Autoriteit Persoonsgegevens legt boete op aan gemeente Enschede wegens wifitracking

Noot bij boetebesluit 11 maart 2021

S.C. van Schaik[1]

Op 11 maart 2021 legt de Autoriteit Persoonsgegevens (AP) een boete van € 600.000 op aan het college van burgemeester en wethouders van de gemeente Enschede (het college)[2] voor het gebruik van wifitracking. Het college wilde met deze techniek alleen meten hoeveel personen er in het centrum van de stad aanwezig waren, maar de techniek maakte het ook mogelijk om voorbijgangers te volgen en leefpatronen af te leiden. Dat is volgens de AP in strijd met de Algemene Verordening Gegevensbescherming (AVG).

1. Wat was er aan de hand?

In 2017 besluit het college tot het toepassen van wifitracking in het centrum van de stad Enschede om de drukte in de binnenstad te meten. Vanaf mei 2018 registreren 11 sensoren voorbijgangers. De sensoren lezen onder andere het MAC-adres uit van alle mobiele apparaten waarop wifi ingeschakeld staat. Het MAC-adres is een uniek identificatienummer van de netwerkmodule in een apparaat, zoals een smartphone, laptop of printer. Dit nummer maakt het mogelijk om het apparaat te herkennen binnen een (wifi-)netwerk. De volgende gegevens worden gedurende 6 tot 7 maanden opgeslagen:

- het gepseudonimiseerde (en afgeknipte) MAC-adres van het apparaat van de voorbijganger;[3]
- de datum en het tijdstip waarop de voorbijganger binnen het bereik van de sensor is (op circa 20 meter ingesteld); en
- het identificatienummer van de sensor.

Het onderzoek van de AP gaat met name over de vraag of het college persoonsgegevens verwerkt en zo ja, of hier een grondslag voor bestaat.

2. Persoonsgegevens

Het college voerde aan dat het geen persoonsgegevens verwerkte, omdat het MAC-adres werd gepseudonimiseerd en afgeknipt en het college alleen geaggregeerde rapporten ontving. De AP maakt daar korte metten mee.

Er is sprake van persoonsgegevens in de zin van de AVG wanneer het gaat om informatie over 'een geïdentificeerde of identificeerbare persoon' (art. 4 sub 1 AVG). In dit geval gaat het om de vraag of personen direct of indirect te identificeren zijn aan de hand van identificatoren. Volgens de AP zijn het MAC-adres en de locatiegegevens dergelijke identificatoren. De locatiegegevens bestaan in dit geval uit de combinatie van het identificatienummer van de sensor en de datum en het tijdstip waarop de voorbijganger binnen het bereik van de sensor was.[4] Nu van iedere sensor de locatie bekend was, kon hieruit heel precies worden afgeleid wanneer een mobiel apparaat waar was.

De AP onderscheidt verschillende fases in de verwerking met betrekking tot het uitlezen en tijdelijk opslaan van de gegevens op de sensor en in databases en maakt onderscheid tussen de periode voor en na het afknippen van het MAC-adres.[5] De AP komt echter in alle gevallen tot de conclusie dat personen op basis van de combinatie van het (al dan niet afgeknipte) gepseudonimiseerde MAC-adres en de locatiegegevens identificeerbaar zijn, omdat het mogelijk is om ter plaatse of via een camera vast te stellen

1. Silvia van Schaik is advocaat informatierecht bij bureau Brandeis te Amsterdam.
2. Het boetebesluit is gepubliceerd op de website van de Autoriteit Persoonsgegevens, vindplaats: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_ap_gemeente_enschede.pdf
3. Tot 1 januari 2019 werd het gehele gepseudonimiseerde MAC-adres opgeslagen. Vanaf 1 januari 2019 werd een deel verwijderd. In het besluit wordt dit 'afknippen' genoemd.
4. Het bereik van de sensor was ingesteld op 20 à 30 meter.
5. Tot 1 januari 2019 werd het gehele gepseudonimiseerde MAC-adres opgeslagen. Vanaf 1 januari 2019 werd een deel verwijderd. In het besluit wordt dit 'afknippen' genoemd.

