Geachte heer Opstelten,

Namens de DHPA en haar deelnemers treft u hieronder de reactie op het concept-wetsvoorstel tot wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten (hierna: "het wetsvoorstel"), zoals onlangs ter consultatie voorgelegd.[1]

Het wetsvoorstel vormt, onverminderd, een zeer ruime en bijzonder zware inmenging op het recht op privacy, zoals gewaarborgd door de artikelen 7 en 8 van het Handvest, artikel 8 van het EVRM en artikel 10 van de Grondwet. Bij brief van 10 december 2014 heeft de Eerste Kamer aangegeven dat de regering er niet mee kan volstaan om de huidige wet ongewijzigd te handhaven tot het wetsvoorstel is aangenomen. De DHPA deelt deze zienswijze. Genoemde bezwaren kunnen niet met de kleine aanpassingen van het concept wetsvoorstel worden weggenomen. Een structureel andere aanpak is daarvoor nodig.

Toelichting

Burgers en bedrijven vertrouwen hun informatie toe aan online bedrijven, met de verwachting dat hun persoons- en bedrijfsdata afdoende worden beschermd. Hosting bedrijven vormen een essentieel onderdeel van verreweg de meeste waardeketens van online toepassingen. Deelnemers van de DHPA beschermen de hun toevertrouwde data afdoende tegen toegang door onbevoegden.

De overheid heeft zichzelf met de dataretentierichtlijn het recht toegekend om aan hostingbedrijven die aangemerkt worden als leveranciers van telecommunicatiediensten, data op te mogen vragen. Het wetsvoorstel komt onvoldoende tegemoet aan de bezwaren van het Europese Hof van Justitie in het arrest van 8 april 2014, waarin de Dataretentierichtlijn met terugwerkende kracht ongeldig is verklaard.[2] Het door de regering in vervolg daarop gevraagde advies van de Raad van State wordt op belangrijke punten niet gevolgd.[3] Zou het wetsvoorstel in deze vorm worden aangenomen, dan zal dat bij alle burgers het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden. Kortom, de overheid blijkt de zwakste schakel te zijn in de keten van partijen die persoonsgegevens van de betrokkenen bewaren en verwerken. Dat brengt schade toe aan het vertrouwen in de online economie, en bedreigt daarmee één van de weinige sectoren in Nederland die gezonde groei laten zien[4]. Een illustratie van dit effect is een analyse van de schade aan bedrijfsleven in de Verenigde Staten als gevolg van het onzorgvuldig handelen van die overheid.[5]

---

[1] Bijlage bij de brief van Minister Opstelten aan de Tweede Kamer d.d. 17 november 2014, Kamerstukken II 2014/14, 33 542, nr. 16.

[2] HvJEU 8 april 2014, gevoegde zaken C-293/12 en C-594/12 (Digital Rights Ireland/Ireland en Seitlinger)

[3] Advies van 17 juli 2014, bijlage bij de brief van Minister Opstelten aan de Tweede Kamer d.d. 17 november 2014, Kamerstukken II 2014/14, 33 542, nr. 16.

[4] *"Digital Infrastructure in the Netherlands, Driver for the Online Ecosystem", Deloitte, 2014 http://dinl.nl/Digital_Infrastructure_-_Driver_for_the_Online_Ecosystem__2014__v_1_1.pdf*

[5] *"How Much will Prism cost the US Cloud Computing Industry?" A study by the Itif - http://www2.itif.org/2013-cloud-computing-costs.pdf*

Tegelijkertijd is de DHPA zich terdege bewust van het feit dat de overheid middelen tot haar beschikking moet hebben voor opsporing en handhaving in het digitale domein. De sector ontwikkelt en bedenkt met regelmaat initiatieven die bij kunnen dragen aan verbetering van handhaving, en er wordt thans samengewerkt met NCSC/NCTV, THTC, LMIO bij opsporing van cybercrime. In dat licht is het betreurenswaardig dat uw ministerie onvoldoende gebruik maakt van de meermaals door de sector uitgestoken hand, om ook voor opsporing samen effectieve oplossingen te verkennen die recht doen aan vertrouwen en de bescherming van privacy.

Het wetsvoorstel dient dan ook met inachtneming van onderstaande 7 aandachtspunten te worden aangepast. Wij danken mr. F.F. Blokhuis en mr. O.M.B.J. Volgenant van Boekx advocaten voor hun bijdragen, welke wij integraal van hen hebben overgenomen.

De DHPA en haar partners staan onverminderd open voor verdere toelichting en een constructieve samenwerking om oplossingen uit te werken voor opsporing en handhaving in het digitale domein.

December 2014

M. Steltman
Directeur DHPA

--

1. **De wet moet duidelijk en precies zijn en moet voldoende waarborgen bevatten**
   Het wetsvoorstel moet voldoende waarborgen tegen misbruik en willekeur bevatten en moet voldoende duidelijk en precies zijn geformuleerd. Duidelijk moet zijn onder welke omstandigheden en voorwaarden de overheid maatregelen mag inzetten.[6] Het EHRM eist een gedetailleerde wettelijke regeling: *'the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity'.*[7]
   Het Hof van Justitie heeft bepaald dat er minimumregels moeten bestaan om te zorgen *'dat de personen van wie de gegevens zijn bewaard over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens'*, met name wanneer de

[6] EHRM Khan t. VK, 12 mei 2000, appl.nr. 35394/97, par. 26; EHRM Uzun t. Duitsland, 2 september 2010, appl.nr.35623/05, par. 63; EHRM Weber en Saravia (n-o), 29 juni 2006, 54934/00, par. 93; EHRM Liberty and others t. VK, 1 juli 2008, appl.nr. 58243/00, par. 62-63. Of een wettelijke regeling aan deze eisen voldoet, hangt onder meer af van *'the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law.'*

[7] EHRM Weber en Saravia (n-o), 29 juni 2006, 54934/00, par. 94; EHRM Liberty and others t. VK, 1 juli 2008, appl.nr. 58243/00, par. 62-63.

gegevens automatisch worden verwerkt en het risico dat ze op onrechtmatige wijze worden geraadpleegd aanzienlijk is.[8] Het wetsvoorstel voldoet niet aan deze algemene uitgangspunten.

