

Aan:
Ministerie van Justitie en Veiligheid

Uw ref. :
Onze ref. : SPF20180914
Datum : 14 september 2018
Betreft : reactie Privacy First op consultatie bij wetsvoorstel gegevensverwerking door samenwerkingsverbanden

Geachte heer/mevrouw,

Met verbijstering heeft Stichting Privacy First kennisgenomen van het concept-wetsvoorstel *gegevensverwerking door samenwerkingsverbanden*. Dit wetsvoorstel is flagrant in strijd met zowel het Europese als nationale (grondwettelijke) privacyrecht. Privacy First adviseert u hierbij dan ook met klem om dit wetsvoorstel in te trekken. Hieronder licht Privacy First dit op hoofdlijnen toe.

Gebrek aan maatschappelijke noodzaak en proportionaliteit

Artikel 8 EVRM vereist een harde maatschappelijke noodzaak voor wetgeving waardoor inbreuk op de privacy van burgers kan worden gemaakt. Dat het onderhavige wetsvoorstel inbreuk maakt op het recht op privacy is evident: middels dit wetsvoorstel zullen alle beschikbare (persoons)gegevens over burgers in alle mogelijke samenwerkingsverbanden van zowel publieke als private partijen voor vrijwel alle mogelijke doeleinden kunnen worden uitgewisseld en gebruikt. De feitelijke noodzaak hiervan wordt in de toelichting bij het concept-wetsvoorstel echter niet gesteld, laat staan onderbouwd en aangetoond. Het wetsvoorstel spreekt slechts over een politieke “wens” voor meer samenwerking om op allerlei beleidsterreinen afgeleide sturingsinformatie te kunnen bieden.¹ Dit is ambtelijk jargon om op grote (rijksbrede) schaal Big Data te kunnen gaan toepassen voor massale, grotendeels heimelijke *profiling* van vrijwel de gehele bevolking. Juridisch is dit echter niet toegestaan; dit past immers niet in een democratische rechtsstaat, en is daarom verboden onder art. 8 EVRM. Terecht spreekt de memorie van toelichting bij het concept-wetsvoorstel in dit verband dan ook over (juridische) “knelpunten”.² Deze “knelpunten” zijn echter inherent aan het geldende privacyrecht, waaronder het fundamentele vereiste van doelbinding.³ Middels dit wetsvoorstel tracht de rijksoverheid die “knelpunten” op nationaal niveau op te heffen en de bestaande rechtsbescherming te doorbreken. Zowel het Europese als nationaal-grondwettelijke privacyrecht staan deze doorbreking echter niet toe.

¹ Zie memorie van toelichting (MvT), par. 1.1.

² Zie MvT, par. 1.1, 2, 3.1, 3.3.

³ MvT, par. 3.3.1: “Het principe van doelbinding is immers één van de belangrijkste principes in het gegevensbeschermingsrecht en dient daarom ook voor samenwerkingsverbanden het uitgangspunt te blijven.”

Onrechtmatige grondslag

In de toelichting bij het wetsvoorstel wordt gesteld dat e.e.a. rechtstreeks kan worden gebaseerd op art. 6 lid 3 AVG.⁴ Deze bepaling in de AVG is enkele jaren geleden door de Nederlandse regering zelf in Brussel ingestoken met als doel om wetsvoorstellen zoals de onderhavige (en reeds bestaande buitenwettelijke praktijken) te kunnen legitimeren, in lijn met de Big Data agenda van diverse ministeries, met name het ministerie van Justitie en Veiligheid.⁵ Art. 6 lid 3 AVG is echter al jaren controversieel en wordt door de meeste privacy-experts gezien als een gevaarlijke, makkelijk door nationale regeringen te misbruiken “loophole” in het nieuwe EU-dataprotectierecht. Deze bepaling zet voor overheden immers vrijwel alle geldende AVG-rechten opzij. De AVG is echter ondergeschikt aan art. 8 EU Grondrechten Handvest en art. 8 EVRM, waaronder het strikte vereiste van doelbinding. In geen enkel geval mag de rechtsbescherming onder de AVG een lager niveau hebben dan die door het EU Grondrechten Handvest en EVRM worden gegarandeerd. Middels parlementaire moties is de Nederlandse regering hier bij de totstandkoming van de AVG uitdrukkelijk voor gewaarschuwd.⁶ Bij gelegenheid zullen Privacy First en het Platform Bescherming Burgerrechten c.s. art. 6 lid 3 AVG dan ook aanvechten en trachten om deze bepaling middels prejudiciële vragen onrechtmatig te laten verklaren door het Europees Hof van Justitie, bijvoorbeeld in onze lopende civiele rechtszaak tegen het (met dit wetsvoorstel vergelijkbare) Systeem Risico Indicatie.⁷

In de toelichting bij het concept-wetsvoorstel wordt tevens opgemerkt dat art. 6 AVG voorrang zou hebben op art. 10 Grondwet, waardoor een formeel-wettelijke grondslag (parlementaire wet in formele zin) voor privacy-inbreuken zoals die door dit wetsvoorstel worden beoogd niet langer nodig zou zijn, maar e.e.a. rechtstreeks op art. 6 AVG en later vast te stellen AMvB's kan worden gebaseerd. Dit berust echter op een onjuiste toepassing en interpretatie van het Europees recht: art. 6 lid 3 AVG verwijst immers naar nationaal recht, inclusief de waarborgen van een nationale

⁴ Zie MvT, par. 3.2.1, 5-6.