welke persoon zich binnen het bereik van de sensor bevindt. De AP benadrukt hierbij dat zij al eerder in het kader van wifitracking oordeelde dat het registreren van MAC-adressen en locatiegegevens via sensoren kwalificeert als verwerking van persoonsgegevens[6] en verwijst in dit verband ook naar een tweetal opinies van de Europese privacy-toezichthouders.[7]

De AP overweegt daarbij uitdrukkelijk dat de pseudonimisatie en het afknippen van het MAC-adres onvoldoende de risico's op koppelbaarheid, herleidbaarheid en deduceerbaarheid uitsluit en dat de verzamelde gegevens daarom nog steeds kwalificeren als persoonsgegevens.[8] Hierbij acht de AP onder meer relevant dat koppeling van gegevens over dezelfde betrokkene ook daadwerkelijk plaatsvond. De wijze van pseudonimisering en afknippen van het MAC-adres was gedurende de hele periode van de verwerking en op iedere sensor hetzelfde. De identificator was daardoor dus steeds hetzelfde. Gegevens gekoppeld aan deze identificator werden samengevoegd en er werd ontdubbeld. Ook volgens de medewerkers van het bedrijf dat de sensors leverde was het detailverlies door pseudonimisering en afknippen zo klein, dat die koppeling mogelijk was. Het voor langere tijd opslaan van de onveranderde identificatoren en locatiegegevens maakte het bovendien mogelijk om individuen te volgen en leefpatronen af te leiden. Dat in 70% van de gevallen voorbijgangers maar één keer werden geregistreerd en daaruit dus geen patronen konden worden afgeleid, maakt dat niet anders. Het college heeft van tienduizenden burgers wel meerdere tellingen verwerkt. Van '*robuuste anonimiseringstechnieken*' was dan ook geen sprake.

Dit oordeel past in het patroon van de AP om gegevens snel als persoonsgegevens aan te merken. Opvallend is dat de AP daarbij met name verwijst naar oudere opinies[9] en haar eigen eerdere oordeel over wifitracking[10] en niet naar de recentere richtsnoeren van de EDPB zoals die over het gebruik van locatiegegevens bij contacttracering in verband met Covid-19.[11] De EDPB overweegt hierin dat een redelijkheidstoets moet worden toegepast om te beoordelen of anonimiseringstechnieken het onmogelijk maken dat de betrokkene nog geïdentificeerd wordt. De vraag is of de gegevens met een '*redelijke inspanning*' nog te koppelen zijn aan een identificeerbare persoon.[12] Aan de ene kant, lijkt de mogelijkheid om ter plaatste of via een camera vast te stellen wie zich op een bepaald moment binnen het beperkte bereik van de sensor bevond, wellicht meer dan een 'redelijke inspanning'. Aan de andere kant, had het college die vorm van mogelijke (re-)identificatie eenvoudig kunnen wegnemen door niet het precieze tijdstip dat iemand binnen het bereik van de sensor is, vast te leggen.[13] Wat een redelijke inspanning in het kader van anonimiseringstechnieken precies is, wordt niet uitgelegd in de richtsnoeren. Volgens het Hof van Justitie van de EU leidt het kunnen herleiden van iemands identiteit via een wettelijke mogelijkheid om gegevens op te vragen tot identificeerbaarheid.[14] Gegevens worden dus kennelijk niet snel aangemerkt als anoniem.

