PELS RIJCKEN

Advies

voor	Centraal Bureau voor de Statistiek
van	Gerrit-Jan Zwenne & Lars Groeneveld
datum	31 januari 2020
inzake	Advies Telecommunicatiewet
zaaknr	11012720

1 Inleiding

1.1 Het Centraal Bureau voor de Statistiek (hierna: CBS) onderzoekt de mogelijkheid om verkeersgegevens van telecomaanbieder(s) (hierna: Telco(s)), te gebruiken voor statistisch onderzoek. Daarbij zijn enkele vragen gerezen ten aanzien van de rechtmatigheid van dat onderzoek onder de Telecommunicatiewet (of Tw). De vragen van CBS luiden (geparafraseerd) als volgt:

> *1) Voldoet het door CBS voorgestane onderzoek aan de Telecommunicatiewet? Zo ja, waarom? Zo nee, welke aanpassing in het onderzoek of regelgeving zijn nodig om het onderzoek in lijn te brengen met deze wet.*
>
> *2) Welke (juridische) aanbevelingen kunnen wij aan het Agentschap Telecom of de wetgever doen ten aanzien van dit terrein van onderzoek?*

1.2 Voor de beantwoording van deze vragen wordt eerst een analyse gegeven van de onderzoeksmethoden die op Europees niveau zijn ontwikkeld, en wordt een procesbeschrijving gegeven van het statistisch onderzoek dat CBS beoogd uit te voeren (par. 2). Daarna wordt ingegaan op de eisen die de artikel 11.5 Tw aan de verwerking van verkeersgegevens stelt, daarbij wordt ook ingegaan op het anonimiseren van verkeer- en locatiegegevens (par. 3). Dit advies wordt afgesloten met een conclusie (par. 4).

2 Onderzoeksmethodiek en verwerkingsinfrastructuur

2.1 Op Europees niveau zijn verschillende methoden ontwikkeld om verkeersgegevens in overeenstemming met de Algemene Verordening Gegevensbescherming (hierna: AVG) en de Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie

(hierna: e-Privacy richtlijn), te verwerken. In het onderstaande zal eerst ingegaan worden op methoden die door bekende buitenlandse partijen zijn ontwikkeld. Vervolgens wordt de door CBS voorgestane onderzoeksmethode en verwerkingsinfrastructuur beschreven.

Europese context

2.2 Op Europees niveau wordt de mogelijkheid om verkeersgegevens te gebruiken voor statistisch onderzoek door meerdere partijen onderzocht, en zijn verschillende onderzoeksmethoden ontwikkeld.

2.3 Voor zover wij uit openbare en niet-openbare bronnen hebben kunnen nagaan, is het gemeenschappelijk uitgangspunt van de ontwikkelde onderzoeksmethoden dat gegevens in geanonimiseerde vorm worden aangeleverd door de betreffende Telco. Uit de verschillende onderzoekmethoden die wij hebben bestudeerd, wordt niet duidelijk hoe de anonimisering van de aangeleverde gegevens is vormgegeven. Ook is niet duidelijk of de gegevens geanonimiseerd zijn volgens de eisen die de AVG daaraan stelt (zie verder randr. 3.17).

2.4 Als voorbeeld kan een onderzoekmethode dienen die wordt gehanteerd door een bekend statistisch onderzoeksbureau in Europa. Bij deze onderzoeksmethode wordt door de betreffende Telco een versleutelde gegevensset aangeleverd, welke vervolgens door een statistisch onderzoeksbureau wordt verwerkt tot statistische informatie. De gegevensset wordt in dit model geacht geanonimiseerd te zijn door de versleuteling die daarop is toegepast. Nadere technische specificatie van deze versleuteling ontbreekt in de door ons geraadpleegde bronnen.

2.5 Ook andere technische maatregelen worden toegepast om de-anonimisering van de versleutelde gegevensset te voorkomen. Zo wordt de niet geanonimiseerde gegevensset, die is opgeslagen bij de betreffende Telco, ontoegankelijk gemaakt voor derde partijen. Ook hierbij ontbreekt nadere technische specificatie in de door ons geraadpleegde bronnen.

2.6 Naast technische maatregelen om de aangeleverde gegevensset te anonimiseren en de oorspronkelijke gegevens ontoegankelijk te maken, zijn ook organisatorische maatregelen genomen. Zo worden de methoden en de algoritmes die bij het statistisch onderzoek worden gehanteerd door het statistisch onderzoeksbureau, de betreffende Telco, en de nationale privacytoezichthouder gevalideerd en goedgekeurd.

