Is een dynamisch IP-adres een persoonsgegeven?

Noot bij arrest van het Europese Hof van Justitie inzake Patrick Breyer tegen Bondsrepubliek Duitsland

mr. Y. van den Winkel[1]

Op 19 oktober 2016 heeft het Europese Hof van Justitie (HvJ EU) uitspraak gedaan over onder meer de vraag of dynamische IP-adressen persoonsgegevens kunnen zijn. Het HvJ EU komt in de zaak Breyer tegen de Bondsrepubliek Duitsland tot de conclusie dat een dynamisch IP adres een persoonsgegeven is.[2] *'In de zaak Breyer versus de Bondsrepubliek Duitsland'* zal een belangrijke nuancering blijken want deze uitspraak van het HvJ EU kent zijn 'beperkingen'.

1. Persoonsgegevens

De vraag of gegevens persoonsgegevens zijn in de zin van art. 2 onder a van de richtlijn 95/46[3] (Privacyrichtlijn), geïmplementeerd in art. 1 onder a van de Wet bescherming persoonsgegevens (WBP) is van belang voor de toepasselijkheid van privacy wet- en regelgeving. Een persoon moet identificeerbaar zijn, anders is geen sprake van een persoonsgegeven en is de privacy wet- en regelgeving niet van toepassing.[4] In de Privacyrichtlijn zijn persoonsgegevens gedefinieerd als *'iedere informatie betreffende geïdentificeerde of identificeerbare natuurlijke persoon, hierna: 'betrokkene' te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit'*. In de WBP is het begrip persoonsgegevens bondiger gedefinieerd namelijk als: *'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'*.

Over de vraag of een IP-adres altijd een persoonsgegeven is bestaat al langere tijd onduidelijkheid. De Nederlandse privacywaakhond, de Autoriteit Persoonsgegevens (AP), en de Werkgroep 29 (WG 29)[5] menen in ieder geval dat een IP-adres een persoonsgegeven kan zijn.[6]

Een IP-adres is een reeks van nummers dat wordt toegekend aan een computer die met het internet verbonden is. Wanneer u bijvoorbeeld een website bezoekt wordt het IP-adres van de computer waarmee u de website bezoekt doorgegeven aan de server waar de website is opgeslagen. Zo kunnen de gegevens aan de juiste ontvanger worden overgedragen. In geval van IP-adressen kan het dynamische IP-adres worden onderscheiden van een statisch IP-adres (ook wel vast IP-adres genoemd). Een dynamisch IP-adres wijzigt, in tegenstelling tot een statisch IP-adres, bij iedere nieuwe verbinding met het internet. Een statisch IP-adres is onveranderlijk.

In de zaak Breyer/ Bondsrepubliek Duitsland heeft het HvJ EU de vraag beantwoord of het dynamisch IP-adres van Breyer een persoonsgegeven is. Breyer stelt zich op het standpunt dat een IP-adres (in casu een dynamisch IP-adres) een persoonsgegeven is nu het op basis van een combinatie van gegevens mogelijk is een persoon te identificeren, waarbij het

1. Yentl van den Winkel is als jurist werkzaam bij SOLV advocaten te Amsterdam.
2. HvJ EU 19 oktober 2016, C-582/14.
3. Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB 1995, L 281, blz. 31).
4. Zie G-J Zwenne, *De verwaterde privacywet*, oratie te Leiden, 12 april 2013, over de drie aspecten van het begrip persoonsgegeven.
5. De Werkgroep 29 is het onafhankelijke advies -en overlegorgaan waarin de Europese privacytoezichthouders zijn vertegenwoordigd.
6. Zie daarover onder meer G-J Zwenne, 'Nog enkele opmerkingen over IP-adressen en persoonsgegevens, identificeerbaarheid en 'single out', *Privacy & Informatie*, afl. 6, december 2015.

er verder niet toe doet of die combinatie feitelijk in de praktijk wordt gebracht. De Duitse Bondsrepubliek stelt daar tegenover het dynamische IP-adres de persoon niet 'geïdentificeerd maken' omdat identificatie alleen mogelijk is met aanvullende informatie die in handen is van een derde en waarover zij dus niet beschikken.

