PRIVACY FIRST

Postbus 16799
1001 RG Amsterdam
Tel. 020 - 8100279

Aan:
Eerste Kamer der Staten-Generaal
Vaste commissie voor Veiligheid en Justitie
Per email: postbus@eerstekamer.nl

Uw ref.	:	
Onze ref.	:	SPF20170609
Datum	:	9 juni 2017
Betreft	:	Position paper t.b.v. deskundigenbijeenkomst wetsvoorstel 33542 (ANPR) 20 juni 2017

Geachte Kamerleden,

Dank voor uw uitnodiging om deel te nemen aan de deskundigenbijeenkomst inzake het wetsvoorstel ANPR (automatische nummerplaatregistratie).[1] Onder dit wetsvoorstel zal de politie de bevoegdheid krijgen om alle kentekens op de openbare weg 4 weken te bewaren voor opsporing en vervolging. In de optiek van Privacy First vormt dit een massale privacyschending. Hieronder zullen wij dit kort toelichten.

Huidige regels

Onder de huidige wetgeving dienen de ANPR-gegevens van onschuldige burgers binnen 24 uur te worden gewist. Alle kentekens die niet verdacht zijn (zogeheten "no-hits") dienen zelfs direct uit de databases te worden verwijderd, aldus de Autoriteit Persoonsgegevens.[2] In een democratische rechtsstaat dienen onschuldige burgers immers zoveel mogelijk met rust te worden gelaten: het klassieke rechtsbeginsel is dat de overheid pas inbreuk mag maken op de privacy van een burger bij een redelijke verdenking van een concreet strafbaar feit. De huidige ANPR-praktijk is hiermee in lijn in die zin dat de "hits" kunnen worden gebruikt en de "no-hits" worden gewist. Deze praktijk vindt echter al jaren plaats op basis van een algemene vangnetbepaling: artikel 3 Politiewet. Daarbij is sprake van *profiling*. Dit voldoet geenszins aan de moderne eisen die het Europese privacyrecht aan het gebruik van ANPR stelt. Privacy First adviseert allereerst dan ook om de huidige ANPR-praktijk in te perken en alsnog van een specifieke wettelijke basis met strikte privacywaarborgen te voorzien.

Gebrek aan noodzaak en proportionaliteit

In plaats van de actuele ANPR-praktijk alsnog op privacyvriendelijke wijze te reguleren, vormt het huidige ANPR-wetsvoorstel een verregaande schending van het recht op privacy van vrijwel iedere automobilist. Onder dit wetsvoorstel zullen

[1] Wetsvoorstel Vastleggen en bewaren kentekengegevens door politie, *Kamerstukken* 33542.

[2] Zie College bescherming persoonsgegevens, *Politiekorpsen handelen in strijd met de wet bij toepassing ANPR* (28 januari 2010), https://autoriteitpersoonsgegevens.nl/nl/nieuws/politiekorpsen-handelen-strijd-met-de-wet-bij-toepassing-anpr.

immers alle kentekens op openbare wegen (oftewel ieders reisbewegingen, locatiedata) 4 weken in een nationale ANPR-databank worden opgeslagen. Bovendien zullen deze ANPR-data onder meer worden gedeeld met de AIVD (onder de nieuwe Wet op de inlichtingen- en veiligheidsdiensten zelfs middels directe toegang tot de ANPR-databank). Iedere automobilist wordt hierdoor een potentiële verdachte. Uit het ANPR-wetgevingstraject blijkt tot op heden echter geen enkele maatschappelijke noodzaak hiertoe: de laatste jaren lijkt ANPR slechts bij een handjevol misdrijven te hebben bijgedragen aan succesvolle opsporing en vervolging. Naar objectieve maatstaven weegt dit niet op tegen het opofferen van de privacy, bewegingsvrijheid en onschuldpresumptie van miljoenen automobilisten. Ter vergelijking: toen na 9/11 door het CDA werd voorgesteld om van de gehele bevolking vingerafdrukken af te nemen voor opsporingsdoeleinden, werd dit door minister van Justitie Korthals (VVD) direct verworpen. Korthals achtte dit voorstel disproportioneel, omdat op jaarbasis sprake was van circa 10.000 sporenzaken (met vingerafdrukken).[3] De Tweede Kamer was dit destijds met de minister eens. Massale opslag van ieders vingerafdrukken en telecommunicatiedata zijn inmiddels verboden. Derhalve valt niet in te zien waarom de opslag van ieders ANPR-data wel toegestaan zou moeten worden.