2.7 Daarbij hebben de betreffende Telco en nationale privacytoezichthouder de mogelijkheid om te controleren of de verkeersgegevens exact volgens de vooraf goedgekeurde methode zijn verwerkt, en dat door het statistisch onderzoeksbureau geen persoonsgegevens zijn verkregen.

Tussenconclusie

2.8 Gelet op het bovenstaande wordt in Europese context een combinatie van technische en organistische maatregelen gehanteerd om te waarborgen dat enkel gebruik wordt gemaakt van geanonimiseerde gegevens voor de aggregatie van statistische informatie.

2.9 Het is evenwel (nog) niet volledig duidelijk in hoeverre deze maatregelen beantwoorden aan de vereisten die de AVG stelt aan het anonimiseren van gegevens (zie daarover randnr. 3.17 e.v.).

Methode CBS

2.10 In het door het CBS voorgestane onderzoek zijn een aantal stappen te onderscheiden. Hieronder worden deze stappen toegelicht.

2.11 Het proces begint bij het verwerken en opslaan van verkeersgegevens met betrekking tot abonnees en gebruikers van de communicatiediensten van de betreffende Telco Zodra deze verkeersgegevens niet langer nodig zijn ten behoeve van de overbrenging van de communicatie, worden zij versleuteld en voorzien van een identificatienummer.

2.12 De versleuteling van de verzamelde verkeersgegevens zorgt ervoor dat alle direct tot de abonnee of gebruiker herleidbare informatie ontoegankelijk wordt gemaakt. Elke 30 dagen versleutelt de Telco de verkeersgegevens opnieuw. De sleutels worden bij deze tweede versleutelingsstap direct vernietigd. Het CBS heeft enkel toegang tot de sleutels die de tweede versleutelingsstap hebben doorgemaakt. Na zes maanden worden de versleutelde gegevens door de Telco definitief verwijderd.

2.13 Na de versleuteling worden de verkeersgegevens aan CBS ter beschikking gesteld voor het uitvoeren van hun statistisch onderzoek. Het CBS voert zijn werkzaamheden uit bij de betreffende Telco. Gedurende hun werkzaamheden hebben CBS-medewerkers geen toegang tot de niet-versleutelde verkeergegevens. Ook hebben zij ten behoeve van hun werkzaamheden bij de betreffende Telco een geheimhoudingsverklaring ondertekend.

2.14 Bij het onderzoek dat CBS uitvoert is gewaarborgd dat de verwerking van de geanonimiseerde verkeersgegevens niet ertoe leidt dat de versleutelde gegevens herleidbaar worden tot een specifieke, geidentificeerde of identificeerbare abonnee of gebruiker.

2.15 Zo zorgt het geautomatiseerde proces er onder meer voor dat locatiebepaling van specifieke toestellen is uitgesloten. Daarvoor wordt gebruik gemaakt van randomisatietechnieken. Verkeersgegevens afkomstig uit een gespecificeerd gebied worden *at random* herverdeeld.

2.16 Door het toepassen randomisatie blijft de gegevensset geanonimiseerd en kan ook de locatie van de gebruikte (mobiele) toestellen niet worden bepaald. Voor zover het

bepalen van de locatie nodig is voor het statistisch onderzoek van CBS, wordt deze geschat aan de hand van een Bayesiaanse analyse. De gegevensset wordt vervolgens ingedikt door een selectie te maken van de gegevens uit een te bepalen gebied en tijdsperiode. Bij een output waarbij minder dan 15 *devices* zijn betrokken vindt een correctie plaats door de betreffende Telco waarbij het aantal devices worden opgehoogd.

Tussenconclusie

2.17 Uit het bovenstaande volgt dat het CBS, in lijn met Europese ontwikkelingen, door de Telco geanonimiseerde gegevens als uitgangspunt neemt voor zijn onderzoek.

3 Verwerking van verkeersgegevens onder de Telecommunicatiewet

3.1 Het juridisch kader voor de verwerking van verkeersgegevens wordt in belangrijke mate gevormd door de Tw en de AVG. Hieronder wordt het bovenstaande proces aan beide regelingen getoetst.

