

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING

Samenvatting van het advies van de Europese Toezichthouder voor gegevensbescherming over online-manipulatie en persoonsgegevens

(De volledige tekst van dit advies is beschikbaar in het Engels, Frans en Duits op de EDPS-website:
www.edps.europa.eu)

(2018/C 233/06)

De digitalisering van de maatschappij en de economie heeft een wisselend effect op de deelname van burgers aan de besluitvorming en op belemmeringen voor betrokkenheid van het publiek bij democratische processen.

Met big data analytics en kunstmatige-intelligentiesystemen kunnen enorme hoeveelheden gegevens verzameld, gecombineerd, geanalyseerd en onbeperkt opgeslagen worden. In de afgelopen twee decennia is voor de meeste internetdiensten een dominant bedrijfsmodel ontstaan waarmee mensen online worden gevolgd en hun persoonsgegevens worden verzameld, onder andere over hun gezondheid, relaties, gedachten en overtuigingen. Doel is geld verdienen aan digitale reclame. De digitale markten concentreren zich rond enkele ondernemingen die optreden als effectieve poortwachters voor het internet en die hogere voor inflatie gecorrigeerde marktkapitalisatiewaarden noteren dan elk ander bedrijf in het verleden.

Dit digitale ecosysteem heeft via internet mensen over de hele wereld met elkaar verbonden — meer dan 50 % van de wereldbevolking, hoewel de cijfers sterk variëren naargelang wordt gemeten naar geografie, welvaart of geslacht. Het aanvankelijke optimisme over de mogelijkheden van internettools en sociale media voor burgerparticipatie heeft plaats gemaakt voor ongerustheid dat mensen worden gemanipuleerd, eerst via het constant binnenhalen van vaak zeer persoonlijke informatie over hen en vervolgens door het uitoefenen van controle over de informatie die zij online zien, afhankelijk van de categorie waarin zij zijn ingedeeld. Het viraal gaan van op algoritmen gebaseerde diensten is een belangrijke aanjager van waarde. Producten en toepassingen worden ontworpen om maximale aandacht te trekken en een dusdanig sterke behoefte te creëren dat consumenten niet meer zonder lijken te kunnen. Verbondenheid heeft, althans in het huidige model, geleid tot verdeeldheid.

Dit heeft een discussie op gang gebracht die draait om misleidende, onjuiste of hatelijke „content” richting het publiek bedoeld om het politieke discours en verkiezingen te beïnvloeden, een verschijnsel dat met termen als „nepnieuws” of „online-desinformatie” wordt aangeduid. Oplossingen zijn vooral gericht op betere transparantie. Daarbij wordt de informatiebron weliswaar blootgelegd maar blijven actoren in het ecosysteem die garen spinnen bij schadelijk gedrag, buiten schot. Ondertussen zorgen de marktconcentratie in de sector en de opkomst van dominante platforms voor nieuwe dreigingen voor het pluralisme in de media. Het digitale ecosysteem kampt met een vertrouwenscrisis die volgens de Europese Toezichthouder voor gegevensbescherming (EDPS) illustreert dat privacy en vrijheid van meningsuiting onderling afhankelijk zijn. Het is een onvermijdelijk gegeven dat overheden en bedrijven mensen digitaal volgen. Dit schaadt de privacy en creëert een klimaat waarin mensen minder geneigd zijn vrijelijk meningen te uiten en contacten aan te gaan, ook in het publieke domein, iets wat essentieel is voor een gezonde democratie. Vandaar dit advies, dat gaat over de wijze waarop persoonsgegevens van individuen en groepen worden gebruikt om diezelfde individuen en groepen gericht te benaderen met specifieke content (microtargeting). Daarnaast wordt aandacht besteed aan de fundamentele rechten en waarden die op het spel staan, en aan toepasselijke wetgeving om aan de dreigingen het hoofd te bieden.

