



Tweede Kamer

DER STATEN-GENERAAL

Brief van de rapporteur "Twee jaar toepassing van de AVG" T. van Gent (VVD)

Vaste commissie voor Justitie en Veiligheid

aan Leden van de vaste commissies voor Justitie en Veiligheid
in afschrift aan Leden van de vaste commissies voor Europese Zaken

datum 15 januari 2021

ons kenmerk 2021Z00788
pagina 1/15

Inleiding

De vaste Kamercommissie voor Justitie en Veiligheid heeft mij op 2 juli 2020 een mandaat verleend als rapporteur voor de Algemene Verordening Gegevensbescherming (AVG). Aanleiding vormt het op 24 juni 2020 verschenen verslag van de Europese Commissie (hierna: Commissie) "Twee jaar toepassing van de AVG" ([link](#)). In dat verslag maakt de Commissie de balans op van de toepassing van de AVG, twee jaar nadat deze op 25 mei 2018 van kracht werd.

Conform het mandaat voor mijn rapporteurschap, heb ik het najaar van 2020 aangewend om knelpunten bij de toepassing van de AVG in kaart te brengen. Gegeven de korte beschikbare looptijd voor het rapporteurschap en de beperkingen die de coronacrisis met zich meebracht, heb ik gekozen voor een nauw afgebakende scope. Enerzijds heb ik breed gekeken naar wat op EU-niveau de belangrijkste vraagstukken zijn die zich voordoen bij toepassing van de AVG. Anderzijds heb ik ingezoomd op drie specifieke casussen. De nadruk bij mijn activiteiten lag op deze casussen.

Bij de totstandkoming en zeker ook na de invoering is in de Tweede Kamer met regelmaat gedebatteerd over de AVG. Door sommigen wordt deze als te stringent ervaren, terwijl anderen de regels niet ver genoeg vinden gaan. Mijn rapporteurschap heb ik gebruikt om knelpunten bij de toepassing van de AVG in kaart te brengen. Zo bekeek ik onder meer of knelpunten uit de AVG zelf volgden, of dat de wijze van toepassing in Nederland hiertoe leidde.

De activiteiten die ik voor mijn rapporteurschap heb ondernomen bestonden onder meer uit het voeren van gesprekken met toezichthouders uit binnen- en buitenland, verantwoordelijken op EU-niveau, maatschappelijke belangenbehartigers, academici, advocaten en vertegenwoordigers van het bedrijfsleven. Verder vond op 19 november 2020 in het kader van het rapporteurschap een speciaal rondetafelgesprek plaats in de Kamer: "Twee jaar toepassing van de AVG" ([link](#)). Om een beeld te krijgen van knelpunten in andere lidstaten werden middels het ECPRD-netwerk¹ interparlementair vragen uitgezet.

Voor mijn onderzoek heb ik veel hulp gehad van naaste medewerkers en ambtelijke ondersteuners, in het bijzonder van Pieter Rook, Lennart van der Plas en Lucas Ponfoort.

¹ European Centre for Parliamentary Research and Documentation



Daarnaast heb ik veel formele en informele gesprekken gevoerd in het kader van mijn activiteiten. Langs deze weg wil ik eenieder mijn grote dank toezeggen voor hun beschikbaarheid, openheid en waardevolle bijdragen aan mijn onderzoek.

Dit verslag bestaat uit drie delen. In het eerste deel zal ik beknopt ingaan op het ontstaan van de AVG, de context waarbinnen deze tot stand kwam en de basisprincipes waarop de verordening inzet. In het tweede deel staan de eerste ervaringen met de AVG centraal en dan met name de casussen waarop ik mijn onderzoek gericht heb. In deel drie vat ik mijn bevindingen samen en geef ik suggesties voor aandachtspunten voor nader debat in de Kamer.

1. Algemene Verordening Gegevensbescherming

Op 25 januari 2012 publiceerde de Commissie het voorstel voor een nieuwe verordening gegevensbescherming ter vervanging van de sinds 1995 van kracht zijnde richtlijn gegevensbescherming 95/46/EG². Aan de herziening ging in 2010 een brede consultatie vooraf ([link](#)). De Commissie stelde bij haar initiatief dat de dubbeldoelstelling van de richtlijn gegevensbescherming, het waarborgen van het fundamentele recht op gegevensbescherming en het reguleren van het vrij verkeer van gegevens binnen de interne markt, onverminderd voorop moesten blijven staan. Tegelijk wees de Commissie erop dat de stormachtige ontwikkeling van ICT-technologie en de daaruit volgende snelle digitalisering van de samenleving een nieuwe, meer omvattende en samenhangende aanpak noodzakelijk maakten. De Commissie refereerde hierbij aan de opkomst van snel internet, mobiele apparaten zoals smartphones, internethandel en de groei van sociale media, waarbij in 2010 één netwerkbedrijf (Facebook) met ruim 500 miljoen accounts al meer gebruikers kende dan er inwoners zijn in de EU (als contrast: in 1995 gebruikte nog slechts één procent van de EU-burgers internet).

Van meet af aan maakte de Commissie duidelijk dat zij, gezien het 'grenzeloze' karakter van dataverkeer en dataopslag, met de verordening de ambitie had tot het zetten van een wereldwijde standaard: "Een uniforme aanpak op EU-niveau zal Europa sterker maken bij het bevorderen van hoge normen voor gegevensbescherming wereldwijd", aldus de Commissie in 2010 in een persbericht³.

Daar waar het beschikkende deel van de richtlijn uit 1995 33 artikelen bevatte, telt de in 2012 gepubliceerde AVG uiteindelijk 99 artikelen. Voor burgers zette het voorstel voornamelijk in op versterkte controle over en bescherming van de eigen persoonsgegevens. Dit onder meer door een recht op inzage, rectificatie, overdraagbaarheid ('portability') en desgewenst verwijdering ('recht op vergetelheid') van persoonsgegevens, en betere bescherming van rechten binnen, maar ook buiten de EU. Voor organisaties en bedrijven zette het voorstel in op een significante professionalisering van de omgang met persoonsgegevens met strikte eisen aan interne processen en personeel. Anderzijds zette het voorstel in op meer uniforme regels bij het zakendoen binnen de EU, inclusief een meer gelijk speelveld met bedrijven zonder

² richtlijn 95/46/EG betreffende "de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens" ([link](#))

³ MEMO/10/542, 4 November 2010, Data protection reform - frequently asked questions ([link](#))



formele vestiging in de EU, en op vermindering van administratieve lasten in grensoverschrijdende situaties, onder meer door de introductie van één leidende toezichthouder voor bedrijven actief in meerdere lidstaten ('één-loketmechanisme').

