Indirecte herleidbaarheid van persoonsgegevens: hoe moeilijk is het?

*Quinten Kroes**

Hoe moeilijk is het? Die ogenschijnlijk eenvoudige vraag raakt aan de kern van een jarenlang gevoerde discussie in het privacyrecht: wanneer is sprake van een persoonsgegeven in de zin van de AVG? Is het voldoende dat gegevens in abstracto tot een persoon herleidbaar zijn, of moet worden gekeken naar de concrete mogelijkheden van degene die de gegevens ontvangt? Over deze vraag woedt in het privacyrecht al jaren een fundamentele scholenstrijd – de absolute versus de relatieve benadering. Met zijn arrest van 4 september 2025 heeft het Hof van Justitie van de Europese Unie die strijd nu beslist – en daarbij een duidelijke koers uitgezet met potentieel verstrekkende gevolgen, ook voor de mediapraktijk als het gaat om het publiceren van gepseudonimiseerde informatie.

Inleiding

In dit blad is met enige regelmaat aandacht besteed aan belangrijke rechtspraak van het Hof van Justitie over de uitleg van het in de Algemene Verordening Gegevensbescherming (AVG) centrale begrip 'persoonsgegeven'.[1] Op 4 september 2025 wees het Hof arrest[2] in het hoger beroep van de Europese privacytoezichthouder voor instellingen (EDPS) tegen een eerder hier geannoteerde uitspraak van het Gerecht.[3] In die uitspraak had het Gerecht een door de EDPS aan een Europese instelling (de GAR[4]) opgelegde boete vernietigd, mede omdat de EDPS volgens het Gerecht was uitgegaan van een onjuiste opvatting van het begrip persoonsgegeven. In zijn arrest heeft het Hof nu uitdrukkelijk gekozen voor een relatieve benadering: bij de beoordeling of niet-direct identificerende gegevens als persoonsgegevens moeten worden aangemerkt, is doorslaggevend welke mogelijkheden de ontvanger of lezer redelijkerwijs heeft om tot heridentificatie over te gaan. Daarmee verwierp het Hof de door Europese toezichthouders bepleite absolute benadering. Concreet betekent dat dat als er gegevens worden gedeeld of gepubliceerd waarin direct identificerende gegevens zijn vervangen door pseudoniemen, het erom gaat welke mogelijkheden de ontvanger of lezer redelijkerwijs heeft om die informatie toch weer te herleiden tot bepaalde personen. Met andere woorden: hoe moeilijk is het voor de ontvanger om tot heridentificatie over te gaan?

Het begrip "persoonsgegeven" is in de Algemene Verordening Gegevensbescherming 2016(AVG) gedefinieerd als "alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon", met daarbij de verduidelijking dat als "identificeerbaar" wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd.[5] De AVG noemt in de definitie enkele voorbeelden aan de hand waarvan identificatie kan plaatsvinden.[6] Die lijst is niet uitputtend. In de preambule is namelijk verduidelijkt dat ter beoordeling of een persoon aan de hand van een bepaald gegeven identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs inzetbaar zijn door degene die voor de verwerking verantwoordelijk is, dan wel door enig ander persoon.[7] In die laatste zes woorden ligt eigenlijk de kern besloten van het verschil tussen de absolute of de relatieve opvatting. In de absolute opvatting is enkel van belang of zulke middelen bestaan, en wordt niet gekeken naar de kans dat die worden ingezet door de gebruiker van de informatie. In de relatieve opvatting moet dat wel worden beoordeeld, en wel vanuit het perspectief van de gebruiker van de informatie.[8] Het verschil doet zich met name voelen bij pseudonimisering. Dit is in de AVG gedefinieerd als het proces waarbij persoonsgegevens een zodanige bewerking ondergaan "dat die 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 gekoppeld."[9] Bij 'aanvullende gegevens' in deze definitie kan worden gedacht aan een tabel die een medisch

* Mr. Q.R. Kroes is advocaat te Amsterdam (Brinkhof) en redacteur van dit blad.

1 *Mediaforum* 2017-1, nr. 2, *Mediaforum* 2023-3, nr. 7; zie over het onderwerp ook mijn bespreking van de oratie van Zwenne, *Mediaforum* 2014-2, p. 27.
2 HvJ EU 4 september 2025, C-413/23 P (*EDPS/GAR*), ECLI:EU:C:2025:645; zie Jurisprudnie nr. 2 verderop in dit nummer, p. 28-35.
3 *Mediaforum* 2023-3, nr. 7.
4 GAR staat voor Gemeenschappelijke Afwikkelingsraad. De Engelse afkorting is SRB.
5 Art. 4 1) AVG.
6 Bijv. aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die persoon.
7 Preambule overweging 26.
8 Om die reden wordt ook wel gesproken van de objectieve, respectievelijk de subjectieve benadering.
9 Artikel 4 5) AVG

