun dienstverlening strikt nodig is. Er spreekt ook een nogal bevoogdende opvatting uit richting consumenten die kennelijk niet in staat worden geacht de verleiding van dergelijk aanbod te weerstaan, zelfs niet na over de verwerking van hun gegevens geïnformeerd te zijn.²³ Dat is fnuikend voor de innovatie, juist in een sector (online dienstverlening) waar die essentieel is om te kunnen concurreren. Nu kan men zich afvragen wat erop tegen is dat zulke aanbieders de gebruikers niet gewoon netjes om toestemming vragen. Maar zoals al bleek, biedt toestemming lang niet altijd een alternatief.

Gelet op het voorgaande zal zowel voor werkgevers als voor cloud-aanbieders in de praktijk alleen het gerechtvaardigd belang nog uitkomst kunnen bieden, de laatste hier te bespreken rechtmatigheidsgrondslag.

Voorbeeld 4: clouddiensten

Het gebruik van cloudoplossingen vindt steeds meer toepassing in de maatschappij, en heeft door de toename van thuiswerken tijdens de COVID-crisis een verdere impuls gekregen. Denk aan kantoorapplicaties en videoconferentie-software die door werkgevers en scholen zijn uitbesteed aan aanbieders als Microsoft, Google of Zoom. Bij al dit soort applicaties worden persoonsgegevens verwerkt. Het gaat daarbij niet alleen om inhoud (bijvoorbeeld opgeslagen documenten), maar ook om technische data die op de achtergrond wordt verzameld (bijvoorbeeld wie maakt wanneer gebruik van een applicatie).

Voor de werkgever is hier de vraag aan de orde of de verwerking van persoonsgegevens van werknemers noodzakelijk kan worden geacht voor de uitvoering van de arbeidsovereenkomst. Hierover heeft de Duitse rechter prejudiciële vragen gesteld.²⁴ Daartegen zou kunnen worden aangevoerd dat inzet van cloud-applicaties niet strikt noodzakelijk is; er zijn alternatieven, ook al zijn die niet gelijkwaardig (software op eigen servers van de werkgever, telefonische conferenties in plaats van videoconferenties). Als de arbeidsovereenkomst geen rechtmatigheidsgrondslag biedt, staat voor de werkgever evenmin de optie van toestemming open vanwege de hiërarchische relatie tussen werkgever en werknemer.

Voor cloud-aanbieders die persoonsgegevens verwerken voor eigen doeleinden (bijvoorbeeld voor de beveiliging van het cloud-platform, of het personaliseren

van diensten) geldt dat die niet altijd een overeenkomst hebben met de gebruikers (maar alleen met hun werkgever), zodat de uitvoering van de overeenkomst met de betrokkene daarom al geen rechtmatigheidsgrondslag biedt. Ook voor aanbieders zal toestemming als grondslag moeilijk te verenigen zijn met het standpunt van Europese toezichthouders dat werknemers meestal niet in de positie verkeren dat ze werkelijk vrije toestemming kunnen geven.

Het voorbeeld illustreert hoe toezichthouders op de stoel van de ondernemer gaan zitten door voor hen 'objectief' te bepalen wat wel en niet voor hun dienstverlening strikt nodig is

4. De derde voorwaarde: noodzaak voor een gerechtvaardigd belang, behalve wanneer de rechten en vrijheden van de betrokkene zwaarder wegen

4.1. Betekenis

Het gaat bij deze laatste rechtmatigheidsvoorwaarde volgens het Hof van Justitie om een driestappentoets: ten eerste moet het gaan om een belang dat gerechtvaardigd is, ten tweede moet de verwerking noodzakelijk zijn voor de behartiging van dat belang, en ten derde mogen de fundamentele rechten en vrijheden van de betrokkene niet prevaleren.²⁵ Het mag daarbij gaan om een eigenbelang van degene die de persoonsgegevens verwerkt, maar ook om het gerechtvaardigd belang van een derde.