Hoewel er dus sprake is van Europese wetgeving, die naast de bescherming van persoonsgegevens van burgers moet zorgen voor een gelijk speelveld op de gemeenschappelijke markt, is in de AVG geregeld dat de controle van de regels door onafhankelijke, nationale toezichthouders geschiedt. De organisatie en capaciteit van deze uiteenlopende nationale gegevensbeschermingsautoriteiten laat verschillen zien. Ook cultuurverschillen kunnen er toe leiden dat de AVG niet in alle Europese lidstaten op eenzelfde wijze wordt toegepast. Wel vindt er tussen de nationale toezichthouders afstemming plaats in de European Data Protection Board (EDPB). De EDPB neemt besluiten en publiceert regelmatig aanwijzingen (inclusief richtsnoeren, aanbevelingen en best practices) om de Europese privacywetgeving – ook richting de nationale toezichthouders – te verduidelijken.

Met name nieuw aan de AVG is dat deze Europese wet verplicht tot een risicogedreven aanpak, zo stelde een van mijn gesprekspartners in de voorgesprekken. De wetgever is hierbij overgeschakeld van een principiële benadering van privacy naar een data-ethiekbenadering, door aan te geven dat 1) gegevensverwerking ten dienste moet staan van de burger en gegevensbescherming niet prevaleert boven andere belangen; en 2) niet op voorhand mag worden aangenomen dat de verwerking van persoonsgegevens risicovol is, maar dat dit moet blijken uit een objectieve beoordeling. Hét instrument voor het doen van zulke objectieve beoordelingen is een analyse van het risicomitigerend effect van gegevensbeschermingseffectbeoordelingen (DPIA). De AVG helpt daarbij om 'privacyneutraal' te werk te gaan.

Passende gegevensbescherming moet zowel geboden worden bij bestaande verwerking van persoonsgegevens, alsmede bij de vormgeving van nieuwe verwerkingen (artikel 24-25 AVG). Bij het ontwerp van nieuwe diensten moeten databeschermingsvereisten ('privacy by design') meteen worden meegenomen, met daarbij dataminimalisatie (enkel opvragen werkelijk benodigde data – toereikend en terzake dienend) en 'privacy by default' (privacy moet de standaardinstelling zijn). Een kernbepaling is dat gegevensgebruik beperkt dient te worden tot die gegevens waar een legitieme grondslag voor is. Aan het verwerken van bijzondere persoonsgegevens (bv. medische of strafrechtelijke gegevens) worden extra hoge eisen gesteld.

Een element van de toepassing van de AVG dat in het oog springt en uitgebreid de pers heeft gehaald, zijn de sancties bij niet-naleving. Boetes kunnen oplopen tot maximaal 20 miljoen euro of 4% van de wereldwijde jaaromzet van een onderneming, al naar gelang welk bedrag hoger is. Daarbij is het goed te benoemen dat het opleggen van sancties primair een taak is van nationale toezichthouders. Er is weliswaar samenspraak met de gegevensbeschermingsautoriteiten in andere landen via de EDPB, maar uiteindelijk is het in eerste aanleg aan nationale toezichthouders om vervolging dan wel sancties in te stellen.

Hierbij is het goed om te realiseren dat toezicht en handhaving primair zijn belegd bij Functionarissen Gegevensbescherming (FG's) volgens artikel 37-39 AVG. In de EDPB



Guidelines on Data Protection Officers ([link](#)) worden deze FG's dan ook aangeduid als hoeksteen en sleutelfiguur voor 'accountability'⁴. FG's handhaven met 'zachte' middelen; wanneer zij er niet uitkomen, is het proportioneel dat de toezichthouders op landelijk niveau in actie komen. Daarbij is bepaald dat de circa zesduizend FG's die Nederland telt in dezen met de AP samenwerken, die er zodoende niet alleen voor staat. De kwaliteitseisen en het voldoen hieraan door FG's zijn een aandachtspunt. Een suggestie kan zijn om een landelijk kwaliteitssysteem in te stellen, hetgeen bijvoorbeeld ook voor de advocatuur is georganiseerd.

Na publicatie van het Commissievoorstel in januari 2012, duurden de onderhandelingen in Brussel tot april 2016 toen de Raad en het Europees Parlement een akkoord op de definitieve versie van de tekst van de verordening bereikten. Op 24 mei 2016 werd de verordening van kracht waarna, na een voorbereidingsperiode van twee jaar, de verordening op 25 mei 2018 EU-breed van toepassing werd. Tijdens de onderhandelingen in Brussel bedong de Tweede Kamer middels een toezegging om door het kabinet periodiek, door middel van rapportages, over de stand van de onderhandelingen in Brussel geïnformeerd te worden. De bij de AVG horende Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) die invulling geeft op punten waar de AVG ruimte laat voor nationale keuzes, werd op 16 mei 2018 van kracht ([link](#)). De tot dan toe van toepassing zijnde Wet Bescherming Persoonsgegevens werd gelijktijdig ingetrokken.

2. Twee jaar AVG – eerste ervaringen

2.1 Algemene bevindingen

Op 25 mei 2020 was de AVG twee jaar van toepassing. Zoals bepaald in artikel 97 van de verordening, gold hierbij voor de Commissie de plicht om een eerste verslag over de staat van de toepassing van de AVG in de EU te publiceren ([link](#)). Een dergelijk verslag zal de Commissie vanaf nu vierjaarlijks publiceren. In Nederland heeft het kabinet op verzoek van de Kamer een uitvoerige reactie gegeven op het verslag van de Commissie ([link](#))⁵. Ook in de academische wereld en de media zijn in de voorbije jaren artikelen verschenen over de eerste ervaringen met de AVG. Alvorens in te gaan op mijn eigen bevindingen als rapporteur, vat ik in deze sectie de hoofdlijnen van de impressies van Commissie, kabinet en andere auteurs kort samen.

Impressies van de Commissie

Het positiefst van toon is het Commissieverslag. Teneur van het stuk is dat de EU goed op weg is om de doelstellingen van de AVG te behalen. Burgers zijn zich meer bewust van hun rechten, bedrijven zetten volgens de Commissie in op naleving en zien ook commerciële voordelen van een sterk gegevensbeschermingsregime. Veel nationale toezichthouders hebben hun budget en bestaande sterk zien toenemen, en de harmonisering in de lidstaten neemt toe. Einddoel moet zijn te komen tot een echte Europese gegevensbeschermingscultuur en een strikte handhaving.