Anonimiseren

3.2 Voor de toepassing van de Telecommunicatiewet in het onderhavige geval is allereerst de definitie van verkeersgegevens van belang. In artikel 11.1, onderdeel b, Tw worden verkeersgegevens als volgt gedefinieerd:

> *verkeersgegevens: gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan;*

3.3 Hieronder vallen bijvoorbeeld het oproepende en opgeroepen telefoonnummer, de duur van de oproep, en bij mobiele telefonie ook de locatiegegevens van de oproep.

3.4 Voor zover deze informatie kan worden gerelateerd aan geïdentificeerde of identificeerbare abonnees van de betreffende Telco is daarbij sprake van persoonsgegevens als bedoeld in artikel 4, onderdeel 1, AVG. In het onderhavige geval kwalificeren de door de betreffende Telco versleutelde gegevens als verkeersgegevens.

3.5 In artikel 11.1, onderdeel c, Tw wordt de verwerking van de bovengenoemde verkeersgegevens gedefinieerd. Daarbij wordt verwezen naar het begrip ‘verwerking’ zoals dat in de AVG wordt gehanteerd.

> *verwerking van verkeersgegevens: verwerking als bedoeld in artikel 4, onderdeel 2, van de Algemene verordening gegevensbescherming, met dien verstande dat de desbetreffende handelingen mede betrekking hebben op verkeersgegevens van abonnees die geen natuurlijke personen zijn;*
>
> Zie artikel 11.1, onderdeel c, Tw.

En:

„verwerking": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

Zie artikel 4, onderdeel 2, AVG.

3.6 De definitie van 'verwerking van persoonsgegevens' in artikel 11.1, onderdeel c, Tw verwijst naar de AVG om de aansluiting met de AVG zoveel mogelijk te behouden.

3.7 In het onderhavige geval worden de verkeersgegevens door een Telco verwerkt zoals bedoeld in artikel 11.1, onderdeel c, Tw. Dit betekent dat ook aan de vereisten van artikel 11.5 Tw moet worden voldaan. Dit omdat, in artikel 11.5 Tw de verwerking van verkeersgegevens door de aanbieder van openbare elektronische communicatienetwerken of –diensten (Telco's) wordt geregeld.

3.8 De hoofdregel uit artikel 11.5, eerste lid, Tw bepaalt dat Telco's, de verwerkte en opgeslagen verkeersgegevens moeten verwijderen dan wel moeten anonimiseren, zodra deze niet meer nodig zijn voor het overbrengen van de communicatie.

Artikel 11.5, eerste lid, Tw

De aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst <u>verwijderen dan wel anonimiseren</u> de door hen verwerkte en opgeslagen verkeersgegevens met betrekking tot abonnees of gebruikers, zodra deze verkeersgegevens niet langer nodig zijn ten behoeve van de overbrenging van communicatie, onverminderd het tweede, derde en vijfde lid.
(onderstreping toegevoegd)

3.9 Het moment waarop de Telco over moet gaan tot verwijdering dan wel anonimisering is in beginsel het moment dat de verkeersgegevens niet meer nodig zijn voor het overbrengen van de communicatie. Veelal is dat het moment waarop één van de gebruikers een gesprek heeft beëindigd, althans wanneer de gegevens niet meer nodig zijn voor factureringsdoeleinden (art. 11.5, tweede lid, Tw)

Zie Zwenne, in: *T&C privacy- en telecommunicatierecht* 2018, art. 11.5 Tw, aant. 2 en 3

3.10 Het verwijderen of anonimiseren van de verkeersgegevens heeft tot gevolg dat de AVG niet meer van toepassing is. Uit artikel 2 AVG jo. artikel 4, onderdeel 1, AVG blijkt dat de toepassing van de AVG zich niet uitstrekt over anonieme gegevens. Zoveel blijkt ook uit overweging 26 bij de AVG.

> *De gegevensbeschermingsbeginselen dienen derhalve niet van toepassing te zijn op anonieme gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is. Deze verordening heeft derhalve geen betrekking op de verwerking van dergelijke anonieme gegevens, onder meer voor statistische of onderzoeksdoeleinden.*
> (onderstreping toegevoegd)

3.11 Een vereiste is daarbij wel dat de verkeersgegevens zijn geanonimiseerd. Slechts als sprake is van voldoende geanonimiseerde gegevens mist de AVG toepassing.

3.12 In de AVG ontbreekt een duidelijke definitie van anonimiseren of anonieme gegevens. Wel blijkt uit overweging 26 AVG dat, om te bepalen of een natuurlijke persoon identificeerbaar is, rekening moet worden gehouden met 'alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren'.