4.2. Het gerechtvaardigd belang als vangnet

Hoewel de verschillende rechtmatigheidsgronden volgens het Hof van Justitie als onderling gelijkwaardig moeten worden beschouwd, fungeert het in artikel 6 lid 1 sub f AVG genoemde gerechtvaardigd belang (ook wel aangeduid als de 'f-grond') in de praktijk soms als restgrond of vangnetbepaling waar andere rechtmatigheidsgronden niet beschikbaar zijn.²⁶

Dat is omdat toestemming en de uitvoering van een overeenkomst lang niet altijd een alternatieve

19. Advies 06/2014 over het begrip 'gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke' in art. 7 Richtlijn 95/46/EG, WP 217, p. 20 e.v.

20. Richtsnoeren 2/2019 betreffende de verwerking van persoonsgegevens op

grond van art. 6 lid 1 onder b) AVG in het kader van de verlening van online diensten aan betrokkenen, beschikbaar op edbp.europa.eu.

21. Richtsnoeren 2/2019, voorbeeld 2.

22. Oberster Gerichtshof 20 juli 2021,

beschikbaar op noyb.eu.

23. Zie ook de opinie van G.-J. Zwenne & I. Brouwer hierover: 'Wie gaat er over onze privacy? Wijzelf of onze Privacytoezicht-houder?', *Tijdschrift voor Internetrecht* 2018/3.

24. Zaak nr. C-34/21.

25. HvJ EU 4 mei 2017, C-13/16, ECLI:EU:C:2017:336 (*Rīgas satiksme*).

26. Vgl. de MvT op dit punt bij de Wet bescherming persoonsgegevens, *Kamerstukken II* 1997/98, 25892, nr. 3, p. 86.

De situatie dat er geen contractuele relatie met de betrokkene bestaat en het vragen van toestemming niet tot de mogelijkheden behoort, doet zich vaker voor dan men wellicht zou denken

grondslag bieden. De situatie dat er geen contractuele relatie met de betrokkene bestaat en het vragen van toestemming niet tot de mogelijkheden behoort, doet zich vaker voor dan men wellicht zou denken. Denk aan de advocaat die gegevens over een werknemer ontvangt van de werkgever in het kader van de afwikkeling van een arbeidsgeschil. En zo zijn er meer dienstverleners die van hun klanten persoonsgegevens verkrijgen over derden, welke zij naar eigen inzicht verwerken om hun diensten te kunnen bieden. Dat gebeurt in het zakelijke domein (pensioenverzekeraars of autoleasemaatschappijen die werknemersgegevens verkrijgen van werkgevers), maar ook bij dienstverlening aan consumenten: een bank verkrijgt van haar klant naam, woonplaats en rekeningnummer van een derde persoon naar wie een overboeking moet worden uitgevoerd. Met die ontvanger heeft de bank niet noodzakelijkerwijs een contract, noch voor die verwerking diens toestemming gevraagd. Het Comité heeft bevestigd dat aanbieders van betaaldiensten de gegevens van dit soort 'silent third parties' op basis van het gerechtvaardigd belang mogen verwerken.²⁷

Maar ook daar waar er wel sprake is van een contract, en/of in theorie wel een vorm van toestemming kan worden gevraagd, biedt dat in de praktijk niet altijd een grondslag voor rechtmatige verwerking.

Hiervoor is al de juridische onhaalbaarheid van toestemming in de arbeidsrelatie genoemd. Daarnaast is er bij toestemming het praktische bezwaar van de intrekbarebaarheid: een betrokkene moet zich kunnen bedenken en als de toestemming wordt herroepen, dient de verdere verwerking van persoonsgegevens te worden gestaakt. Dat is niet altijd mogelijk of wenselijk. Een bijzondere complicatie doet zich voor bij online dienstverlening aan minderjarigen: als de verwerkingsverantwoordelijke zich wil beroepen op toestemming, dan dient die te worden verkregen van de wettelijk vertegenwoordiger.²⁸ De verificatie van zowel de leeftijd als de relatie tussen de minderjarige en wettelijke vertegenwoordiger levert daarbij in de praktijk een formidabel obstakel op, vooral in een online setting waarin een fysiek contact- en controlemoment ontbreekt.