2. Het geschil

Patrick Breyer, een Duitse onderdaan, heeft een aantal voor het publiek toegankelijke websites bezocht die worden aangeboden door Duitse federale instellingen. Om cyberaanvallen af te weren en strafvervolging van de aanvallers mogelijk te maken, registreren deze websites logebestanden van ieder bezoek. Deze logbestanden bewaren na afloop van iedere sessie gegevens omtrent het bezoek aan de website waaronder ook het IP-adres van de computer van waaraf de opvraging heeft plaats gevonden. Breyer heeft bij de Duitse bestuursrechter (het Amtsgericht) gevorderd dat de Bondsrepubliek Duitsland, die de websites aanbiedt, een verbod wordt opgelegd om na zijn bezoek aan de websites het IP-adres te bewaren of door derden te doen bewaren, voor zover de bewaring van dat IP-adres niet nodig is om de beschikbaarheid van die websites te herstellen in geval van een storing. De rechter in eerste aanleg heeft de vordering van Breyer afgewezen, waarna Breyer hoger beroep heeft ingesteld tegen die afwijzende beslissing. De Duitse appelrechter wijst de vordering van Breyer gedeeltelijk toe namelijk voor die gevallen dat de gebruiker tijdens zijn bezoek zijn identiteit bekend heeft gemaakt, onder andere door het opgeven van een e-mailadres, en de bewaring niet nodig was om de beschikbaarheid van de website te herstellen. De websitehouder kan volgens de appelrechter in dit geval de gebruiker identificeren door zijn naam te koppelen aan het IP-adres. In andere gevallen kan het beroep van Breyer volgens de appelrechter niet slagen, omdat wanneer de identiteit van de gebruiker bij het bezoek aan de website niet bekend is gemaakt, enkel de internet serviceprovider (ISP) het IP-adres kan koppelen aan een persoon, de abonnee. De websitehouder, in dit geval de Bondsrepubliek, beschikt dan niet over gegevens die kunnen worden gekoppeld teneinde een persoon te identificeren, zelfs niet indien zij de beschikking heeft over het IP-adres en het tijdstip.

Zowel Breyer als de Bondsrepubliek kunnen zich niet vinden in de beslissing van de Duitse appelrechter en stellen beide een verzoek tot Revision in bij het Bundesgerichtshof , de hoogste Duitse rechter, te vergelijken met de Hoge Raad in Nederland. Breyer is het niet eens met de door de appelrechter opgelegde beperking en het Bundesgerichtshof vordert wederom integrale afwijzing van de vorderingen van Breyer.

Het Bundesgerichtshof stelt vast dat de identiteit van Breyer niet rechtstreeks door de Bondsrepubliek Duitsland kan worden achterhaald op basis van een IP-adres, maar alleen indien zij van de ISP nadere informatie ontvangt over de identiteit van Breyer. Het Bundesgerichtshof vraagt zich dan ook af of het dynamische IP-adres van Breyer een persoonsgegeven kan zijn indien een derde beschikt over de aanvullende gegevens die nodig zijn om hem (de betrokkene) te identificeren en zo ja, of de bewaring van de IP-adressen na afloop van het bezoek aan de website wel is toegestaan op grond van de Privacyrichtlijn.

3. Prejudiciële vragen

Op 17 december 2014 dient het Bundesgerichtshof een verzoek tot prejudiciële beslissing in bij het HvJ EU en legt de volgende twee prejudiciële vragen voor[7]:

> *'1) Dient artikel 2, onder a), van richtlijn 95/46 aldus te worden uitgelegd dat een internetprotocoladres (IP-adres) dat een aanbieder van [online-media]diensten opslaat wanneer zijn internetsite wordt bezocht, voor deze aanbieder reeds dan een persoonsgegeven vormt, wanneer een derde (in casu: de internetprovider) beschikt over de aanvullende gegevens die nodig zijn om de betrokken persoon te identificeren?*
> *2) Verzet artikel 7, onder f), van [deze richtlijn] zich tegen een regel van nationaal recht op grond waarvan de aanbieder van [onlinemedia]diensten persoonsgegevens van een gebruiker zonder diens toestemming enkel mag verzamelen en benutten voor zover dit nodig is om het concrete gebruik van [het onlinemedium] door de betrokken gebruiker mogelijk te maken en te factureren en op grond waarvan de doelstelling, die erin bestaat de goede werking van [het onlinemedium] in het algemeen te waarborgen, niet rechtvaardigt dat de gegevens worden benut na afloop van [de desbetreffende sessie]?'*

