POSITION PAPER

prof dr. G-J. (Gerrit-Jan) ZWENNE[1]

Inbreng ten behoeve van de rondetafelbijeenkomst in de Tweede Kamer van 4 december 2024

INLEIDING

Over de Verzamelwet gegevensbescherming (*kamerstukken II* 2022/23, 36 264) valt veel te zeggen. Op verzoek van de Commissie Digitale Zaken houd ik het kort en beperk ik mij tot enkele observaties en suggesties die, naar mijn beoordeling, betrekkelijk eenvoudig zouden kunnen worden meegenomen in het lopende wetgevingstraject.

Eerst een algemene observatie met een suggestie over de wijze waarop de vele open begrippen en vage normen uit de Algemene verordening gegevensbescherming ("Avg") worden opgehelderd en de rol van de toezichthouder daarbij (§A). Daarna een meer specifieke opmerking van meer juridisch-technische aard en nog een suggestie, namelijk over het verbod op de verwerking van biometrische gegevens met het oog op unieke identificatie (§B).

§A. OVER DE OPHELDERING VAN OPEN BEGRIPPEN EN VAGE NORMEN

Op 4 oktober jl. kwam het Hof van Justitie van de Europese Unie ("het Hof") met een arrest in een Nederlandse zaak, de zgn. KNLTB-zaak.[2] In het arrest gaat het Hof in op de uitleg van het begrip 'gerechtvaardigd belang', als bedoeld artikel 6, eerste lid, onderdeel f, Avg. In het arrest beantwoordt het Hof de vraag of een 'commercieel belang' als zodanig kan worden opgevat. Onze nationale toezichthouder, de Autoriteit persoonsgegevens ("AP"), vond van niet en legde om deze reden forse boetes op, onder andere aan de KNLTB. De rechtbank Amsterdam, die moest oordelen over die boete, stelde vervolgens aan het Hof de prejudiciële vraag of de opvatting van AP houdbaar was, dus of een commercieel belang al dan niet zo een gerechtvaardigd belang kan zijn.[3]

---

[1] Gerrit-Jan Zwenne is hoogleraar recht en de informatiemaatschappij in Leiden en hoogleraar gegevensbeschermingsrecht in de Nederlandse rechtspraktijk aan de Open Universiteit, alsmede advocaat in Den Haag. Deze bijdrage is uiteraard op persoonlijke titel.

[2] HvJ EU 4 oktober 2024, (*KNLTB*), C-621/22, ECLI:EU:C:2024:858

[3] Rechtbank Amsterdam 22 september 2022, ECLI:NL:RBAMS:2022:5565

Voorafgaand aan de beantwoording van deze rechtsvraag maakt het Hof in het arrest een veelzeggende opmerking. Het Hof vraagt zich af of deze vraag überhaupt moet worden beantwoord. Dit omdat het deze vraag allang heeft beantwoord, betrekkelijk recent nog in het Meta/Bundeskartellamt-arrest van 4 juli 2023. Echter, om redenen die niet uit het arrest blijken heeft de rechtbank Amsterdam de aan het Hof gestelde vraag gehandhaafd. Het antwoord van het Hof daarop was, zoals verwacht en door het Hof al aangekondigd, geen verrassing: uiteraard kan een commercieel belang een gerechtvaardigd belang zijn. Immers, zo zegt het Hof, dat heeft de uniewetgever zelf duidelijk gemaakt in de overwegingen van de Avg en dat blijkt ook uit meer dan een handvol eerdere arresten van het Hof, alsmede uit conclusies bij die arresten én daarbij uit de richtsnoeren van de European Data Protection Board ("EDPB").[4]

Ik denk dat we met een understatement wel kunnen zeggen dat er iets nogal is misgegaan. We kunnen wel spreken van een ongelukkig bedrijfsongeval. AP kwam met een onhoudbare normuitleg en publiceerde die op haar website. Op basis van die normuitleg heeft AP, voor zover bekend, aan ten minste twee partijen forse boetes opgelegd waarvan duidelijk had moeten zijn dat die geen stand kunnen houden. En, zoals dat gaat, dat zal ongetwijfeld aanleiding zijn tot serieuze schadevergoedingsacties van degenen aan wie boetes zijn opgelegd.