onderzoeker hanteert met voor elke patiëntnaam een unieke code,[10] en die hem in staat stelt patiëntgegevens in een databank aan anderen te ontsluiten voor wetenschappelijke analyse zonder onnodige privacyinbreuk. De databank bevat in plaats van de patiëntnamen alleen hun unieke codes. Het aldus hanteren van een pseudoniem maakt het mogelijk voor elke patiënt gegevens door de tijd heen te kunnen blijven toevoegen. Mocht het nodig zijn om individuele patiënten op de hoogte te stellen van relevante uitkomsten van wetenschappelijk onderzoek, dan kan de identiteit via de tabel zo nodig achterhaald worden.

Het is duidelijk dat in dit voorbeeld de gegevens voor de onderzoeker die de tabel bijhoudt, persoonsgegevens zijn, en dat – ondanks de door hem toegepaste pseudonimisering – blijven. Hij heeft immers toegang tot de 'aanvullende gegevens' die nodig zijn om de wetenschappelijke gegevens met alleen de unieke codes, weer terug te herleiden naar individuele patiënten. Maar hoe zit het met andere wetenschappers die de databank met alleen de unieke codes zien, en die geen toegang hebben tot de pseudonimeringstabel? Precies over zo'n casus ging het arrest in de zaak van de EDPS tegen de GAR. Het was echter niet de eerste keer dat het Hof zich uitliet over de materie, zoals ook blijkt uit de verwijzingen van het Hof naar eerdere jurisprudentie.

Eerdere jurisprudentie van het Hof over gepseudonimiseerde persoonsgegevens

In het standaardarrest *Breyer*[11] was eigenlijk ook een pseudonimiseringscasus aan de orde. Het ging daar om de vraag of een websiteaanbieder (in dit geval: de Duitse overheid) die IP-adressen van bezoekers bijhoudt, daarmee persoonsgegevens verwerkt. In dit geval was het mogelijk om, zo nodig, via de internetaanbieder de identiteit van de gebruiker van ee IP-adres op een bepaald moment te achterhalen, omdat ISPs bijhouden aan welke klanten zij welke IP-adressen beschikbaar stellen. Anders gezegd: het was duidelijk dat weliswaar de websiteaanbieder die de IP-adressen van de bezoekers opsloeg, niet zelf over middelen beschikte die identificatie mogelijk maakten, maar dat er wel een derde was, de ISP van de websitebezoeker, met zulke middelen. Het Hof oordeelde dat het enkele feit dat die middelen bij een derde berusten, niet meebrengt dat er voor de websiteaanbieder geen sprake is van persoonsgegevens. Nagegaan moet worden of die websiteaanbieder zich daartoe legaal toegang kan verschaffen.[12] Dat gaf dus eigenlijk al blijk van een relatieve/subjectieve benadering, in die zin dat het perspectief van de gebruiker van de data telt. Maar de subjectiviteit gaat niet zo ver dat het oogmerk van die gebruiker bepalend is; het gaat om de middelen waartoe die zich redelijkerwijs toegang kan verschaffen, niet of die ook daadwerkelijk van plan is van die mogelijkheid gebruik te maken. In het *Breyer*-arrest liet het Hof het aan de nationale rechter om na te gaan of een websiteaanbieder inderdaad over wettige middelen beschikte om de identiteit via de ISP te achterhalen, weliswaar met de vingerwijzing dat daarbij ook rekening gehouden moest worden met de mogelijkheid dat de opsporingsautoriteiten dit zouden kunnen afdwingen na een aangifte van de websiteaanbieder.

Een later voorbeeld, waarin het Hof wel zelf overging tot toepassing van de *Breyer*-toets of toegang tot de pseudonimisatiesleutel wettig kon worden afgedwongen, biedt de *IAB Europe*-casus.[13] Daar ging het om codes (de zogeheten TC-strings[14]) die als onderdeel van cookies worden opgeslagen en waarmee wordt vastgelegd of een specifieke gebruiker op een website toestemming heeft gegeven voor het wel of niet plaatsen of lezen van trackingcookies voor advertentiedoeleinden. IAB Europe is de Europese brancheverenigingen voor ondernemingen in digitale reclame en marketing, en heeft daarvoor een uniform protocol opgesteld,[15] zodat haar leden deze informatie met elkaar kunnen uitwisselen. In zijn arrest bevestigde het Hof opnieuw dat een gegeven niet in isolatie moet worden beschouwd en dat ook moet worden gekeken naar eventuele aanvullende informatie bij derden. Toegepast op de TC-string, oordeelde het Hof dat de TC-string gekoppeld kon worden aan andere gegevens (zoals het IP-adres van het apparaat waarop het cookie is geplaatst en waarmee een website wordt bezocht), waarmee weer aanvullende gegevens over individueel surfgedrag kunnen worden verzameld en een gebruikersprofiel kan worden gemaakt. Dat IAB Europe zelf als faciliterende brancheverenigingen noch beschikt over de TC-strings, noch over IP-adressen en eventuele overige gegevens die door TCF-deelnemers worden verwerkt, achtte het Hof niet doorslaggevend, want het kan al genoeg zijn dat die informatie bij anderen berust.[16] Wel speelt daarbij dus de vraag of IAB beschikt over wettige middelen om zich daartoe toegang te verschaffen. Dat achtte het Hof hier het geval, nu in de contractuele afspraken tussen IAB Europe en haar leden was vastgelegd dat die op verzoek alle informatie aan IAB moeten verstrekken waarover zij beschikken om gebruikers te identificeren. Daarmee was sprake van middelen ter identificatie waarvan redelijkerwijs moet worden aangenomen dat IAB Europe die kan inzetten.[17]

