Online politieke microtargeting

Een zegen of een vloek voor de democratie?

Zuiderveen Borgesius, F.J.; Möller, J.; Dobber, T.; Kruikemeier, S.; Irion, K.; Stapel, S.; Fathaigh, R.; Bodo, B.; de Vreese, C.

Published in:
Nederlands Juristenblad

Online politieke microtargeting

Een zegen of een vloek voor de democratie?

Frederik J. Zuiderveen Borgesius, Judith Möller, Tom Dobber, Sanne Kruikemeier, Kristina Irion, Sarah Stapel, Ronan Fathaigh, Balazs Bodo, Claes de Vreese[1]

Voor online politieke microtargeting wordt het online-gedrag van mensen in kaart gebracht en worden de verzamelde gegevens gebruikt om mensen gerichte politieke advertenties te tonen. Microtargeting is vanuit de VS komen overwaaien naar Europa en heeft voor- en nadelen voor de democratie. Microtargeting kan politieke partijen helpen om mensen effectief te bereiken en kan politieke betrokkenheid stimuleren. Maar microtargeting kan ook een bedreiging vormen voor de democratie. Zo kan een politieke partij zich verschillend voordoen aan verschillende mensen. Bovendien bedreigt het verzamelen van persoonsgegevens onze privacy. Dit artikel brengt de beloftes en bedreigingen van microtargeting voor de democratie in kaart en schetst mogelijkheden voor beleidsmakers om het gebruik van microtargeting te reguleren.

1. Inleiding

Politieke campagnes combineren steeds vaker kiezersonderzoek met gepersonaliseerde politieke reclame: online politieke microtargeting, of kortweg: microtargeting. Met microtargeting kan een politieke partij stemgerechtigden identificeren die makkelijk te beïnvloeden zijn. Een politieke partij kan daarmee haar boodschap afstemmen op de specifieke interesses van kiezers. Microtargeting wordt voornamelijk toegepast in de Verenigde Staten maar wint nu ook aan populariteit in Nederland en de rest van Europa.[2]

Microtargeting is een vorm van gepersonaliseerde communicatie waarbij persoonsgegevens worden verzameld die vervolgens worden gebruikt voor gerichte politieke advertenties. Gerichte advertenties kunnen worden toegespitst op specifieke individuen. Politieke partijen verwachten dat gerichte advertenties effectievere zijn dan ongerichte advertenties.

Microtargeting kan een zegen en een vloek zijn voor de democratie. Microtargeting kan de politieke betrokkenheid van de stemgerechtigden vergroten en hun kennis over specifieke onderwerpen verdiepen. Maar microtargeting brengt ook risico's met zich mee. Zo kan een partij zich voordoen als een *one issue*-partij, maar steeds met andere issues voor verschillende stemgerechtigden, waardoor het onduidelijk wordt wat een partij precies belooft. Verder roept microtargeting zorgen op omtrent privacy.

Dit artikel richt zich op de volgende vragen: wat is microtargeting en wat zijn de voor- en nadelen voor onze democratie? Dit artikel combineert inzichten uit de juridische en sociaalwetenschappelijke disciplines. Par. 2 introduceert online politieke microtargeting. Par. 3 bespreekt de beloftes van microtargeting en par. 4 de bedreigingen. Par. 5 bespreekt waarom de bedreigingen (hoe belangrijk ze ook zijn), niet overdreven moeten worden. Par. 6 verkent hoe beleidsmakers zouden kunnen ingrijpen, en par. 7 sluit af.[3]

2. Online politieke microtargeting

Microtargeting kan gezien worden als politieke *behavioural targeting*. Voor de marketingtechniek *behavioural targeting* volgen bedrijven het online-gedrag van mensen en gebruiken de verzamelde informatie om hen gerichte advertenties te tonen.[4] Vaak spitsen politieke partijen boodschappen toe op individuele kiezers door hun interesses te voorspellen op grond van grote hoeveelheden persoonsgegevens.[5]

Microtargeting is vanuit de VS komen overwaaien naar Europa. Politieke partijen in het Verenigd Koningrijk maakten al bij de verkiezingen in 2015 gebruik van microtargeting.[6] De Labour Party, de Conservative Party en de Liberal Democrats hebben met hulp van consultants en data-handelaren kiezersdatabanken gebouwd.[7] Het microtargetingbedrijf *Cambridge Analytica* wordt ervan

beschuldigd het Brexit-referendum te hebben beïnvloed.[8] In Nederland gebruikten politieke partijen tijdens de Tweede Kamerverkiezingen van 2017 vooral Facebook om de kiezer op maat gemaakte boodschappen te sturen. Partijen verschillen onderling in *hoe* ze Facebook gebruiken. Sommige partijen richten zich via het platform op wat algemenere groepen (zoals boeren), andere maken ook gebruik van *lookalike audiences*. Hiermee kan een partij een lijst emailadressen of telefoonnummers uploaden naar Facebook. Facebook gaat vervolgens geautomatiseerd op zoek naar gebruikers die qua online gedrag en eigenschappen lijken op de geüploade personen. Het idee achter deze functie is dat politieke partijen emailadressen van bijvoorbeeld hun eigen leden uploaden. Facebookgebruikers die lijken op deze mensen zullen deze politieke partijen waarschijnlijk ook een warm hart toedragen en daarmee openstaan voor hun politieke boodschap.[9]

