

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2992

Vragen van het lid **Gesthuizen** (SP) aan de ministers van Veiligheid en Justitie en van Economische Zaken over *het bericht dat online zoeken naar gezondheidsgelateerde informatie privacyrisico's met zich meebrengt* (ingezonden 16 juli 2013).

Antwoord van minister **Kamp** (Economische Zaken), mede namens de minister van Veiligheid en Justitie (ontvangen 20 augustus 2013).

Vraag 1

Wat is uw reactie op het artikel «Online zoeken naar herpes is privacyrisico», waarin wordt belicht dat het online zoeken naar gezondheidsgelateerde informatie privacyrisico's met zich meebrengt?¹

Antwoord 1

Uit de onlangs aan uw Kamer verzonden brief met de Kabinetvisie op e-privacy, moge blijken dat het kabinet sterk hecht aan een doeltreffende bescherming van persoonsgegevens en de persoonlijke levenssfeer van internetgebruikers. Controle, transparantie en verantwoordelijkheid van bedrijven zijn essentiële randvoorwaarden en zijn bovendien bepalend voor de mate waarin bedrijven, organisaties en instellingen bijdragen aan het digitale vertrouwen van betrokkenen in online diensten. Het in het artikel besproken onderzoek van de Universiteit van Zuid-Californië over «tracking» cookies heeft betrekking op Amerikaanse websites en de daar geldende wet- en regelgeving. In Nederland zijn gegevens die kunnen worden herleid tot een identificeerbaar persoon (persoonsgegevens) beschermd door de Wet bescherming persoonsgegevens (hierna Wbp). Gezondheidsgelateerde persoonsgegevens worden in artikel 16 van deze wet aangemerkt als bijzondere persoonsgegevens en extra beschermd vanwege hun grotere privacygevoeligheid. Als gegevens over het zoeken van gezondheidsgelateerde informatie op internet kunnen worden gekoppeld aan de persoon die naar deze informatie heeft gezocht, kan er sprake zijn van een persoonsgegeven betreffende iemands gezondheid. Dergelijke persoonsgegevens mogen alleen onder de voorwaarden uit artikel 21 of 23 van de Wbp worden verwerkt. Voor de in het artikel beschreven situatie houdt dit voor zover ik kan beoordelen in dat

¹ https://www.security.nl/artikel/46970/1/%27Online_zoeken_naar_herpes_is_privacyrisico%27.html

dergelijke gegevens, indien deze herleid kunnen worden tot een identificeerbaar persoon, alleen met uitdrukkelijke toestemming van de betrokkene mogen worden verwerkt.

De zogenaamde cookiebepaling (artikel 11.7a Telecommunicatiewet (Tw)) bepaalt dat voor het plaatsen en lezen van cookies toestemming nodig is van de internetter en dat deze toestemming moet worden verkregen nadat de internetter hierover duidelijk en volledig is geïnformeerd. Voor «tracking» cookies, waarmee het surfgedrag van internetgebruikers kan worden gevolgd, geldt per januari 2013 het bij amendement Van Bommel/Van Dam geïntroduceerde rechtsvermoeden dat hierbij sprake is van verwerking van persoonsgegevens. De plaatser van tracking cookies zal dan ook aan de Wbp moeten voldoen, tenzij hij kan aantonen dat hij géén persoonsgegevens verwerkt.

Vraag 2

Deelt u de mening van de onderzoeker dat de vertrouwelijkheid van het zoeken naar gezondheidsgerelateerde informatie wordt bedreigd door het lekken van informatie aan derde partijen? Zo nee, waarom niet?

Antwoord 2

De vertrouwelijkheid wordt inderdaad geschonden wanneer een site, waarop een internetgebruiker zoekt naar gezondheidsgerelateerde informatie, tot de gebruiker herleidbare informatie over dit zoekgedrag met derden deelt zonder dat aan de in antwoord 1 genoemde voorwaarden is voldaan.

Vraag 3

Zijn er Nederlandse providers, adverteerders en websites die met behulp van «tracking» codes persoonsgevoelige informatie van de internetgebruiker achterhalen om deze vervolgens te lekken of te verkopen aan een derde partij? Zo ja, welke risico's lopen de Nederlandse internetgebruikers?

Antwoord 3

Het College bescherming persoonsgegevens (CBP) en de Autoriteit Consument en Markt (ACM) werken sinds 1 januari 2013 nauw samen in onderzoeken naar tracking cookies. Het CBP heeft op dit moment een aantal onderzoeken onderhanden waarin (ook) de (eventuele) verwerking van persoonsgegevens bij het gebruik van tracking cookies wordt beoordeeld. Over deze lopende onderzoeken kan het CBP geen nadere mededelingen doen.

Via tracking cookies verkregen informatie over het surfgedrag kan inzicht bieden in de interesses en (afgeleide) belangstelling van mensen. Dergelijke informatie raakt aan de inhoud van hun communicatiegedrag en kan gebruikt worden om mensen anders te behandelen dan anderen. Verder zijn bij het gebruik van tracking codes op websites of apps veelal derde partijen betrokken, zoals advertentienetwerken. In zijn algemeenheid geldt dat hoe meer partijen toegang hebben tot de genoemde informatie, hoe groter het risico wordt op een datalek of een andere vorm van onrechtmatige gegevensverwerking.

Vraag 4

Bent u, indien ook in Nederland gezondheidsgerelateerde informatie wordt gelekt, voornemens hier tegen op te treden? Zo ja, welke middelen kunt u inzetten om dit te voorkomen? Bent u daarnaast voornemens de Nederlandse internetgebruiker te informeren over deze handelwijze?

Antwoord 4

De ACM ziet toe op de naleving van de Tw. Het CBP ziet toe op de verwerking van persoonsgegevens overeenkomstig het bepaalde bij de Wbp en andere wet- en regelgeving op grond waarvan persoonsgegevens worden verwerkt. Zij beschikken daartoe over diverse bevoegdheden, waaronder het opleggen van een last onder dwangsom of een sanctie. ACM informeert op <http://www.consuwijzer.nl/telecom-post/internet/privacy/uitleg-cookies> over het gebruik van cookies. Het CBP informeert op www.mijnprivacy.nl over het gebruik van (bijzondere) persoonsgegevens.