Was dit te voorkomen geweest? In alle eerlijkheid ik weet het niet. Maar ik kan mij goed voorstellen dat we het risico op dit soort bedrijfsongevallen in belangrijke mate kunnen beperken. Voor de hand ligt om in de Uitvoeringswet AVG ("UAVG") op te nemen dat de toezichthouder, voorafgaand aan het hanteren van zo een normuitleg, eerst het concept daarvan ter consultatie beschikbaar te stelt via www.internetconsultatie.nl of de eigen website – en door te verlangen dat bij de onderbouwing van de definitieve normuitleg wordt ingegaan op hetgeen in de consultatie naar voren is gebracht. We kunnen dit zien als een *best practise*. Of, in goed Nederlands, als behoorlijk bestuur.

SUGGESTIE

Een nieuw zesde lid toevoegen aan artikel 15 UAVG

6. Ter bevordering van de doeltreffende en voorspelbare uitvoering van de verordening maakt de Autoriteit persoonsgegevens haar opvattingen over de uitleg van begrippen en regels uit de verordening bekend. Voorafgaand aan deze bekendmaking worden belangstellende in staat gesteld om via internetconsultatie opmerkingen daarover te maken.

[4] HvJ EU 4 oktober 2024, (*KNLTB*), C-621/22, ECLI:EU:C:2024:858, nrs. 21-22.

Doet dit af aan de onafhankelijkheid van de toezichthouder? Ik denk het niet. Het is en blijft aan AP om haar toezichthoudende taken uit te oefenen op de door haar als best beoordeelde wijze. Wél mag van AP worden verlangd dat ze uitleg geeft van de keuzes die ze daarbij maakt, en dat zij daarbij ook ingaat op de bezwaren die daartegen mogelijk zijn. Anders dan wel wordt betoogd,[5] betekent onafhankelijk toezicht níet dat er geen publieke verantwoording behoeft te worden afgelegd.[6] Integendeel. Juist vanwege de onafhankelijkheid van het toezicht is het noodzakelijk dat de besluitvorming transparant is en dat daarover verantwoording wordt afgelegd – iets dat niet zonder reden wordt vereist door het Handvest van de Grondrechten van de Europese Unie.[7]

§B. HET VERBOD OP DE VERWERKING VAN BIOMETRISCHE GEGEVENS

In de Verzamelwet gegevensbescherming worden de regels voor het gebruik van biometrische gegevens aangescherpt. Er worden — terecht — extra eisen gesteld aan de uitzondering op het verbod om dergelijke gegevens te gebruiken met het doel om vast te stellen wat iemands identiteit is (identificatie). In de praktijk blijkt er evenwel verwarring te zijn over de reikwijdte van het verbod op verwerking van biometrische gegevens. En daarom zou het goed zijn dat op te helderen. Ik licht dit toe.

In de Avg (art. 4, onderdeel 14) worden biometrische gegevens gedefinieerd als

> *persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens.*

De definitie heeft dus betrekking op gegevens die het mogelijk te maken om enerzijds iemands identiteit vast te stellen (*identificeren*) of anderzijds om iemands identiteit te bevestigen (*verifiëren*). Het is goed om het verschil tussen een en ander te onderkennen:

Identificeren betreft het vaststellen wie iemand is. Om een fictief voorbeeld te geven kunnen we denken aan een voetbalstadium waar met behulp van biometrische gezichtsherkenning wordt uitgezocht wie de hooligan is die de aansteker gooide waardoor de voetbalspeler (zeg:

---

[5] Aleid Wolfsen, 'De Autoriteit Persoonsgegevens als algoritme-waakhond; Toezichtreflex of …', *NJB* 2022/750, afl. 12, p. 912-922.