Nederlandse politieke partijen targeten kiezers ook buiten Facebook om. Zo richtte Denk zich op mensen die met een Lebara-simkaart bellen. De partij Denk neemt hierbij aan dat vooral de eigen achterban (Nederlanders met een niet-westerse achtergrond) een dergelijke simkaart bezitten. Met de simkaart kun je immers goedkoop naar buiten de EU bellen.[10] Op deze manier kan Denk met zijn kiezers communiceren zonder geld en moeite te besteden aan mensen die toch nooit op Denk zullen stemmen (bijvoorbeeld witte welgestelde senioren). Een volgende stap kan zijn, zoals Denk lijkt te hebben overwogen, om een nepadvertentie naar deze simkaartbezitters te versturen met als doel de achterban te mobiliseren op verkiezingsdag.[11]

In 2019 vinden de Europese Parlementsverkiezingen plaats. Doordat de kieslijsten nationaal zijn en de overkoepelende fracties (zoals bijvoorbeeld 'ALDE', waar VVD en D66 toe behoren) weinig bekendheid genieten, is het onwaarschijnlijk dat er een gecoördineerde microtargetingcampagne op touw wordt gezet. Waarschijnlijker is het dat nationale politieke partijen hun eigen kandidaten en standpunten aanprijzen, op een vergelijkbare manier als bij landelijke verkiezingen. Partijen kunnen wel op EU-niveau samenwerken door gezamenlijk diensten, data en kennis in te kopen.

3. Beloftes

In dit deel bespreken we de belangrijkste voor- en nadelen van microtargeting. We onderscheiden voor- en nadelen voor burgers, politieke partijen en het publieke debat. Tabel 1 geeft een overzicht van de beloftes en bedreigingen van microtargeting.

Tabel 1.
Mogelijke voor- en nadelen van microtargeting voor burgers, partijen, en de publiek debat.

	Voordelen	Nadelen
Burgers	• Relevantere politieke advertenties • Bereiken van groepen die anders moeilijk te bereiken zijn	• Inbreuk op privacy • Manipulatie van kiezers • Negeren van groepen kiezers
Politieke partijen	• Goedkoop (sommige soorten microtargeting) • Efficiënt • Effectief	• Duur (sommige soorten microtargeting) • Meer macht voor commerciële tussenpersonen
Publiek debat	• Diversificatie van de campagne • Meer kennis over individueel relevante zaken onder de kiezers	• Gebrek aan openheid over de prioriteiten van politici • Versplintering van publiek debat

3.1 Burgers

Microtargeting kan politieke participatie stimuleren en daarmee de democratie versterken. Op maat gemaakte boodschappen kunnen extra relevant en dus overtuigend zijn. Dit is bijvoorbeeld anders bij televisiereclame dat een massapubliek bereikt terwijl niet alle kijkers geïnteresseerd zijn in dezelfde boodschap.

Auteurs

1. Prof. F.J. Zuiderveen Borgesius is hoogleraar recht en ICT bij het Institute of Computing and Information Sciences (iCIS), Radboud Universiteit Nijmegen, en onderzoeker bij het IViR Instituut voor Informatierecht van de Universiteit van Amsterdam. Dr. B. Bodo, R.Ó. Fathaigh, en dr. K. Irion werken bij het IViR Instituut voor Informatierecht van de Universiteit van Amsterdam. Dr. J. Möller, T. Dobber, dr. S. Kruikemeier, en prof. C. de Vreese werken bij de ASCoR Amsterdam School of Communication Research van de Universiteit van Amsterdam. S. Stapel is student-assistant Privacy Law & Policy bij het IViR. Het onderzoek werd ten dele ondersteund door de European Research Council, door de beurs 638514 (PersoNews) en door de Marie Curie beurs 748514 (Profile). De auteurs danken prof. Natali Helberger en de andere leden van het Personalised Communications team, en Jan Kabel, voor hun nuttige suggesties. Contact: f.j.zuiderveenborgesius@uva.nl.

Noten

2. Zie T. Dobber, D. Trilling, N. Helberger & C. de Vreese, 'Two crates of beer and 40 pizzas: the adoption of innovative political behavioural targeting techniques', *Internet Policy Review*, 2017, 6(4), hierna: Dobber e.a. 2016.

3. Dit artikel is gebaseerd op een eerder artikel, in het Engels, door de auteurs: F.J. Zuiderveen Borgesius, J. Möller, S. Kruikemeier, R.. Fathaigh, K. Irion, T. Dobber, B. Bodo, & C. de Vreese, 'Online political microtargeting: promises and threats for democracy', *Utrecht Law Review*, vol. 14, iss. 1, 2018, p. 82-96.

4. Zie F.J. Zuiderveen Borgesius, 'Privacybescherming online kan beter: de mythe van geïnformeerde toestemming', *NJB* 2015/680, afl. 14, p. 878-883; F. J. Zuiderveen Borgesius, *Improving Privacy Protection in the Area of Behavioural Targeting*, Deventer: Kluwer 2015 (hierna Zuiderveen Borgesius 2015).

5. I. Rubinstein, 'Voter Privacy in the Age of Big Data', *Wisconsin Law Review*, 2014, nr. 5: p. 861-936, p. 882.

6. N. Anstead, 'Data-Driven Politics in the 2015 UK Election', *International Journal of Press/ Politics*, 2017-22, nr. 3, p. 294-313 (hierna Anstead 2017); M. Wallace, 'The computers that crashed. And the campaign that didn't. The story of the Tory stealth operation that outwitted Labour last month', www.conservativehome.com/thetorydiary/2015/06/the-computers-that-crashed-and-the-campaign-that-didnt-the-story-of-the-tory-stealth-operation-that-outwitted-labour.html. Alle in de voetnoten genoemde websites zijn geraadpleegd op 6 maart 2019.

7. N. Anstead, 'Was this the 'social media election'? We don't know yet', in: *UK Election Analysis 2015: Media, Voters and the Campaign*, www.psa.ac.uk/psa/news/uk-election-analysis-2015-media-voters-and-campaign.

