

Aan:
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie Constitutionele Zaken en Wetgeving
Via www.internetconsultatie.nl

Uw ref. :
Onze ref. : SPF-20150831
Datum : 31 augustus 2015
Betreft : Commentaar Privacy First op concept-wetsvoorstel ter invoering van een nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv)

Geachte heer/mevrouw,

Hierbij geeft Stichting Privacy First graag een eerste reactie op het huidige concept-wetsvoorstel ter herziening van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) 2002. Daarbij herinnert Privacy First allereerst graag aan de inhoud van de openbare toespraak die het hoofd van de AIVD (de heer Rob Bertholee) in september 2012 ten kantore van Privacy First in Amsterdam hield. Het door Privacy First gepubliceerde verslag van deze toespraak¹ is destijds door de AIVD zelf geaccordeerd. Enkele relevante passages uit dit verslag luiden als volgt:

“[Bertholee] kan zich voorstellen dat correlatie (koppeling) en internationale uitwisseling van gegevens door de burger ervaren wordt als “Big Brother” en dat men zich daar zorgen om maakt. Als burger maakt Bertholee zich daar zelf ook zorgen over.

(...)

Bij het vragen om informatie door de AIVD aan burgers mag overigens geen sprake zijn van enige vorm van druk. Hetzelfde geldt voor het vragen van informatie aan journalisten: journalisten zijn geheel vrij om daar wel of niet aan mee te werken. “Als een journalist er niet aan wil meewerken, dan is dat jammer voor de AIVD, maar daar houdt het mee op,” aldus Bertholee.

(...)

Wat eventuele herziening van de Wiv2002 betreft merkt Bertholee op dat de huidige wettelijke ruimte voor de AIVD voldoende is en dat hij niet meer bevoegdheden nodig heeft.

(...)

Bertholee eindigt zijn lezing door nog eens te benadrukken dat de AIVD geen dossiers van iedereen bijhoudt, niet iedereen onder de tap houdt, (...) niet elke

¹ Zie *Hoofd AIVD: “Ik ben geen voorstander van Big Brother”* (20 september 2012), <https://www.privacyfirst.nl/aandachtvelden/metaprivacy/item/576-hoofd-aivd-geen-voorstander-van-big-brother.html>. Zie tevens <https://www.security.nl/posting/38120/Hoofd+AIVD+geen+voorstander+van+Big+Brother>.

computer hackt, geen handhavende bevoegdheden heeft [en] geen druk op mensen uitoefent (...).”

De belangrijkste boodschap van Bertholee aan het publiek destijds was dat “hij geen voorstander was van Big Brother.” Begin 2015 herhaalde hij deze boodschap ter gelegenheid van het semi-openbare ReuringCafé bij de Vereniging voor OverheidsManagement: “Het recht op privacy is voor mij net zo heilig als voor Privacy First”, aldus Bertholee tegenover een zaal vol topambtenaren.

Als het hoofd van de AIVD zélf al vindt dat hij voldoende bevoegdheden heeft en waarschuwt voor Big Brother, dan heeft de Nederlandse regering bij iedere uitbreiding van deze bevoegdheden bij voorbaat de schijn tegen zich. In het licht hiervan kunnen met name de volgende aspecten uit het huidige concept-wetsvoorstel in de optiek van Privacy First niet door de beugel:

Strafbare feiten

Allereerst opvallend is dat de huidige bevoegdheid van agenten om strafbare feiten te plegen vrijwel ongemoeid wordt gelaten en niet nader juridisch wordt ingekaderd. Dit ondanks de reeds bestaande (maar nooit uitgevoerde) opdracht in de huidige Wiv om deze bevoegdheid alsnog van juridische waarborgen te voorzien middels een algemene maatregel van bestuur (AMvB).² Ook de commissie Dessens achtte dergelijke nadere normering – terecht – wenselijk. Desondanks wenst het kabinet de grondslag voor de betreffende AMvB af te schaffen.³ Het plegen van strafbare feiten door agenten blijft daarmee grotendeels plaatsvinden in een juridisch vacuüm. Privacy First acht dit onwenselijk, riskant en ronduit gevaarlijk.