> *Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken. Om uit te maken of van middelen redelijkerwijs valt te verwachten dat zij zullen worden gebruikt om de natuurlijke persoon te identificeren, moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen.*
>
> Zie overweging 26 AVG.

3.13 Uit de memorie van toelichting bij de Telecommunicatiewet blijkt dat sprake is van anonieme gegevens als bedoeld in artikel 11.5, eerste lid, Tw, wanneer gegevens zodanig worden bewerkt dat deze redelijkerwijs niet meer zijn te herleiden tot individuele natuurlijke personen. Met andere woorden: de betreffende gegevens dienen volledig en op onomkeerbare wijze te worden ontdaan van hun persoonsidentificerende kenmerken.

Zie *Kamerstukken II* 2002/03, 28851, 3, p. 154.

3.14 Bij de uitleg van artikel 11.5, eerste lid, Tw moet aangesloten worden bij de begrippen zoals deze worden gehanteerd in de AVG. Dit omdat, artikel 11.5 Tw een implementatie vormt van artikel 6 e-Privacyrichtlijn. En in de e-Privacyrichtlijn wordt voor de uitleg van de daarin gehanteerde begrippen, in artikel 2 e-Privacyrichtlijn, verwezen naar Richtlijn 95/46/EG, welke is opgeheven en vervangen is door de AVG. Voor zover relevant luidt artikel 2 e-Privacyrichtlijn al volgt:

> Artikel 2
> *Definities*
>
> *Tenzij anders is bepaald, zijn de definities van Richtlijn 95/46/EG van het Europees Parlement en de Raad en Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten (kaderrichtlijn)(8) van toepassing.*

3.15 Gelet op het bovenstaande is voor de uitleg van het begrip anonimiseren of anonieme gegevens de AVG leidend, ook wanneer dergelijke begrippen in context van de Telecommunicatiewet worden gehanteerd.

3.16 Privacytoezichthouders hebben op verschillende wijze invulling geven aan deze begrippen. Hieronder volgt een korte uiteenzetting van de opvattingen over anonimiseren en anonieme gegevens van de Europese Article 29 Working Party (hierna: WP29; nu European Data Protection Board (EDPB)), AP, en de Information Commissioner's Office (hierna: ICO)

WP29 en anonieme gegevens

3.17 WP29 heeft zich over het anonimiseren van gegevens voor het laatst uitgelaten in zijn advies over anonimiseringstechnieken uit 2014.

> Zie WP29, Advies 5/2014 over anonimiseringstechnieken, WP216, Goedgekeurd op 10 april 2014.

3.18 Volgens WP29 is van anonimiseren sprake zodra elke mogelijkheid tot identificatie van betrokkenen onherroepelijk wordt uitgesloten. Daarbij moet volgens WP29 rekening gehouden worden met diverse factoren, en moet worden gekeken naar 'alle middelen waarvan mag worden aangenomen dat zij 'redelijkerwijs' door de verwerkingsverantwoordelijke – dan wel door enige andere derde – in te zetten zijn om een persoon te identificeren'. Daarbij hanteert WP29 de onderstaande drie criteria om de deugdelijkheid van een anonimiseringstechniek te toetsen:

(i) de herleidbaarheid, dat wil zeggen de mogelijkheid om een persoon te individualiseren;

(ii) de koppelbaarheid, dat wil zeggen de mogelijkheid om records in verband te brengen met een persoon, en;

(iii) de deduceerbaarheid, dat wil zeggen de mogelijkheid om persoonsgebonden informatie af te leiden.

Zie WP29, Advies 5/2014 over anonimiseringstechnieken, WP216, Goedgekeurd op 10 april 2014, p. 3.

3.19 Een door de WP29 geaccepteerde anonimiseringstechniek moet op alle drie de bovenstaande onderdelen hoog scoren. Door WP29 wordt slechts een zeer laag risico op re-identificatie geaccepteerd. In het advies noemt WP29 enkele anonimiseringstechnieken die op adequate wijze persoonsgegevens kunnen anonimiseren. Zo stelt WP29 over ruistoevoeging dat:

Wordt deze techniek op doeltreffende wijze toegepast, dan is het voor een derde niet mogelijk om een persoon te identificeren, noch om de oorspronkelijke gegevens terug te rekenen of te achterhalen hoe de gegevens werden gewijzigd.