Bij de grondslag van de uitvoering van de overeenkomst vloeit de beperking van de grondslag onder meer voort uit de strenge noodzakelijkheidstoets die door toezichthouders wordt toegepast als een soort conditio sine qua non: kan het contract worden uitgevoerd zonder de verwerking? De voorafgaande beoordeling van de krediet-

waardigheid van de klant ('credit-check') is volgens de Europese toezichthouders zo'n voorbeeld van een verwerking die niet noodzakelijk is.²⁹ Daarnaast geldt voor pre-contractuele maatregelen de eis dat de betrokkene daarom verzocht moet hebben.

Het gerechtvaardigd belang vervult daarom voor de praktijk een cruciale rol als vluchtheuvel binnen de rechtmatigheidsgrondslagen.³⁰ Die rol kan het ook vervullen omdat een beroep op het gerechtvaardigd belang met bijzondere wettelijke waarborgen is omkleed.³¹ Zo dient de verantwoordelijke een belangenafweging te verrichten waarbij de vraag centraal staat of de privacy van de betrokkene voldoende beschermd is, bijvoorbeeld door extra transparantie over de verwerking of doordat de betrokkenen een onvoorwaardelijk verzetsrecht wordt geboden. Daarnaast biedt de wet aan betrokkenen het recht zich tegen de verwerking op grond van het gerechtvaardigd belang te verzetten vanwege hun specifieke omstandigheden.³² In het verleden hebben toezichthouders deze vangnet-functie van het gerechtvaardigd belang onderkend. In een opinie over het gerechtvaardigde belang uit 2014³³ schreven zij bijvoorbeeld dat als in een grensgeval niet duidelijk is of sprake is van een echte noodzaak voor de uitvoering van de arbeidsovereenkomst, meestal het gerechtvaardigd belang van de werkgever uitkomst zal kunnen bieden. Als voorbeelden noemden zij het smoelenboek op intranet, de controle op naleving van huisregels en fraudepreventie.³⁴ Iets soortgelijks overwogen zij over kredietwaardigheid-scheets, die ook geoorloofd werden geacht onder het gerechtvaardigd belang.³⁵ Zij leken daarmee te onderkennen dat hun strikte interpretaties van de ene grond, noodzakelijkerwijs gepaard moest gaan met een ruimere interpretatie van de andere, als men tenminste geen halt wil toeroepen aan allerlei verwerkingen die tot dan toe als maatschappelijk geoorloofd en zelfs wenselijk werden beschouwd.

Die opvatting sloot aan bij die van de Nederlandse wetgever. Deze had bij de implementatie van Richtlijn 95/46/EG rond de eeuwwisseling al het standpunt ingenomen dat voor ondernemingen sprake was van een gerechtvaardigd belang als de verwerking noodzakelijk was voor of in wezenlijke zin ondersteunend aan hun reguliere bedrijfsactiviteiten, waarbij direct marketing als voorbeeld werd genoemd.³⁶ Sindsdien biedt ook de rechtspraak van het Hof van Justitie verschillende voorbeelden die blijf geven van een ruime interpretatie van deze grond. In 2014 oordeelde het Hof bijvoorbeeld dat de verwerking van persoonsgegevens die noodzakelijkerwijs gepaard gaat met het geautomatiseerd indexeren van webpagina's door een online zoekmachine zoals die van Google, gegrond kan worden op het gerechtvaardigd belang.³⁷ Ook de beschikkingspraktijk van de AP en haar rechtsvoorganger het College bescherming persoonsgegevens (CBP) laat vele voorbeelden zien van bedrijfsmatige verwerkingen met een primair commerciële achtergrond die onder het gerechtvaardigd belang werden toegestaan.³⁸ Dat die commerciële achtergrond de verwerking niet uitsluit van een beroep op het gerechtvaardigd belang, blijkt tenslotte uit de overwegingen van de AVG, die direct marketing uitdrukkelijk als voorbeeld noemen.³⁹