8. C. Cadwalladr, 'The great British Brexit robbery: how our democracy was hijacked', *The Guardian* 7 mei 2017, www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy.

9. Dobber e.a. 2016.

10. https://nos.nl/artikel/2219004-podcast-dedag-hoe-sociale-media-denk-aan-drie-zetels-hielpen.html.

11. https://nos.nl/artikel/2237443-denk-werkte-aan-nepadvertentie-pvv.html.

Ter illustratie: stel dat Anna een 18-jarige jonge vrouw is, die niet geïnteresseerd is in politiek. Zij bekijkt en leest wel regelmatig berichten van haar vrienden op Facebook die politiek actief zijn. Op Facebook ontvangt Anna als gevolg daarvan een advertentie gericht op jongeren over standpunten van een politieke partij, over studiefinanciering. Omdat deze advertentie gaat over een belangrijke kwestie voor jongeren besluit Anna meer informatie te zoeken over de standpunten van de partij. Zo kunnen gerichte politieke advertenties mensen aanmoedigen meer politieke kennis te vergaren.

Online microtargeting kan ook potentiele kiezers bereiken die normaal gesproken moeilijk te bereiken zijn via televisie en kranten. Mensen die politiek oninteressant vinden, bekijken zelden een krant of het televisiejournaal, waardoor het lastig is die mensen te betrekken bij de politiek.[12] Maar ze bezoeken vaak wel entertainment- en sociale media-sites.[13] Een politieke partij kan mensen via die sites op maat gemaakte advertenties tonen, waardoor ook deze ongeïnteresseerde burgers politieke informatie krijgen en mogelijk ook gaan stemmen.

3.2 Politieke partijen

Voor politieke partijen is microtargeting aantrekkelijk vanwege de lage prijs, de effectiviteit, en de efficiëntie. In vergelijking met televisiereclames of krantenadvertenties kan microtargeting goedkoop zijn, vooral microtargeting via Facebook of andere sociale media. Met microtargeting kunnen partijen ook vrijwilligers werven. Op deze manier biedt microtargeting een alternatief voor kleine en nieuwe partijen die geen dure tv-campagnes kunnen betalen.[14]

De eerste politieke partij die microtargeting-technieken inzet, kan daarmee een voordeel halen ten opzichte van de andere partijen, zoals de Conservatieve Partij van het Verenigd Koninkrijk deed tijdens de verkiezingen van 2015.[15] Maar al snel zullen andere partijen ook microtargeting gebruiken, waardoor het voordeel voor de eerste gebruiker afneemt.[16]

Met microtargeting kunnen politieke partijen ook efficiënter campagnevoeren. In plaats van een breed publiek dezelfde politieke advertenties te tonen op Facebook, kunnen partijen zich met specifieke boodschappen richten op hun bestaande en potentiele achterban. Zo kan een politieke 'Partij voor de Boeren' geld, tijd en moeite besparen door zich voornamelijk te richten op mensen die op het platteland wonen (zoals, bijvoorbeeld, SGP doet)[17] en stedelingen links te laten liggen.

3.3 Publiek debat

Microtargeting kan de diversiteit van politieke campagnes en de kennis van kiezers over bepaalde kwesties vergroten. Ten eerste kan microtargeting bijdragen aan de diversiteit van verkiezingscampagnes. In verkiezingstijd dragen alle partijen hun politieke ideeën en prioriteiten uit aan het publiek, dat vervolgens een partij kiest die het beste past bij hun politieke voorkeuren. Kiezers worden overstelpt met informatie, omdat er veel partijen zijn, elk met hun eigen programma.[18] Daarom nemen kiezers slechts een klein deel van alle politieke informatie tot zich. Op basis van dat kleine beetje informatie brengen ze hun stem uit.

Met microtargeting kunnen politieke partijen kiezers informatie geven over de paar thema's die individuele kiezers echt belangrijk vinden, waardoor kiezers de partijstandpunten op die specifieke thema's makkelijker kun-

nen vergelijken.[19] Met traditionele tv-reclame is dat niet mogelijk: partijen kunnen op televisie slechts een paar grote en algemene thema's uitlichten.[20] Die algemene thema's zullen niet iedereen aanspreken. Met microtargeting kan een politieke partij mensen informeren over specifiekere onderwerpen. Op deze manier kunnen kiezers hun stem baseren op betere informatie en kiezen voor de partij met de beste ideeën over specifieke thema's die voor hen het belangrijkst zijn.

4. Bedreigingen

4.1 Burgers

We bespreken een aantal van de voornaamste bedreigingen die microtargeting met zich brengt. Opnieuw onderscheiden we bedreigingen voor burgers, politieke partijen en het publieke debat.

Drie bedreigingen voor burgers zijn: hun privacy kan geschonden worden, en ze kunnen gemanipuleerd of genegeerd worden. Ten eerste bedreigt microtargeting privacy. Voor microtargeting worden op grote schaal persoonsgegevens verzameld en verder verwerkt. Hierdoor treedt mogelijk een *'chilling effect'* op: mensen passen hun gedrag aan als zij weten dat hun gedrag wordt geobserveerd. Als mensen denken dat hun surfgedrag wordt gemonitord, zullen ze bepaalde sites misschien vermijden.[21] Als mensen bijvoorbeeld verwachten dat een extreemrechtse partij de verkiezingen gaat winnen, zouden ze kunnen aarzelen om websites over de islam te bezoeken.[22]

Een tweede gevaar voor privacy is datalekkage. Datalekken, waar hackers of anderen toegang krijgen tot persoonsgegevens, komen veel voor. Ter illustratie: in de eerste helft van 2018 ontving de Autoriteit Persoonsgegevens al bijna 9000 meldingen van een datalek.[23] Over heel 2017 ontving de AP 10.300 meldingen.[24] In 2017 werd een marketingbedrijf dat voor de Amerikaanse conservatieven