Ook de EDBP overweegt in de richtsnoeren overigens dat locatiegegevens 'die als anoniem worden beschouwd' dat niet altijd zijn. Zo kan een gegevenspatroon waarmee de locatie van een persoon voor langere tijd wordt getraceerd niet volledig worden geanonimiseerd en kunnen gegevens ook herleidbaar zijn als de nauwkeurigheid van de locatie onvoldoende is beperkt, aldus de EDPB.[15] In het onderhavige geval zijn vrij precieze locaties vastgelegd. Het gebruikte pseudoniem werd bovendien daadwerkelijk gebruikt om gegevens van dezelfde voorbijganger aan elkaar te koppelen.[16] Door over een langere periode hetzelfde pseudoniem te gebruiken, kon bovendien een patroon worden afgeleid. Naar mijn mening komt de AP dan ook terecht tot de conclusie dat sprake is van persoonsgegevens, maar wellicht moet ik daar na publicatie van de aangekondigde nieuwe richtsnoeren over anonimiseringstechnieken van de EDPB[17] op terugkomen.

3. Rechtmatigheid

De AP oordeelt dat het college met de verwerking in strijd met het rechtmatigheidsbeginsel (art. 5 lid 1 sub b en 6 lid 1 AVG) handelt. Dit beginsel komt erop neer dat een verwerking gebaseerd moet zijn op een van de in artikel 6 lid 1 AVG genoemde grondslagen. Voor het gebruik van wifitracking door het college kwamen de volgende grondslagen in aanmerking:
- De verwerking is noodzakelijk voor de uitvoering van een wettelijke plicht (art. 6 lid 1 sub c AVG);
- De verwerking is noodzakelijk voor de uitvoering van een publieke taak (art. 6 lid 1 sub e AVG); en

6. Rapport definitieve bevindingen College Bescherming Persoonsgegevens 13 oktober 2015, z2014-00944 (Bluetrace).
7. WP202 Opinion 02/2013 on apps on smart devices en WP247 Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation.
8. Kort na de publicatie van het boetebesluit publiceerde de AP tevens een techblogpost over het afknippen van hashes, zie https://autoriteitpersoonsgegevens.nl/nl/nieuws/techblogpost-praktische-problemen-bij-het-afknippen-van-hashes.
9. WP202 Opinion 02/2013 on apps on smart devices en WP247 Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation.
10. Rapport definitieve bevindingen College Bescherming Persoonsgegevens 13 oktober 2015, z2014-00944 (Bluetrace).
11. Richtsnoeren 04/2020 voor het gebruik van locatiegegevens en instrumenten voor contacttracering in het kader van de uitbraak van COVID-19, 21 april 2020.
12. Richtsnoeren 04/2020, par. 15.
13. Vgl. Richtsnoeren 04/2020, par. 27.
14. HvJEU 19 oktober 2016, ECLI:EU:C:2016:779 (Breyer).
15. Richtsnoeren 04/2020, par. 20 en 21.
16. Vgl. Richtsnoeren 04/2020, par. 16.
17. Blijkens het EDPB work programme 2021-2022 publiceert de EDPB in 2021 of 2022 een nieuwe versie van WP216 Advies 5/2014 over anonimiseringstechnieken.

– De verwerking is noodzakelijk voor een gerechtvaardigd belang (art. 6 lid 1 sub f AVG).

Het college voert hoofdzakelijk aan dat wifitracking nodig was voor het meten van de effectiviteit van investeringen in de binnenstad van Enschede. Het beroept zich onder meer op een aantal artikelen uit de Gemeentewet, de APV en enkele regelingen. De AP overweegt dat het college geen wettelijke verplichting heeft om wifimetingen in de binnenstad te verrichten. Daarmee valt de grondslag sub c af. Ten aanzien van de grondslag genoemd in sub e (publieke taak) overweegt de AP dat die grondslag weliswaar niet voor elke afzonderlijke verwerking specifieke wetgeving vereist,[18] maar dat wel een bepaalde mate van concreetheid en voorzienbaarheid vereist is.[19] Er moet een voldoende precieze wettelijke grondslag zijn zodat de burger kan begrijpen welke gegevens in verband met een overheidstaak kunnen worden verwerkt. Een algemene taakstelling kan volgens de AP daarom '*niet in alle gevallen [..] dienen als rechtsgrond voor gegevensverwerking*'.[20] Artikel 160 Gemeentewet, op grond waarvan het college bevoegd is om het dagelijks bestuur van de gemeente te voeren, is volgens de AP onvoldoende concreet waardoor de verwerking in verband met wifitracking niet voorzienbaar is. De overige artikelen uit de Gemeentewet waar het college naar verwijst, scheppen geen bevoegdheden voor het college maar voor andere organen binnen de gemeente en kunnen dus geen grondslag bieden voor de verwerkingsverantwoordelijke in deze kwestie: het college. De APV van Enschede bevat geen bepalingen waaruit de burger kan afleiden dat zijn persoonsgegevens voor wifitracking worden verwerkt en de overige regelingen waarop het college zich op beroept, zijn geen wettelijke voorschriften, oordeelt de AP.