Zie WP29, Advies 5/2014 over anonimiseringstechnieken, WP216, Goedgekeurd op 10 april 2014, p. 14.

3.20 Het versleutelen van gegevens acht WP29 in datzelfde advies geen toereikende anonimiseringstechniek. Echter, in combinatie met andere privacywaarborgen kan het versleutelen van gegevens wel leiden tot anonieme gegevens. WP29 merkt daarover het volgende op:

De dataset kan alleen als anoniem worden beschouwd wanneer extra stappen worden ondernomen, bijvoorbeeld attributen wegnemen en generaliseren, de oorspronkelijke gegevens verwijderen of op zijn minst samenvoegen tot op een hoog aggregatieniveau.

Zie WP29, Advies 5/2014 over anonimiseringstechnieken, WP216, Goedgekeurd op 10 april 2014, p. 25.

3.21 In het onderhavige geval zijn bij de versleuteling van de verkeersgegevens door de betreffende Telco extra stappen ondernomen, waaronder het wegnemen van attributen en het herhaaldelijk versleutelen, waarbij de sleutel wordt verwijderd.

3.22 Daarbij verdiend opmerking dat in de literatuur kritiek wordt geuit op de rigide benadering van WP29. De huidige informatiemaatschappij is gebaat bij het volgen van een *risk-based approach* met betrekking tot anonimiseren.

> Zie R.P. Santifort, 'Naar een meer genuanceerde benadering van 'pseudonimisering' in het privacyrecht', P&I 2019/187, afl. 5.

AP en anonieme gegevens

3.23 AP volgt de lijn van WP29. In meerdere adviezen wordt bij de bespreking van 'geanonimiseerde gegevens' verwezen naar het advies over anonimiseringstechnieken van WP29 en de daarin gehanteerde definitie van anonimiseren.

> Zie onder meer AP, Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace, Rapport definitieve bevindingen, 13 oktober 2015.

ICO en anonieme gegevens

3.24 De ICO volgt de lijn van WP29 niet. In het rapport *Anonymisation: managing data protection risk code of practice* heeft de ICO meerdere technieken aangewezen die volgens hem verkeersgegevens kunnen anonimiseren. Volgens de ICO kunnen encryptie, tokenisation, en randomisatie bijdragen aan het anonimiseren van verkeersgegevens.

> Zie ICO, *Anonymisation: managing data protection risk code of practice* p. 67.

Locatiegegevens, verkeersgegevens en anonieme gegevens

3.25 Zoals opgemerkt in randr. 3.12 is slechts sprake van geanonimseerde gegevens wanneer rekenschap is gegeven van 'alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren'. Met andere woorden: elke mogelijkheid tot identificatie van betrokkenen moet onherroepelijk zijn uitgesloten.

3.26 Ten aanzien van locatiegegevens is het notoir ingewikkeld om elke mogelijkheid tot identificatie onherroepelijk uit te sluiten. Hieronder zal worden ingegaan op de mogelijkheid tot het anonimiseren locatiegegevens.

3.27 Locatiegegevens worden op verschillende wijze gedefinieerd. In artikel 11.1 onderdeel d Tw is het begrip locatiegegevens als volgt gedefinieerd:

> Artikel 11.1, onderdeel d Tw
>
> *locatiegegevens: gegevens die worden verwerkt in een openbaar elektronisch communicatienetwerk of een openbare elektronische communicatiedienst*

waarmee de geografische positie van de randapparatuur van een gebruiker van een openbare elektronische communicatiedienst wordt aangegeven;

3.28 Vanwege de ruime uitleg van het begrip verkeersgegevens (zie randr. 3.2) bestaat een overlap tussen het begrip verkeersgegevens en het begrip locatiegegevens. Met als gevolg dat in sommige gevallen locatiegegevens tevens aangemerkt kunnen worden als verkeersgegevens, zoals bedoeld in art. 11. onderdeel b Tw.

3.29 Gegevens waarbij sprake is van de bovenstaande overlap zijn bijvoorbeeld gegevens betreffende basisstations waarmee mobiele apparaten in contact staan, en die noodzakelijk zijn voor het mogelijk maken van mobiele communicatie. Deze gegevens, zoals *Cell ID* gegevens, kunnen zowel als locatiegegevens als verkeersgegevens worden aangemerkt.