Hack-bevoegdheid en decryptiebevel

Een tweede verwerpelijk onderdeel van het wetsvoorstel is de bevoegdheid om ieders computer te kunnen hacken en mensen te kunnen verplichten om versleutelde bestanden voor de diensten te ontsleutelen, dit laatste op straffe van 2 jaar hechtenis.⁴ Privacy First acht dit volstrekt in strijd met het recht op privacy, want niet noodzakelijk en disproportioneel. Daarnaast is het voorstel in strijd met het verbod van zelfincriminatie (*nemo tenetur*). Het voorstel legt de basis voor toekomstig machtsmisbruik en vormt in de optiek van Privacy First een typische bouwsteen voor een politiestaat i.p.v. een democratische rechtsstaat. Dit geldt eveneens voor het onderdeel in het wetsvoorstel met betrekking tot de invoering van een massale internettap; deze bevoegdheid is ronduit totalitair. De door het kabinet veronderstelde noodzaak hiervan wordt in het voorstel slechts gesteld en nauwelijks onderbouwd, laat staan aangetoond.⁵ In een democratische samenleving is de maatschappelijke noodzaak van een dergelijke bevoegdheid echter überhaupt ondenkbaar. Dit voorstel is daarmee bij voorbaat onrechtmatig.

² Zie Wiv 2002, art. 21 lid 7.

³ Zie concept-Memorie van Toelichting (MvT), pp. 42-43.

⁴ Zie concept-artt. 30 & 132 Wiv; zie tevens concept-MvT, pp. 51-55.

⁵ Zie concept-MvT, pp. 62-63.

Datamining & profiling

De bevoegdheden tot het opvragen en gebruiken van gegevens zijn in het huidige wetsvoorstel vrijwel onbegrensd. Het voorstel maakt daartoe zelfs directe toegang tot de databanken van derde partijen (overheid én bedrijfsleven) mogelijk. Bij al deze partijen zullen bovendien complete databanken opgevraagd kunnen worden. Dit alles ten behoeve van koppeling, *datamining* en *profiling*, waarmee een uiterst gedetailleerd (zelfs voorspellend) beeld van groepen en individuen kan worden gecreëerd.⁶ Deze bevoegdheden zijn volstrekt disproportioneel en zouden in dit wetsvoorstel juist ingeperkt moeten worden, in elk geval waar het gevoelige (bijvoorbeeld medische of biometrische) data betreft.

Notificatieplicht

Een lichtpuntje in het wetsvoorstel is de handhaving van de notificatieplicht. Deze geldt echter slechts jegens individuen en niet jegens organisaties die (als zodanig) evengoed *targets* kunnen zijn geweest.⁷ Privacy First adviseert dan ook om deze bepaling te amenderen in de zin dat de notificatieplicht tevens voor organisaties zal gaan gelden.

Informanten

Privacy First adviseert om de huidige Wiv alsnog te voorzien van een verbod om journalisten als informanten in te zetten. Dit in het belang van een vrije pers en de journalistieke bronbescherming. In het belang van een gezond maatschappelijk middenveld zou een dergelijk verbod eveneens kunnen worden ingevoerd met betrekking tot de inzet van agenten en informanten bij maatschappelijke (non-gouvernementele) organisaties.

Actieve openbaarheid

Privacy First adviseert om de huidige Wiv alsnog te voorzien van bepalingen ter actieve openbaarmaking van (historische) documenten van de diensten. De praktijk van “declassification and transparency” in andere landen (waaronder voorheen de Verenigde Staten) kan in dit opzicht een bron van inspiratie vormen.

Internationale uitwisseling

De rechtsbasis voor internationale uitwisseling van inlichtingen werd de laatste jaren gevormd door het obscure artikel 59 Wiv. Dit artikel voldoet bij lange na niet aan de moderne eisen die art. 8 EVRM aan een dergelijke bepaling stelt. In wezen vindt de huidige praktijk van uitwisseling tussen AIVD/MIVD en buitenlandse geheime diensten daardoor al jaren plaats in een juridisch zwart gat. Het verheugt Privacy First dan ook dat art. 59 Wiv grotendeels wordt herzien en mensenrechtelijk wordt versterkt in de nieuwe artikelen 76-78. Deze herziening vormt *grosso modo* een positieve stap vooruit. Probleem blijft echter de internationale uitwisseling van

⁶ Zie concept-artt. 22 & 47 Wiv; zie tevens concept-MvT, pp. 24-27, 77-78, 102-103.