⁴ EDPB Guidelines on Data Protection Officers ([link](#), pagina 4-5)

⁵ Het kabinet heeft in april 2019 tevens een Kamerbrief gezonden over de toepassing van de UAVG ([link](#))



De Commissie stelt verder dat de AVG richtinggevend is bij de huidige digitale transitie van samenleving en economie, en een leidraad biedt waarbij de mens centraal staat. Ook betoogt de Commissie dat de AVG wereldwijd een referentiepunt is geworden voor landen die voor hun burgers een hoog niveau van bescherming van persoonsgegevens nastreven. Verder vindt de Commissie dat de AVG de nodige flexibiliteit getoond heeft om in onvoorziene omstandigheden – zoals de huidige coronacrisis – digitale oplossingen te kunnen faciliteren.

De Commissie ziet ook verbeterpunten. Burgers dienen zich nog beter bewust te worden van de rechten en de mogelijkheden die de AVG hun biedt. Ook de samenwerking tussen de nationale gegevensbeschermingsautoriteiten binnen de EDPB bij grensoverschrijdende zaken kan verder verdiepen. Daarnaast constateert de Commissie een zekere mate van versnippering, met name doordat lidstaten in hun wetgeving gebruik maken van facultatieve clausules. De Commissie stelt hierbij dat het essentieel is dat nationale wetgeving niet verder gaat dan de marges die de AVG toestaat, en geen aanvullende eisen stelt waar geen marge is. Omdat deze kwestie nog onderzocht wordt en sectorspecifieke wetgeving in veel lidstaten nog wordt herzien, acht de Commissie het te vroeg om definitieve conclusies te trekken over de mate waarin versnippering een probleem is. Ook toont de Commissie zich bewust van de zorgen over de lasten die de AVG met zich meebrengt voor het bedrijfsleven en dan met name het mkb. De Commissie schrijft: "sommige belanghebbenden melden dat de toepassing van de AVG vooral voor kleine en middelgrote ondernemingen een uitdaging vormt. Volgens de risico-gebaseerde aanpak is het niet juist om derogaties toe te passen op basis van de omvang van een bedrijf, aangezien omvang op zich geen indicatie geeft van de risico's die de verwerking van persoonsgegevens kan opleveren voor particulieren. Verschillende gegevensbeschermingsautoriteiten hebben praktische hulpmiddelen geboden om de toepassing van de AVG makkelijker te maken voor kleine en middelgrote ondernemingen waarvan de activiteiten een laag risico met zich meebrengen. Deze benadering moet intensiever en breder worden toegepast, bij voorkeur binnen het kader van een gemeenschappelijke Europese aanpak, zodat er geen belemmeringen voor de eengemaakte markt ontstaan."

Impressies van het kabinet

Het kabinet gaat in zijn Kamerbrief uitvoerig in op het Commissieverslag en geeft aan de bevindingen in belangrijke mate te onderschrijven. In het algemeen hint het kabinet wel sterker dan de Commissie op de noodzaak van een beperkte, gerichte amendering van de AVG op punten waar zich knelpunten voordoen. Het kabinet wijst hierbij in het kader van harmonisatie onder meer op het verschil tussen lidstaten voor wat betreft leeftijdsgrenzen die nationaal gelden voor het kunnen geven van toestemming voor gebruik van digitale diensten door kinderen. In het kader van knelpunten die zich voordoen in het mkb, wijst het kabinet voorts op de verplichting om een verwerkingsregister bij te houden. Het kabinet heeft deze punten als suggesties ingebracht voor het Commissieverslag. De Commissie heeft hier nota van genomen en schrijft in haar verslag na te zullen gaan "of in het licht van nieuwe ervaring en relevante jurisprudentie, het passend zou kunnen zijn om mogelijke gerichte wijzigingen voor te stellen" en noemt daarbij specifiek de verwerkingsregisterplicht voor mkb-bedrijven die verwerking van persoonsgegevens niet als kernactiviteit verrichten, en de mogelijke harmonisering van de leeftijdsgrens voor toestemming voor gebruikmaking van digitale



diensten door kinderen. De Commissie lijkt dus een opening te bieden. Als rapporteur merk ik hierbij op dat een dergelijke gerichte amendering – indien die er komt – in de praktijk al snel een proces van jaren zal zijn.

Over het toezicht op grote techbedrijven, merkt het kabinet op dat “krachtige handhaving van de AVG geboden [is] jegens grote digitale platforms, specifiek als het gaat om online reclame en microtargeting”. Ook tekent het kabinet aan dat bij de ontwikkeling van zijn onderzoeks- en beleidsagenda⁶ ‘normering en toezicht algoritmen’ bezien moet worden of het toezicht op algoritmen in de private sector voldoende geborgd is. In het kader van nieuwe technologie en autonome systemen/algoritmen, hoopt het kabinet op (spoedige) additionele richtsnoeren van de EDPB, bijvoorbeeld ter verduidelijking van het begrip ‘menselijke tussenkomst’. In meerdere passages in de brief onderstreept het kabinet het belang om bij nieuwe technologieën de afstemming tussen nieuwe toepassingen en de AVG nauwlettend in de gaten te houden.

Impressies algemeen

Artikelen in de pers, niet zelden van auteurs uit de academische wereld, zijn vaak meer uitgesproken in hun beoordeling van de AVG. Zij zijn veelal positief over de AVG als concept en als normatief kader, zien de aanpassingsproblemen met de AVG in een aantal toepassingsgebieden, wijzen erop dat het, gezien de complexiteit van de AVG, na twee jaar eigenlijk nog te vroeg is om tot een afgewogen oordeel over de toepassing van de verordening te komen, en zijn vooral kritisch op de mechanismen binnen de AVG en de samenwerking tussen nationale toezichthouders bij de aanpak van grote, multinationalaal opererende techbedrijven⁷.

Impressies rapporteur

Sinds mijn toetreding tot de Kamer heb ik veelvuldig gehoord dat individuele bedrijven, overheden en organisaties dagelijks ongemak van de AVG ervaren. Denk hierbij aan het opslaan van klantgegevens of het publiceren van foto’s in clubblaadjes of op websites. In sommige gevallen is hierbij sprake van een gebrek aan ervaring met de AVG en blijkt er meer mogelijk te zijn dan gedacht. Vaak echter lijkt in dergelijke gevallen de bescherming van persoonsgegevens te botsen met andere belangrijke rechten en belangen zoals veiligheid, gezondheidszorg, wetenschappelijk onderzoek, onderwijs en commerciële belangen. Ik onderschrijf dan ook de zorgen die de Commissie al aanstipte: vooral voor kleine en middelgrote bedrijven en organisaties kunnen de verplichtingen die de AVG met zich meebrengt een zware last zijn. De onzekerheid over toepassing van de AVG en de angst voor boetes leiden bovendien tot verkramping.