De EDPS pleit er al jaren voor dat gegevensbeschermingsautoriteiten en andere toezichthouders meer samenwerken om de rechten en belangen van individuen in de digitale samenleving te waarborgen. Daarom hebben wij in 2017 het Digital Clearinghouse opgericht. Vanwege de bezorgdheid dat voor politieke campagnes digitale ruimte kan worden benut om wetgeving te omzeilen⁽¹⁾, zijn wij van mening dat het tijd is om ook instituten die toezicht houden op verkiezingen en audiovisuele media bij deze samenwerking te betrekken.

1. WAAROM DIT ADVIES?

i. Felle, aanhoudende maatschappelijke discussie

Er woedt een felle maatschappelijke discussie over de invloed die het grote en complexe ecosysteem van digitale informatie uitoefent op zowel de markteconomie als de politieke economie, en over de wisselwerking tussen de politieke omgeving en de economie. De grote platforms vormen het middelpunt van dit ecosysteem. Zij profiteren onevenredig veel van de groei in digitale reclame en worden gaandeweg steeds machtiger. Persoonsgegevens zijn nodig om boodschappen te segmenteren naar, te richten op en op maat te snijden voor individuen. De meeste adverteerders weten echter niet hoe de besluitvorming daaromtrent plaatsvindt, en de meeste mensen weten niet hoe persoonsgegevens worden gebruikt. Het systeem belooft sensationele content die viraal gaat en maakt in het algemeen geen onderscheid tussen zakelijke en politieke adverteerders. Nu bekend is geworden hoe doelbewust desinformatie („nepnieuws”) via

⁽¹⁾ Zie bijvoorbeeld <http://www.independent.co.uk/news/uk/politics/election-2017-facebook-ads-marginal-seats-tories-labour-outdated-election-spending-rules-a7733131.html> (bezoekt op 18.3.2018).

dit systeem wordt verspreid, is de angst ontstaan dat de integriteit van democratieën in gevaar komt. Ook de markt voor kunstmatige-intelligentiesystemen wordt gekenmerkt door concentratie. Het zijn systemen die zelf door gegevens worden gevoed en die — als er niet wordt ingegrepen — de besluitvorming in deze omgeving steeds diffuser maken en het zicht ontnemen op degenen die op besluiten kunnen worden aangesproken.

ii. Belang van wetgeving inzake gegevensbescherming en politieke campagnes

Het is duidelijk dat de fundamentele rechten inzake privacy en gegevensbescherming een cruciale factor zijn bij inspanningen om verbetering in deze situatie te brengen. Dit maakt van deze kwestie een strategische prioriteit voor alle onafhankelijke gegevensbeschermingsautoriteiten. De toezichthouders inzake gegevensbescherming hebben in 2005 de *Resolution on the Use of Personal Data for Political Communication (besluit inzake het gebruik van persoonsgegevens voor politieke communicatie)* uitgebracht, waarin zij hun bezorgdheid verwoorden over belangrijke wereldwijde vraagstukken op het gebied van gegevensbescherming in verband met de toenemende verwerking van persoonsgegevens door niet-commerciële actoren. In het besluit wordt specifiek aandacht geschonken aan de verwerking van gevoelige gegevens in verband met echte of veronderstelde morele en politieke overtuigingen of met stemactiviteiten, en aan vergaande profilering van verschillende personen die momenteel — soms onnauwkeurig of op basis van een oppervlakkig contact — worden bestempeld als sympathisanten, aanhangers, voorstanders of partijleden⁽¹⁾. Ook wordt opgeroepen tot striktere handhaving van de voorschriften inzake gegevensminimalisering, rechtmatige verwerking, toestemming, transparantie, rechten van betrokkenen, doelbinding en gegevensbescherming. Het is wellicht tijd om deze oproep opnieuw kracht bij te zetten.