Een interessante variant, waaruit blijkt dat ook tijdsverloop een rol kan spelen, biedt een arrest inzake voertuigidentificatienummers (VINs).[18] In de marge van een geschil tussen een brancheverenigingen voor de handel in auto-onderdelen en vrachtwagenfabrikant Scania, speelde de vraag of VINs persoonsgegevens vormen. VINs worden door de autofabrikant aan elk nieuw voertuig toegekend, al voordat de eigenaar of gebruiker van dat voertuig bekend is. Op dat moment kan dus moeilijk worden volgehouden dat dit gegeven betrekking heeft op een geïdentificeerd of identificeerbaar natuurlijk persoon. Zodra die eigenaar bekend is, wordt deze informatie echter tezamen met het nummer vastgelegd in registratiesystemen, die onder meer toegankelijk zijn voor reparatiedoeleinden. Hier bevestigde het Hof dat het VIN weliswaar op het moment dat het wordt toegekend, geen persoonlijk karakter heeft, maar dat later wel verkrijgt zodra de mogelijkheid ontstaat

10 Naast het handmatig bijhouden van een pseudonimisatietabel, zijn er verschillende andere methoden, zoals het geautomatiseerd toepassen van hashing algoritmen. Dit zijn cryptografische formules die bij een unieke invoer (bijv. een IP-adres, telefoonnummer of emailadres) steeds eenzelfde unieke code als uitvoer berekenen.

11 HvJ EU 19 oktober 2016, ECLI:EU:C:2016:779, *Mediaforum* 2017-1, nr. 2, m.nt. Q.R. Kroes.

12 In de woorden van het Hof: "beschikt over wettige middelen waarmee hij de betrokken persoon kan identificeren aan de hand van extra informatie die bij de internetprovider van deze persoon berust" (r.o. 49).

13 HvJ EU 7 maart 2024, C-604/22, ECLI:EU:C:2024:214.

14 TC-string staat voor Transparency and Consent String.

15 Het zogeheten Transparency & Consent Framework (TCF).

16 R.o, 46.

17 R.o. 48 en 49.

18 HvJ EU 9 november 2023, C-319/22, ECLI;EU:C:2023:837 (*Gesamtverband Autoteile-Handel/Scania*).

om het aan een bepaalde persoon te relateren, zoals de eigenaar of een ander die over het voertuig mag beschikken.[19] Dat brengt mee dat de fabrikant die het VIN verstrekt aan derden, moet uitgaan van deze toekomstige identificatiemogelijkheid, en het VIN als persoonsgegeven zal moeten aanmerken.