Ook in de gesprekken die ik als rapporteur de afgelopen maanden heb gevoerd, kwam daar waar het knelpunten met de AVG op EU-niveau betreft, het vraagstuk hoe effectief toezicht te houden op de grote techbedrijven als prominent onderwerp naar voren. In de AVG is ervoor gekozen dat voor grensoverschrijdend opererende bedrijven de toezichthouder in de thuislidstaat de leidende toezichthouder is (‘één-loketmechanisme’). Dit betekent niet dat deze ene toezichthouder zelf beslissingen kan nemen over databeschermingskwesties waarbij sprake is van grensoverschrijdende aspecten. Daarvoor is binnen de AVG het ‘consistentiemechanisme’ opgenomen, dat toelaat dat

⁶ Een Kamerbrief over deze agenda staat gepland voor december 2020

⁷ Zie bijvoorbeeld bijdragen sprekers aan het rondetafelgesprek: [link](#)



ook andere betrokken toezichthouders invloed kunnen uitoefenen op beslissingen betreffende het betrokken bedrijf. Daarmee is met de AVG impliciet de fundamentele keuze gemaakt toezicht op grote internationaal opererende bedrijven niet primair te beleggen op EU-niveau. Op de tekentafel kan dit functioneren, maar in de praktijk plaatst dit toezichthouders in kleinere EU-lidstaten zoals vooral Ierland en Luxemburg tegenover dominante, kapitaalkrachtige techbedrijven als Facebook en Google. Getuige de *Twitter-casus* ([link](#)) leidt dit verder tot lange procedures, waarbij het eerst de leidende toezichthouder veel tijd kost om tot een voorstel voor een handhavingsbesluit te komen en daarna de consultatieronde van andere toezichthouders nog vele maanden in beslag neemt.

In de Twitter-casus was het door een softwarefout jarenlang mogelijk dat tweets van gebruikers die de optie 'tweets afschermen' hadden ingeschakeld, toch breder zichtbaar waren. Toen de fout bekend werd, duurde het langer dan de 72 uur die de AVG toelaat voordat het bedrijf het datalek bij de (in dit geval Ierse) toezichthouder meldde. In deze casus kostte het de Ierse toezichthouder bijna anderhalf jaar om tot een besluit te komen. Nadat in de EDPB bleek dat een aantal andere betrokken toezichthouders zich niet konden vinden in het door de Ierse toezichthouder voorgestelde besluit, duurde het tot 15 december 2020 voordat een definitief oordeel viel, waarbij Twitter uiteindelijk een boete kreeg opgelegd van €450.000,-. Uit de notulen van de EDPB wordt duidelijk dat er onder de EU-toezichthouders onenigheid bestond over de hoogte van de boete, waarbij de Duitse toezichthouder een boete met een omvang van 7 tot 22 miljoen euro bepleitte ([link](#)).

Behalve ongemak over de duur van de Twitter-casus en de hoogte van de uiteindelijke boete, werden in de media zorgen uitgesproken over het feit dat bij de Ierse toezichthouder nog meer dan twintig actieve zaken op afhandeling wachten. Dit betreft zaken tegen grote techbedrijven als Facebook, WhatsApp, Google, Apple en LinkedIn die vaak veel complexer zijn dan de relatief eenvoudige Twitter-casus. Het werpt de vraag op of het theoretisch concept van de AVG van een leidende toezichthouder past bij de praktijk, waarbij dit betekent dat de toezichthouder in een kleine EU-lidstaat als Ierland met een staf van circa 160 medewerkers het EU-toezicht op vrijwel alle wereldwijd opererende grote techbedrijven voor zijn rekening moet nemen. Ook tijdens het eerder genoemde rondetafelgesprek in de Kamer stelden experts dat dit probleem van tijdig en strikt toezicht op grote techbedrijven geen probleem is dat zich met meer tijd en meer ervaring met toepassing van de AVG vanzelf oplost, maar een weeffout in de AVG is die aanpassing vergt.

2.2 Casussen

Gegeven de beperkte tijd beschikbaar voor het rapporteurschap en de beperkingen die de coronacrisis met zich meebracht, is het in het kader van mijn rapporteurschap niet mogelijk een alomvattende impressie van de staat van toepassing van de AVG te geven. Gelet op deze restricties heb ik de keuze gemaakt me bij mijn activiteiten hoofdzakelijk te focussen op drie casussen die heel concreet de dilemma's schetsen bij de toepassing van de AVG in de praktijk. Het zijn casussen die primair respectievelijk een bedrijf, een maatschappelijke organisatie en de overheid betreffen.



2.2.1 VoetbalTV

De eerste casus is VoetbalTV, een initiatief uit 2017 gelanceerd door de Koninklijke Nederlandse Voetbalbond (KNVB) en mediabedrijf Talpa Network. Het bedrijf richt zich op volautomatische videoregistraties van voetbalwedstrijden van aangesloten amateurverenigingen. De streaming betreft beelden van elftallen waarvan de spelers minimaal 13 jaar oud zijn. De gestreamde beelden van spelers, en eventueel trainers, scheidsrechters en toeschouwers, zijn te kwalificeren als persoonsgegevens, waarmee het initiatief onder bereik van de AVG ligt. Aan spelers en andere betrokkenen wordt geen expliciete, individuele toestemming gevraagd voor het delen van de beelden. Wel worden spelers door hun club over het streamingbeleid geïnformeerd. Ook kunnen spelers/elftallen bij hun club dan wel bij VoetbalTV bezwaar maken en is er de mogelijkheid om de opname van beelden te stoppen en/of deze te laten verwijderen.

VoetbalTV formuleert op haar website haar doelstelling als “de betrokkenheid en het voetbalplezier van alle voetballiefhebbers te [willen] vergroten. Voetbal TV is in het leven geroepen om 1) iedereen de mogelijkheid te bieden om amateurwedstrijden live te volgen en 2) vanuit een centraal punt beelden beschikbaar te stellen die voor alle voetballiefhebbers te delen zijn. Ook kan VoetbalTV gebruikt worden voor video-analyse om zo een bijdrage te leveren aan de ontwikkeling van het voetbal. Daarnaast kunnen derden zoals bijvoorbeeld (sic) clubs en familieleden er belang bij hebben om beeldmateriaal van VoetbalTV te zien” ([link](#)).