De vraag of een IP-adres een persoonsgegeven is, is in 2011 al aan bod gekomen bij het HvJ EU in de zaak Scarlet Extended tegen SABAM.[8] In die zaak heeft het HvJ EU – kort gezegd - overwogen dat IP-adressen persoonsgegevens kunnen zijn indien zij de 'precieze identificatie' van personen mogelijk maken. In de zaak Scarlet ging het echter om het geval waarin de IP-adressen werden verzameld en geïdentificeerd door de ISP.[9] Nieuw in de zaak

7. Verzoek om een prejudiciële beslissing d.d. 17 december 2015, C- 582/14.
8. HvJ EU 24 november 2011 C-70/10, EU:C:2011:771.
9. In de verordening 2016/679 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) die in werking treedt op 25 mei 2018 is het begrip persoonsgegeven in art. 4 sub 1 als volgt gedefinieerd: *'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene');*

Breyer is dus de vraag hoe relevant het is dat niet de verantwoordelijke zelf, maar een derde over de aanvullende gegevens beschikt om de betrokkene te kunnen identificeren.

3.1. Eerste prejudiciële vraag

Uit de eerste prejudiciële vraag kan een afbakening worden afgeleid. Zo is de vraag beperkt tot *de aanbieder van [online]mediadiensten*', in dit geval de websitehouder. Een andere afbakening is die van de precisering van de derde. De vraag ziet enkel op *'een derde (in casu: de internetprovider)*', een heel specifieke derde dus. Iedere willekeurige derde is hierdoor in de beoordeling van deze zaak uitgesloten. Het Bundesgerichtshof gaat er kennelijk vanuit dat alleen de ISP beschikt over de aanvullende gegevens.
Voorts stelt de Advocaat-Generaal in zijn conclusie dat het Bundesgerichtshof uitsluitend doelt op dynamische IP-adressen.[10] Ook het HvJ EU stelt vast dat de IP-adressen waaraan de verwijzende rechter refereert dynamische IP-adressen zijn.[11] Waaruit dit blijkt is mij niet direct duidelijk. De prejudiciele vragen zijn mijns inziens niet zo geformuleerd dat hiermee alleen dynamische IP-adressen zijn bedoeld. Vermoedelijk is dit gebaseerd op het feit dat het in casu om uitsluitend een dynamisch IP-adres ging.[12]
Het HvJ EU beperkt zich dus tot een oordeel of dynamische IP-adressen persoonsgegevens zijn voor een aanbieder van internetdiensten indien de ISP over aanvullende gegevens beschikt die identificatie van een persoon mogelijk maken. De beoordeling van het HvJ EU geeft dus geen antwoord op de vraag of dynamische IP-adressen in alle gevallen en onder alle omstandigheden zijn aan te merken als persoonsgegeven – voor zover dit al mogelijk zou zijn.