Het *GAR*-arrest

Daarmee zijn we beland bij het *GAR*-arrest zelf, dat naar alle hiervoor genoemde arresten verwijst en daarop voortbouwt. De GAR kwam in actie toen een Spaanse bank van dreigend faillissement gered moest worden. Het privacygeschil zag op online-inschrijvingsformulieren met opmerkingen van aandeelhouders en crediteuren die voor compensatie van de GAR in aanmerking wilden komen, vooruitlopend op een hoorzitting. Binnen de GAR vond eerst verificatie plaats (kwamen deze aandeelhouders /crediteuren in aanmerking voor compensatie), en werden direct-identificerende gegevens geschrapt. Wat overbleef was een unieke alfanumerieke code die aan elk formulier was toegekend, en die dus feitelijk als pseudoniem fungeerde. De aldus gepseudonimiseerde formulieren verstrekte de GAR aan Deloitte, die per aanvrager een bepaalde berekening moest maken. De EDPS legde vervolgens een boete op aan de GAR, omdat zij vond dat de GAR tegenover de betrokkenen transparant had moeten zijn over deze verstrekking van hun persoonsgegevens aan een derde. In het beroep van de GAR tegen die boete, ging het Gerecht over tot vernietiging van die boete omdat de EDPS onvoldoende feitenonderzoek had gedaan om te concluderen dat de GAR persoonsgegevens had verstrekt aan Deloitte. Dat had de EDPS namelijk alleen vanuit het perspectief van de GAR beoordeeld, terwijl zij had moeten onderzoeken of het voor Deloitte mogelijk was om de verstrekte formulieren met redelijke middelen te herleiden naar de personen.[20] Tegen die uitspraak kwam de EDPS in hoger beroep bij het Hof van Justitie. Daarbij bepleitte de EDPS de absolute benadering: het enkele feit dat de GAR beschikte over middelen die identificatie mogelijk maakten, zou al meebrengen dat sprake is van persoonsgegevens. De toets of de inzet van dat middel door Deloitte redelijkerwijs te verwachten is, kan in de visie van de EDPS achterwege blijven. Hoewel geen unanimiteit bestond onder Europese privacytoezichthouders in deze discussie, was wel duidelijk dat de meerderheid van hen deze absolute benadering voorstond; de EDPB, het comité met vertegenwoordigers van alle Europese privacytoezichthouders, kwam in het beroep op aan de zijde van de EDPS. Het belang dat toezichthouders aan deze discussie hechten, werd nog verder onderstreept toen de EDBP begin 2025 concept-richtsnoeren publiceerde over pseudonimisatie en anonimisatie.[21] Dat in de *GAR*-zaak de zitting bij het Hof van Justitie al had plaatsgevonden en het arrest nog gewezen moest worden, weerhield de EDPB er niet van om haar pleidooi voor de absolute benadering in dat document voort te zetten. Dat kwam het in de consultatie op felle kritiek te staan van, onder meer, de IAB.[22]

Het heeft de EDPS niet mogen baten. In zijn arrest heeft het Hof geoordeeld dat het vereiste van identificeerbaarheid bij pseudonieme datasets aan de hand van de concrete omstandigheden moet worden onderzocht. Hierin wijken pseudonieme datasets af van anonieme datasets (dat wil zeggen: datasets waarmee de betrokkene niet of niet meer geïdentificeerd kan worden). Het relevante verschil – zo volgt uit de definitie van pseudonimisering – is dat bij gepseudonimiseerde datasets nog aanvullende informatie beschikbaar is die identificatie mogelijk maakt, en bij anonieme datasets niet (meer). Tegelijkertijd is het doel van pseudonimisering (en de technische en organisatorische maatregelen (ook wel afgekort als: TOMs) die worden getroffen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld) wel om te voorkomen dat de ontvanger van de pseudonieme dataset die gegevens nog kan herleiden naar een individu. In het concrete geval van de GAR moest daarom beoordeeld worden of Deloitte over redelijke middelen beschikte om de betrokkenen te identificeren. Die beoordeling omvat volgens het Hof twee aspecten: ten eerste of Deloitte de pseudonimisatiemaatregelen ongedaan kon maken (bijvoorbeeld door medewerking af te dwingen van GAR) en ten tweede of de TOMs beletten dat Deloitte tot heridentificatie kon overgaan door inzet van andere identificatiemiddelen, zoals vergelijking met andere elementen (kon Deloitte zelf op zoek gaan naar aanvullende informatie, bijvoorbeeld door de in het formulier vermelde precieze jaaromzet en sector te proberen te herleiden naar de concrete ondernemer?).[23] Bij de vraag welke middelen redelijkerwijs inzetbaar zijn, moet rekening worden gehouden met "alle objectieve factoren, zoals kosten en tijd die nodig zijn voor identificatie, met inachtneming van beschikbare technologie op tijdstip van verwerkingen en de technologische ontwikkelingen". De enkele aanwezigheid van die identificerende informatie volstaat niet: het gaat erom hoe moeilijk het is om die te achterhalen.[24] Het Hof verwerpt uitdrukkelijk de onder toezichthouders vigerende opvatting dat pseudonieme gegevens altijd persoonsgegevens zijn en blijven: dat zou de identificeerbaarheidstoets namelijk zinledig maken.[25] Hiermee trekt het Hof een duidelijke grens aan de gestaag uitdijende[26] betekenis van het begrip persoonsgegeven: die is volgens het Hof weliswaar ruim maar niet onbeperkt.[27]

Toepassing in de context van publicaties

Het Hof verwijst in zijn arrest ook naar een eerdere zaak die illustreert hoe de nu omarmde relatieve opvatting uitpakt als gepseudonimiseerde gegevens worden gepubliceerd (en dus niet op voorhand duidelijk is wie daarvan kennis zal nemen). Daar ging het om een persbericht dat was uitgebracht door OLAF, het Europees Bureau voor Fraudebestrijding, waarin een niet met naam genoemde wetenschapper werd beschuldigd van subsidiefraude. De wetenschapper diende een schadeclaim in tegen OLAF, onder meer omdat zij het persbericht in strijd achtte met de privacyregels. In dat kader stelde zij zich op het standpunt dat haar identiteit relatief gemakkelijk te

19 R.o. 46.

20 *Mediaforum* 2023-3, nr. 7, m.nt. Q.R. Kroes.