De Autoriteit Persoonsgegevens (AP) liet zich voor het eerst publiekelijk uit over VoetbalTV op 10 september 2018, via Twitter in reactie op een tweet van een bezorgde voetbalvader⁸. In reactie op het bericht zocht VoetbalTV contact met de AP. Als eerste formele stap gaf de AP op 5 december 2018 aan dat het een onderzoek is gestart naar VoetbalTV. Naar valt af te leiden uit een rechtszaak die in 2020 zou volgen, heeft dit geleid tot een concept-onderzoeksrapport van 15 mei 2019 en, nadat VoetbalTV een zienswijze had ingediend, tot een definitief onderzoeksrapport van 6 november 2019, waarin de AP concludeert dat VoetbalTV onrechtmatig persoonsgegevens verwerkt. De AP heeft vervolgens op 22 november 2019 het voornemen uitgebracht om tot handhaving over te gaan ([link](#), paragraaf 4 vonnis). Gezien de onzekerheid die dit voornemen meebracht voor haar bedrijfsvoering, drong VoetbalTV aan op een spoedig definitief besluit en spande, na het uitblijven hiervan, op 4 juni 2020 een rechtszaak aan ([link](#) mediabericht). Op 16 juli 2020 legde de AP VoetbalTV een boete op ter hoogte van €575.000,- voor het onrechtmatig verwerken van persoonsgegevens.

In de rechtszaak gaat het primair om de vraag of een commercieel belang – onder voorwaarden – een gerechtvaardigd belang kan zijn voor de verwerking van persoonsgegevens. Bij het ontbreken van expliciete toestemming voor het verwerken van persoonsgegevens, laat de AVG in artikel 6, lid 1f de ruimte middels een driestappen-toets een afweging te maken tussen het belang van een partij die persoonsgegevens wil gebruiken (hier VoetbalTV) en het belang van de bescherming van

⁸ De tweet luidt: “Beste autoriteit, kijken jullie ook mee? Groepsdruk is zo groot om mee te doen, dat afwijken eigenlijk niet mag? Is dat toegestaan? Kun je nog voetballen als je niet gefilmd op internet wil?” De AP reageert met de tweet “Plannen voor @VoetbalTV roepen idd veel privacyvragen op. Mensen hebben zorgen over privacy. De AP gaat daarom met de @KNVB in gesprek. Het is een groot goed om je onbespied te mogen wanen, geldt zeker voor kinderen”



persoonsgegevens (hier de bescherming van beelden/persoonsgegevens van amateurvoetballers). Bij deze drie-stappen-toets gelden drie cumulatieve eisen: is er een gerechtvaardigd belang, is de verwerking van persoonsgegevens noodzakelijk voor de behartiging van dit belang, en weegt het gerechtvaardigde belang zwaarder dan het recht op bescherming van persoonsgegevens? De AP publiceerde in november 2019 een normuitleg over wat in haar ogen als gerechtvaardigd belang kan gelden. Hierin stelt de AP onder meer: "Wat ook niet als een gerechtvaardigd belang kwalificeert, is bijvoorbeeld: het enkel dienen van zuiver commerciële belangen, [...]".

De rechtbank deed op 23 november 2020 uitspraak ([link](#)). Zij stelt mede op basis van uitspraken van het Europees Hof: "Eiseres [= VoetbalTV] stelt [...] dat zij een gerechtvaardigd belang heeft om persoonsgegevens te verwerken, zoals bedoeld in artikel 6, eerste lid, aanhef en onder f, van de AVG. Verweerder [= de AP] vindt dat niet. Hij stelt dat het te gelde maken van persoonsgegevens nooit een gerechtvaardigd belang kan opleveren. De rechtbank volgt [de AP] hierin echter niet. Dat [VoetbalTV] ook een commercieel belang heeft, betekent niet zonder meer dat zij geen gerechtvaardigd belang kan hebben. Het op voorhand uitsluiten van een bepaald belang als gerechtvaardigd belang, is in strijd met de Europese rechtspraak. [De AP] moet een onderzoek doen naar de belangen van eiseres en vervolgens een afweging maken of zij door het uitzenden van de amateurvoetbalwedstrijden de bescherming van persoonsgegevens van betrokkenen ontoelaatbaar schendt. De manier waarop [de AP] deze toetsing moet uitvoeren volgt uit de in de uitspraak genoemde arresten van het [Europees] Hof van Justitie". VoetbalTV had verder gesteld dat "het opnemen en uitzenden van de wedstrijden valt onder de journalistieke exceptie". De rechtbank oordeelt hierover "dat dit in dit geval niet uitsluitend zo is". In het vonnis wordt de boete die de AP het – inmiddels failliet gegane - VoetbalTV had opgelegd, geschrapt.

Het vonnis betekent niet dat het livestreamen van amateurvoetbalbeelden is toegestaan; daar laat de uitspraak zich niet over uit. Essentie van het vonnis is dat de rechtbank oordeelt dat de AP de eerste toets in de drie-stappen-toets niet correct doorlopen heeft. Een commercieel belang kan een gerechtvaardigd (deel)belang zijn, waarna vraag 2 – betreft het een noodzakelijke gegevensverwerking? – en vooral vraag 3 van de toets beantwoord moeten worden: in dit geval, wegen de belangen die VoetbalTV nastreeft op tegen het inboeten aan bescherming van persoonsgegevens door amateurvoetballers? Aangezien de AP in haar onderzoek niet op de vragen 2 en 3 is ingegaan, kan de AP geen boete opleggen, zo oordeelt de rechtbank.

Bevindingen rapporteur

Als rapporteur wil ik mij, los van dit feitenrelaas, niet over de inhoud van deze casus uitspreken, temeer omdat er mogelijk nog gerechtelijke procedures over de zaak gevoerd worden. Wel plaats ik mijn vraagtekens bij het verloop van het proces in deze specifieke casus, waarbij er langdurig onderzoek heeft plaatsgevonden en ondanks herhaalde verzoeken geruime tijd geen uitsluitsel werd gegeven door de AP.

Ook constateer ik dat op dit moment in andere EU-lidstaten initiatieven actief zijn die in veel aspecten lijken op de activiteiten van VoetbalTV. Ik wijs dan bijvoorbeeld op het in Duitsland actieve Soccerwatch.tv ([link](#)). Op de website van Soccerwatch staat in de 'Frequently Asked Questions' bij de vraag "Wer muss einer Veröffentlichung der Videos



zustimmen?“ als antwoord: “Es ist ausreichend, wenn die Zuschauer, Spieler und Schiedsrichter mit einem gut sichtbaren Schild (wird von soccerwatch.tv zur Verfügung gestellt) auf die Videoaufnahmen hingewiesen werden“.

De tijdspanne en de scope van mijn rapporteurschap laten niet toe om een precieze vergelijking te maken tussen VoetbalTV en Soccerwatch die hun eigen kenmerken hebben en in een andere lidstaat onder een andere jurisdictie actief zijn, maar ik ben wel van mening dat de AVG ertoe zou moeten leiden dat binnen de EU vergelijkbare initiatieven vergelijkbare kansen hebben om tot ontwikkeling te komen. Uniforme regelgeving en een gelijk speelveld voor bedrijven zijn hierbij van groot belang.