Voor microtargeting worden op grote schaal persoonsgegevens verzameld en verder verwerkt

werkte het slachtoffer van een datalek waardoor gegevens van bijna 200 miljoen Amerikaanse burgers op straat kwamen te liggen. Bij de gelekte persoonsgegevens waren ook gegevens over religie, etniciteit en politieke voorkeuren.[25]

Een derde bedreiging voor de privacy is dat persoonsgegevens gebruikt kunnen worden voor onvoorziene en soms schadelijke nieuwe doelen. Burgers staan kritisch tegenover microtargeting. Uit een enquête die we hebben gehouden, blijkt dat 83% van de ondervraagde Nederlanders het gebruik van persoonsgegevens voor politieke microtargeting onacceptabel vindt.[26]

Naast privacy-risico's, brengt microtargeting het gevaar van kiezersmanipulatie met zich mee. Een partij kan bijvoorbeeld racistische kiezers informatie tonen over hoge misdaadcijfers onder immigranten.[27] De politieke informatie hoeft niet eens waar te zijn om invloed te hebben.

Politieke partijen zouden microtargeting ook kunnen gebruiken om de opkomst onder de achterban van hun tegenstanders te laten dalen. Zo toonde Brandpunt onlangs aan dat het gemakkelijk is via Facebook een advertentie, waarin staat dat de stembussen in 'jouw gemeente' gesloten zijn, op verkiezingsdag te tonen aan VVD-sympathisanten.[28] In 2016 heeft Donald Trump's campagne, naar verluidt, bepaalde advertenties gericht aan Afro-Amerikaanse kiezers. Trump herinnerde Afro-Amerikanen in die advertenties aan oude uitspraken van Hillary Clinton, waarbij ze Afro-Amerikaanse mannen *'super predators'* had genoemd. Deze advertentie was

12. A. Blekesaune e.a., 'Tuning Out the World of News and Current Affairs – An Empirical Study of Europe's Disconnected Citizens', *European Sociological Review*, 2012-28 nr. 1, p. 110-126.
13. Mensen ontvangen politieke informatie terwijl ze sociale media gebruiken voor entertainmentdoeleinden. Y. Kim e. a., 'Stumbling upon news on the Internet: Effects of incidental news exposure and relative entertainment use on political engagement', *Computers in human behavior*, 2013-29 nr. 6, p. 2607-2614.
14. European Parliamentary Research Service, 'Social media in election campaigning,' Briefing, 21 maart 2014, www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140709/LDM_BRI(2014)140709_REV1_EN.pdf.
15. Anstead 2017.
16. D. Kreiss, *Prototype Politics*, Oxford University Press 2016.
17. Dobber e.a. 2016.
18. A. Downs, 'An economic theory of political action in a democracy', *Journal of Political Economy*, 1957, 65, nr. 2, p. 135-150.
19. Zie ook Staatscommissie Parlementair Stelsel, 'Probleemverkenning', 18 oktober 2017, www.staatscommissieparlementairstelsel.nl/, p. 49.
20. D. Hopmann e. a., 'Party media agenda-setting: How parties influence election news coverage', *Party Politics*, 2012, 18, nr. 2, p. 173-191.
21. Voor 'chilling effects' in het algemeen, zie: N. Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age,* Oxford University Press 2015, en voor 'chilling effects' in de context van online tracking: Zuiderveen Borgesius 2015, p. 73-78.
22. Regeringen vragen soms informatie op over het surfgedrag van mensen. Zie bijv. J. Carrie Wong & O. Solon, 'US government demands details on all visitors to anti-Trump protest website', *The Guardian* 15 augustus 2017, www.theguardian.com/world/2017/aug/14/donald-trump-inauguration-protest-website-search-warrant-dreamhost.
23. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/meldplicht_datalekken_halfjaarrapportage_q1_en_q2_2018_algemeen.pdf.
24. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/01_2018-02-23_2017_jaarrapportage_algemeen.pdf.
25. 'Personal details of nearly 200 million US citizens exposed', *BBC News*, 19 juni 2017, www.bbc.com/news/technology-40331215. Bij een datalek in Mexico werd informatie over meer dan 90 miljoen kiezers openbaar: Dissent, 'Personal info of 93.4 million Mexicans exposed on Amazon', 22 april 2016, www.databreaches.net/personal-info-of-93-4-million-mexicans-exposed-on-amazon/.
26. De vraag luidde als volgt: 'Vindt u het acceptabel als politieke partijen, zoals D66, uw persoonlijke gegevens gebruiken om u online advertenties te laten zien?'. Mensen konden een keuze maken van 1 tot en met 7; 1 stond voor 'helemaal niet acceptabel'; 7 stond voor 'helemaal wel acceptabel'. De 83% bestaat uit mensen die optie 1, 2, of 3 kozen. De vraag is gesteld in een panelonderzoek onder 1214 personen. Uitgevoerd in november 2016 door CentERdata, in opdracht van het Personalised Communications project van de Universiteit van Amsterdam.
27. W. Gorton, 'Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy', *New Political Science* 2016-38. 1, https://doi.org/10.1080/07393148.2015.1125119, p. 61-80.
28. https://brandpuntplus.kro-ncrv.nl/brandpuntplus/facebook-verkiezingen/.

bedoeld om Afro-Amerikanen het vertrouwen in Clinton te doen verliezen, zodat ze thuis zouden blijven op de verkiezingsdag.[29] Trump gebruikte hiervoor een *'dark post'*: een bericht op Facebook dat uitsluitend zichtbaar is voor een specifieke doelgroep. Doordat dit soort berichten onzichtbaar waren voor de meeste mensen, waren ze lastig te controleren op onwaarheden.[30]