21 https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_en.

22 "*the EDPB's adoption of Guidelines that reflect the view of the EDPS (as party to the EDPS v SRB case) creates the impression of an attempt to influence the judgment of the Court of Justice*", volledige zienswijze is te vinden op https://www.edpb.europa.eu/sites/default/files/webform/public_consultation_reply/iab-europe-s-response-to-the-edpb-public-consultation-on-draft-guidelines-1_2025-on-pseudonymisation.pdf.

23 R.o. 77.

24 R.o. 82.

25 R.o. 80.

26 Vgl. de kritiek van A-G Bobek in zijn opinie voor zaak C-245/20, aangehaald in de annotatie van Q,R. Kroes bij HvJ EU 24 maart 2022, ECLI:EU:C:2022:216, *Mediaforum* 2022-2, nr. 4.

27 R.o. 88.

achterhalen was geweest aan de hand van enkele elementen uit het persbericht (namelijk haar nationaliteit, geslacht, jonge leeftijd, het feit dat haar vader werkzaam was aan de betrokken Griekse universiteit, en het bedrag van de toegekende subsidie). Het was een journalist ook daadwerkelijk gelukt de identiteit van de betrokken wetenschapper vast te stellen en haar naam op Twitter/X te onthullen, met als gevolg dat zij een aanstelling bij een andere universiteit verloor. Het Gerecht stelde zich op het standpunt dat alleen moet worden gekeken naar de informatie die in het persbericht zelf was opgenomen, en dat geen rekening behoeft te worden gehouden met andere informatie die een lezer erbij kan zoeken.[28] Daarbij overwoog het Gerecht dat haar identiteit in dit geval niet achterhaald was door een gemiddelde lezer, maar door een onderzoeksjournalist die gespecialiseerd was in wetenschappelijk onderzoek en die beschikte over subjectieve, externe kennis over de betrokkene. In beroep gooit het Hof het echter over een andere boeg.[29] De elementen uit het persbericht vormen volgens het Hof in hun geheel beschouwd informatie aan de hand waarvan de persoon op wie dat persbericht betrekking heeft, kan worden geïdentificeerd, met name door personen die op hetzelfde wetenschappelijke gebied werkzaam zijn en die de beroepsloopbaan van de betrokkene kennen. Het risico op heridentificatie is daarmee niet onbeduidend; voor personen die op hetzelfde wetenschappelijke gebied werkzaam zijn, vergt identificatie geen inspanning die gelet op de daarmee gemoeide tijd, kosten en mankracht als excessief kan worden beschouwd.[30] Daarbij weegt het Hof mee dat een persbericht met deze strekking nu eenmaal de belangstelling van het publiek kan wekken en de lezers, met name journalisten, ertoe kan aanzetten zoekopdrachten te verrichten naar de persoon op wie het persbericht betrekking heeft. De publicatie van het persbericht vormde dus een verwerking van persoonsgegevens die moet voldoen aan de regels ter bescherming daarvan, onder meer het vereiste dat daarvoor een in die regels erkende grondslag moet bestaan. Het resulteerde in een terugverwijzing naar het Gerecht, dat moest nagaan of de regels ter bescherming van persoonsgegevens met het persbericht waren nageleefd. In deze herkansing oordeelde het Gerecht dat dit niet het geval was geweest.[31] Het achtte weliswaar een grondslag aanwezig, omdat de verwerking had plaatsgevonden voor de vervulling van een taak in het algemeen belang of in het kader van de uitoefening van het openbaar gezag dat aan OLAF is verleend, maar vond de mate van detail in het persbericht niet noodzakelijk voor die taak of gezagsuitoefening. Dergelijke informatie had het niet alleen mogelijk gemaakt om de betreffende onderzoeker te identificeren, maar vond het Gerecht bovendien (met uitzondering van het bedrag van de toegekende subsidie) niet noodzakelijk om het publiek te informeren over de feiten die de wetenschapper na het onderzoek van OLAF werden verweten. Volgens het Hof leidde toevoeging van persoonlijke details zelfs af van het doel om het publiek te informeren over activiteiten van OLAF omdat er media-aandacht werd gevestigd op randzaken.[32] Daarnaast oordeelde het Gerecht dat OLAF met het persbericht in strijd had gehandeld met het vermoeden van onschuld en de beginselen van behoorlijk bestuur. Het kwam de Commissie te staan op een veroordeling tot betaling van een schadevergoeding van € 50.000.

