Universiteit Gent - Faculteit Rechtsgeleerdheid - Universiteit Gent

Ref.: T.F.R. 513 , 1ste januari 2017, blz. [3]

Vrij Gesteld
In "Vrij Gesteld" geeft een lid van de redactie of een gastauteur zijn eigen mening, kritiek of commentaar op een fiscaal item dat hem of haar is opgevallen. Er is ook ruimte voor reactie hierop.
108.
Geolokalisatie en privacy

In TFR nr. 512 wees Frank Mortier ons in een boeiende "Vrij Gesteld" op het nut van geolokalisatiegegevens voor de fiscale administratie. Er blijkt sinds de laatste 30 jaren inderdaad een spectaculaire toename te zijn van het gebruik van lokalisatiegegevens [1] . De oorzaak is uiteraard de toename in de creatie van lokalisatiegegevens door enerzijds het wijdverspreide gebruik van mobiele telefonie waardoor de gebruiker potentieel constant kan worden gelokaliseerd alsook door de technologische ontwikkelingen inzake lokalisatie via satelliet. De commerciële diensten die rond het gebruik van deze informatie worden ontwikkeld blijken zich in een eerste fase vooral te hebben gericht tot de "lokaliseerbare" persoon zelf (bv. GPS-navigatie), maar er is daarnaast een duidelijk toename aan de gang van commerciële diensten die worden aangeboden aan derden rond het lokaliseren van bijvoorbeeld werknemers, hetzij direct, hetzij indirect via bijvoorbeeld het voertuig waarin zij zich verplaatsen. Frank Mortier verwijst in zijn "Vrij Gesteld" ook naar dit type van lokalisatiediensten. Het gebruik van deze lokalisatiegegevens voor het opsporen van fraude door de overheid, waaronder de fiscale overheid, lijkt op het eerste gezicht veel opportuniteiten te kennen, al rijzen er bij de toegang tot deze gegevens door de fiscale administratie ook evenveel vragen en moeilijkheden.

De moeilijkheden vanuit het oogpunt van het recht op privéleven worden daarbij in de "Vrij Gesteld" nr. 512 wellicht enigszins onderschat. Zo lijkt het probleem van de beperkte *bewaartermijn*, dat door Frank Mortier enkel werd aangehaald in het kader van de verplichtingen van telecomoperatoren om op grond van de telecomwet gegevens te bewaren voor hoofdzakelijk strafrechtelijk onderzoek, van aard te zijn dat heel veel lokalisatiegegevens onbruikbaar zijn voor controle van het fiscale inwonerschap, van de 183-dagen-regel, van het bestaan van vaste inrichting en van de feitelijke woonplaats, waarnaar in de "Vrij Gesteld" nr. 512 wordt verwezen. Bij de controle van deze elementen is het juist relevant te weten of de belastingplichtige de locatie gedurende een zekere periode heeft aangehouden.

Eenieder die lokalisatiegegevens verzamelt, zal immers verplicht zijn het persoonsgegevensbeschermingsrecht na te leven [2] . Een basisprincipe in dit persoonsgegevensbeschermingsrecht is het principe dat persoonsgegevens, en dus ook lokalisatiegegevens in de mate dat ze toelaten de natuurlijke persoon waarop ze slaan te identificeren, niet langer mogen worden bewaard dan nodig voor de doeleinden waarvoor ze zijn verzameld. Een telecomoperator zal lokalisatiegegevens dus niet langer mogen bewaren dan nodig voor de realisatie van de diensten die met deze lokalisatiegegevens worden verstrekt [3] . De telecomoperator zal dan overigens ook over de toestemming van de betrokkene moet beschikken [4] . De Belgische telecomwet maakt hierop een uitzondering en verplicht de telecomoperatoren om bepaalde gegevens, waaronder de lokalisatiegegevens,

toch te bewaren tot 12 maanden na de communicatie [5] , doch dit enkel ten behoeve van welbepaalde overheden waarvan de gerechtelijke overheden, de veiligheids- en inlichtingendiensten en de hulpdiensten wellicht de belangrijkste zijn [6] . De fiscale administratie behoort hier niet toe. Wanneer de fiscus dus lokalisatiegegevens zou opvragen aan een telecomoperator, in de mate dat dit al kan (zie *infra*), zal hij het dus moeten stellen met lokalisatiegegevens die zich over een zeer beperkte periode uitstrekken. Hetzelfde geldt voor de bedrijven die diensten aanbieden waarbij gebruik wordt gemaakt van deze door de telecomoperator verschafte lokalisatiegegevens. Dit zal het geval zijn voor bedrijven die ten behoeve van bijvoorbeeld de werkgever de verzamelde lokalisatiegegevens omzet in voor de werkgever bruikbare informatie. Maar dit is ook het geval voor bedrijven die aan de betrokkene zelf diensten aanbieden waarbij gebruik wordt gemaakt van hun locatie (bv. apps die toelaten om een restaurant in de buurt te zoeken). Ook deze bedrijven mogen de lokalisatiegegevens niet langer bijhouden dan nodig voor het verstrekken van deze diensten, of voor het factureren ervan [7] . Ten slotte zal ook de afnemer van de lokalisatiediensten dezelfde regel inzake bewaartermijn moeten respecteren. Inzake het verzamelen van lokalisatiegegevens door de werkgever met het oog op een welbepaalde controle van de werknemers, wordt aanbevolen deze gegevens slechts voor een beperkte periode van 2 maanden te bewaren [8] . Op deze wijze leveren de lokalisatiegegevens voor de fiscale administratie weinig nuttige informatie op.