Ook kan een politieke partij microtargeting gebruiken om zich bij verschillende kiezers als een *one issue*-partij voor te doen, maar steeds met andere issues. Dit leidt al snel tot een onjuist beeld van de prioriteiten van die partij. Ook kan onduidelijk zijn wat een politieke partij nu eigenlijk aan de kiezer heeft beloofd. 'Digitale verkiezingscampagnes kunnen (...) grotendeels buiten de openbaarheid plaatsvinden op de schermen van individuele kiezers', merkt de Staatscommissie Parlementair Stelsel op.[31]

Ter illustratie, stel dat een partij een profiel heeft opgebouwd van Anna. Uit dat profiel blijkt dat Anna tegen immigratie is. Aan Anna stuurt de partij gepersonaliseerde advertenties over hun plan om immigratie terug te dringen. Dezelfde partij heeft ook een profiel van Bob, waaruit blijkt dat Bob progressiever is. Bob ontvangt een gepersonaliseerde advertentie waarin die partij stelt discriminatie van immigranten op de arbeidsmarkt te willen bestrijden. De gepersonaliseerde advertentie voor Bob vermeldt echter niet dat de partij ook van plan is om immigratie te beperken. Verder ontvangen werklozen de boodschap dat de partij de sociale uitkeringen wil verhogen. Mensen die tegen een belastingverhoging zijn, krijgen juist berichten over het plan tot inkorten van de uitkeringsperiode. Op deze manier kan de partij, zonder formeel te liegen, verschillende beloften doen aan verschillende groepen.

Microtargeting kan de macht van online tussenpersonen vergroten

Behalve privacy-risico's en kiezersmanipulatie, bestaat het gevaar dat politieke partijen bepaalde kiezersgroepen negeren.[32] Zo kan een politieke partij bepaalde groepen bewust niet benaderen met advertenties, bijvoorbeeld omdat de partij verwacht dat die groepen toch niet gaat stemmen. Het risico bestaat dat bepaalde groepen amper informatie krijgen tijdens de verkiezingscampagne.

4.2 Politieke partijen

De belangrijkste gevaren van microtargeting voor politieke partijen zijn de potentiële kosten en de macht die microtargeting kan geven aan digitale tussenpersonen. Ten eerste kan professionele microtargeting duur zijn.[33] Bepaalde vormen van microtargeting kunnen alleen worden uitgevoerd door externe expertise in te huren, datasets te kopen en advertentieruimte in te kopen bij digitale platforms. Vooral voor partijen met een wat kleiner budget kan dit een uitdaging zijn. Microtargeting kan de macht van grotere en goed gefinancierde partijen versterken, terwijl de kleinere partijen niet mee kunnen komen.[34]

Ten tweede kan microtargeting de macht van online tussenpersonen vergroten. Platforms zoals Facebook bieden politieke partijen de infrastructuur om met de kiezers te communiceren.[35] Sommige tussenpersonen hebben een monopolie-achtige positie. Alleen zij beschikken over de data van de burger en de infrastructuur om de burger te bereiken. Dit geeft tussenpersonen de macht om prijzen vast te stellen en voorwaarden op te leggen. Tussenpersonen kunnen diensten aan politieke partijen op hun eigen voorwaarden verlenen en kunnen zelfs weigeren om met bepaalde politieke partijen te werken. Zo heeft een tussenpersoon (*Blue State Digital*) eens aangegeven nooit voor een bepaalde Nederlandse politieke partij te werken.[36]

4.3 Publiek debat

Microtargeting brengt meerdere bedreigingen met zich voor het publieke debat. Zo missen we door microtargeting cruciale informatie: hoe belangrijk is een maatschappelijke kwestie voor een politieke partij?

Als kiezers veel politieke advertenties ontvangen over één specifiek onderwerp, kunnen zij ten onrechte concluderen dat dit onderwerp een speerpunt is voor de politieke partij. Het is vaak moeilijk te ontdekken of een politieke advertentie op maat gemaakt is. Als gevolg daarvan kan microtargeting leiden tot een verkeerd beeld van de prioriteiten van politieke partijen. Dit is bijvoorbeeld problematisch als partijen compromissen moeten sluiten in een coalitie. Ter illustratie: microtargeting kan leiden tot een situatie waarin een kiezer op een partij heeft gestemd vanwege hun standpunt over gezondheidszorg. Maar eenmaal gekozen, kan die partij haar eisen over gezondheidszorg weggeven tijdens onderhandelingen met coalitiepartners.

Ook kan microtargeting het mandaat van gekozen politici beïnvloeden. Omdat een politieke partij niet weet op basis van welke thema's een kiezer haar stem heeft uitgebracht, is het voor een politieke partij die campagne heeft gevoerd over een veelvoud aan onderwerpen lastig te interpreteren welke onderwerpen doorslaggevend waren voor de kiezer en welke niet.[37]

Een tweede bedreiging is de versplintering van het publieke debat. Een campagne die via massamedia zoals televisie wordt gevoerd, bestaat uit een klein aantal grote thema's, bijvoorbeeld gezondheidszorg, immigratie en de economie. De meerderheid van de kiezers kent de standpunten van politieke partijen over deze paar onderwerpen. Met deze kennis kunnen kiezers zich mengen in maatschappelijke discussies. Maar als elke kiezer alleen in aanraking komt met ideeën over specifieke onderwerpen die persoonlijk relevant zijn en die stroken met zijn of haar persoonlijke opvattingen, wordt het lastig discussiëren.