'*Ten overvloede*' overweegt de AP dat ook niet is voldaan aan het noodzakelijkheidsvereiste. Dit vereiste maakt onderdeel uit van onder andere de grondslag genoemd in sub e en valt uiteen in de beginselen van proportionaliteit en subsidiariteit.

De verwerking is volgens de AP niet proportioneel omdat de inbreuk op de privacy van honderdduizenden burgers onevenredig is in verhouding tot het doel: het meten van de effectiviteit van investeringen. Ook wordt afbreuk gedaan aan het gevoel en de redelijke verwachtingen van het publiek om zich in het openbaar onbespied te wanen en vertrouwen te hebben in de overheid.

De verwerking voldoet ook niet aan het subsidiariteitvereiste, omdat het doel van het college ook op een minder vergaande wijze kon worden bereikt. Naar eigen zeggen wilde het college uitsluitend meten en was het volgen van burgers niet de bedoeling. Het vastleggen en bewaren van de gegevens was daarom niet nodig en bovenmatig. De AP noemt zelfs een aantal methodes om drukte en bezoekersaantallen te meten waarbij in het geheel geen persoonsgegevens worden verwerkt.[21] Ook daarom kan geen beroep gedaan worden op de grondslag genoemd in sub e.

Tot slot overweegt de AP dat het college geen beroep kan doen op de grondslag genoemd in sub f (gerechtvaardigd belang). Uit de laatste zin van artikel 6 lid 1 AVG volgt dat op deze grondslag geen beroep kan worden gedaan als het gaat om de verwerking van gegevens in de uitoefening van overheidstaken. Overheidsorganen kunnen slechts voor 'typisch bedrijfsmatige handelingen', zoals de beveiliging van overheidsgebouwen, een beroep doen op deze grondslag. In dit geval was duidelijk dat de wifitracking, ook naar de eigen stellingen van het college, samenhing met haar publieke taak. Daarom is een beroep op deze grondslag uitgesloten.

4. Boete

De AP legt het college een boete op van € 600.000,- wegens het verwerken van persoonsgegevens zonder geldige grondslag. Zij past daarbij haar boetebeleidsregels toe. De basisboete voor een overtreding als de onderhavige is € 525.000,-. De AP verhoogt dit basisbedrag met € 75.000,- onder meer omdat:
– het geschonden rechtmatigheidsbeginsel de kern raakt van het recht op eerbiediging van de persoonlijke levenssfeer en de bescherming van persoonsgegevens;
– de schending afbreuk doet aan het gevoel van de burger zich in het openbaar onbespied te wanen en aan het vertrouwen in de overheid;
– het honderdduizenden burgers betrof;
– de verwerking structureel was en gedurende een langere periode (ca. twee jaar) plaatsvond; en
– de verzamelde data een gedetailleerd beeld kon scheppen van een betrokkene.