4.3. De normuitleg gerechtvaardigd belang van de AP

Het kwam dan ook als donderslag bij heldere hemel toen de AP in de loop van 2019 in een aantal toen lopende handhavingssdossiers het standpunt begon in te nemen dat een belang alleen als gerechtvaardigd kan kwalificeren als dat in (algemene) wetgeving of elders in het recht is erkend als een rechtsbelang.⁴⁰ Het enkel dienen van zuiver commerciële belangen en winstmaximalisatie kunnen volgens de AP niet als zodanig kwalificeren, omdat die niet specifiek genoeg zijn en een dringend 'wettelijk' karakter missen. Deze nieuwe normuitleg is vervolgens neergelegd in een document dat zonder ruchtbaarheid op de website van de AP is gepubliceerd.⁴¹ In een aantal dossiers is de AP overgegaan tot oplegging van aanzienlijke boetes op basis van haar nieuwe interpretatie. De eerste gepubliceerde boete van € 525.000 werd opgelegd aan de Koninklijke Nederlandse Lawn Tennis Bond (KNLTB).⁴² Die had een deel van haar ledenbestand beschikbaar gesteld aan twee sponsors voor tennisgerelateerde mailings, nadat dit door de algemene ledenvergadering was goedgekeurd.⁴³ De tweede boete, van € 575.000 trof ook de amateursport en werd opgelegd aan VoetbalTV.⁴⁴ Deze joint venture van de KNVB en Talpa bood amateurverenigingen de mogelijkheid een slimme camera te laten plaatsen op het veld, waarmee geautomatiseerd rapportages werden gemaakt van de ingeroosterde competitiewedstrijden. Deze beelden konden worden teruggekeken door de trainers en door belangstellenden die de app van VoetbalTV hadden geïnstalleerd. Waar voorheen in zaken over het

De opvatting dat een onderneming die gegevens verwerkt voor commerciële doeleinden, zich niet op het gerechtvaardigd belang mag beroepen, heeft vergaande gevolgen

gerechtvaardigd belang de discussie zich toespitste op de tweede en de derde stap (noodzaak en belangenafweging; wat concreet vaak neerkwam op de vraag of de verwerking evenredig was en er passende waarborgen waren getroffen om de privacybelangen te beschermen), kwam de AP daar nu niet eens aan toe. De opvatting dat een onderneming die gegevens verwerkt voor commerciële doeleinden zich niet op het gerechtvaardigd belang mag beroepen heeft vergaande gevolgen.

Voorbeeld 5: Antecedentenonderzoek

Er zijn verschillende zakelijke dienstverleners die antecedentenonderzoeken in opdracht van anderen uitvoeren zoals een kredietwaardigheidsonderzoek naar een nieuwe klant of een *pre-employment screening* van een sollicitant. Zulke dienstverleners hebben niet dezelfde wettelijke plicht als hun opdrachtgever, noch staan zij zelf in een (pre)contractuele relatie met de betrokkene. Als zij persoonsgegevens naar eigen inzicht verwerken, kunnen zij dat alleen rechtmatig doen met een beroep op het gerechtvaardigd belang. Onder de normuitleg van de AP is twijfelachtig of dat mag; strikt genomen is het belang van de dienstverlener alleen gelegen in het kunnen aanbieden van zijn dienst, en daarmee louter commercieel.

