PRIVACY FIRST

Keizersgracht 127
1015 CJ Amsterdam
Tel. 020 - 8100279

Aan:
Tweede Kamer der Staten-Generaal
Vaste commissie voor Economische Zaken en Klimaat
Per email: cie.ezk@tweedekamer.nl

Uw ref.	:	
Onze ref.	:	SPF20200609
Datum	:	9 juni 2020
Betreft	:	Standpunten Privacy First inzake wetsvoorstel informatieverstrekking RIVM i.v.m. COVID-19 (35479)

Geachte Kamerleden,

Met grote zorg heeft Stichting Privacy First kennisgenomen van het "tijdelijke" wetsvoorstel informatieverstrekking RIVM i.v.m. COVID-19. Privacy First adviseert u om dit wetsvoorstel te verwerpen wegens de volgende fundamentele bezwaren en risico's:

Strijdig met fundamentele bestuurlijke en privacy principes

- De maatschappelijke noodzaak voor dit wetsvoorstel ontbreekt. Het Corona-virus ebt momenteel immers weg uit de Nederlandse samenleving. Andere vormen van monitoring zijn reeds voldoende effectief gebleken. De noodzaak voor dit wetsvoorstel is niet aangetoond, en net zomin bestaan er voorbeelden uit het buitenland waar toepassing van vergelijkbare technieken een wezenlijke bijdrage leverde.
- Het wetsvoorstel is volstrekt disproportioneel, want het omvat alle telecom-locatiedata in heel Nederland. Van enige differentiatie is geen sprake. Hetzelfde geldt voor dataminimalisatie: een steekproef zou kunnen volstaan.
- Het wetsvoorstel werkt met terugwerkende kracht vanaf 1 januari 2020. Dit is in strijd met de rechtszekerheid en het legaliteitsbeginsel, zeker omdat deze datum ver vóór de Nederlandse 'start' van de pandemie ligt (11 maart).
- De in het wetsvoorstel gekozen systematiek van nadere aanwijzingen door de Minister is ronduit ondemocratisch. Het holt de democratische rechtsstaat en toezicht door de volksvertegenwoordiging verder uit.
- In het wetsvoorstel wordt niet gerept over privacy-by-design of hoe dit toegepast zal worden, terwijl dat juist bij dit wetsvoorstel aan de orde zou moeten zijn.

Alternatieven zijn minder invasief: subsidiariteit

- Privacyvriendelijker alternatieven zijn door de staatssecretaris onvoldoende onderzocht. Heeft zij hierin wel interesse?

- Data bij telecomproviders worden gepseudonimiseerd met een uniek ID-nummer en als zodanig aangeleverd bij het CBS. Massale aantallen gevoelige persoonsgegevens worden hierdoor enorm kwetsbaar. Anonimisering door het CBS gebeurt pas in een later stadium.
- De data worden bij gebruik gefilterd op geografische herkomst. Dit creëert een risico van verboden discriminatie naar nationaliteit.
- Onduidelijk is of men de gebruikte data bij CBS of RIVM zal willen "verrijken" met andere data, met *function creep* (doelverschuiving) en mogelijk data-misbruik tot gevolg.

Transparantie en onafhankelijk toezicht ontbreken

- De Privacy Impact Assessment (PIA) bij het wetsvoorstel is vooralsnog niet openbaar.
- Onafhankelijk toezicht op de maatregelen en effecten (door een rechter of onafhankelijke commissie) ontbreekt.
- De AVG is wellicht slechts deels op het wetsvoorstel van toepassing, aangezien anonieme data en statistieken van de werking van de AVG uitgezonderd zijn. Dit veroorzaakt nieuwe risico's op data-misbruik, slechte beveiliging, datalekken etc. Algemene privacy-beginselen zouden daarom in elk geval van toepassing verklaard moeten worden.

Structurele wijzigingen en *chilling effect*

- Dit wetsvoorstel lijkt nu formeel tijdelijk, maar de geschiedenis rond dergelijke wetgeving leert dat het hoogstwaarschijnlijk permanent zal worden.
- Ongeacht de "anonimiteit" van e.e.a. zullen veel mensen zich door dit wetsvoorstel gemonitord gaan wanen en zich onnatuurlijk gaan gedragen. Het risico van een maatschappelijk *chilling effect* is enorm.

Gebrekkige methode met grote impact

- De effectiviteit van het wetsvoorstel is onbekend. Het wetsvoorstel vormt in wezen dus een massaal experiment. De Nederlandse maatschappij is echter niet bedoeld als levend laboratorium.
- Anonieme data kunnen middels koppeling alsnog herleidbaar blijken. Ook bij de gekozen drempelwaarde van minimaal 15 eenheden per datapunt is het risico van unieke "singling out" en identificatie waarschijnlijk nog steeds te groot.
- Het wetsvoorstel leidt tot valse signalen en blinde vlekken door mensen met meerdere telefoons, kwetsbare groepen zonder telefoon etc.
- Er is een groot risico op *function creep* (doelverschuiving), heimelijk gebruik en misbruik van data door andere overheidsdiensten (waaronder AIVD), toekomstige overheden, internationale uitwisseling etc.
- Naast het recht op privacy komen ook andere mensenrechten door dit wetsvoorstel onder druk te staan, waaronder de vrijheid van beweging en

het recht op demonstratie. Dit wetsvoorstel kan gemakkelijk leiden tot structurele *crowd control* die niet past in een democratische samenleving.

Specifieke toestemming vooraf

Naast bovenstaande bezwaren en risico's betwijfelt Privacy First of het gebruik van telecomdata zoals door dit wetsvoorstel beoogd voor telecom-providers überhaupt rechtmatig is. In de optiek van Privacy First zou daartoe tenminste sprake moeten zijn van expliciete, specifieke toestemming vooraf (opt-in) door de klant in kwestie, danwel van de mogelijkheid van een opt-out achteraf en het individuele recht op verwijdering van alle data.

Het is aan u als Kamerleden om onze maatschappij voor dit wetsvoorstel te behoeden. Bij gebreke daarvan behoudt Privacy First zich het recht voor om juridische stappen inzake deze wet te nemen.

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

Vincent Böhre
directeur