Over (niet-?)herleidbaarheid van statistische locatiegegevens

Position paper voor het rondetafelgesprek op 15 oktober 2020 van de vaste commissie voor EZK inzake 'Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19'

dr.ing. Matthijs Koot
Principal Security Specialist, Secura B.V.
Gastonderzoeker, Universiteit van Amsterdam
9 oktober 2020

De 'Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19' (voorts: het wetsvoorstel) regelt een tijdelijke verplichting voor telecomaanbieders om statistische locatiegegevens aan het CBS beschikbaar te stellen in het kader van de bestrijding van COVID-19.

Eén van de discussiepunten omtrent het wetsvoorstel is de vraag of deze statistische gegevens herleidbaar kunnen zijn naar individuele personen. Daarover is in uw Kamer al van gedachten gewisseld. In deze notitie ga ik nogmaals op dat punt in, gebruikmakend van kennis in [Koot2012] die ik eerder heb toegepast op een gedeeltelijk vergelijkbare casus bij het bedrijf Mezuro. Mezuro, vandaag ook vertegenwoordigd, was reeds eerder actief met een verwerking in samenwerking met één van de drie Nederlandse operators van mobiele telecommunicatienetwerken.

Privacy is een grondrecht en een noodzakelijke voorwaarde voor een goed functionerende samenleving. Het beeld dat locatiegegevens in potentie zeer gevoelig kunnen zijn onderschrijf ik ten volle, ongeacht de bron waaruit deze afkomstig zijn: gsm-masten, GPS, Wi-Fi, Bluetooth, beeld- of geluidsopnames, et cetera.

Voorkoming van de-anonimisering

Bij anonimiseringsvraagstukken moet rekening worden gehouden met de vraag welke scenario's van de-anonimisering realistisch zijn en welke niet: niet alles dat in theorie mogelijk is vormt in de praktijk een reëel risico. Het is in het algemeen belangrijk om niet alleen te denken in mogelijkheden, maar ook in waarschijnlijkheden[1]. Staatssecretaris Mona Keijzer merkt in haar brief van 2 oktober 2020 met kenmerk 'WJZ / 20237781' op dat het Europese Hof heeft overwogen dat het heridentificeren van personen "in ieder geval niet aan de orde is als de identificatie van de betrokkene bij de wet verboden wordt of in de praktijk ondoenlijk is, bijvoorbeeld omdat zij — gelet op de vereiste tijd, kosten en mankracht — een excessieve inspanning vergt, zodat het gevaar voor identificatie in werkelijkheid onbeduidend lijkt". Daarin kan een impliciete onderschrijving van het denken in waarschijnlijkheden worden gezien[2].

De belangrijkste strategieën om herleidbaarheid te voorkomen of te minimaliseren zijn 'ophoging' van gegevens (veralgemeniseren, generaliseren), het verstoren van gegevens (statistische ruis, perturberen), en het minimaliseren van gegevens (weglaten, onderdrukken). Binnen de context van het wetsvoorstel zijn voorbeelden het gebruik van gemeenteniveaus in plaats van mastniveaus. De vraag is of het mogelijk is, en zo ja, hoe waarschijnlijk, dat de resulterende gegevens kunnen worden gede-anonimiseerd.

De-anonimisering: wel of niet reëel?

In april 2020 refereerde de Autoriteit Persoonsgegevens (AP) in een presentatie getiteld 'Over de anonimiteit van geaggregeerde telecomlocatiedata' aan een aantal publicaties. Reflecterend op de referenties kan in elk geval worden gesteld dat de methoden beschreven in [Zang2011] en [DeMontjoye2013] niet van toepassing zijn op het wetsvoorstel: die methoden zijn gebaseerd op analyses van CDR/EDR-traces van individuele apparaten. Het wetsvoorstel regelt geen beschikbaarstelling van die gegevens.

De methode beschreven in [Xu2017] richt zich op de-anonimisering van locatiegegevens die zijn geaggregeerd als tellingen per uur en locatie. Die methode maakt gebruik van coherentie en repetitie in menselijke bewegingspatronen, waarmee een 'grondwaarheid-tabel' (Ground Truth) is gegenereerd uit individuele CDR/EDR-traces. Die tabel vormt de statistische weerslag van heuristiek rondom menselijke bewegingspatronen. Via de grondwaardheid-tabel leiden de auteurs potentiële individuele bewegingspatronen af uit geaggregeerde locatiegegevens. Vervolgens tonen de auteurs aan dat hun methode ook

[1] Deze opmerking is ontleend aan een uitspraak van wijlen econoom Arnold Heertje.

[2] Een wettelijk verbod op identificatie lijkt volgens het Hof te kunnen betekenen dat geen sprake is van herleidbaarheid, maar biedt uiteraard geen bescherming tegen scenario's waarin gegevens in handen komen van personen of organisaties die zich niet aan dat verbod houden, bijvoorbeeld na diefstal, verlies, of computerinbraak.

accurate resultaten oplevert wanneer het aggregatieniveau wordt verhoogd (in dat geval resulterend in bewegingspatronen van lagere resolutie). Ze hebben hun methode gevalideerd door deze toe te passen op aggregaties die ze zelf maakten uit de CDR/EDR-brongegevens. Die methode is voor zover bekend niet extern gevalideerd.