In algemene zin roept de normuitleg van de AP de vraag op of dienstverleners die onder eigen verantwoordelijkheid persoonsgegevens verwerken voor hun klanten, zich nog mogen beroepen op het gerechtvaardigd belang. Zo niet, dan kunnen zij alleen hun werkzaamheid voortzetten in de hoedanigheid van verwerker, dat wil zeggen: door hun gegevensverwerking strikt te beperken tot datgene wat hen door de klant wordt opgedragen. In dat geval behoeven zij zich niet te kunnen beroepen op een zelfstandige verwerkingsgrond, en kunnen ze meeliften op de verwerkingsgrond van de opdrachtgever. Maar dat is een schijnoplossing die zich niet laat rijmen met de praktijk waar dienstverleners vaak juist om hun expertise of eigen verantwoordelijkheid onder hun beroepsreglementering worden gekozen, en de opdrachtgever zich maar beperkt bemoeit met de verwerking van persoonsgegevens door hun opdrachtnemer (denk aan het hier-

27. Richtsnoeren 06/2020 inzake de samenwerking tussen de tweede richtlijn betalingsdiensten en de AVG, p. 20.

28. Art. 8 lid 1 AVG.

29. Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679, WP251rev.01.

30. E.M.L. Moerel & J.E.J. Prins hebben zelfs voorgesteld alleen het gerechtvaardigd belang als grondslag te hanteren en andere grondslagen af te schaffen in hun preadvies voor de NJV (2016), *Privacy voor de home digitalis*.

31. Zie ook P-G Rank-Berenschot in

ECLI:NL:PHR:2021:831, par. 3.14.

32. Art. 21 AVG.

33. Advies 06/2014 over het begrip 'gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke' in art. 7 Richtlijn 95/46/EG, WP 217.

34. WP 217, p. 21.

35. WP 217, p. 22.

36. *Kamerstukken II 1997/98*, 25892, nr. 3, p. 86.

37. HvJ EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain*).

38. Bijvoorbeeld de verwerking door Nike van persoonsgegevens om haar hardlooppapp te verbeteren of door een leverancier

van wifi-tracking technologie waarmee bezoekersgedrag in en om winkels wordt gemeten.

39. Overweging 47, laatste zin, bij de AVG.

40. Het moet volgens de AP gaan om een belang dat een min of meer dringend en specifiek karakter heeft dat uit een (geschreven of ongeschreven) rechtsregel of rechtsbeginsel voortvloeit; het moet in zekere zin onontkoombaar zijn dat deze gerechtvaardigde belangen worden behartigd. Zuiver commerciële belangen en het belang van winstmaximalisatie zijn niet specifiek genoeg en missen een dringend 'wettelijk' karakter.

41. autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf.

42. autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_knltb.pdf.

43. Zie hierover M. Jansen, 'KNLTB-boete: wie kaatst kan de bal verwachten of toch een misslag?', *Computerrecht* 2020/180.

44. Dit boetebesluit is nog niet gepubliceerd. De auteur trad op als de gemachtigde van VoetbalTV.

voor genoemde voorbeeld van de arbeidsrechtadvocaat). Op zich mag het gerechtvaardigd belang uitdrukkelijk ook dat van een derde zijn; in dit geval dat van de klant. Als die belangen van de klant een 'louter commercieel belang' overstijgen (en bijvoorbeeld zien op de noodzaak te voldoen aan een wettelijke plicht of om de integriteit en veiligheid van de eigen bedrijfsvoering te beschermen), zou een beroep op de 'f-grond' door de dienstverlener dus – ook onder de strenge normuitleg van de AP – wel degelijk mogelijk moeten zijn. Ook dat is echter een onwenselijke oplossingsrichting. In dat geval moeten opdrachtnemers zich bij elke klantinstructie die verwerking van persoonsgegevens vergt, de vraag stellen of hun klant daarbij een gerechtvaardigd belang heeft. Bij een arbeidsrechtadvocaat is dat weliswaar onwenselijk maar nog denkbaar; bij een overboekingsopdracht aan een bank is het ondoenlijk.