De EU-wetgeving inzake gegevensbescherming en vertrouwelijkheid van elektronische communicatie is van toepassing op gegevensverzameling, profilering en microtargeting. Als deze wetgeving naar behoren wordt gehandhaafd zou dat moeten helpen de schade door pogingen om individuen en groepen te manipuleren, zo veel mogelijk te beperken. Politieke partijen die gegevens van kiezers in de EU verwerken, vallen binnen de werkingssfeer van de Algemene Verordening Gegevensbescherming (AVG). Op grond van de AVG worden persoonsgegevens waaruit politieke overtuigingen blijken, als speciale gegevenscategorieën aangemerkt. Het is in het algemeen verboden om deze gegevens te verwerken, tenzij een van de genoemde uitzonderingen van toepassing is. In het kader van politieke campagnes zijn de volgende twee uitzonderingen van dusdanig groot belang dat ze hier voluit worden geciteerd:

- „d) de verwerking wordt verricht door een stichting, een vereniging of een andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is, in het kader van haar gerechtvaardigde activiteiten en met passende waarborgen, mits de verwerking uitsluitend betrekking heeft op de leden of de voormalige leden van de instantie of op personen die in verband met haar doeleinden regelmatig contact met haar onderhouden, en de persoonsgegevens niet zonder de toestemming van de betrokkenen buiten die instantie worden verstrekt;
- e) de verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt [...];
- g) de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene.”

Overweging 56 verduidelijkt artikel 9, lid 2, onder g): „Als het bij verkiezingsactiviteiten voor de goede werking van de democratie in een lidstaat vereist is dat politieke partijen persoonsgegevens over de politieke opvattingen van personen verzamelen, kan de verwerking van zulke gegevens op grond van een algemeen belang worden toegestaan, mits er passende waarborgen worden vastgesteld.”

Diverse gegevensbeschermingsautoriteiten hebben regels of richtsnoeren opgesteld voor de verwerking van gegevens voor politieke doeleinden:

- In maart 2014 heeft de Italiaanse autoriteit voor gegevensbescherming regels vastgesteld inzake de verwerking van persoonsgegevens door politieke partijen. De regels leggen de nadruk op het verbod tot gebruik van persoonsgegevens die op internet openbaar zijn gemaakt — zoals gegevens op sociale netwerken of fora — ten behoeve van politieke communicatie, indien deze gegevens voor andere doeleinden waren verzameld⁽²⁾.
- In november 2016 heeft de Franse nationale commissie voor gegevensbescherming (CNIL) aanvullende richtsnoeren uitgebracht voor haar aanbevelingen uit 2012 inzake politieke communicatie, waarin de regels worden vastgesteld voor de verwerking van persoonsgegevens op sociale netwerken. De CNIL heeft met name onderstreept dat de aggregatie van persoonsgegevens van kiezers om profielen van hen op te stellen en ze te benaderen op sociale netwerken slechts rechtmatig kan zijn wanneer ze gebaseerd is op toestemming als grond voor de gegevensverwerking⁽³⁾.

⁽¹⁾ Het besluit is beschikbaar op <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Personal-Data-for-Political-Communication.pdf> (bezoekt op 18.3.2018).

⁽²⁾ <http://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267> „Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale”, bekendgemaakt in het Publicatieblad van de Italiaanse gegevensbeschermingsautoriteit, nummer 71, 26.3.2014 (doc. web n. 3013267).

⁽³⁾ <https://www.cnil.fr/fr/communication-politique-queles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux> „Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?”, gepubliceerd door de Commission Nationale de l'informatique et des libertés (Franse nationale commissie voor informatica en vrijheden), 8.11.2016.

- In april 2017 heeft Britse privacytoezichthouder ICO (Information Commissioner's Office) een bijgewerkte versie uitgebracht van de *Guidance on political campaigning*, waarin ook richtsnoeren zijn opgenomen voor het gebruik van data-analyse bij het voeren van politieke campagnes. Het ICO legde uit dat als een politieke organisatie aan een derde partij opdracht geeft om data-analyses uit te voeren, de onderneming in kwestie waarschijnlijk een gegevensverwerker is en de organisatie een voor de verwerking verantwoordelijke. Voor een rechtmatige verwerking moet rekening worden gehouden met specifieke bepalingen van de wet inzake gegevensbescherming over de rolverdeling tussen de verantwoordelijke en de verwerker⁽¹⁾.