De principes inzake bewaartermijn zijn van toepassing op eenieder die persoonsgegevens (en dus ook lokalisatiegegevens) verwerkt in het kader van activiteiten van een vestiging op het grondgebied van een lidstaat zelf [9] . De bedrijven die lokalisatiediensten aanbieden waarbij gebruik wordt gemaakt van de "ruwe" lokalisatiegegevens die door de telecomoperator worden verzameld, zijn wel eens gevestigd buiten de Unie, wellicht dan vooral in de VS (Apple, Uber, …). De principes van het persoonsgegevensbeschermingsrecht (op dit moment nog de richtlijn nr. 95/46) zijn niet op deze bedrijven van toepassing. Evenwel zal in dat geval de telecomoperator die het ruwe lokalisatiemateriaal heeft verzameld en die doorgaans wel in de Unie zal zijn gevestigd, rekening houdende met de richtlijn nr. 95/46, deze gegevens slechts kunnen doorgeven aan een staat buiten de Europese Unie indien deze staat een zogenaamd "passend beschermingsniveau" waarborgt [10] . Dit betekent evenwel niet noodzakelijk dat er in deze staat gelijkaardige regels inzake bewaartermijn moeten gelden. Bovendien kunnen lidstaten beslissen om persoonsgegevens toch door te geven aan een derde land dat geen passend beschermingsniveau waarborgt, in welbepaalde gevallen, zoals wanneer de betrokkene zijn toestemming heeft gegeven. Het is dus goed mogelijk dat er bij een buiten de Unie gevestigde onderneming die lokalisatiediensten aanbiedt wel lokalisatiegegevens beschikbaar zijn over een zekere termijn. Nog los van de vraag of de fiscale administratie wel over de rechtsgrond beschikt (zie *infra*) en het rechtsinstrument van internationale samenwerking om deze informatie te bekomen, lijkt deze kwestie ook van tijdelijke aard. Op het ogenblik dat de verordening nr. 2016/679 inzake de bescherming van persoonsgegevens van toepassing wordt (25 mei 2018) en de richtlijn nr. 95/46 wordt opgeheven, worden de Europese regels inzake de beperkte bewaartermijn ook van toepassing op bedrijven die weliswaar gevestigd zijn buiten de Unie maar die binnen de Unie persoonsgegevens verwerken *van betrokkenen die zich in de Unie bevinden*, wanneer de verwerking verband houdt met (onder meer) het aanbieden van goederen of diensten aan deze betrokkene in de Unie (art. 3, 2. van de verordening nr. 2016/679). Rekening houdende met het feit dat bedrijven zoals Apple al niet happig zijn op het verstrekken van informatie aan overheden [11] , zullen zij zich ongetwijfeld graag beroepen op de principes van de beperkte bewaartermijn om de informatie niet te moeten verstrekken.

Het inzamelen van informatie over de locatie van een natuurlijke persoon moet daarnaast zonder twijfel worden beschouwd als een inmenging in het privéleven dat wordt beschermd door – in hoofdzaak – artikel 8 EVRM en artikel 22 van de Grondwet [12] . Dit houdt in dat de inmenging moet gebaseerd zijn op een wettelijke basis, en noodzakelijk moet zijn om een welbepaald legitiem doel te bereiken. Een mogelijke wettelijke basis voor het opvragen van locatiegegevens door de fiscale administratie bij anderen dan de belastingplichtige zelf, vormen de artikelen 322 en 323 WIB 1992. Zowel het Europees Hof voor de Rechten van de Mens, als het Grondwettelijk Hof vereisen evenwel dat een wet die de basis vormt voor een inmenging in het privéleven voldoende voorzienbaar is en de burger met andere woorden voldoende weet of kan weten wat hem te wachten staat. De vraag rijst dus of de zeer algemeen geformuleerde artikelen 322 en 323 WIB 1992 wel een voldoende voorzienbare wettelijke basis kunnen vormen voor het opvragen van lokalisatiegegevens.