5. Afsluitende beschouwingen

Deze rondgang langs de voor de commerciële praktijk belangrijkste rechtmatigheidsgronden toont een patroon waarbij de AP stevast kiest voor de strengst mogelijke uitleg. De AP doet dat onder het motto dat iedere verwerking een inmenging vormt met het fundamentele recht op bescherming van persoonsgegevens en daarom in beginsel kennelijk suspect is. Als het aan de AP ligt, kan die inmenging alleen gelegitimeerd worden ofwel door een wilsbeschikking van de betrokkene (die vervat is in toestemming of het aangaan van een contract dat tot de verwerking noopt), ofwel door de wetgever (met een wet die de verwerking nodig of gerechtvaardigd maakt). De min of meer open afweging van belangen waarin de f-grond volgens de gangbare opvatting voorziet, en de talloze verwerkingen die daaronder geoorloofd worden geacht, worden zo in de ban gedaan. De discussie rond toestemming en cookiemuren is een ander voorbeeld. Daar heeft de AP met een strengere uitleg van de bestaande regels een halt willen toeroepen aan een fenomeen dat tot nu toe getolereerd werd, maar dat inmiddels politiek en maatschappelijk meer ter discussie staat.

Het is op zich toe te juichen dat rechters zich in een aantal dossiers kritisch hebben uitgelaten over dergelijk activisme door toezichthouders. In Frankrijk oordeelde de hoogste bestuursrechter dat het niet aan de Franse toezichthouder was om door middel van een strengere uitleg van het begrip toestemming cookiemuren te verbieden.⁴⁵ Dat was volgens die rechter aan de wetgever, die nota bene bezig is om de EU-regels over cookies te herzien.⁴⁶ Of en hoe cookiemuren daarin worden gereguleerd, vormt in die discussie een heet hangijzer. De Rechtbank Midden-Nederland vernietigde de boete die de AP aan VoetbalTV had opgelegd, en maakte in zijn uitspraak inhoudelijk korte metten met de nieuwe normuitleg van de AP.⁴⁷

Met deze rechterlijke correcties in het achterhoofd, zou men zich op het standpunt kunnen stellen dat toezichthouders – zoals alle deelnemers aan het rechtsverkeer – er hun eigen opvattingen op na mogen houden, en dat het alleen maar toe te juichen is dat zij op de bres springen voor de bescherming van privacy. Dat is tenslotte ook hun kerntaak. Zij zijn daarbij sneller dan de wetgever in staat om te reageren op nieuwe ontwikkelingen, die elkaar door technologische innovatie pijlsnel opvolgen.

Er kan niet aan voorbijgegaan worden dat de AP toeziet op slechts één fundamenteel recht dat nogal eens botst met andere fundamentele rechten die net zozeer door het Handvest worden beschermd

Als zij daarbij doorschieten in hun interpretaties, is er de rechter om hen terug te fluiten.

Dergelijke argumenten gaan echter voorbij aan enkele fundamentele problemen van deze activistische richting binnen het privacytoezicht.

In de eerste plaats kan er niet aan voorbijgegaan worden dat de AP toeziet op slechts één fundamenteel recht dat nogal eens botst met andere fundamentele rechten die net zozeer door het Handvest worden beschermd. Dit draagt een risico in zich op een monomane aanpak. Ook andere fundamentele rechten en belangen moeten worden meegewogen, juist als die tegenstrijdig zijn. De hiervoor geschetste voorbeelden laten echter zien dat andere fundamentele rechten, zoals de ondernemersvrijheid, het beginsel van contractsvrijheid en meer collectieve belangen zoals veiligheid en volksgezondheid,⁴⁸ in de visie van de AP nogal gemakkelijk het onderspit delven.