De richtsnoeren van de nationale gegevensbeschermingsautoriteiten kunnen voorzien in een aanvullende gezaghebbende uitlegging van wetgevingsbepalingen op het gebied van gegevensbescherming en privacy die de verschillen verklaart in de inrichting van nationale politieke systemen⁽²⁾.

iii. Doel van dit EDPS-advies

De EDPS wil de EU helpen een voorbeeldfunctie te vervullen in de internationale discussie over gegevensbescherming en privacy in het digitale tijdperk door interdisciplinaire beleidsoplossingen aan te reiken voor big data-uitdagingen en een ethische dimensie te ontwikkelen voor de verwerking van persoonsgegevens⁽³⁾. Wij hebben gevraagd de betrokkene te behandelen „als een individu en niet enkel als consument of gebruiker” en de nadruk gelegd op ethische vraagstukken omtrent de gevolgen van het opstellen van voorspellende profielen en via algoritmes bepaalde personalisatie⁽⁴⁾. Wij hebben gevraagd om een verantwoordelijke en duurzame ontwikkeling van de digitale samenleving waarin de burger de regie over zijn of haar eigen persoonsgegevens voert, rekening wordt gehouden met de persoonlijke levenssfeer van betrokkenen, rekenschap wordt afgelegd en de regels op coherente wijze worden gehandhaafd⁽⁵⁾. De Ethics Advisory Group van de EDPS stelt in haar rapport van januari 2018 dat „microtargeting bij verkiezingscampagnes de regels van het spreken in het openbaar verandert en de ruimte voor discussie en uitwisseling van ideeën kleiner maakt. Er moet dan ook dringend een democratisch debat worden gevoerd over de inzet en het gebruik van gegevens voor politieke campagnes en besluitvorming⁽⁶⁾.”

Het gebruik van informatie en persoonsgegevens om mensen en de politiek te manipuleren is een vraagstuk dat uiteraard veel meer omvat dan het recht op gegevensbescherming. Een met microtargeting gepersonaliseerde online-omgeving zorgt voor een filterbubbel waarin mensen worden blootgesteld aan informatie die „meer van hetzelfde” is en minder pluriforme meningen bevat. Deze omgeving leidt tot meer politieke en ideologische polarisering⁽⁷⁾ en is een voedingsbodem voor onwaarheden en complottheorieën⁽⁸⁾. Uit onderzoek blijkt dat de manipulatie van nieuws dat mensen voorgeschoteld krijgen of zoekresultaten hun stemgedrag kan of kunnen beïnvloeden⁽⁹⁾.

De EDPS wil ertoe bijdragen dat, in de woorden van de AVG, de verwerking van persoonsgegevens ten dienste staat van de mens, en niet andersom⁽¹⁰⁾. De technologische vooruitgang zou niet belemmerd maar eerder overeenkomstig onze

⁽¹⁾ https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf Information Commissioner's Office „Guidance on political campaigning” (20170426).

⁽²⁾ Artikel 57, lid 1, onder d), van de AVG bepaalt dat elke toezichthoudende autoriteit op haar grondgebied „de verwerkingsverantwoordelijken en de verwerkers beter bekend [maakt] met hun verplichtingen uit hoofde van deze verordening”.

⁽³⁾ Zie *Leading by Example: The EDPS Strategy 2015-2019*, blz. 17. Met de term „big data” wordt naar onze mening verwezen naar de praktijk waarin grote hoeveelheden informatie afkomstig uit verschillende bronnen worden gecombineerd en geanalyseerd, vaak met behulp van zelflerende algoritmen, om weldoordachte besluiten te nemen. Een van de belangrijkste waarden van big data voor ondernemingen en overheden is afgeleid van de monitoring van menselijk gedrag, zowel gezamenlijk als individueel: het voorspellende potentieel; Advies 4/2015 van de EDPS, Naar een nieuwe digitale ethiek: data, waardigheid en technologie, 11.9.2015, blz. 6.

⁽⁴⁾ Het gevaar van profielen die worden gebruikt om het gedrag van mensen te voorspellen is dat ze stigmatiserend kunnen zijn en bestaande stereotypen, sociale en culturele segregatie en uitsluiting kunnen versterken, waarbij deze „collectieve inlichtingen” de individuele keuze en gelijke kansen ondermijnen. Deze „filterbubbels” of „persoonlijke echoruimten” kunnen ertoe leiden dat de creativiteit, innovatie, vrijheid van meningsuiting en vrijheid van vereniging worden onderdrukt die er juist voor hebben gezorgd dat de digitale technologie tot bloei kon komen; Advies 4/2015 van de EDPS, blz. 13 (verwijzingen weggelaten).