2.2.2 Kankeronderzoek

Een andere casus waarop ik mijn rapporteurschap gefocust heb, is de impact van de AVG op de medische zorg en het medisch-wetenschappelijk onderzoek. Concreet ging het hierbij om de impact van de AVG op het gebruik van medische dossiers/persoonsgegevens bij kankeronderzoek en in de regionale kankerzorg. De AVG en de uitvoeringswet UAVG kennen speciale bepalingen met betrekking tot de verwerking van persoonsgegevens voor medische en onderzoeksdoeleinden.

Het kernelement in de gesprekken die ik als rapporteur voerde met vertegenwoordigers uit de medische sector, was opnieuw onzekerheid over hoe de AVG uit te leggen en toe te passen. Al eeuwenlang leren dokters van de patiënten die ze gezien hebben, om daarmee de patiënten van de toekomst beter te kunnen behandelen. Het gebruik van zorgdata is dan ook essentieel om, door middel van wetenschappelijk onderzoek, de gezondheidszorg te innoveren. Het spreekt voor zich dat het gebruik van deze gegevens goed geregeld moet worden. De AVG erkent dit belang en kent daarom diverse bepalingen die het doen van medisch onderzoek faciliteren, zoals bewaartermijnen, brede consent, nader gebruik, etc. De AVG laat daarbij ook ruimte voor de nationale wetgever voor nadere facilitering van (medisch) onderzoek. Omdat het hier gaat om een afweging van belangen (bescherming van persoonsgegevens versus zorginnovatie), voorziet de AVG daarbij steeds in ‘counterveiling measures’, zoals informatie, mogelijkheid van bezwaar en organisatorische en technische beschermingsmaatregelen tegen datalekken en onbevoegde toegang.

Uit de gesprekken die ik heb gevoerd, kwam voor mij naar voren dat de onderzoekers die zich bezighouden met medisch-wetenschappelijk kankeronderzoek tegen diverse obstakels aanlopen. Zij zijn van mening dat door de AVG het onderzoek in de praktijk sterk wordt belemmerd en daarmee innovatie en verbetering van gezondheidspreventie en -zorg wordt gefrustreerd. Volgens de onderzoekers hebben zij al met veel wetgeving te maken, waar de AVG er één van is. Zij stellen dat het beter was geweest wanneer bij de invoering van de AVG privacywetgeving in relatie tot medisch-wetenschappelijk onderzoek helder en haalbaar zou zijn geregeld, zowel via de Europese AVG alsmede de Nederlandse UAVG. De AVG zorgt voor een grijs gebied, waarbij verschillende partijen een sterk wisselende uitleg geven met betrekking tot de (on)mogelijkheden van data-uitwisseling. Ook vinden mijn gesprekspartners dat de AP, in vergelijking met andere landen, een nogal restrictieve uitleg van de AVG hanteert ten aanzien van medisch-wetenschappelijk (kanker)onderzoek, wat zorgt voor onzekerheid en angst voor boetes en reputatieschade. Dit remt volgens hen onderzoek af of doet onderzoekers en



instellingen soms helemaal van bepaald onderzoek afzien. Voorts bestaat er frustratie over sterk oplopende uitgaven aan juridisch advies, om de onzekerheid rond toepassing van de AVG te beteugelen. Dit zijn significante kosten, welke drukken op het budget bestemd voor medisch onderzoek zelf. Vanuit het veld is het initiatief genomen om te komen tot een nationale data-infrastructuur voor gezondheidsonderzoek en -innovatie (via Health-RI). Dit netwerk biedt ook een brede maatschappelijke basis om oplossingen voor de problemen met betrekking tot het gebruik van gezondheidsdata en regelgeving gezamenlijk vorm te geven. Tot slot wijzen de onderzoekers mij op knelpunten die zich voordoen bij het grensoverschrijdend samenwerken met medische onderzoeksgegevens, binnen de EU maar meer nog daar waar ook landen buiten de EU betrokken zijn, iets wat bij medisch-wetenschappelijk onderzoek zeer veelvuldig het geval is.

Bij kankerzorg is het eerder regel dan uitzondering dat de zorg wordt verleend door middel van regionale netwerken waarin zorgprofessionals samenwerken. Op deze manier wordt over instellingsgrenzen heen optimaal gebruik gemaakt van de kennis, kunde en capaciteit van iedere zorgprofessional, ten faveure van de best mogelijke behandeling voor de kankerpatiënt. Een snelle en volledige overdracht van alle relevante patiëntgegevens tussen zorgprofessionals in de regionale netwerken is daarbij van groot belang.

Tijdens het rondetafelgesprek werd betreffende dit onderwerp ook ingegaan op de consequenties van de AVG voor de regionale kankerzorg. Binnen deze vaak in de vorm van ketenonderzoek georganiseerde zorg leidt interactie tussen de AVG en samenhangende nationale wetgeving tot situaties waarbij meermalen een hernieuwde toestemmingsvraag nodig is om essentiële patiëntgegevens beschikbaar te krijgen voor alle bij de zorg van de patiënt betrokken hulpverleners, werkzaam bij de verschillende zorgaanbieders. Dit onder meer omdat de zorgverleners binnen de verschillende zorgaanbieders geacht worden ieder een eigen behandelovereenkomst met de patiënt te hebben in plaats van een gezamenlijke behandelovereenkomst als team. In het rondetafelgesprek werd naar voren gebracht dat de huidige wetgeving frustraties in de hand werkt bij zorgverlener en patiënt, en tot onwenselijke situaties leidt bij het te laat of incompleet beschikbaar komen van medische gegevens. Daarnaast werd gesteld dat modernisering van de relevante Nederlandse wetgeving, zoals de Wet op de geneeskundige behandelingsovereenkomst (WGBO) in relatie tot de AVG, essentieel is. Ter tafel werden nog suggesties opgebracht ter verbetering van de wetgeving, waarbij werd benoemd dat een dergelijke moderniseringsslag al vele jaren op zich laat wachten.