Van 'mass surveillance' naar 'targeted surveillance'

Het huidige wetsvoorstel legt een fundamentele bouwsteen voor Nederland als toekomstige "*surveillance society*". Nederland overschrijdt hiermee een principiële grens. Zowel binnen de Nederlandse maatschappij als in het buitenland maakt men zich hier grote zorgen over, zo bleek onlangs uit gesprekken tussen Privacy First en diverse ambassades in Den Haag. Op Europees niveau is immers juist sprake van een ontwikkeling in omgekeerde richting: van ineffectieve, inefficiënte en onrechtmatige "*mass surveillance*" naar effectieve, efficiënte en legitieme "*targeted surveillance*", zo blijkt uit diverse baanbrekende uitspraken van de hoogste Europese rechters en groeiende *communis opinio* onder experts. Door dit wetsvoorstel aan te nemen slaat Nederland dus niet alleen een juridische en beleidsmatige flater, maar creëert het ook een gevaarlijk internationaal precedent.

Mogelijke rechtszaak

Het huidige wetsvoorstel dateert reeds van begin 2013 en heeft sindsdien – terecht – een moeizame geschiedenis achter de rug.[4] Reeds een jaar nadat het wetsvoorstel door voormalig minister Opstelten bij de Tweede Kamer was ingediend bleek het juridisch onhoudbaar, toen het Europees Hof van Justitie de massale opslag van ieders telecommunicatiedata (waaronder locatiedata) onrechtmatig verklaarde.[5] Wegens

[3] Zie Brief van de minister van Justitie d.d. 10 december 2001, *Kamerstukken II*, 2001-2002, 19637, nr. 635, p. 7.

[4] Voorheen was ook minister van Justitie Hirsch Ballin al in 2010 van plan om een vergelijkbaar voorstel in te dienen met een bewaartermijn van 10 dagen. Vervolgens verklaarde de Tweede Kamer dit voorstel echter controversieel.

[5] Hof van Justitie van de Europese Unie 8 april 2014, gevoegde zaken C-293/12 & C294/12 (*Digital Rights*).

privacyzorgen lag de verdere behandeling van het wetsvoorstel vervolgens twee jaar stil, totdat dit door voormalig minister Van der Steur in september 2016 opnieuw werd geactiveerd. Drie maanden later volgde echter de genadeklap: in een nieuw, scherper verwoord arrest verklaarde het Europees Hof van Justitie de ongerichte, massale opslag van data van onschuldige burgers voor opsporingsdoeleinden (dataretentie) definitief onrechtmatig. Dit zou slechts rechtmatig kunnen zijn middels strikte gerichtheid in tijd, locatie, strafrechtelijk relevante personen en doelen.[6] Bij het gebruik van dergelijke data is bovendien voorafgaande rechterlijke toestemming geboden. Het huidige wetsvoorstel ANPR voldoet aan geen van deze eisen. Het wetvoorstel is daarmee onrechtmatig en dient door uw Kamer te worden verworpen. Bij gebreke hiervan zal Privacy First (in brede coalitie) de Nederlandse Staat dagvaarden en het wetsvoorstel onverbindend laten verklaren wegens schending van het recht op privacy (art. 8 EVRM).

Voor nadere informatie of vragen met betrekking tot bovenstaande is Privacy First te allen tijde bereikbaar op telefoonnummer 020-8100279 of per email: info@privacyfirst.nl.

Hoogachtend,

Stichting Privacy First

mr. Vincent A. Böhre
director of operations

[6] Hof van Justitie van de Europese Unie 21 december 2016, gevoegde zaken C‑203/15 & C‑698/15 (*Tele2*).