⁽⁵⁾ Advies 7/2015 van de EDPS, Het hoofd bieden aan de uitdagingen van big data, blz. 9.

⁽⁶⁾ Rapport van de Ethics Advisory Group van de EDPS, januari 2018, blz.28.

⁽⁷⁾ Zie bijvoorbeeld *The Economist*, How the World Was Trolled (november 4-10, 2017), Vol. 425, No 9065, blz. 21-24.

⁽⁸⁾ Allcott H. en Gentzkow M., *Social Media and Fake News in the 2016 Election* (voorjaar 2017). Stanford University, *Journal of Economic Perspectives*, Vol. 31, No. 2, blz. 211-236. <https://web.stanford.edu/~gentzkow/research/fakenews.pdf>, blz. 219.

⁽⁹⁾ In een van de experimenten werd gebruikers van sociale platforms verteld hoe hun vrienden naar eigen zeggen hadden gestemd, wat zorgde voor een statistisch significante stijging van het populatiesegment (0,14 % van de populatie op stemgerechtigde leeftijd, ofwel ca. 340 000 kiezers) dat bij de tussentijdse verkiezingen in 2010 voor het Congres een stem uitbracht; Allcott H. en Gentzkow M., *Social Media and Fake News in the 2016 Election* (voorjaar 2017), Stanford University, *Journal of Economic Perspectives*, Vol. 31, No. 2, blz. 211-236., blz. 219). In een andere studie stelden de onderzoekers dat verschillen in zoekresultaten van Google konden resulteren in een verschuiving van 20 % in voorkeuren bij zwevende kiezers; Zuiderveen Borgesius, F. & Trilling, D. & Möller, J. & Bodó, B. & de Vreese, C. & Helberger, N. (2016). Should we worry about filter bubbles?. *Internet Policy Review*, 5(1). DOI: 10.14763/2016.1.401, blz. 9.

⁽¹⁰⁾ Overweging 4 van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, hierna „AVG” genoemd.

waarden gestuurd moeten worden. De eerbiediging van fundamentele rechten, met inbegrip van het recht op gegevensbescherming, is van cruciaal belang om eerlijke verkiezingen te waarborgen, zeker met het oog op de verkiezingen voor het Europees Parlement in 2019 ⁽¹⁾. Dit EDPS-advies is het laatste in een reeks van brede visies op de vraag hoe gegevensbescherming moet worden toegepast voor de aanpak van de meest dringende zorgen met betrekking tot het overheidsbeleid. Het bouwt voort op eerder werk van de EDPS betreffende big data en digitale ethiek en de noodzaak om de regulering van concurrerende en eerlijke markten te coördineren ⁽²⁾. Het advies begint met een samenvatting van het proces waarin persoonsgegevens de bepalende factor zijn in en de brandstof vormen voor de heersende cyclus van „digital tracking”, microtargeting en manipulatie. Daarna wordt ingegaan op de rollen die de verschillende actoren vervullen in het ecosysteem van digitale informatie, waarbij aandacht wordt geschonken aan de fundamentele rechten die op het spel staan en de gegevensbeschermingsbeginselen en wettelijke verplichtingen die van toepassing zijn. Het advies sluit af met de stelling dat online-manipulatie een probleem is dat waarschijnlijk alleen maar groter wordt, dat geen enkele op zichzelf staande aanpak toereikend zal zijn en dat de toezichthouders daarom zo snel mogelijk moeten samenwerken om zowel gelokaliseerde misstanden als structurele verstoringen die voortvloeien uit de buitensporige marktconcentratie aan te pakken.