In de tweede plaats is de kern van het probleem niet zozeer gelegen in de kritische opstelling van de AP en andere Europese toezichthouders, maar in het middel dat zij daarvoor kiezen. De rechtmatigheidsgrondslagen vormen een te bot instrument om specifieke ontwikkelingen of spelers te reguleren. De AVG is een omnibuswet die alle verwerkingen van persoonsgegevens beoogt te reguleren. De rechtmatigheidsgrondslagen kunnen binnen die wet worden gezien als een eerste algemene drempel waaraan alle verwerkingen moeten voldoen. Zoals de voorgaande bespreking heeft laten zien, resulteert een iets strengere uitleg van een rechtmatigheidsgrond onvermijdelijk in onbedoelde en ongewenste bijvangst: ook andere verwerkingen worden verboden terwijl die niet ter discussie stonden. Die onvoorziene gevolgen moeten dan later weer gerepareerd worden met gekunstelde redeneringen. Het eindresultaat raakt steeds verder losgezongen van opvattingen in andere rechtsgebieden en van 'common sense'. Daardoor is er zeker voor leken maar in toenemende mate voor ingewijden nauwelijks nog een touw aan vast te knopen. Dat is des te onwenselijker nu het hier niet gaat om details waar alleen privacy-professionals zich in behoeven te verdiepen (en waar vingerwijzingen van de toezichthouders juist zeer welkom kunnen zijn), maar om de fundamentele en voor iedere verwerkingsverantwoordelijke onontkoombare voorvraag of verwerking is toegestaan. De rechtmatigheidsgrondslagen vergen vanwege hun algemene toepassingsbereik een 'light touch' door de toezichthouder.

Als de toezichthouder misstanden wil aanpakken, biedt de AVG genoeg andere voorschriften die zich beter lenen voor handhaving. Daarbij kan gedacht worden aan de specifieke eisen die de AVG stelt aan informatievoorziening aan betrokkenen,⁴⁹ en de regels voor verwerkingen die bijzondere risico's meebrengen, zoals de bepalingen over gevoelige gegevens,⁵⁰ profilering en geautomatiseerde besluitvorming.⁵¹ Binnen de grondslag van het gerechtvaardigd belang lenen de tweede en de derde stap (is de verwerking proportioneel in het licht van het gestelde belang en zijn er voldoende waarborgen getroffen om de conclusie te rechtvaardigen dat deze gestelde belangen zwaarder mogen wegen dan die van de betrokkenen?) zich beter voor het aanpakken van misstanden en bijsturen van gedrag dan de eerste stap (is sprake van een belang dat als gerechtvaardigd kan worden gekwalificeerd?). Aldus beschouwd is handhaving met de 'botte bijl' van de grondslagen ook een gemakzuchtige vorm van toezicht: de toezichthouder hoeft niet toe te komen aan de gedetailleerde analyse van de verwerking zelf maar verwerpt die met min of meer principiële argumenten. Het kan wellicht verklaren waarom deze benadering school heeft gemaakt bij een toezichthouder die al jaren klaagt over onderbezetting,⁵² maar rechtvaardigt daarmee niet alle *collateral damage* van dien.

In de derde plaats moet bedacht worden dat een algemene normuitleg van de toezichthouder in Nederland als zodanig niet door de rechter getoetst kan worden. Voor organisaties die persoonsgegevens verwerken, zit er dus weinig anders op dan zich neer te leggen bij de strengere opvattingen van de toezichthouder, of om het op handhaving te laten aankomen. Dat laatste is een weinig aantrekkelijk vooruitzicht voor de meeste organisaties: die boetes kunnen oplopen tot € 20 miljoen of, als dat meer is, 4% van de jaaromzet. Daarbij komt nog de publicitaire schade van handhaving, waarbij bij het publiek toch vooral de boodschap zal beklijven dat de betreffende organisatie de privacy schendt. Dat is een aanzienlijk – en voor de meeste organisaties prohibitief – prijskaartje voor het voeren van een principiële juridische discussie. En zo is en blijft de praktijk vooral gestuurd door de beschikkingspraktijken van toezichthouders, en hun eigen richtsnoeren en opinies. De drempel voor rechterlijke controle ligt hier dus in de praktijk behoorlijk hoog; toezichthouders hebben tot nu toe weinig rechterlijke tucht te vrezen voor hun meer extreme opvattingen.