5. De gevaren moeten niet overdreven worden

In de Europese context moet men het gevaar van microtargeting niet overdrijven. Ten eerste wordt microtargeting bemoeilijkt door de strenge Europese privacyregels (in vergelijking met die in de VS). Ten tweede is microtargeting minder praktisch in landen met een meerpartijenstelsel

(zoals Nederland) dan in landen met een tweepartijenstelsel (zoals de VS). Ten derde zijn er grenzen aan de invloed van politieke marketing op de mening van kiezers, omdat mensen ook niet-gepersonaliseerde politieke informatie tot zich nemen. Hieronder bespreken we deze drie punten.

5.1 Rechtssysteem

Door de strenge Europese privacyregels is microtargeting in Europa lastiger dan in de VS.[38] De belangrijkste privacyregels in Europa staan in de Algemene Verordening Gegevensbescherming (AVG). De AVG is een juridisch instrument dat ervoor probeert te zorgen dat de verwerking van persoonsgegevens eerlijk en rechtmatig gebeurt. De AVG legt verplichtingen op aan organisaties die persoonsgegevens verwerken (verantwoordelijken) en kent rechten toe aan de mensen wiens gegevens worden verwerkt (betrokkenen). Onafhankelijke privacy-toezichthouders, zoals in Nederland de Autoriteit Persoonsgegevens, houden toezicht op de naleving van de AVG.

De AVG is extra streng als het gaat om persoonsgegevens over iemands politieke voorkeuren. In principe verbiedt de AVG het verzamelen van zulke gegevens, omdat die behoren tot 'bijzondere categorieën van persoonsgegevens' (soms 'gevoelige gegevens' genoemd).[39] Er zijn uitzonderingen op het verbod. Bijzondere persoonsgegevens mogen bijvoorbeeld verwerkt worden als de betrokkene daar uitdrukkelijke toestemming voor heeft gegeven. En politieke partijen mogen, grofweg samengevat, persoonsgegevens van hun leden verwerken.[40]

De AVG eist transparantie over het verwerken van persoonsgegevens, en over de meeste vormen van gerichte online marketing. De AVG eist onder meer dat verantwoordelijken uitleggen welke gegevens ze waarom verwerken, bijvoorbeeld in een privacyverklaring op hun website.[41] En de AVG kent mensen een inzagerecht toe: een verantwoordelijke moet op verzoek uitleggen welke gegevens hij over iemand heeft.[42]

Afgezien van de AVG eist de e-Privacyrichtlijn, kort gezegd, transparantie en toestemming voor het gebruik van tracking cookies en vergelijkbare technieken.[43] Als een bedrijf cookies gebruikt voor politieke microtargeting, moet het bedrijf mensen dus informeren over het doel van het cookie – in dit geval: mensen volgen op het internet om hen gerichte politieke marketing te laten zien. Zulke transparantievereisten zouden kunnen helpen om microtargeting transparanter te maken.

Omdat de privacyregels in Europa strenger zijn dan in de VS, is het in Europa lastiger om gedetailleerde informatie over keizers te verzamelen. *Data brokers*, bedrijven die handelen in persoonsgegevens, vormen een grote industrie in de VS.[44] In Europa is die industrie veel kleiner. Het is dus moeilijker om gegevens over kiezers te kopen in Europa.

We beweren zeker niet dat de AVG alle privacyproblemen oplost. Naleving en handhaving laten te wensen over. Bovendien leiden transparantieverplichtingen er doorgaans niet toe dat mensen daadwerkelijk geïnformeerd worden.[45] Toch is het aannemelijk dat de Europese privacyregels microtargeting bemoeilijken.

5.2 Kies- en politieke stelsels

Een tweede reden waarom microtargeting in Europa waarschijnlijk niet even populair wordt als in de VS is het verschil in kiesstelsels. De stelsels van meerderheidsvertegenwoordiging in de VS en het VK kennen een *'winner takes all'*-principe waar sommige stemmen meer waard zijn dan andere. Zo'n kiesstelsel kan leiden tot een situatie waarin een klein aantal staten of regio's beslissend zijn voor de hele verkiezing. Omdat stemmen in zulke kantelstaten de grootste invloed hebben, investeren politieke partijen vaak meer of zelfs alleen in die staten.

Nederland kent een stelsel van evenredige vertegenwoordiging, waardoor de waarde van stemmen gelijker is verdeeld.[46] In ons systeem is het aantrekkelijker voor partijen om hun campagne gelijkmatig over de kiezers te verspreiden. Bovendien concurreren in Nederland veel meer

29. J. Green & S. Issenberg, 'Inside the Trump Bunker, With Days to Go', 27 oktober 2016, www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go.

30. M. Funk, 'The Secret Agenda of a Facebook Quiz', *New York Times*, 19 november 2016, www.nytimes.com/2016/11/20/opinion/the-secret-agenda-of-a-facebook-quiz.html?_r=0.

31. Staatscommissie parlementair stelsel, Tussenstand, 21 juni 2018, www.staatscommissieparlementairstelsel.nl.

32. D. Nickerson & T. Rogers, 'Political Campaigns and Big Data', *Journal of Economic Perspectives*, (2014) 28, nr. 2, p. 51-74, http://pubs.aeaweb.org/doi/abs/10.1257/jep.28.2.51.

33. C. Bennett, 'The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western democracies', First Monday, 2013-18, nr. 8, http://firstmonday.org/ojs/index.php/fm/article/view/4789/3730#1.

34. Idem.

35. Idem.

36. F. Hendrickx, 'Campagnebureau Obama helpt Jesse Klaver: we kunnen leren van Nederland', *de Volkskrant* 17 december 2017, www.volkskrant.nl/binnenland/campagnebureau-obama-helpt-jesse-klaver-we-kunnen-leren-van-nederland~a4435841.

37. D. Hillygus & T. Shields, *The Persuadable Voter: Wedge Issues in Presidential Campaigns*, Princeton University Press 2008, p. 14.

