

Vergaderjaar 2023–2024

32 761

Verwerking en bescherming persoonsgegevens

Nr. 296

BRIEF VAN DE MINISTER VOOR RECHTSBESCHERMING

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 8 april 2024

Op 6 december 2022 bood ik uw Kamer het onderzoeksrapport *The influence of (technical) developments on the concept of personal data in relation to the GDPR* aan (Kamerstuk 32 761, nr. 254). Het rapport ging gepaard met de zelfstandig leesbare Nederlandse samenvatting *De invloed van (technische) ontwikkelingen op het begrip persoonsgegevens in relatie tot de AVG*. Het onderzoek is door het Ministerie van Justitie en Veiligheid (JenV) bij het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) uitgezet en is uitgevoerd door het Tilburg Institute for Law, Technology and Society (TILT). Met deze brief ontvangt u mijn reactie op het onderzoek.

Aanleiding

De voortgaande digitalisering, waaronder ontwikkelingen op het terrein van big data en artificiële intelligentie (AI), leiden tot wat wel een «onlife samenleving» wordt genoemd: het dagelijks leven van mensen raakt steeds dieper verweven met informatietechnologie en data. Dat heeft als consequentie dat steeds meer gegevens kunnen worden gerelateerd aan personen. Daarmee kunnen deze worden aangemerkt als persoonsgegevens, waarop de Algemene verordening gegevensbescherming (AVG) van toepassing is. Bij het in werking treden van de AVG beschreef prof. dr. Purtova van de Universiteit Utrecht al hoe de AVG daardoor een haast alomvattende wet kan worden, die weliswaar recht doet aan het toenemende belang van persoonsgegevens in het leven van mensen en daarmee aan de beschermwaardigheid daarvan, maar tegelijkertijd in de praktijk steeds moeilijker te handhaven is.¹ De ontwikkelingen kunnen dus aanzienlijke gevolgen hebben voor de privacy van burgers. Daarom is het van groot belang dat nader in kaart wordt gebracht hoe de veranderende stand van de techniek zich verhoudt tot de AVG en rechtsbescherming in

¹ Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10(1), 40–81.

brede zin.² Op 20 november 2020 schreef de toenmalig Minister voor Rechtsbescherming aan uw Kamer over het voornemen om een onderzoek uit te laten voeren naar de invloed van de voortgaande technologische ontwikkelingen op het begrip persoonsgegevens.³ Het betrof een eerste verkennend onderzoek, waarin aandacht is voor socio-technologische ontwikkelingen rond anonimisering, pseudonimisering en herleidbaarheid van persoonsgegevens en mogelijke scenario's worden geschetst over de ontwikkeling van het begrip persoonsgegevens in de AVG.

Het onderzoek

De onderzoekers schrijven dat de AVG regels stelt aan en normen bevat voor de verwerking van persoonsgegevens. Hoewel de AVG sinds 2018 van kracht is, stammen de regels in essentie uit de jaren '70 van de vorige eeuw. Doorslaggevend voor de toepassing van het gegevensbeschermingskader was toen, en is vandaag de dag nog steeds, of de verwerkte gegevens direct of indirect kunnen leiden tot een identificeerbaar individu (natuurlijke persoon). Dat vaststellen is in de loop van de tijd steeds complexer geworden, vooral in het licht van technologische ontwikkelingen, de algemene toegankelijkheid van technologieën en de groeiende beschikbaarheid van open data.

Tegen die achtergrond komen de onderzoekers tot de volgende onderzoeksvraag voor het onderzoek: *Welk effect hebben huidige en toekomstige technische ontwikkelingen op het gebied van anonimisering, pseudonimisering, aggregatie en identificatie van gegevens, op het gegevensbeschermingskader en de bescherming van de verschillende soorten gegevens?*

Volgens de onderzoekers hebben de huidige technische ontwikkelingen grote invloed op de vraag of datasets persoonsgegevens bevatten. Big Data, AI, Quantum Computing en andere technieken maken het gemakkelijker om persoonsgegevens af te leiden uit geaggregeerde, geanonimiseerde of versleutelde datasets, de algemene toegankelijkheid van technologieën maakt het nog moeilijker om de toekomstige status van een dataset te bepalen, en het voortdurende streven naar open data en het hergebruik van overheidsinformatie betekent dat de juridische status van data nog volatieler zal worden. Waar het wettelijke regime anonimiteit als een binair vraagstuk beschouwt, zien de door de onderzoekers geraadpleegde experts anonimiteit in toenemende mate als een schaal die afhankelijk is van de inspanning van verwerkingsverantwoordelijken en de inzet van tijd, geld en technologie.