⁵ Zie brief van minister Van der Steur (Veiligheid en Justitie) aan Tweede Kamer d.d. 7 januari 2016: “In artikel 6(3a) is (...) voorts voorzien in de mogelijkheid voor de publieke sector om gegevens verder te verwerken voor een ander gespecificeerd doel dan waarvoor ze oorspronkelijk zijn verzameld indien dit bij wet wordt geregeld. Ook dit was een Nederlands voorstel.” *Kamerstukken II*, 2015-2016, 32761, nr. 91, p. 2, <https://zoek.officielebekendmakingen.nl/kst-32761-91.html>.

⁶ Zie bijvoorbeeld motie Elissen c.s. d.d. 5 juli 2012: “(...) constaterende dat deze verordening in artikel 6 het principe van doelbinding, een van de fundamenteën van het gegevensbeschermingsrecht, wijzigt en daarmee meer ruimte biedt voor verwerkingen van persoonsgegevens van burgers voor andere doelen dan waarvoor de gegevens verzameld zijn, ongeacht de vraag of die doelen verenigbaar zijn met het oorspronkelijke doel; constaterende dat het deels loslaten van het beginsel van doelbinding een verzwakking van het privacybeschermingsniveau oplevert; verzoekt de regering, om er zorg voor te dragen dat de verordening zal voorzien in een bepaling die verwerking van persoonsgegevens voor andere doelen dan het doel waarvoor de gegevens oorspronkelijk zijn verzameld, uitsluitend mogelijk is in geval van verenigbaarheid en op basis van een wettelijke grondslag (...).” *Kamerstukken II*, 2011-2012, 32761, nr. 38, <https://zoek.officielebekendmakingen.nl/kst-32761-38.html>.

⁷ Zie voor meer informatie over deze rechtszaak <https://bijvoorbeeldverdacht.nl>. Zie tevens <https://platformburgerrechten.nl/2018/04/30/nieuwe-eu-regels-luiden-onbeperkte-informatiemacht-overheden-in/> en <https://platformburgerrechten.nl/2016/05/24/nederland-had-niet-akkoord-mogengaan-met-nieuwe-privacyregels-eu/>.

Grondwet. In Nederland dient iedere privacy-inbreuk (nationaal, regionaal en lokaal) te worden gebaseerd op een deugdelijke grondslag bij of krachtens wet in formele zin, zo vereist artikel 10 Grondwet. In die zin biedt artikel 10 Grondwet meer bescherming dan art. 8 EVRM (waaronder immers ook lagere wetgeving en zelfs jurisprudentie als wettelijke grondslag voor privacy-inbreuken kunnen gelden). De betreffende Nederlandse wet in formele zin dient op zijn beurt voldoende specifiek, kenbaar, voorzienbaar en met strikte privacy-waarborgen omgeven te zijn, zo vereist art. 8 EVRM. Deze hogere vereisten kunnen dan ook niet worden omzeild door onderhavig kader-wetsvoorstel als lege huls of “Big Data carte blanche” die later door diverse ministers naar believen kan worden “ingevuld” door in allerlei (nu nog totaal onvoorzienbare) samenwerkingsverbanden middels allerlei AMvB’s allerlei privacy-inbreuken op diverse beleidsterreinen te kunnen gaan doorvoeren.⁸ Om deze reden acht Privacy First dit wetsvoorstel fundamenteel onhoudbaar.

Overige aspecten

Met onderhavig wetsvoorstel wordt de basis gelegd voor toekomstige massasurveillance op ongekenne schaal: in de meest uiteenlopende samenwerkingsverbanden van publieke en private partijen zullen alle mogelijke gegevens over burgers continu kunnen worden uitgewisseld en voor onvoorziene doelen kunnen worden gebruikt middels *datamining* en *profiling*. Naast het recht op privacy komen hierdoor diverse andere burgerrechten, democratische waarden en rechtsstatelijke *checks & balances* onder druk te staan, waaronder de onschuldpresumptie, het verbod van automatische besluitvorming, het recht op toegang tot de rechter, een effectief rechtsmiddel en een eerlijk proces, het verbod van discriminatie en de vrijheid van meningsuiting. Wanneer alle mogelijke gegevens voortaan door de overheid (en private partijen) voor alle mogelijke doelen kunnen worden gebruikt, zal niemand zich immers nog daadwerkelijk vrij en onbespied kunnen wanen. Daarmee vormt dit wetsvoorstel niet alleen een bedreiging voor ieders recht op privacy en vrije ontwikkeling, maar ook voor de verdere ontwikkeling van Nederland als vrije democratische rechtsstaat. Dit zal op termijn leiden tot een maatschappelijk *chilling effect* en sociale stratificatie met desastreuze gevolgen. Hierbij roept Privacy First u dan ook nogmaals op om dit wetsvoorstel in te trekken.

Voor nadere informatie of vragen met betrekking tot bovenstaande is Privacy First te allen tijde bereikbaar op telefoonnummer _____ of per email: _____

Hoogachtend,

⁸ De MvT spreekt in dit verband zelf over een “kapstok”-wet waaraan allerlei samenwerkingsverbanden (en hun respectievelijke Big Data projecten) zullen kunnen worden “opgehangen”; zie par. 3.2.2.