2. **Langdurig opslaan van gegevens van niet-verdachte personen is een schending van de privacy**
   Het wetsvoorstel brengt geen verandering in de praktijk dat er van álle telecommunicerende burgers gegevens worden bewaard, ook van personen bij wie er geen enkele aanwijzing bestaat dat hun gedrag verband heeft met zware criminaliteit. Daarmee blijft de voortdurende grote schending van de privacy voortbestaan. Er wordt geen enkel verband gelegd tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid.

   Het Hof van Justitie heeft de Dataretentierichtlijn ongeldig verklaard omdat die richtlijn de bewaring is niet beperkte tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit, of op personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het voorkomen, opsporen of vervolgen van zware criminaliteit. Het wetsvoorstel bevat desondanks nog al deze elementen.

3. **De bewaarstermijnen zijn te lang**
   Het wetsvoorstel beoogt de huidige bewaartermijnen in stand te houden. Die bewaartermijnen zijn te lang. Nu de Datarententierichtlijn met terugwerkende kracht ongeldig is verklaard, dient de lengte van de bewaartermijn opnieuw te worden bezien, in het licht van het arrest van het Hof van Justitie, de e-privacyrichtlijn, de artikelen 7 en 8 van het Handvest, de artikel 8 en 10 EVRM en artikel 10 van de Grondwet. De regering dient te motiveren welke bewaartermijnen noodzakelijk en proportioneel zijn, mede in het licht van de effectiviteit van de opsporing. Uitgangspunt dient te zijn dat de bewaartermijnen op basis van objectieve criteria worden vastgesteld om te waarborgen dat deze beperkt zijn tot wat strikt noodzakelijk is. De bewaartermijnen dienen in ieder geval substantieel ingekort te worden. Het verschil met de bewaartermijn voor kentekenplaten (4 weken) valt daarbij op.

4. **De voorgestelde rechterlijke toetsing is met onvoldoende waarborgen omgeven**
   De voorgestelde rechterlijke toetsing voldoet niet aan de eisen die de jurisprudentie van het EVRM en het arrest van het Hof van Justitie van 8 april 2014 daaraan stellen. De door de rechter te hanteren criteria zijn niet duidelijk, en ook de procedurele aspecten zijn onvoldoende omschreven.

5. **Geen waarborgen voor geheimhouders**
   Het wetsvoorstel bevat geen waarborgen voor personen die vanuit hun functie een speciale positie als geheimhouder hebben (zoals advocaten, artsen, notarissen en journalisten die hun bronnen moeten beschermen). Voor geheimhouders klemt te meer dat rechterlijke toetsing plaatsvindt voordat de overheid informatie opvraagt die kan leiden tot toegang tot vertrouwelijke informatie. De Nederlandse Staat is al drie maal veroordeeld door het EHRM in zaken over journalistiek brongeheim

[8] Hof van Justitie van de Europese Unie, Digital Rights Ireland en Seitlinger, 8 april 2014, C-293/12 en C594/12, par. 54; EHRM (GK) S en Marper t. VK, 4 december 2008, appl.nrs. 30562/04 en 30566/04, par. 103; EHRM M. K. t. Frankrijk, 18 april 2013, appl.nr. 19522/09, par. 35.

wegens schending van artikelen 8 en 10 EVRM en daarbij is expliciet gewezen op het ontbreken van een voorafgaande rechterlijke toetsing.[9] Tot op heden ontbreekt een dergelijke wettelijke regeling.

6. **Onvoldoende waarborgen met betrekking tot het gebruik van gegevens**
   Het wetsvoorstel dient de kring van personen die de bewaarde gegevens mogen raadplegen en gebruiken te beperken, en dient een strikte binding aan het doel waarvoor de gegevens mogen worden gebruikt te bevatten. Er dienen voorts waarborgen te komen met betrekking tot het vernietigen van gegevens.

7. **Bescherming tegen alle overheidsdiensten is noodzakelijk**
   De wettelijke bescherming dient te gelden tegenover alle overheidsdiensten die zich met onderzoek en opsporing bezighouden. Het wetsvoorstel richt zich echter uitsluitend op strafzaken (OM en politie). Er dient gewaarborgd te worden dat alle overheidsdiensten, inclusief de AIVD, de MIVD en de FIOD, zich hier aan houden.

[9] EHRM, *Voskuil v. Nederland*, 22 november 2007, nr. 64752/01, EHRM, Grote Kamer, Sanoma v. Nederland, 14 september 2010, nr. 38224/03: *First and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial decision-making body. (…) It is clear, in the Court's view, that the exercise of any independent review that only takes place subsequently to the handing over of material capable of revealing such sources would undermine the very essence of the right to confidentiality,* en EHRM, *Telegraaf v. Nederland*, 22 november 2012, nr. 39315/06: *Review post factum (…) cannot restore the confidentiality of journalistic sources once it is destroyed. The Court thus finds that the law did not provide safeguards appropriate to the use of powers of surveillance against journalists with a view to discovering their journalistic sources. There has therefore been a violation of Articles 8 and 10 of the Convention.*