[6] Zie daarover allereerst het essay van de voormalig voorzitter van de privacytoezichthouder en EDPS, Peter Hustinx, 'Onafhankelijk toezicht en publieke verantwoording – de AP revisited', *NJB* 2023/885, afl. 13, p. 967-987; Marlies van Eck, 'Grensverkenningen door de Autoriteit Persoonsgegevens', *NJB* 2022/233, afl. 4, p. 255; 2022/2795, afl. 39, p. 3233-3238; Corien Prins 'Toezichthouders en publiekelijke verantwoording', *NJB* 2021/1799, afl. 25, p. 2025.

[7] Art. 41 Handvest van de Grondrechten van de Europese Unie.

Davy Klaassen) werd verwond aan het hoofd. De camerabeelden van de hooligan worden vergeleken met de biometrische templates in een gegevensverzameling met templates van alle seizoenkaarthouders. Als er een match is, weten we wie een stadionverbod moet krijgen (d.w.z. één-op-veel matching).

Verifiëren is iets anders. Bij verifiëren gaat het erom dat iemand een bepaalde identiteit heeft of zegt te hebben, waarna de op dat moment verkregen biometrische kenmerken van deze persoon worden vergeleken met het al vastgelegde het biometrische template van degene die deze persoon zegt te zijn (één-op-één matching).

Waarom is het verschil tussen identificeren en verifiëren van belang? Omdat, in termen van gegevensbescherming identificeren veel verder gaat dan verifiëren. Het is, zogezegd, veel ingrijpender om van iemand die onbekend wil blijven te achterhalen wie hij of zij is, dan het nagaan of iemand inderdaad degene is die hij of zij zegt te zijn. En het is om deze reden dat de Uniewetgever er uitdrukkelijk voor heeft gekozen om het verwerkingsverbod te beperken tot het gebruik van biometrische gegevens met het oog op unieke identificatie (één-op-veel matching). Het heeft géén betrekking op het bevestigen of verifiëren van iemands identiteit (één-op-één matching), bijvoorbeeld als wij met behulp van een vingerafdruk of gezicht-scan telefoon of laptop openen.

Dit blijkt uit de tekst van de desbetreffende bepaling in de Avg, en ook uit de totstandkomings–geschiedenis ervan. De Uniewetgever heeft, nadat de Raad en het Parlement daarover verschillende voorstellen hadden gedaan, er uitdrukkelijk voor gekozen om het verwerkingsverbod van artikel 9, eerste lid, Avg te beperken tot biometrische gegevens voor zover die worden gebruikt voor unieke identificatie. Er staat immers dat verboden is:

> *"[v]erwerking van persoonsgegevens […] biometrische gegevens met het oog op de unieke identificatie van een persoon"*

Ook in de doctrine wordt ervan uitgegaan dat het verbod alleen betrekking heeft op het gebruik van biometrische gegevens om iemand te *identificeren* (één-op-veel matching) en niet op het bevestigen of *verifiëren* van iemands identiteit (één-op-één matching). In de bijlage bij dit position paper heb ik, voor de liefhebbers, de uiteenzetting opgenomen uit het standaardwerk van Kuner *et al*, dat bij de meeste serieuze Avg-juristen in de boekenkast staat, als het al niet op het bureau ligt.[8]

[8] Luca Tosoni & Lee Bygrave, 'Comments on Article 9 GDPR', in: Kuner et al (eds), *Data Protection Regulation (GDPR). A Commentaryi,* Oxford University Press 2020, p. 213 e.v.