Gevolgen van het *GAR-arrest*

Het Hof van Justitie heeft met het *GAR*-arrest een belangrijke knoop doorgehakt in het gegevensbeschermingsrecht. In feite heeft het bevestigd dat de risicogebaseerde benadering, die de AVG voorschijft bij de toepassing van verschillende normen die in acht moeten worden genomen bij de verwerking van persoonsgegevens,[33] al zit ingebakken in de definitie van het begrip persoonsgegevens zelf. Als het risico op herleidbaarheid van gegevens door de ontvanger gering is, dan zijn die normen op de verwerking van zulke gegevens helemaal niet meer van toepassing. Het verbaast dan ook niet dat het arrest al een belangrijke impact heeft gehad, en ongetwijfeld ook nog zal blijven hebben, al roept het ook nieuwe vragen op en zijn de repercussies dus nog niet geheel te overzien. Een korte opsomming volgt hieronder.

Codificatie in de Digitale Omnibus

Kort na het arrest van het Hof publiceerde de Commissie haar voorstel tot vereenvoudiging van het digitale wetgevingskader en tot intrekking van een aantal verordeningen op dat vlak, onder de naam Digitale Omnibus.[34] Met deze Digitale Omnibus wil de Commissie gehoor geven aan de oproep in het Draghi-rapport om het concurrentievermogen te versterken door het EU-acquis te vereenvoudigen, te verduidelijken en te verbeteren. Ook het vlaggenschip van het Europese regelgeving, de AVG, ontkomt daarbij niet aan aanpassing. Opvallend onderdeel van die aanpassing is de codificatie van de kersverse relativiteitslijn van het Hof. Het voorstel doet dat door voor de definitie van persoonsgegevens te verduidelijken dat informatie voor een bepaalde entiteit niet als persoonsgegevens wordt beschouwd wanneer deze niet beschikt over de middelen die redelijkerwijs kunnen worden gebruikt om de natuurlijke persoon te identificeren op wie de informatie betrekking heeft.[35] De verdere verwerking door een dergelijke entiteit valt dus in beginsel niet binnen het toepassingsgebied van de AVG.

Herziening bestaande richtsnoeren

Ongeacht wat er verder met de Digitale Omnibus gebeurt, is wel duidelijk dat ook Europese toezichthouders huiswerk hebben te doen. Er zijn de afgelopen jaren de nodige richtsnoeren uitgevaardigd die uitgaan van de premisse dat pseudonimisering slechts een beveiligingsmaatregel is die er nooit toe kan leiden dat het resultaat van die bewerking niet meer onder de AVG valt. Hiervoor werden al de recente ontwerp-

28 Gerecht 4 mei 2022, T-384/20, EU:T:2022:273.

29 HvJ EU 7 maart 2024, C-413/23, ECLI:EU:C:2024:215.

30 R.o. 60 en 61.

31 Gerecht 1 oktober 2025, T-384/20 RENV, ECLI:EU:T:2025:925.

32 R.o. 59 en 60.

33 Zie bijv. de artikelen 24 en 32 AVG, die voorschrijven dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen moet treffen, en daarbij rekening houdt met de aard, omvang, de context en het doel van de verwerking, en als het gaat om beveiligingsmaatregelen ook de stand van de techniek en de uitvoeringskosten, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen.

34 COM(2025) 837 final, 2025/0360(COD).

35 Aan de definitie van persoonsgegevens wordt door artikel 3 van de voorgestelde Digitale Omnibus de volgende tekst toegevoegd: "Informatie over een natuurlijke persoon is niet noodzakelijkerwijs persoonsgegevens voor elke andere persoon of entiteit, louter omdat een andere entiteit die natuurlijke persoon kan identificeren. Informatie is voor een bepaalde entiteit niet persoonlijk indien die entiteit de natuurlijke persoon op wie de informatie betrekking heeft, niet kan identificeren, rekening houdend met de middelen die redelijkerwijs door die entiteit kunnen worden gebruikt. Dergelijke informatie wordt voor die entiteit niet persoonlijk louter omdat een potentiële latere ontvanger over middelen beschikt die redelijkerwijs kunnen worden gebruikt om de natuurlijke persoon op wie de informatie betrekking heeft, te identificeren."

richtsnoeren over pseudonimisatie en anonimisatie genoemd, waarin de EDPB nog een laatste lans brak voor die opvatting. Als Nederlands voorbeeld kan worden gewezen op de AP-handreiking over scraping. Daarin staat nu nog te lezen: "Verwerkt u persoonsgegevens doordat u scraping inzet? Of verwerkt u gescrapete persoonsgegevens? Dan moet u voldoen aan de eisen die de AVG aan de verwerking van persoonsgegevens stelt."[36] Uit de relatieve leer volgt dat deze stelling niet zonder meer is vol te houden. Het zal van de concrete dataset en de gebruiker afhangen of sprake is van persoonsgegevens. Een effectieve pseudomiseringsslag door een scraper die de data van het internet verzamelt, kan er – in elk geval in theorie – toe leiden dat voor de ontvanger van de dataset geen sprake meer is van persoonsgegevens.