De AP acht het bovendien verwijtbaar dat het college geen nader onderzoek heeft gedaan naar de verwerking of juridisch advies heeft ingewonnen, maar in plaats daarvan vertrouwde op een leverancier die een commercieel belang had. Dat het college niet de bedoeling had om persoonsgegevens te verwerken door burgers te volgen en '*gestuurd heeft*' op het waarborgen van privacy, is volgens de AP geen boeteverlagende omstandigheid nu van een overheidsinstantie verwacht mag worden dat zij zich van de geldende normen vergewist en deze naleeft.

18. De AP verwijst hierbij naar overweging 45 AVG.
19. De AP verwijst hierbij naar overweging 41 AVG en naar artikel 8 EVRM.
20. De AP verwijst hierbij naar HR 24 februari 2017, ECLI:NL:HR:2017:288 (Belastingdienst ANPR zaak).
21. Zie pagina 25, tweede alinea van het boetebesluit.

5. Wat betekent dit?

De beslissing van de AP is principieel: verwerkingen door overheden moeten gebaseerd zijn op een voldoende concrete wettelijke bepaling waaruit de burger kan opmaken dat zijn gegevens worden verwerkt. Dat is in lijn met artikel 8 EVRM en bijvoorbeeld het ANPR-arrest van de Hoge Raad.[22] Op grond van artikel 8 EVRM moet een inmenging in het privéleven zijn voorzien bij wet, hetgeen wil zeggen dat die moet berusten op een wettelijk voorschrift waaruit de burger met voldoende precisie kan opmaken welke gegevens voor de vervulling van een overheidstaak worden verwerkt. In de ANPR zaak oordeelde de Hoge Raad dat verschillende belastingwetten geen '*voldoende precieze wettelijke grondslag voor het verzamelen, vastleggen, bewaren, bewerken en gebruiken*' van door snelwegcamera's vastgelegde gegevens voor belastingdoeleinden bieden.[23]

Overigens laat andere Nederlandse jurisprudentie soms een ander beeld zien door zeer algemene bepalingen als voldoende duidelijke en voorzienbare wettelijke grondslag te beschouwen.[24] Mijns inziens heeft de AP het, in dit geval, bij het juiste eind.
Overigens denk ik dat de boete ook op andere gronden had kunnen worden gebaseerd, nu voorbijgangers onbedoeld en onnodig gevolgd werden. Het gebruik van wifitracking was onnodig en bovenmatig en dus in strijd met het beginsel van minimale gegevensverwerking (art. 5 lid 1 sub c AVG). Dat de gegevens herleidbaar waren, is (zoals de AP ook overweegt) het gevolg van een onjuiste ontwerpbeslissing. Daarmee heeft het college ook gehandeld in strijd met het vereiste van privacy-by-design (art. 25 lid 1 AVG), wat inhoudt dat privacy in het ontwerp van een verwerking meegenomen moet worden. Dat de gegevens onnodig werden bewaard in herleidbare vorm, resulteert bovendien in schending van het beginsel van opslagbeperking (art. 5 lid 1 sub e AVG).

Het college heeft bezwaar ingesteld tegen de beslissing, waarop vermoedelijk beroep zal volgen. Om bovengenoemde redenen verwacht ik niet dat de uitkomst daarvan heel anders zal zijn.

22. HR 24 februari 2017, ECLI:NL:HR:2017:288 (Belastingdienst ANPR)
23. HR Belastingdienst ANPR, r.o. 2.3.5.
24. Zie bijvoorbeeld CRvB 5 februari 2018, ECLI:NL:CRVB:2018:269 (DUO gebruik OV-reisgegevens) en rechtbank Amsterdam 11 juni 2020, ECLI:NL:RBAMS:2020:2917 (UvA online surveillancesoftware). De vraag of de UvA online surveillance software inzette in het kader van een voldoende specifiek omschreven publieke taak maakte geen onderdeel uit van het hoger beroep in die zaak, zie Hof Amsterdam 1 juni 2021, ECLI:NL:GHAMS:2021:1560 (Hoger beroep UvA online surveillancesoftware), r.o. 3.3.2.