De begrippen en normen uit de Avg worden autonoom uitgelegd. Het is dus niet aan de nationale wetgever om te bepalen wat wél of niet onder het verwerkingsverbod van artikel 9, eerste lid, Avg, valt. Niettemin zou het, al was het maar omdat daarover in de praktijk de nodige misverstanden bestaan, goed zijn dat dit wordt opgehelderd. En, omdat dit ook van belang is voor de betekenis van de aangepaste uitzondering van artikel 29 UAvg, zou dat goed kunnen in de parlementaire stukken bij de Verzamelwet gegevensbescherming.

SUGGESTIE

Maak in het verslag van deze rondetafelbijeenkomst of elders in de parlementaire documentatie bij het wetsvoorstel, onder verwijzing naar de voorgestelde wijziging van artikel 29 UAvg, duidelijk dat het verwerkingsverbod van artikel 9, eerste lid, Avg betrekking heeft op identificatie (één-op-veel) van natuurlijke personen, en niet op verificatie van de identiteit van iemand (één-op-één).

BIJLAGE

Luca Tosoni & Lee Bygrave, 'Comments on Article 9 GDPR', in: Kuner et al (eds), *Data Protection Regulation (GDPR). A Commentaryi,* Oxford University Press 2020, p. 213 e.v.

The immediate goal of biometric systems is typically identification of a person (i.e. establishing who a person is relative to other persons) or the authentication (also termed verification) of a person (i.e. establishing whether a person is who she/ he pretends to be). Achieving identification typically involves comparing data on a person with data on multiple other persons (a 1:n comparison), whereas achieving authentication typically involves comparing data on a person with data on one other person (a 1:1 comparison), where a successful match verifies that the former person is the same as the latter person. As elaborated by WP29:

> *The identification of an individual by a biometric system is typically the process of comparing biometric data of an individual (acquired at the time of the identification) to a number of biometric templates stored in a database (i.e. a one- to- many matching process). The verification of an individual by a biometric system is typically the process of comparing the biometric data of an individual (acquired at the time of the verification) to a single biometric template stored in a device (i.e. a one- to- one matching process).*

The definition in Article 4(14) appears to cover both goals ('which allow or confirm the unique identification'). This is also indicated by the wording of recital 51 which links biometric data to processing 'through a specific technical means allowing the unique identification or authentication of a natural person'.

It is important to note, though, that this duality of goals is not replicated in Article 9 (1) GDPR, which, in respect of biometric data, is limited to cases when such data are processed 'for the purpose of uniquely identifying a natural person'. In other words, Article 9(1) only pertains to biometric data that are used for the purpose of identification as opposed to authentication/ verification. This is presumably because the legislator has deemed biometrics- based identification schemes as presenting a greater threat to data subjects' fundamental rights and freedoms than schemes used for the purpose of verification.

Indeed, use of biometric data for identification is often regarded as more problematic from a data protection perspective than their use for verification/ authentication, mainly because the latter use does not require storage of personal data in a centralised database and, concomitantly, typically involves processing of data on fewer numbers of persons. This limitation in the coverage of Article 9 is also evidenced in the trilogue negotiations on the GDPR. Summing up the negotiations held on 24 November 2015, the Council stated:

> *Concerning Article 9 relating to the processing of special categories of data, the European Parliament insists to include a reference to biometric data in the list of sensitive data in Article 9(1). The modernised Convention 108 of the Council of Europe foresees to restrictively define biometric data that 'uniquely identify a person' to qualify as sensitive data. Such a reference would ensure that biometric data are considered as sensitive only in those situations where they would uniquely identify a person or are used to verify his or her identity. The Presidency invites delegations to indicate their flexibility on a possible inclusion of 'biometric data uniquely identifying a person' in the list of sensitive data, keeping in mind the specific definition of 'biometric data' in Article 4(11).*

However, the reference to 'verify his or her identity' in the sentence beginning 'Such a reference . . .' does not accurately reflect the intended ambit of Modernised Convention108. As mentioned above, Article 6(1) of Modernised Convention 108 is intended to cover biometric data only when these are 'precisely used to uniquely identify the data subject'— which seemingly does not include situations where such data are used for authentication/ verification purposes.