Bovendien moet een inmenging in het privéleven steeds noodzakelijk zijn om het beoogde legitieme doel te bereiken. Het vestigen van het juiste bedrag van de belastingen is welis-waar zonder twijfel een legitiem doel in de zin van artikel 8 EVRM en artikel 22 Gw. Dit betekent evenwel nog niet dat elke inmenging in het privéleven ook noodzakelijk is om dit doel te bereiken. Een inmenging moet niet alleen relevant en toereikend zijn om het gestelde doel te bereiken, maar de inmenging moet daarnaast ook proportioneel zijn. Het verzamelen van lokalisatiegegevens zal in vele gevallen, waarvan Frank Mortier voorbeelden geeft, relevant zijn voor de vestiging van het juiste bedrag van de belasting, doch niet *per se* ook proportioneel aan dit doel. Dit zal van geval tot geval moeten worden bekeken. Een bijzonder vraagstuk op dat vlak ontstaat in ieder geval bij het opvragen van lokalisatiegegevens op grond van artikel 323 WIB 1992, zijnde lokalisatiegegevens in verband met niet nader genoemde belastingplichtigen. In "Vrij Gesteld" nr. 511 werd reeds de zaak *DIGITAL RIGHTS IRELAND* [13] aangehaald. In deze zaak oordeelde het Hof van Justitie dat de dataretentie-richtlijn [14] die telecombedrijven verplichtte om bepaalde door hen verzamelde gegevens, waaronder lokalisatiegegevens, te bewaren en ze beschikbaar te houden voor strafrechtelijk onderzoek (in België geïmplementeerd via de telecomwet [15]), niet bestaanbaar is met het recht op privéleven. De algemene bewaarplicht werd beschouwd als *on-evenredig* met het beoogde legitieme doel, met name het bestrijden van ernstige criminaliteit en terrorisme, omdat deze bewaarplicht verder gaat dat wat geschikt en noodzakelijk is om dat doel te bereiken. Zo onder meer was de bewaarplicht zonder enig onderscheid van toepassing op a*lle* verkeersgegevens van *alle* abonnees en geregistreerde gebruikers, zodat ze van toepassing was op personen waarvoor geen enkele aanwijzing van betrokkenheid met criminele feiten bestaat. In dezelfde zin lijkt het *opvragen* door de fiscale administratie van een reeks lokalisatiecriteria van niet nader-genoemde belastingplichtigen zonder enige indicatie dat er reden is om aan te nemen dat er sprake is van een overtreding van de fiscale wet, niet proportioneel te zijn aan het beoogde doel.

Sylvie De Raedt [16]

---

[1] Zie hierover: opinion 5/2005 van de art. 29 Working Party on the use of location data with a view to providing value added services (art. 29 Working Party is een onafhankelijk raadgevend orgaan dat werd opgericht op grond van art. 29 van de richtlijn nr. 95/46 inzake de bescherming van de persoonsgegevens).

[2] Met name de wet verwerking persoonsgegevens die de omzetting vormt van de richtlijn nr. 95/46 inzake de bescherming van persoonsgegevens, en vanaf 25 mei 2018 de verordening nr. 2016/679 inzake de verwerking van persoonsgegevens.

---

[3] Zie art. 9, 1. van de richtlijn nr. 2002/58 (op de telecomsector zijn ook de principes van toepassing van de richtlijn nr. 2002/58 inzake de bescherming van persoonsgegevens specifiek op het vlak van telecommunicatie, waarin evenzeer wordt uitgegaan van de beperking van de bewaartermijn); zie ook art. 123, § 1 van de wet van 13 juni 2005 (telecomwet).

---

[4] Art. 123, § 2 van de wet van 13 juni 2005 (telecomwet). Het ontbreken van een toestemming kan worden opgeheven ingeval lokalisatiegegevens moeten worden verwerkt in het kader van een noodoproep (art. 123, § 5 van de wet van 13 juni 2005).

---

[5] Art. 126, § 3 van de wet van 13 juni 2005.

---

[6] Art. 126, § 1-2 van de wet van 13 juni 2005.

---

[7] Opinion 5/2005 van de art. 29 Working Party on the use of location data with a view to providing value added services.

---

[8] Opinion 5/2005 van de art. 29 Working Party on the use of location data with a view to providing value added services.

---

[9] Art. 4 van de richtlijn nr. 95/46.

---

[10] Opinion 5/2005 van de art. 29 Working Party on the use of location data with a view to providing value added services.

---

[11] www.apple.com/nl/privacy/government-information-requests/ .

---

[12] HvJ 8 april 2014, C-293/12 en C-594/12, *DIGITAL RIGHTS IRELAND*.

---

[13] HvJ 8 april 2014, C-293/12 en C-594/12, *DIGITAL RIGHTS IRELAND*; zie ook GwH 11 juni 2015, nr. 84/2015.

---

[14] Richtlijn nr. 2006/24.

---

[15] Art. 126 van deze telecomwet, zoals ingevoegd door art. 5 van de wet van 30 juli 2013, werd vernietigd bij arrest nr. 84/2015 van het Grondwettelijk Hof om quasi identieke redenen als deze aangehaald in het arrest *DIGITAL RIGHTS IRELAND* en vervangen door art. 4 van de wet 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie (*BS* 18 juli 2016). Ingevolge deze bepaling heeft men de algemene bewaartermijn van 12 maanden behouden, maar verstrengd en differentieert men de toegang tot deze informatie om tegemoet te komen aan de kritieken van het Hof van Justitie en het Grondwettelijk Hof.

---

[16] Assistent UGent en advocaat.