Het antwoord op de vraag of een dataset persoonsgegevens bevat, bepaalt welk reguleringskader voor de dataset van toepassing is. Met de *Regulation on the free flow of non-personal data* is een ander kader vastgesteld voor de verwerking van niet-persoonsgegevens. In dat geval mogen er juist geen onnodige beperkingen worden gesteld aan het vrije verkeer van de niet-persoonsgegevens. De reguleringskaders kennen dus een diametraal verschillende benadering.

Conclusies van het onderzoek

Volgens de onderzoekers zal het in de toekomst steeds moeilijker worden om de (juridische) anonimiteit van datasets te waarborgen. De meeste technologieën en tegen-technologieën voor gegevensbescherming zijn

² Kamerstukken II 2020/21, 26 643, nr. 726.

³ Kamerstukken II 2020/21, 26 643, nr. 726, p. 5.

verwikkeld in een kat-en-muisspel. Een algemene maar fundamentele verschuiving daarbij is de groeiende algemene toegankelijkheid van dergelijke technologieën. De brede beschikbaarheid van open data en de algemene toegankelijkheid van datatechnologieën leiden volgens de onderzoekers tot drie fundamentele vragen met betrekking tot aspecten van de AVG:

1. *De aard van de data in Big Data-processen is niet stabiel, maar volatiel.*
Een dataset zonder persoonsgegevens kan worden gekoppeld aan of verrijkt worden met een andere dataset om er persoonsgegevens uit af te leiden; de gegevens kunnen vervolgens worden samengevoegd of ontdaan van identificatiegegevens en weer niet-persoonlijk worden. Vervolgens kunnen de gegevens worden gedeanonimiseerd of geïntegreerd in een andere dataset om opnieuw persoonsgegevens te creëren. Dit alles kan in een fractie van een seconde gebeuren.
2. *De precieze juridische status van een databestand is medeaafhankelijk van de context.*
De toenemende volatiliteit van data leidt ertoe dat het steeds moeilijker wordt om de precieze status van gegevens te bepalen. Om de aard van een dataset te bepalen, moet rekening worden gehouden met de verwachte toekomstige status van de gegevens. De juridische categorie waartoe de gegevens behoren, is dus niet langer een kwaliteit van de gegevens zelf, maar een product van de intenties, inspanningen en investeringen van een verwerkingsverantwoordelijke.
3. *Profilering zonder persoonsgegevens heeft een steeds grotere impact op het individu.*
Het profileren van doelgroepen in plaats van individuen wordt een gangbare verwerkingshandeling in de informatiemaatschappij. Profilering wordt in toenemende mate gebaseerd op geaggregeerde gegevens, die weliswaar buiten het persoonsgegevensbeschermingskader vallen, maar wel degelijk een aanzienlijke impact op individuele personen en sociale verbanden kunnen hebben. De gevolgen van deze activiteiten kunnen negatief zijn voor de individuen in een groep, zonder dat de schade direct te relateren is aan individuen. Het idee dat hoe gevoeliger de gegevens zijn en hoe directer ze aan een persoon kunnen worden gekoppeld, des te strikter de verwerking ervan moet worden gereguleerd, kan daarom in twijfel worden getrokken.

De technologische ontwikkelingen en de algemene beschikbaarheid van data maken dat de status van data steeds volatieler wordt, aldus de onderzoekers. Ze wordt steeds minder een kenmerk van data en datasets zelf en in toenemende mate een effect van de inspanningen van de verwerkingsverantwoordelijke. Gezien deze trends in combinatie met de begrippen «identificeerbaarheid» en «alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt» in de AVG, zullen steeds meer gegevens onder het gegevensbeschermingskader vallen.