⁷ Zie concept-MvT, p. 99.

ongeevalueerde bulk-data; dergelijke uitwisseling wordt door het concept-wetsvoorstel en de bijbehorende Memorie van Toelichting (MvT) ten onrechte gelegitimeerd.⁸ Deze thematiek speelt sinds eind 2013 een cruciale rol in de rechtszaak *Burgers tegen Plasterk* van Privacy First c.s. tegen de Staat.⁹ De voortzetting van deze zaak in hoger beroep blijft door het huidige wetsvoorstel onverminderd actueel en urgent.

Internationale rechtsorde

Nederland heeft de algemene mensenrechtelijke plicht om het recht op privacy in eigen land voortdurend te *bevorderen* i.p.v. te beperken. Door dit wetsvoorstel schendt Nederland deze algemene plicht; het recht op privacy wordt hierdoor immers massaal ingeperkt. Dit zet de vertrouwensrelatie tussen de Nederlandse overheid en de Nederlandse bevolking op scherp, wat zal leiden tot een maatschappelijk *chilling effect*. Dit is funest voor de vrije dynamiek in onze democratische rechtsstaat. Het wetsvoorstel en bijbehorende technologie zullen bovendien worden gekopieerd en misbruikt door minder democratische regimes in het buitenland. Het wetsvoorstel vormt daarmee een internationaal precedent voor een wereldwijde *Rule of the Jungle* i.p.v. de *Rule of Law*. Dit is in strijd met de grondwettelijke plicht van de Nederlandse regering om de ontwikkeling van de internationale rechtsorde te bevorderen.¹⁰ In het licht van het Nederlandse buitenlands beleid dient dit wetsvoorstel derhalve verworpen te worden.

Toezicht

In het huidige wetsvoorstel is het toezicht op de diensten te vrijblijvend en te politiek van aard. In de optiek van Privacy First dient dit toezicht te worden versterkt en onafhankelijker te worden gemaakt, hetzij middels bindend rechtmatigheidstoezicht vooraf door de CTIVD, hetzij middels bindend toezicht vooraf door de rechter. Dergelijk toezicht dient te gelden bij de uitoefening van alle bijzondere bevoegdheden van de diensten. Pas dan zal een rechtsstatelijke uitoefening van deze bevoegdheden optimaal gewaarborgd en voldoende toekomstbestendig zijn.

Vingerafdrukken

Saillant detail is tenslotte nog dat op p. 44 van de MvT wordt opgemerkt dat “[v]an een afzonderlijke regeling voor het onderzoek naar vingerafdrukken wordt afgezien, omdat de resultaten van een dergelijk onderzoek in de praktijk niet altijd bruikbaar zijn en als gevolg daarvan de inzet van deze mogelijkheid uitermate beperkt is.” Dit sluit aan bij de eerdere bekentenissen van voormalig minister Donner en staatssecretaris Teeven dat bij biometrische verificatie van de vingerafdrukken die de

⁸ Zie concept-MvT, pp. 20, 107, 141-142.

⁹ Zie <https://www.privacyfirst.nl/acties/rechtszaken/item/691-rechtszaak-tegen-staat-wegens-illegale-dataspionage.html>.

¹⁰ Art. 90 Grondwet.

laatste jaren zijn afgenomen t.b.v. Nederlandse paspoorten sprake bleek te zijn van een foutenpercentage van maar liefst 21-30%.¹¹ Privacy First doet hierbij dan ook nogmaals de oproep om de afname van vingerafdrukken voor paspoorten per direct af te schaffen.

Conclusie

Het huidige concept-wetsvoorstel komt, in de woorden van het Europees Hof voor de Rechten van de Mens, neer op “destroying democracy on the ground of defending it”.¹² Dit wetsvoorstel dient dan ook grondig verbeterd danwel verworpen te worden. Bij gebreke hiervan behoudt Privacy First zich het recht voor om dit wetsvoorstel, zodra van kracht, door de rechter te laten toetsen en onrechtmatig te laten verklaren.

Privacy First hoopt u met dit advies van dienst te zijn. Desgevraagd zijn wij graag tot een nadere toelichting op bovenstaande punten bereid.

Hoogachtend,

Stichting Privacy First

Vincent A. Böhre
director of operations

¹¹ Zie *Kamerstukken II* 2010/2011, 25764, nr. 47, p. 19 en *Kamerstukken II* 2012/2013, nr. 32317, nr. 163, p. 15.

¹² EHRM, *Klass and others v. Germany* (Appl. no. 5029/71), 6 september 1978, par. 49.