[Xu2017] is in potentie relevant voor het wetsvoorstel, omdat ook in het wetsvoorstel sprake is van tellingen per uur en per locatie (en per herkomstgemeente). De ophoging van locatiegegevens tot gemeenteniveau geeft in zekere zin gevolg aan een van twee aanbevelingen die de auteurs doen voor privacybescherming (ophoging), maar betekent alleen dat de-anonimisering resulteert in bewegingspatronen die minder precies zijn: gemeenteniveau in plaats van mastniveau. Aan de tweede aanbeveling (ruis) wordt gevolg gegeven, doordat schattingen worden gebruikt van kansen dat een telefoon zich in een bepaalde gemeente bevond, in plaats van zekere vaststelling daarvan.

De methode blijft probabilistisch van aard, en eist aanvullende combinatie met externe gegevens om tot betekenisvolle uitspraken te komen over de accuraatheid van een bewegingspatroon en bij welke persoon een bepaald patroon hoort. Met betrekking tot Mezuro, dat geen (herkomst)gemeenten maar herkomst- en bestemmingsrichtingen verwerkt, heeft [Xu2017] niet direct geleid tot een andere conclusie dan in 2016. Andere literatuur, zoals [Pyrgelis2018], [Tu2018] en [Tu2019], geeft ook geen aanleiding tot een andere conclusie.

Verder is bekend dat ook binnen de kaders van het wetsvoorstel, er sprake kan zijn van randgevallen, waarvan de staatssecretaris in haar brief een voorbeeld geeft. Onbekend is in hoeverre zulke randgevallen zich in de praktijk voordoen en of ze überhaupt relevant zijn voor een kwaadwillende.

Conclusie

Mijn conclusie, op basis van huidige literatuur, is dat ten aanzien van de gegevens die ingevolge het wetsvoorstel bij het CBS bekend worden, niet volledig kan worden uitgesloten dat de aanval beschreven in [Xu2017] effectief kan zijn. Een succesvolle aanval zou resulteren in een beeld, met foutmarges (onzekerheid), van de bewegingspatronen tussen gemeentes van individuele apparaten. Bewijs daarvoor ontbreekt echter. Een manier om daarover meer zekerheid te krijgen, is de methode daadwerkelijk toe te passen of te simuleren, indien dat niet reeds heeft plaatsgevonden.

Ten aanzien van Mezuro geldt dat [Xu2017] niet van toepassing is, omdat Mezuro niet werkt met telling van apparaten per locatie, maar met daarvan afgeleide bestemmingsgegevens. Ook werkt Mezuro niet met gegevens van alle telecomaanbieders, maar met één telecomaanbieder: in plaats van gegevens van alle Nederlanders te betrekken, wordt dus volstaan met gegevens van grofweg een derde van de Nederlanders. Daarmee is die werkwijze makkelijker verdedigbaar als proportioneel.

Of ten aanzien van de werkwijze in het wetsvoorstel sprake is van een reëel risico, hangt af van de kans die wordt toegedicht aan de mogelijkheid dat een situatie ontstaat dat een (ongeautoriseerde?) persoon of organisatie beschikt over statistische locatiegegevens, een grondwaarheid-tabel, en de motivatie om een de-anonimiseringsaanval uit te voeren. Over de vraag of dat zich laat kwalificeren als 'in de praktijk ondoenlijk', zoals bedoeld in de uitspraak van het Europese Hof, laat ik me niet uit. Dat risico, en het restrisico inzake randgevallen, moet worden afgewogen tegen het belang dat met de gegevensverwerking wordt gediend, in dit geval een maatschappelijk veiligheidsbelang. Evenals beoordeling van nut en noodzaak van het wetsvoorstel, is dat een politiek vraagstuk.

Bibliografie

DeMontjoye2013 De Montjoye, Y.-A., Hidalgo, C.A., Verleysen, M. and Blondel, V.D., "Unique in the Crowd: The privacy bounds of human mobility", Scientific Reports 3:1376 (2013). DOI: 10.1038/srep01376

Koot2012 Koot, M.R., "Measuring and Predicting Anonymity", Universiteit van Amsterdam (2012).

Pyrgelis2018 Pyrgelis, A., Troncoso, C. en De Cristofaro, E., "Knock Knock, Who's There? Membership Inference on Aggregate Location Data", Proceedings of the 25th Network and Distributed System Security Symposium, NDSS 2018 (2018). DOI: 10.14722/ndss.2018.23183

Tu2018 Tu, Z., Xu, F., Li, Y., Zhang, P., Jin, D., "A New Privacy Breach: User Trajectory Recovery From Aggregated Mobility Data", IEEE/ACM Transactions on Networking 26:3 (2018). DOI: 10.1109/TNET.2018.2829173

Tu2019 Tu, Z. Zhao, K., Xu, F., Li, Y. Su, L. en Jin, D., "Protecting Trajectory From Semantic Attack Considering k-Anonymity, l-Diversity, and t-Closeness", IEEE Transactions on Network and Service Management 16:1 (2019). DOI: 10.1109/TNSM.2018.2877790

Xu2017 Xu, F., Tu, Z., Li, Y., Zhang, P., Fu, X. and Jin, D., "Trajectory Recovery From Ash: User Privacy Is NOT Preserved in Aggregated Mobility Data", WWW 2017 (2017). DOI: 10.1145/3038912.3052620

Zang2011 Zang, H. and Bolot, J., "Anonymization of location data does not work: A large-scale measurement study", Proceedings of the 17th annual international conference on Mobile computing and networking, MobiCom '11 (2011). DOI: 10.1145/2030613.2030630