De bescheiden opzet van dit rapporteurschap laat het niet toe om de ervaren onzekerheid en knelpunten voortvloeiend uit het samenspel tussen AVG, nationale wetgeving in EU-lidstaten en internationale wetgeving in detail te analyseren. Gegeven het grote publieke belang van medische zorg en medisch-wetenschappelijk onderzoek doen de hiervoor genoemde bevindingen bij mij wel de vraag rijzen welke mogelijkheden er zijn voor sector, wetgever, toezichthouder en patiëntenorganisaties om de handen ineen te slaan en proactief tot een kader te komen – eventueel middels sectorale wetgeving – dat zorgprofessionals en onderzoekers duidelijkheid biedt en in staat stelt om binnen dit kader vrij en met vertrouwen met medische persoonsgegevens om te kunnen gaan. Tijdens mijn voorgesprekken en het rondetafelgesprek begreep ik dat hiertoe reeds aanzetten zijn gedaan. Uit de interparlementaire uitvraag die in het kader van het



rapporteurchap is uitgezet, komt naar voren dat landen als België en Denemarken bij hun uitvoeringswetten bij de AVG eigen regelingen hebben opgesteld voor het omgaan met persoonsgegevens bij (medisch-) wetenschappelijk onderzoek. Wellicht dat het beleid in deze en andere landen inspiratie kan bieden voor een aanpak in ons land.

2.2.3 Corona-app

De uitbraak en snelle verspreiding van het coronavirus begin 2020, deed in veel landen de roep ontstaan om apps te ontwikkelen waarmee bron- en contactonderzoek rond coronabesmettingen gefaciliteerd zou kunnen worden. Ook in Nederland werd ingezet op een dergelijke app. Nog los van de ICT-gerelateerde uitdagingen die de snelle ontwikkeling van een dergelijke app stelde, was een kernvraag hoe de bescherming van persoonsgegevens van gebruikers te waarborgen. Het ontwikkeltraject van deze app is de derde casus die ik in het kader van mijn rapporteurchap bekeken heb.

De app die na een kort selectieproces tot stand kwam, de CoronaMelder, herkent via bluetooth andere telefoons in dezelfde omgeving die de app ook gebruiken. Als een persoon langere tijd dicht bij een andere gebruiker in de buurt is, slaat de app de willekeurige code van de andere gebruiker tijdelijk op. Wanneer een gebruiker de diagnose corona krijgt, kan deze persoon anderen waarschuwen via de CoronaMelder. Op basis van de opgeslagen willekeurige codes wordt een signaal gestuurd naar gebruikers die bij deze persoon in de buurt zijn geweest. De app is conform de AVG ontworpen met privacy-by-design als uitgangspunt. Data wordt alleen verwerkt in de app en wordt niet centraal opgeslagen.

Bij het ontwikkeltraject dat leidde tot de CoronaMelder, werd ook de AP betrokken. Betreffende het voornemen om persoonsgegevens te verwerken met een coronanotificatie-app, ontving de AP in juli 2020 een verzoek tot advisering van de minister van Volksgezondheid, Welzijn en Sport over het voorliggende concept. De conclusie van het AP-advies van augustus 2020 luidde dat er, in de opvatting van de AP, om meerdere redenen nog niet voldoende zekerheid was om rechtmatig van start te kunnen gaan met de verwerking. Om hiertoe over te kunnen gaan, kwam de AP met een aantal adviezen. Eén daarvan was dat er een wettelijke grondslag moet komen voor de inzet van de notificatie-app.

De AP ziet als grondslag voor verwerking van persoonsgegevens artikel 6, lid 1e, AVG: "De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen". Artikel 6, derde lid AVG stelt eisen aan de wettelijke invulling van een dergelijke publieke zaak. De Wet publieke gezondheid (Wpg) voorziet volgens de AP niet in een democratisch gelegitimeerde grondslag; deze moet gecreëerd worden. In oktober 2020 is middels instemming met de Tijdelijke wet notificatieapplicatie covid-19 ([link](#)) in een dergelijke gelegitimeerde grondslag voorzien.

Voorafgaand aan de introductie van de tijdelijke wet ontwikkelde zich in de openbaarheid een dispuut tussen de minister en de AP over de wettelijke grondslag voor verwerking van de (deels medische) persoonsgegevens in de app. De AP achtte *toestemming* als grondslag "minder gepast", onder meer omdat na intrekking van toestemming door de gebruiker bepaalde gegevens tot 14 dagen na contact in de app van andere gebruikers



aanwezig blijven (advies AP: [link](#)). De minister geeft in een Kamerbrief ([link](#)) – ook na consultatie van de landsadvocaat - aan een andere mening te zijn toegedaan. De minister schrijft onder meer van mening te zijn dat bij gebrek aan een geëxpliciteerde wettelijke grondslag, expliciete toestemming wel degelijk een goede oplossing is voor de CoronaMelder. In de andere Europese landen die een vergelijkbare app hebben geïntroduceerd (of gaan introduceren) is dezelfde privacywetgeving (AVG) van toepassing en daar wordt voor gegevensverwerking ook gebruik gemaakt van expliciete toestemming, aldus de minister. Ook de Raad van State en het Europees Comité voor gegevensbescherming (de "European Data Protection Board") onderkennen toestemming als mogelijk rechtsgeldige grondslag. De minister geeft evenwel aan dat hij wil tegemoetkomen aan het advies van de AP, mede omdat hij met de tijdelijke wet tevens nadrukkelijk wil "borgen dat gebruik van de app vrijwillig is en dus door niemand mag worden afgedwongen".

Wanneer ik kijk naar de ontwikkeling van de CoronaMelder in vergelijking met apps van andere Europese lidstaten, vallen zowel gelijkenissen als verschillen op. Net als bij vele andere lidstaten het geval is, is gekozen voor een privacyvriendelijke, gedecentraliseerde app. Nederland heeft daarnaast, net als in ieder geval negen andere landen, haar gegevensbeschermingseffectbeoordeling gepubliceerd. Uit deze karakteristieken maak ik op dat de ontwikkeling van de CoronaMelder zeer transparant verlopen is. Deze transparantie ging gepaard met de consultatie van de AP en het levendige publieke debat over de ontwikkeling van CoronaMelder. Hieruit volgt dat verschillen in de belangenafweging tussen lidstaten zorgen voor verschillende accenten bij de toepassing van de AVG op apps als de CoronaMelder.

Bevindingen rapporteur

Als rapporteur frappeert me aan deze casus dat ook in dit geval betrokken (majeure) partijen bij de uitleg van de AVG op heel verschillende standpunten uitkomen. Op zich is het verschil van inzicht met de invoering van de Tijdelijke wet notificatieapplicatie covid-19 snel en effectief overbrugd, maar toch blijft het beeld hangen dat ook in een in het oog springende casus als deze voor wat betreft de persoonsgegevensaspecten nog geen sprake is van een uitgekristalliseerde consensus over hoe de AVG uit te leggen en toe te passen, een consensus waarbij betrokken partijen elkaar soepel vinden.