38. De privacy-toezichthouder in het VK heeft een uitgebreid rapport geschreven over Cambridge Analytica en Facebook: Information Commissioner's Office, 'Democracy disrupted? Personal information and political influence', 11 juli 2018, https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf. Zie over Europese gegevensbescherming en politieke microtargeting ook: C. Bennett, 'Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?', *International Data Privacy Law*, 2016-6 no. 4, https://doi.org/10.1093/idpl/ipw021, p. 261-275.

39. Zie art. 9 AVG.

40. Art. 22(2)(c) van de UAVG.

41. Zie art. 13-15 AVG.

42. Zie art. 13-15 van de Verordering (EG) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad 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/EC (Algemene verordening gegevensbescherming), OJ L 119, 5.4.2016, p. 1.

43. Richtlijn 2002/58/EC, laatst herzien in 2009. Zie ook art. 11.7a van de Telecommunicatiewet.

44. Federal Trade Commission, *Data Brokers. A Call for Transparency and Accountability*, mei 2014, www.ftc.gov.

45. A. Acquisti & J. Grossklags, 'What Can Behavioral Economics Teach Us About Privacy?', in: A. Acquisti e.a. (red.), *Digital Privacy: Theory, Technologies and Practices*, New York: Taylor & Francis 2007; F.J. Zuiderveen Borgesius, 'Behavioural Sciences and the Regulation of Privacy on the Internet', in: A. Alemanno & A.L. Sibony (red.), *Nudge and the Law – A European Perspective*, Oxford: Hart publishing 2015.

46. S. Birch, 'Electoral systems and party systems in Europe East and West', *Perspectives on European Politics and Society* 2001, afl. 3, p. 355-377.

partijen met elkaar om de gunst van de kiezer dan in de VS. Het is lastiger om in te schatten of iemand PvdA, GroenLinks of misschien toch D66 stemt dan of iemand Democraat of Republikein is. Daarom is het in Nederland moeilijker om advertenties te richten op kiezers van één partij.

Daarnaast hebben politieke campagnes in Europa veel kleinere budgetten dan die in de VS. In de VS had Hillary Clinton's campagne meer dan $ 600 miljoen te besteden.[47] De grootste Nederlandse partij heeft minder dan € 10 miljoen in kas.[48] Kleinere budgetten vormen een drempel voor het investeren in microtargeting

5.3 Kiezers leven niet in een digitale informatiebubbel

Een derde reden om de gevaren van microtargeting niet te overdrijven is dat mensen niet in digitale informatiebubbels leven. Ook als mensen gepersonaliseerde politieke advertenties ontvangen, zien ze vaak ook niet-gepersonaliseerde informatie, bijvoorbeeld via de media.[49] Kiezers hebben dus waarschijnlijk nog steeds voldoende toegang tot niet-gepersonaliseerde informatiebronnen die *'filter bubbel'*-achtige effecten van microtargeting kunnen verkleinen.[50] Mensen horen vaak ook over politiek door tv-nieuws te kijken of door met vrienden of collega's te praten.

Kortom, hoewel microtargeting serieuze gevaren met zich meebrengt voor de democratische samenleving, moeten we die gevaren niet overdrijven.

6. Regulering van microtargeting

Welke mogelijkheden hebben beleidsmakers om microtargeting te reguleren? Het is nog te vroeg om definitief beleidsadvies te geven over microtargeting. We weten nog niet genoeg over de praktijk en de invloed van microtargeting. Als uit de praktijk of onderzoek blijkt dat de voordelen duidelijk groter zijn dan de nadelen, zouden beleidsmakers misschien niet veel hoeven doen. Als de voordelen echter niet opwegen tegen de nadelen, moeten oplossingen worden gevonden. Helaas zijn op dit moment de effecten van microtargeting onduidelijk.

Wat kan er op korte termijn worden gedaan? Als aanzet voor een discussie geven we een aantal suggesties. Ten eerste is er behoefte aan meer informatie, en dus onderzoek, over microtargeting.[51] Wat de effecten van politieke microtargeting op burgers zijn, is nog steeds een open vraag. Ook meer normatief onderzoek is nodig: we moeten besluiten wanneer de mogelijke voordelen van microtargeting zwaarder wegen dan de risico's, of andersom. Ten tweede kunnen beleidsmakers overwegen om het gebruik van politieke microtargeting transparanter te maken. Nu eist het Burgerlijk Wetboek kort gezegd dat online advertenties als zodanig herkenbaar moeten zijn, en dat ze vermelden wie achter de advertentie zit.[52] Maar de regel ziet op 'commerciële communicatie'; politieke advertenties vallen daarbuiten. De Stichting Reclame Code, een instantie op het gebied van zelfregulering van reclame, gebruikt een ruime definitie van reclame, die wel politieke advertenties omvat. De Stichting eist ook dat reclame als zodanig herkenbaar is.[53]

Om transparantie te vergoten zou de wetgever politieke partijen bijvoorbeeld kunnen verplichten om hun uitgaven aan microtargeting openbaar te maken. Er zijn precedenten voor zulke regels. Ter illustratie, de database van uitgaven van de Britse kiescommissie bevat de uitgaven van elke partij voor reclame via Facebook, Twitter en Google.[54]

De wet zou politieke partijen ook kunnen verplichten een kopie van elke onlineadvertentie op een centrale website te plaatsen. Op die manier kunnen onderzoekers, journalisten en anderen zien wat een partij aan verschillende mensen belooft.[55] En de wet zou kunnen eisen dat elke politieke advertentie aangeeft of die advertentie gericht is op een bepaalde groep, en of de inhoud van die advertentie is gepersonaliseerd.