Doorgifte naar derde landen

Zoals ik in mijn noot bij de uitspraak van het Gerecht al opperde, kan pseudonimisering ertoe leiden dat bij een doorgifte van gegevens geen sprake meer is van doorgifte van persoonsgegevens vanuit het (volgens het Hof relevante) perspectief van de ontvanger. Dat betekent dat de strenge beperkingen die de AVG stelt aan doorgifte van persoonsgegevens naar landen buiten de Europese Unie[37] in zo'n geval niet gelden. Pseudonimisering kan zo worden ingezet als 'exit-strategie'[38] voor de AVG.

Een in deze context onbeantwoorde vraag is of een dergelijke exit-strategie ook toepasbaar is in de context waarbij de doorgifte binnen een concern plaatsvindt. Concernverhoudingen zullen dan wellicht van invloed zijn voor het antwoord op de vraag of de ontvanger (of een autoriteit onder wier jurisdictie de ontvanger valt) over middelen beschikt die redelijkerwijs ingezet kunnen worden om alsnog tot herleiding over te gaan.

Anonimisatiepraktijken bij pers en rechtspraak

In de praktijk worden soms direct identificerende gegevens (zoals iemands naam) geschrapt voorafgaand aan publicatie om de privacyimpact van een publicatie te verminderen.[39] Gedacht kan worden aan de in de Nederlandse journalistiek gangbare praktijk om verwijzingen naar verdachten te beperken tot voornaam, initiaal van de achternaam en eventueel woonplaats en leeftijd. Het is duidelijk dat deze vorm van anonimisering (die onder de AVG moet worden gekwalificeerd als pseudonimisering) in veel gevallen niet het effect zal hebben dat een publicatie niet onder de reikwijdte van de AVG valt. Dat geldt temeer nu uit de *OLAF*-jurisprudentie volgt dat rekening moet worden gehouden met lezers met bepaalde voorkennis of voor wie het zonder excessieve inspanning met wat zoekopdrachten mogelijk is de identiteit van de verdachte te achterhalen. Ook de journalistieke exceptie[40] brengt niet mee dat de AVG kan worden genegeerd, nu die niet de hele AVG buiten toepassing verklaart. Journalisten moeten (net als OLAF in de hiervoor besproken casus) wel een geldige AVG-grondslag kunnen aanwijzen, en zijn gehouden aan de beginselen van proportionaliteit en dataminimalisatie.[41] Een vergelijkbare problematiek doet zich voor bij de publicatie van rechterlijke uitspraken door de rechtspraak. De nogal mechanische pseudonimiseringsrichtlijn van de rechtspraak[42] voorziet alleen in het pseudonimiseren van gegevens zoals naam en adres, maar laat overige context van de zaak zoals die uitspraak kan blijken, buiten beschouwing. Ook hier geldt dat de OLAF-casus laat zien dat waarschijnlijk in veel gevallen nog steeds sprake zal zijn van publicatie van persoonsgegevens na toepassing van de pseudonimiseringsrichtlijn. Uiteindelijk is de relevante toets hoe moeilijk het is voor iemand met enig verstand van zaken om te achterhalen op wie een rechterlijke uitspraak betrekking heeft, en daarbij moet rekening worden gehouden met wat gericht vervolgonderzoek. Kan dat leiden tot heridentificatie, dan moet ook de rechtspraak zich bij publicatie van rechtspraak houden aan de AVG, ook al zal een overtreding niet kunnen leiden tot een AP-boete.[43]