3. Bevindingen

Wanneer nieuwe wetgeving van kracht wordt, zeker als deze veel impact heeft op de samenleving, dan is er tijd nodig om te 'wennen' aan de veranderende regels. Positief aan de introductie van de AVG is dat deze heeft geleid tot veel meer bewustwording van het belang van de bescherming van persoonsgegevens. Europa loopt zonder meer voorop in de wereld als het gaat om de gegevensbescherming van haar burgers. Gezien de snelle voortschrijdende digitalisering van de samenleving zal dit belang alleen maar toenemen. De AVG is ook een belangrijke randvoorwaarde voor de overheid, die steeds meer diensten digitaal aanbiedt. Een groot nadeel aan de gewenningsperiode van deze privacywetgeving is wel dat deze tot veel rechtsonzekerheid leidt. Bij verschillende bedrijven, overheden en organisaties wordt gesproken van kramp of de regels wel goed gehanteerd worden en is er angst voor mogelijke boetes die geheven zouden kunnen worden bij vermeende overtredingen.



Zonder meer ligt hier een taak voor de AP om door voorlichting en communicatie duidelijke en stabiele verwachtingen te wekken over wat volgens de AVG wel en niet is toegestaan. Deze constatering plaatst twee aandachtspunten ten aanzien van onze nationale toezichthouder hoog op de agenda. Ten eerste is dat de vraag of de AP wel over voldoende capaciteit beschikt om adequate invulling te geven aan haar verschillende taken, in een digitaliserende wereld waar het privacybelang met de dag toeneemt. In het onlangs verschenen rapport van adviesorganisatie KPMG worden verschillende scenario's geschetst betreffende het capaciteitsvraagstuk bij de AP ([link](#)). In de tweede plaats lijkt het me nodig een discussie over ongewenste rolvermenging bij de AP te voeren. Schuurt het niet dat de onafhankelijke toezichthouder zowel als voorlichter ('meedenker') en kennisinstituut, maar tegelijkertijd ook als scheidsrechter, handhaver en boeteoplegger optreedt?

De in mijn onderzoek besproken casussen illustreren naar mijn mening de mate waarin publieke en private partijen nog 'worstelen' met de vraag hoe de AVG precies uit te leggen en toe te passen. Gegeven de complexiteit van de verordening, de mate waarin de regelgeving op vele niveaus van het publieke leven ingrijpt en het feit dat de AVG 'pas' sinds mei 2018 van toepassing is, is dat op zich niet onbegrijpelijk, maar tegelijk brengt dit ontegenzeggelijk veel onzekerheid met zich mee voor burgers, organisaties en bedrijfsleven. Volgens voor mijn onderzoek gehoorde juridische experts zal deze onzekerheid, die veroorzaakt wordt door leemtes binnen de AVG, uiteindelijk deels worden opgevuld door middel van jurisprudentie indien de wetgever niet voorziet in (sectorale) wetgeving.

Wanneer boetes leiden tot rechtszaken, moet de rechter beoordelen of bijvoorbeeld de uitleg van de AP van het 'gerechtvaardigd belang' of de sterke nadruk die zij legt op het toestemmingscriterium juridisch steekhoudend zijn. Ook het Europees Hof kan invulling geven aan de interpretatie van regelgeving. Het nadeel is dat dergelijke procedures doorgaans veel tijd in beslag nemen. Naast de rechtsgang die bedrijven zullen maken naar aanleiding van boetes van toezichthouders, ligt het in de lijn der verwachting dat ook particulieren bij vermeende privacyschendingen bedrijven, overheden of organisaties zullen gaan aanklagen, waarmee ook langs deze weg een striktere toepassing en verduidelijking van de AVG bevorderd kunnen worden.

Een veelgehoorde klacht over de toepassing van de AVG is dat deze soms tot zeer onpraktische of onwenselijke gevolgen leidt. Als voorbeelden worden dan bijvoorbeeld de beperkingen genoemd die de wet zou opleggen aan de informatie-uitwisseling over fraudeurs of het delen van groepsfoto's in het onderwijs of bij sportverenigingen. Vaak wordt in reactie op dergelijke klachten gesteld dat dit het gevolg is van een gebrek aan kennis en dat er binnen de AVG veel meer mogelijk is dan vaak wordt verondersteld. Dit gaat echter zeker niet in alle gevallen op. Een oplossing hiervoor kan soms sectorale wetgeving zijn. De (algemeen geformuleerde) AVG biedt de ruimte om voor specifieke sectoren duidelijke privacyregels op te stellen. In Nederland bestaan hiervan al voorbeelden, zoals de Wet gegevensverwerking door samenwerkingsverbanden (aangenomen door de Tweede Kamer op 17 december 2020), waardoor in het belang van criminaliteitsbestrijding informatie kan worden uitgewisseld tussen publieke en private partijen.



Nadeel van nationale sectorale wetgeving is wel dat deze op gespannen voet kan staan met de Europese harmonisatie van wetgeving. Veel privacyschendingen stoppen niet bij de grens en op een gemeenschappelijke markt is het belangrijk dat er sprake is van een gelijk speelveld. Als bedrijven internationaal opereren, dan geldt in de AVG het 'leidende toezichthouder-principe'. Het land waar het Europese hoofdkwartier van de onderneming is gevestigd controleert of het bedrijf zich aan de privacyregels houdt. Ieder land heeft echter een eigen toezichthouder, die onderscheidend is samengesteld en zelfstandig opereert. Daarnaast is er sprake van cultuurverschillen, waarbij er in diverse EU-landen anders wordt omgegaan met de belangen van burgers, overheid of bedrijfsleven. Het vraagstuk hoe effectief toezicht te houden op de grote internationaal opererende techbedrijven wordt hierbij veelvuldig genoemd. Het harmonisatievraagstuk is in de drie casussen van deze rapportage al aan de orde gekomen en ook hier lijkt nog een wereld te winnen. De EDPB moet door het uitvaardigen van richtsnoeren, aanbevelingen en best practices nog meer dan nu een bijdrage leveren aan het interpreteren van de AVG. Ook bij grote grensoverschrijdende privacykwesties kan door het beschikbaar stellen van complexe juridische- en ICT-kennis een rol voor de EDPB zijn weggelegd.

Concluderend kan gesteld worden dat de AVG tot een veel grotere bewustwording heeft geleid bij de overheid, het bedrijfsleven en burgers van het belang van de bescherming van persoonsgegevens. Tegelijkertijd bestaat er ook veel onzekerheid door de onduidelijkheid over de interpretatie en handhaving van de regels, ook tussen de verschillende Europese lidstaten. Dit schaadt tevens het algemeen belang, bijvoorbeeld in het geval van medische zorg en onderzoek. Ook als politiek hebben we de verantwoordelijkheid om deze onzekerheid en onduidelijkheid zo veel mogelijk weg te nemen en harmonisatie in Europa na te streven.

Rapporteur
T. van Gent