7. CONCLUSIE

Online-manipulatie vormt een bedreiging voor de samenleving omdat filterbubbels en gesloten gemeenschappen het voor mensen moeilijker maken elkaar te begrijpen en ervaringen uit te wisselen. De afname van verbondenheid in de maatschappij kan de democratie en de bijbehorende fundamentele rechten en vrijheden ondermijnen. Online-manipulatie is ook een symptoom van het diffuse beeld van en het gebrek aan verantwoordingsplicht in het digitale ecosysteem. Het probleem is reëel en urgent en wordt waarschijnlijk erger naarmate meer mensen en dingen verbonden raken met het internet en kunstmatige-intelligentiesystemen een grotere rol gaan spelen. De hoofdoorzaak van het probleem is voor een deel gelegen in onverantwoordelijk, onrechtmatig of onethisch gebruik van persoonsgegevens. Transparantie is noodzakelijk, maar er is meer nodig. Contentbeheer kan noodzakelijk zijn maar mag niet ten koste gaan van fundamentele rechten. Een deel van de oplossing is daarom gelegen in strikte handhaving van de bestaande regelgeving, met name de AVG, en in toepasselijke normen op het gebied van verkiezingen en mediapluralisme.

Om het debat vooruit te helpen zal de EDPS in het voorjaar van 2019 een workshop houden waar nationale toezichthouders op het gebied van gegevensbescherming, verkiezingsrecht en audiovisuele wetgeving zich zullen kunnen buigen over de genoemde wisselwerkingen, de uitdagingen waarvoor zij zich gesteld zien en mogelijkheden voor gezamenlijke acties, ook met het oog op de komende verkiezingen voor het Europees Parlement.

In dit advies wordt betoogd dat technologie en gedragingen in de markt voor schade zorgen vanwege structurele onevenwichtigheden en disrupties. Wij hebben gevraagd om bijstelling van de stimulansen voor innovatie. De techreuzen en pioniers hebben er profijt van gehad dat zij tot nu toe in een relatief ongereguleerde omgeving hebben kunnen opereren. Traditionele sectoren en basisconcepten van territoriale bevoegdheid, soevereiniteit, sociale normen en de democratie hebben schade opgelopen. Zij voorzien in waarden die afhankelijk zijn van pluriformiteit van stemmen en evenwicht tussen partijen. Geen enkele speler kan dit probleem alleen aanpakken. Gegevensbescherming is een deel van de oplossing; misschien wel een groter deel dan gedacht. Het volstaat niet te vertrouwen op de goede wil van zakelijke actoren die uiteindelijk geen verantwoording hoeven af te leggen. We moeten nu ingrijpen om de digitaliseringskoek beter te verdelen.

Brussel, 19 maart 2018.

Giovanni BUTTARELLI

Europese Toezichthouder voor gegevensbescherming

⁽¹⁾ In de zaak *Orlovskaya Iskra t. Rusland* heeft het Europees Hof voor de Rechten van de Mens geoordeeld dat „vrije verkiezingen, de vrijheid van meningsuiting en met name de vrijheid van politiek debat aan de basis liggen van ieder democratisch systeem. Deze twee rechten zijn onderling verbonden en versterken elkaar. Zo is bijvoorbeeld de vrijheid van meningsuiting een van de noodzakelijke „voorwaarden voor de vrije meningsuiting van het volk bij het kiezen van de wetgevende macht”. Het is dan ook van groot belang dat in de aanloop naar verkiezingen allerlei standpunten en informatie vrijelijk kunnen circuleren. In het kader van verkiezingsdebatten is het van bijzonder belang dat kandidaten de vrijheid van meningsuiting ongehinderd kunnen uitoefenen” (verwijzingen weggelaten uit de tekst), punt 110, <http://hudoc.echr.coe.int/eng?i=001-171525>

⁽²⁾ 2014 — Voorlopig advies over privacy en concurrentievermogen in het tijdperk van big data; 2015 — Advies 4/2015 Naar een nieuwe digitale ethiek: data, waardigheid en technologie; 2015 — Advies 7/2015 Het hoofd bieden aan de uitdagingen van big data: een oproep tot transparantie, gebruikerscontrole, ingebouwde gegevensbescherming en verantwoording; 2016 — Advies 8/2016 Advies van de EDPS inzake een doeltreffende handhaving in de digitale economie.