Open vragen

Hoewel het Hof van Justitie met zijn arrest in de *GAR*-zaak hoognodige duidelijkheid heeft geboden over de betekenis van het begrip persoonsgegevens, is daarmee niet het laatste woord gesproken. Een belangrijke open vraag is of de relatieve benadering (waarbij bepalend is hoe moeilijk het voor de ontvanger van gegevens is om die te herleiden naar een bepaald persoon) ook opgaat als een dataset door een verwerkingsverantwoordelijke wordt gedeeld met een verwerker, dat wil zeggen: een partij die de gegevens alleen in zijn opdracht verwerkt. Het arrest van het Hof is niet expliciet over de vraag of Deloitte ten opzichte van de GAR handelde als verwerker, of als zelfstandig verwerkingsverantwoordelijke. Daar zou uit kunnen worden afgeleid dat die hoedanigheid niet doorslaggevend is geacht, waar het gaat om het juridisch gevolg van pseudonimisering. Voor zover de relatieve benadering ook van toepassing is in de situatie dat een verwerkingsverantwoordelijke gepseudonimseerde gegevens doorgeeft aan een verwerker, heeft dat potentieel vergaande gevolgen voor verwerking van gegevens in een cloud-context, waar al snel sprake is van een lange keten van leveranciers die op hun beurt gegevens stallen bij andere toeleveranciers. Waar de AVG voorschrijft dat die leveranciers aan strenge contractuele banden moeten worden gelegd, geldt ook hier dat die eisen niet meer van toepassing zijn, zodra een ketenleverancier alleen toegang heeft tot gepseudonimiseerde gegevens en niet over redelijke middelen beschikt om die te herleiden naar geïdentificeerde individuen. Maar, zoals de *IAB*-casus laat zien, kan daarbij de inhoud van de contractuele afspraken relevant blijken. Als die de verwerker een juridisch middel bieden om toegang af te dwingen tot aanvullende, identificerende informatie, is voor die partij wel degelijk sprake van persoonsgegevens.

Een andere open vraag is of ook rekening moet worden gehouden met eventuele illegale inspanningen van een kwaadwillende derde. Met andere woorden: moet worden nagegaan of een hacker of geheime dienst van een vijandige mogendheid (ook wel eufemistisch aangeduid als 'statelijke actoren') over middelen beschikt om een gepseudonimiseerde

36 Handreiking Scraping door particulieren en private organisaties (beschikbaar op de website van de AP), p. 9.

37 In Hoofdstuk V AVG.

38 Vgl. Pseudonymised (Personal) Data as Resolution: The Final Chapter in the Legal Saga of Third-Country Transfers?, Kasper Bjerre Hendrup Andersen, EDPL 3/2025, p. 312-332.

39 De Leidraad van de Raad voor de Journalistiek schrijft onder C.1 ook voor dat een privacy-inbreuk niet onevenredig mag zijn aan het maatschappelijk belang van de publicatie.

40 Art. 43 UAVG.

41 Dit volgt ook uit de Leidraad, zie voetnoot 39.

42 https://www.rechtspraak.nl/Uitspraken/Paginas/Pseudonimiseringsrichtlijn.aspx.

43 Zie over de toepasselijkheid van de AVG op de rechtspraak HvJ EU 24 maart 2022, ECLI:EU:C:2022:216, *Mediaforum* 2022-2, nr. 4.

dataset te herleiden. Uit het *Breyer*-arrest lijkt te volgen dat de redelijkheidstoets niet zo ver gaat. Het moet immers gaan om legale middelen.

Conclusie: enkele belangrijke lessen uit het *GAR*-arrest

Het *GAR*-arrest mag worden beschouwd als mijlpaal in het gegevensbeschermingsrecht, en het feit dat de Commissie de belangrijkste lessen daarvan direct wil codificeren, onderstreept dat. Daarmee is niet gezegd dat het Hof heeft gekozen voor de gemakkelijke of rechtszekere weg. Herleidbaarheid moet immers volgens het Hof worden beoordeeld naar de feitelijke omstandigheden van het geval, en die zijn nu eenmaal notoir lastig op voorhand te duiden. Wat de toepassing van de toets ook niet makkelijker maakt, is dat de verstrekker van een dataset mogelijk zelf geen toegang heeft tot de aanvullende gegevens die tot herleidbaarheid kunnen leiden. Dat blijkt uit het *Scania*-arrest: zelfs een partij voor wie een dataset zelf niet herleidbaar is tot een individu, moet bij verstrekking aan een ander nagaan of die ontvanger wel toegang kan krijgen tot aanvullende informatie die herleidbaarheid mogelijk maakt, nu of in de toekomst. Partijen die structureel gebruik willen maken van pseudonimisering in het licht van de relatieve leer, doen er daarom goed aan hun pseudonimiseringsmethode periodiek tegen het licht te houden van de actuele stand van de techniek en de gegevens die in het publieke domein beschikbaar zijn. Duidelijk is wel dat het arrest gevolgen heeft voor iedereen die unieke gegevens deelt die weliswaar niet direct, maar mogelijk wel indirect herleidbaar zijn. Zij zullen zich moeten afvragen: wat kan de ontvanger ermee, en welke mate van inspanning een ontvanger zich moet getroosten om te achterhalen op wie de gegevens betrekking hebben? Dus: hoe moeilijk is het? Op zich een eenvoudig criterium, maar de praktische toepassing zal nog wel eens weerbarstig kunnen blijken.