De onderzoekers schetsen vijf globale strategieën waarmee het wettelijk regime zou kunnen reageren op de toegenomen beschikbaarheid van open data en de algemene toegankelijkheid van technologie. Aan de vijf strategieën liggen twee denkrichtingen ten grondslag. Dat is enerzijds het ontwikkelen van een regime op basis van eenduidig gedefinieerde categorieën van persoonsgegevens. Dat is behulpzaam voor de handhaving, maar doet weinig recht aan de maatschappelijke praktijk. Daar tegenover wordt een regime geschetst dat gebaseerd is op de contextualiteit van persoonsgegevens. Die benadering doet recht aan de maatschappelijke praktijk, maar is niet eenvoudig te handhaven. Zo bouwen de onderzoekers een continuüm op van vijf globale strategieën:

1. Een nieuw regime ontwikkelen gebaseerd op nieuwe strikte categorieën.
2. Binnen het huidige regime de bestaande categorieën beter definiëren.

3. Het huidige gegevensbeschermingskader intact laten.
4. Binnen het huidige regime meer nadruk leggen op contextualiteit.
5. Een nieuw regime ontwikkelen gebaseerd op contextualiteit.

Het onderzoek geeft hiermee waardevolle inzichten in de socio-technologische ontwikkelingen rond de persoonsgegevensbescherming en de mogelijke gevolgen daarvan voor de werking van de AVG. Tegelijkertijd geeft het rapport een nieuw zicht op ontwikkelingen en nodigt uit tot verdere doordenking en verkenning van de thematiek. Ik geef hieronder aan hoe ik de inzichten uit het rapport duid, welke initiatieven ik voornemens ben te nemen en hoe deze zich verhouden tot het huidige beleid en bestaande activiteiten.

Reactie

De onderzoekers werpen – kort gezegd – de vraag op hoe het wettelijk regime op de in het onderzoek genoemde ontwikkelingen kan reageren, en welk doel de wetgever nastreeft met het beschermen van persoonsgegevens. De onderzoekers schetsen meerdere scenario's waaruit vijf globale strategieën zijn af te leiden voor de toekomst, van een extra streng beschermingsregime tot een regime waarbij beschermingsvraagstukken steeds per situatie bekeken moeten worden.

De AVG stelt regels en voorwaarden voor de verwerking van persoonsgegevens, juist in een digitaliserende wereld. Om de bescherming ervan zo goed mogelijk te laten zijn, is de AVG technologie-neutraal geformuleerd en is haar toepasselijkheid niet afhankelijk zijn van de gebruikte technologieën.⁴ Ze biedt een robuust kader om vraagstukken die opkomen met nieuwe technologische ontwikkelingen te beoordelen en te reguleren. Een belangrijk aspect van de normen uit de AVG is daarnaast dat zij in hoge mate – mede naar aanleiding van technologische ontwikkelingen – worden ingevuld door de rechtspraak. Daarin volgen de ontwikkelingen elkaar in hoog tempo op, niet in de laatste plaats met betrekking tot het vraagstuk waarop het onderhavige onderzoek zag, namelijk in hoeverre (technische) ontwikkelingen invloed hebben op het begrip persoonsgegevens in de AVG.

Zo heeft het Hof van Justitie van de Europese Unie (HvJEU) op 12 januari 2023 bepaald dat bij de uitlegging van een Unierechtelijke bepaling, zoals het begrip «persoonsgegeven», niet alleen rekening moet worden gehouden met haar bewoordingen, maar ook met de context ervan en met de doelstellingen en het oogmerk van de regeling waarvan zij deel uitmaakt.⁵ Op 4 mei 2023 bepaalde het HvJEU dat het gebruik van de woorden «alle informatie» in de definitie van het begrip «persoonsgegevens» in deze bepaling wijst op de bedoeling van de Uniewetgever om een ruime betekenis te geven aan dit begrip, dat zich potentieel uitstrekt tot elk soort informatie, zowel objectieve informatie als subjectieve informatie.⁶ Op 22 juni 2023 oordeelde het HvJEU dat het begrip «persoonsgegevens» zich niet alleen uitstrekt tot de door de verwerkingsverantwoordelijke verzamelde en bewaarde gegevens, maar ook tot alle informatie die voortvloeit uit een verwerking van persoonsgegevens die betrekking hebben op een geïdentificeerde of identificeerbare persoon.⁷ Op 5 december 2023 oordeelde het HvJEU dat ook gegevens die door het gebruik van aanvullende informatie kunnen worden gekoppeld aan een natuurlijke persoon, moeten worden beschouwd als gegevens over een

⁴ Overweging 15 van de AVG (2016/679).

⁵ HvJ EU 4 mei 2023, C-300/21, ECLI:EU:C:2023:370 (Österreichische Post).

⁶ HvJ EU 4 mei 2023, C-487/21, ECLI:EU:C:2023:369 (Österreichische Datenschutzbehörde).