Voorts ligt in de vraagstelling ook al besloten dat ervan uit wordt gegaan dat aan de hand van alleen een (dynamisch) IP-adres een persoon niet kan worden geïdentificeerd. Deze vraag hield partijen overigens ook niet verdeeld. Het HvJ EU stelt dan ook vast dat een dynamisch IP-adres *indirecte* identificatie mogelijk maakt, en dat er dus aanvullende gegevens nodig zijn die met het IP-adres kunnen worden gekoppeld.
De vraag of identificatie mogelijk is, beantwoordt het HvJ EU aan de hand van hetgeen in overweging 26 van de Privacyrichtlijn is bepaald, namelijk dat moet worden gekeken naar *'alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is, dan wel door enige andere persoon, kunnen worden ingezet om voornoemde persoon te identificeren.*'
Het HvJ EU stelt vast dat uit deze overweging volgt dat nu ook *'enige andere persoon*' de middelen in kan zetten om een persoon te identificeren, het niet vereist is dat alle informatie aan de hand waarvan de betrokkene kan worden geïdentificeerd bij een en dezelfde persoon dient te berusten. Een dynamisch IP-adres kan daarom een persoonsgegevens zijn ondanks dat de benodigde gegevens zich niet direct bij de websitehouder bevinden maar bij de ISP.
De vervolgvraag is of de mogelijkheid om een dynamisch IP-adres te combineren met aanvullende gegevens waarover de ISP de beschikking heeft, een middel is dat redelijkerwijs ingezet kan worden om een persoon te kunnen identificeren. Ondanks dat de Duitse Bondsrepubliek hiertoe heeft gesteld dat de ISP de aanvullende gegevens niet rechtstreeks aan de websitehouder mag doorgeven, concludeert het HvJ EU – onder het voorbehoud van verificatie door de Duitse rechter- dat er juridische mogelijkheden lijken te zijn voor de websitehouder om zich te wenden tot de bevoegde autoriteit en te verzoeken om actie te ondernemen om de gegevens van de ISP te verkrijgen en strafvervolging in te stellen.
Het HvJ EU beantwoordt de eerste prejudiciële vraag aldus bevestigend. Een dynamisch IP-adres kan voor een websitehouder een persoonsgegeven zijn wanneer hij beschikt over wettige middelen waarmee hij een persoon kan identificeren aan de hand van aanvullende informatie die zich onder de ISP bevindt.
Deze conclusie schept wellicht duidelijkheid in het geval van Breyer tegen de Bondsrepubliek Duitsland, althans een en ander is nog wel afhankelijk van verificatie door de Duitse rechter, maar laat voor andere gevallen en de praktische toepassing nog wel een aantal onduidelijkheden bestaan. Zoals de advocaat-generaal in de conclusie al opmerkt[13] en door het HvJ EU is overgenomen, kan het verzoek om gegevensverstrekking aan de ISP niet als redelijk middel worden beschouwd indien dit bij wet is verboden of in de praktijk ondoenlijk is omdat zij een excessieve inspanning vergt, gelet op de in te zetten tijd, kosten en mankracht. Het HvJ EU concludeert dat Duitsland lijkt te voorzien in een wettelijke mogelijkheid om gegevens van de ISP te verkrijgen en ook Nederland kent dergelijke mogelijkheden.[14] Echter, het is de vraag of ieder Europees land een dergelijk verzoek tot gegevensverstrekking wettelijk heeft geregeld. Daarnaast zal ook per verantwoordelijke moeten worden beoordeeld of het middel redelijkerwijs kan worden ingezet, nu die beoordeling afhankelijk is van de praktische mogelijkheden. In de praktijk zou dit tot gevolg kunnen hebben dat het dynamisch IP-adres voor de ene verantwoordelijke wel als een persoonsgegeven is aan te merken en voor de andere niet.
Dit kan ermee te maken hebben dat het HvJ EU, in lijn met de aankomende Algemene Verordening Gegevensverwerking (25 mei 2018)[15], vasthoudt aan de 'identificeerbaarheid' van personen. Hierdoor is het mogelijk dat voor de ene verantwoordelijke een betrokkene wel kan worden geïdentificeerd, terwijl dit voor een ander niet mogelijk blijkt.[16] De AP en de WG 29 waren echter al aan het verschuiven naar een beoordeling van het persoonsgegevensbegrip op basis van het ruimere 'onderscheiden' ook wel 'individualiseerbaarheid' genoemd.[17] In dit laatste geval is het voldoende dat een persoon kan worden onderscheiden ('singled-out') van een ander en dus anders kan worden behandeld. Daadwerkelijke bekendheid van de persoon van de betrokkene is daarbij niet vereist. In dat geval is dus veel sneller (vrijwel altijd) sprake van een persoonsgegevens aangezien het begrip persoonsgegeven in dit geval minder afhankelijk is van de omstandigheden van het geval. In die lijn gaat de AP er de laatste tijd ook vanuit dat IP-adressen altijd kwalificeren als persoonsgegeven omdat zij het mogelijk maken de ene persoon van de andere te kunnen onderscheiden. Het HvJ EU gaat daar in geval van dynamische IP-adressen dus niet in mee.