3.30 In het geval een gegevensset valt onder het begrip verkeersgegevens en het begrip locatiegegevens, is de regeling voor verkeersgegevens leidend (zie daarover randnr. 3.14 e.v.).

Zie ook Zwenne, in: *T&C privacy- en telecommunicatierecht* 2018, art. 11.5a Tw, aant. 1.

Voor locatiegegevens die niet tegelijkertijd als verkeersgegevens kunnen worden aangemerkt is een aparte regeling opgenomen in artikel 11.5a Tw. Hierin is onder meer bepaald dat locatiegegevens slechts met toestemming van de betrokkene mogen worden verwerkt. Voor zover wij hebben kunnen nagaan wordt voor de beoogde verwerking van verkeersgegevens door CBS geen gebruik gemaakt van locatiegegevens zoals bedoeld in artikel 11.5a Tw.

3.31 In het advies van WP29 over anonimiseringstechnieken worden locatiegegevens aangemerkt als een categorie van gegevens die zelden anoniem kunnen worden gemaakt. WP29 maakt duidelijk dat alleen het verwijderen van de identiteiten van de betrokkenen, en het versleutelen van de gegevensattributen niet voldoende is om locatiegegevens te anonimiseren. Dit omdat, mobiliteitspatronen van mensen uniek zijn waardoor zelfs zonder gegevensattributen uiteenlopende kenmerken van een betrokkene kunnen worden afgeleid uit de betreffende gegevens.

Zie WP29, Advies 5/2014 over anonimiseringstechnieken, WP216, Goedgekeurd op 10 april 2014, p. 36; Zie ook Brengston e.a., Approaching the Limit of Predictability in Human Mobility, *Science Reports* vol.3, article nr. 22923.

3.32 Als gevolg daarvan is voorzichtigheid geboden bij het gebruik van pseudonimiseringstechnieken voor locatiegegevens. WP29 merkt daarover het volgende op:

> *Wanneer pseudonimisering erin bestaat een identiteit te vervangen door een andere unieke code, is het naïef te veronderstellen dat de informatie daarmee op afdoende wijze niet identificeerbaar is gemaakt. Daardoor wordt immers voorbijgegaan aan de complexiteit van identificatiemethoden en de veelsoortige contexten waarin die toepassing vinden.*
>
> Zie WP29, Advies 5/2014 over anonimiseringstechnieken, WP216, Goedgekeurd op 10 april 2014, p. 36.

3.33 De bovenstaande moeilijkheid die bestaat bij het verwerken van locatiegegevens is door sommige nationale wetgevers opgelost. In Frankrijk worden locatiestatistieken anoniem gemaakt door generalisatie en permutatie methodieken. Echter, het gaat hier om vergaande generalisatie waardoor de bruikbaarheid van de gegevens wordt beperkt. Het Franse bureau voor de statistiek (INSEE) publiceert statistieken die worden gegeneraliseerd door alle gegevens samen te voegen in een gebied dat 40 000 m² bestrijkt. Daarbij voorkomen permutatietechnieken dat de gegevensset alsnog wordt gede-anonimiseerd

3.34 WP29 acht de aanpak van het INSEE voldoende om te spreken van geanonimiseerde locatiegegevens. Daarbij wordt door de toezichthouder opgemerkt dat voorafgaand aan het verwerken van de locatiegegevens gebruik kan worden gemaakt van technische hulpmiddelen om vast te stellen in hoeverre attributen moeten worden gegeneraliseerd.

> Zie WP29, Advies 5/2014 over anonimiseringstechnieken, WP216, Goedgekeurd op 10 april 2014, p. 36.

Tussenconclusie

3.35 Gelet op het voorgaande, kan worden beargumenteerd dat het statistisch onderzoek van CBS, voor zover de bovenstaande procesbeschrijving wordt gevolgd, voldoet aan de vigerende opvattingen over deugdelijke anonimiseringstechnieken.

3.36 Door de gelaagde toepassing van versleutelingen en randomisatie zijn de verkeersgegevens die door CBS worden gebruikt voor het statistisch onderzoek in voldoende mate geanonimiseerd. Met als gevolg dat de AVG niet van toepassing is op de verwerking van de verkeersgegevens in het kader van het statistisch onderzoek.

4 Conclusie

4.1 Gelet op het bovenstaande voldoet de door CBS beoogde onderzoeksmethode aan de eisen die artikel 11.5 Tw daaraan stelt.