Het is op zich waar dat de wetgever soms moeite heeft om de ontwikkelingen bij te benen, en ook dat het eindresultaat niet altijd even duidelijk is. Een rechtvaardig

ging voor de langere doorlooptijden bij de wetgever kan echter worden gevonden in het feit dat die meer belangen heeft te dienen dan alleen privacy en bovendien het democratisch wetgevingsproces moet doorlopen. Dat zal waarschijnlijk ook verklaren waarom de Europese wetgever soms wetten aanneemt die moeilijk te rijmen zijn met de koers die sommige van de meer puristische privacy-toezichthouders voorstaan. Recente voorbeelden hiervan zijn de Europese Telecomcode⁵³ en de Richtlijn modernisering consumentenbescherming⁵⁴ waarin wordt erkend dat een contract in ruil voor persoonsgegevens kan worden aangegaan, terwijl privacy-toezichthouders daar duidelijk bedenkingen bij hebben.⁵⁵

Toch blijft de wetgever de aangewezen instantie om te reageren op maatschappelijk ongewenste ontwikkelingen in het domein van gegevensverwerkingen. Al was het maar omdat de wetgever, anders dan de toezichthouder, democratisch is gelegitimeerd, wetgeving een transparant proces moet doorlopen, en pas geldt na publicatie.⁵⁶ De wetgever kan en moet alle relevante belangen en rechten afwegen. Als we als samenleving bijvoorbeeld in meerderheid vinden dat grote dataplatforms zich met hun handelspraktijken te veel klantgegevens toe-eigenen, dan zou de reactie daarop niet moeten zijn om algemene rechtmatigheidsgrondslagen ineens strenger toe te passen op alle organisaties die persoonsgegevens verwerken. Een meer gepaste reactie is dan dat er een nieuwe wet komt die voorziet in bijzondere regels voor zulke grote platforms, waaronder de verplichting dat die altijd toestemming moeten vragen voor niet-noodzakelijke gegevensverwerkingen.⁵⁷

In geen geval zou een hiaat over de rug van justitiabelen moeten worden ingevuld in handhavingsbesluiten met aanzienlijke boetes. Zij verdienen het voordeel van de twijfel en de bescherming van het *lex-certa*-beginsel. De AVG biedt de AP bovendien verschillende andere, minder vergaande bevoegdheden die bij de invulling van open normen uit oogpunt van subsidiariteit de voorkeur verdienen, zoals de waarschuwing, berisping of last.

De AVG heeft privacy-toezichthouders vergaande handhavingsbevoegdheden gegeven. *With great power comes great responsibility*: in dit geval om de verleiding te weerstaan op de stoel van de wetgever te gaan zitten. Het is aan de wetgever haar verantwoordelijkheid te nemen als specifieke regels gewenst zijn. Als de wetgever verzaakt, brengt die verantwoordelijkheid de verplichting mee voor toezichthouders om hun bevoegdheden terughoudend in te zetten, en daarmee niet het recht een door hen gewenste kant op te duwen. •

45. Conseil d'État, 19 juni 2020, nr. 434684.

46. digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation.

47. Rb. Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111. De AP heeft hoger beroep ingesteld tegen deze uitspraak.

48. Zie voetnoot 10.

49. Art. 12-14 AVG.

50. Art. 9 AVG.

51. Art. 22 AVG.

52. 'Groeit AP noodzakelijk voor burgers en bedrijfsleven in digitaliserende samenleving', beschikbaar op de website van de AP.

53. Richtlijn (EU) 2018/1972, zie overwe-

ging 16.

54. Richtlijn (EU) 2019/2161, zie overwe-
ging 33.

55. Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679, randnr. 26, beschikbaar op edbp.europa.eu.

56. In vergelijkbare zin: J.E.J. Prins,

'Toezichthouders en publiekelijke verantwoording', *NJB* 2021/1799, afl. 25.

57. Precies zo'n regeling wordt voorgesteld in artikel 5 a) van het wetsvoorstel van de Commissie voor een wet inzake digitale markten, COM(2020) 842 final, 2020/0374(COD).