3.2. Tweede prejudiciële vraag

Nu het HvJ EU in de zaak Breyer tot conclusie is gekomen dat het dynamisch IP-adres een persoonsgegeven is, zal ook de tweede vraag moeten worden beantwoord. Het Bundesgerichtshof vraagt zich af of persoonsgegevens wel mogen worden bewaard nadat de gebruiker de website al heeft verlaten.
In de Duitse nationale wetgeving geldt een strikte regel op grond waarvan het enkel is toegestaan om persoonsgegevens van een gebruiker van onlinemediadiensten zonder diens toestemming te verzamelen en te benutten voor zover dit nodig is om het concrete gebruik van het betrokken onlinemedium door deze gebruiker mogelijk te maken en te factureren. Het Bundesgerichtshof vraagt zich meer specifiek af of art. 7 van de Privacyrichtlijn (gerechtvaardigd belang) zich tegen een dergelijke regeling verzet.
Het HvJ EU concludeert bevestigend nu art. 7 van de Privacyrichtlijn in het algemeen verwijst naar de *'behartiging van het gerechtvaardigd belang van de voor de verwerking verantwoordelijke of van de derde(n) aan die de gegevens worden verstrekt*', terwijl de Duitse nationale regeling zich beperkt tot het concrete gebruik van de website. Volgens het HvJ EU is het dus mogelijk om de IP-adressen ook na het bezoek aan de website te bewaren.

4. Slotwoord

Dit arrest van het HvJ EU geeft het beoordelingskader op basis waarvan moet worden beoordeeld of een dynamisch IP-adres voor een websitehouder een persoonsgegeven is. Wanneer de verantwoordelijke beschikt over middelen die redelijkerwijs kunnen worden ingezet om aanvullende informatie van een ISP te verkrijgen teneinde een persoon te identificeren, dan is een dynamisch IP-adres voor die verantwoordelijke een persoonsgegeven. Dit beoordelingskader lijkt ruimte te bieden om in andere gevallen, waarbij de spelers niet de betrokkene, de websitehouder en de ISP zijn om anders te oordelen. Bovendien is de beoordeling afhankelijk van de wettelijke en praktische mogelijkheden, welk oordeel per geval anders uit kan vallen. Hierdoor kan een dynamisch IP-adres voor de ene verantwoordelijke wel als persoonsgegevens worden aangemerkt, terwijl dit voor een ander niet het geval hoeft te zijn. Met dit arrest heeft het HvJ EU dus geen uitspraak gedaan over de vraag of een dynamisch IP-adres altijd moet worden aangemerkt als een persoonsgegeven wanneer de ISP de betrokkene kan identificeren. Die beoordeling blijft ervan afhangen of het benaderen van de ISP voor de betreffende verantwoordelijke als redelijk middel kan worden beschouwd om de gebruiker van de website te kunnen identificeren.

als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name 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 natuurlijke persoon.' In overweging 30 van de considerans is toegelicht wat onder een online identificator moet worden verstaan: '*Natuurlijke personen kunnen worden gekoppeld aan online-identificatoren via hun apparatuur, applicaties, instrumenten en protocollen, zoals internetprotocol (IP)-adressen, identificatiecookies of andere identificatoren zoals radiofrequentie-identificatietags. Dit kan sporen achterlaten die, met name wanneer zij met unieke identificatoren en andere door de servers ontvangen informatie worden gecombineerd, kunnen worden gebruikt om profielen op te stellen van natuurlijke personen en natuurlijke personen te herkennen.*'[mijn onderstreping].

10. Conclusie Advocaat-Generaal M. Campos Sánchez-Bordona 12 mei 2016, C-582/14, overweging 47.
11. HvJ EU 19 oktober 2016, C-582/14, overweging 36.
12. Verzoek om een prejudiciële beslissing d.d. 17 december 2015, C- 582/14, overweging 19.
13. Conclusie Advocaat-Generaal M. Campos Sánchez-Bordona 12 mei 2016, C-582/14, overweging 68 en 72-73.
14. Zie bijvoorbeeld civielrechtelijk HR 25 november 2005, ECLI:NL:PHR:2005:AU4019 en strafrechtelijk bijvoorbeeld op grond van art. 126n, 126u,126ng, 126 ug wetboek van Strafvordering. NB: Ter zake deze wettelijke regelingen staat dus niet vast of deze als redelijk in te zetten middelen kunnen worden aangemerkt.
15. Zie voetnoot 8.
16. Zie het voorbeeld van de vingerafdruk op het glas de oratie van G-J Zwenne, *De verwaterde privacywet*, oratie te Leiden, 12 april 2013, over de drie aspecten van het begrip persoonsgegeven.
17. G-J Zwenne, 'Nog enkele opmerkingen over IP-adressen en persoonsgegevens, identificeerbaarheid en 'single out', *Privacy & Informatie*, afl. 6, december 2015.