⁷ HvJ EU 22 juni 2023, C-579/21, ECLI:EU:C:2023:501 (Pankki).

identificeerbare natuurlijke persoon.⁸ Op 7 maart 2024 kwam het HvJEU tot de slotsom dat ook een letter- en tekenreeks een persoonsgegeven kan zijn als deze tekenreeks het mogelijk maakt om de betrokken gebruiker te identificeren.⁹

Deze jurisprudentie illustreert dat binnen het bestaande wettelijke regime voortdurend en contextueel wordt getoetst aan de bestaande categorieën en definities van de AVG. Zij toont bovendien aan dat van de beoogde technologie-neutraliteit van de AVG in de praktijk daadwerkelijk sprake is. Dit maakt tevens dat de onderzoekers genoemde vijf strategieën goeddeels complementair zijn en elkaar aanvullen, in plaats van dat er een keuze uit dient te worden gemaakt.

Om die reden zie ik geen directe aanleiding om het gegevensbeschermingskader op dit punt te wijzigen. Dat neemt niet weg dat niet alleen de invulling ervan in de rechtspraak, maar ook het gegevensbeschermingsrecht zelf voortdurend in beweging is. Het rapport beschrijft bijvoorbeeld verschillende concrete technologische ontwikkelingen en schetst hun mogelijke maatschappelijke impact. Technologieontwikkeling zorgt voor nieuwe uitdagingen op het gebied van encryptie en bescherming van persoonsgegevens, zoals de onderzoekers overtuigend laten zien. Daarnaast bieden diezelfde technologische ontwikkelingen ook echter nieuwe mogelijkheden voor encryptie (zoals post-quantum encryptie). Daarmee ontstaat wat een encryptie-wapenwedloop genoemd kan worden. Die wapenwedloop krijgt mede vorm en richting door de juridische kaders die worden ontwikkeld, het technologiebeleid dat wordt gevoerd en de ontwikkelingen die worden gestimuleerd dan wel worden afgeremd.

In het rapport worden verschillende technologische ontwikkelingen benoemd, zoals Privacy Enhancing Technologies (PET) en Quantum computing. Deze ontwikkelingen zijn, zoals de onderzoekers ook aangeven, van groot belang voor het gegevensbeschermingsrecht. Het kabinet volgt deze ontwikkelingen dan ook al langere tijd en is daarbij op verschillende manieren ook actief betrokken.

De TechAgenda geeft zicht op wat de komende jaren belangrijke technologieën voor JenV zijn. Digitale veiligheid, PET,¹⁰ AI en Quantumtechnologie,¹¹ waaronder Post-Quantum Encryptie¹² staan prominent op TechAgenda van JenV.¹³

Tot slot

Het denken over het gegevensbeschermingsrecht, de AVG en de ervaringen in de praktijk staan als gezegd niet stil. Het kabinet zal blijven bezien of de bestaande waarborgen toereikend zijn om de rechten van de burgers voldoende te verzekeren. Ook zal ik de inzichten uit het rapport meenemen bij de bespreking van de tweede evaluatie van de AVG en zo onder de aandacht van mijn collega's in de lidstaten brengen. Dit past ook

⁸ HvJ EU 5 december 2023, C-683/21, ECLI:EU:C:2023:949 (Nacionalinis visuomenės sveikatos centras).

⁹ HvJ EU 7 maart 2024, C-604/22, ECLI:EU:C:2024:214 (IAB Europe).

¹⁰ <https://www.fcinet.org/>; <https://magazines.rijksoverheid.nl/jenv/jenvmagazine/2021/13/reportage-ma3tch>.

¹¹ <https://projects.illc.uva.nl/quantumimpact/>.

¹² <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/quantumveilige-cryptografie/bereid-je-voor/>.

¹³ Ministerie Justitie en Veiligheid, TechAgenda, Technologische ontwikkelingen met impact op Recht, Veiligheid en Migratie, april 2022.

bij de aangenomen Raadsconclusies over de toepassing en bevindingen van de AVG ter voorbereiding op de tweede evaluatie van de AVG in mei dit jaar.¹⁴

De Minister voor Rechtsbescherming,
F.M. Weerwind

¹⁴ Raad van de Europese Unie, 15507/23, Standpunt en bevindingen van de Raad over de toepassing van de algemene verordening gegevensbescherming (AVG).