In theorie zou overwogen kunnen worden om te eisen dat politieke advertenties vermelden wie de adverteerder is. Maar soms is het nuttig dat mensen hun politieke mening anoniem kunnen uiten. Anonimiteit kan bijvoorbeeld mensen met impopulaire standpunten beschermen. Er moet dus niet te makkelijk besloten worden om anonieme politieke advertenties te verbieden.[56]

Transparantieverplichtingen kunnen helpen bij het verkrijgen van meer informatie over de omvang van het probleem van microtargeting. Privacy-toezichthouders kunnen hun bevoegdheden gebruiken om de omvang van microtargeting te onderzoeken en om bijvoorbeeld de verwerkingsactiviteiten van politieke partijen te inspecteren. De Franse en de Engelse toezichthouders hebben het gebruik van persoonsgegevens door politieke partijen onderzocht.[57] In Nederland is de Autoriteit Persoonsgegevens in februari 2019 een verkennend onderzoek begonnen.[58]

Hoewel microtargeting serieuze gevaren met zich meebrengt voor de democratische samenleving, moeten we die gevaren niet overdrijven

Als gevolg van het onderzoek naar de invloed van diensten van sociale media tijdens de Amerikaanse presidentsverkiezingscampagne[59] boden bedrijven zelfregulerende maatregelen aan, bijvoorbeeld het onthullen van wie betaalt voor politieke advertenties.[60] Facebook bewaart politieke advertenties bijvoorbeeld in een openbaar archief, zodat iemand advertenties kan bekijken die niet op hem of haar gericht waren.[61] Het is echter moeilijk om te controleren of zelfregulering effectief is.

Als blijkt dat microtargeting inderdaad een groot probleem is kan ingrijpender regulering worden overwogen. Zelfs een verbod op microtargeting zou overwogen kunnen worden. Zo'n verbod zou zich kunnen beperken tot verkiezingsperioden. Het Centraal Planbureau suggereert dat bepaalde vormen van gepersonaliseerde microtargeting verboden zou moeten worden: 'Om te voorkomen dat politieke partijen hun trade-offs kunnen verbergen, zou de inhoud van politieke advertenties niet per burger mogen verschillen.'[62]

Maar beleidsmakers moeten voorzichtig zijn met het reguleren van microtargeting. Politieke partijen hebben een recht op vrijheid van meningsuiting, beschermd door onder meer het Europees Verdrag voor de Rechten van de Mens. In beginsel beschermt dat recht ook hun advertenties.[63] Toch heeft het Europees Hof voor de Rechten van de Mens een totaal verbod op politieke televisiereclame (in het VK) toegestaan.[64] Een verbod op microtargeting zou dus waarschijnlijk ook worden toegestaan door het Hof. Kortom, beleidsmakers hebben diverse opties om de risico's van microtargeting te verminderen. Maar eerst hebben we meer informatie nodig over microtargeting.

Technologische ontwikkelingen gaan snel en voor- en nadelen van microtargeting kunnen daarmee prominenter worden

7. Conclusie

We hebben de voor- en nadelen van online politieke microtargeting voor onze democratie onderzocht. Voor burgers kan microtargeting leiden tot relevantere advertenties. Verder zijn politici door microtargeting beter in staat kiezers te bereiken. Voor politici kan microtargeting efficiënt, effectief en goedkoop zijn. Microtargeting kan bovendien tot meer diverse campagnes en meer politieke kennis leiden.

Maar microtargeting heeft ook nadelen voor de democratie. Microtargeting bedreigt privacy en kan worden gebruikt om mensen te manipuleren of te negeren. Met microtargeting kan een politieke partij zich bij verschillende mensen als een andere *one issue*-partij presenteren. Microtargeting brengt ook risico's voor politici. Sommige vormen van microtargeting zijn zo duur dat grote en goed gefinancierde partijen een oneerlijk voordeel krijgen. Verder geeft microtargeting meer macht aan digitale tussenpersonen, zoals online marketingbedrijven en sociale media-bedrijven. Een risico voor het publieke debat is dat de prioriteiten van politieke partijen minder helder worden. Bovendien kunnen politieke discussies gefragmenteerd raken als verschillende kiezersgroepen zich op verschillende onderwerpen richten, en zich voor andere meningen en onderwerpen afsluiten.

Deze risico's zijn ernstig en bedreigen de democratie – als ze werkelijkheid worden. Maar er is ook geen reden voor paniek. Microtargeting kan in Europa minder invloed hebben dan in de VS vanwege de grote verschillen in de juridische en electorale systemen. Bovendien is de invloed van microtargeting op kiezers beperkt, omdat mensen ook op andere manieren geïnformeerd worden. De technologische ontwikkelingen gaan snel en voor- en nadelen van microtargeting kunnen daarmee prominenter worden. Het is dan ook zaak dat beleidsmakers en wetenschappers een vinger aan de pols houden. •

47. A. Narayanswamy et al., 'How much money is behind each campaign?', *The Washington Post* 1 februari 2017, www.washingtonpost.com/graphics/politics/2016-election/campaign-finance.

48. De cijfers komen uit 2012; het exacte bedrag voor 2017 is nog niet beschikbaar (VVD, 'Jaarrapport 2012, https://vvd.nl/content/uploads/2016/12/jaarrapport2012.pdf).

49. J. Gottfried e. a., 'The 2016 presidential campaign – a news event that's hard to miss', *Pew*, 4 februari 2016, www.journalism.org/2016/02/04/the-2016-presidential-campaign-a-news-event-thats-hard-to-miss.

50. Zie F.J. Zuiderveen Borgesius e.a., 'Should We Worry about Filter Bubbles?', *Internet Policy Review* 2016, afl. 1, p. 1-16.

51. Zie ook H. Hazenberg, J. van den Hoven, S. Cunningham, M. Alfano, H. Asghari, E. Sullivan, A. Fard & E. Rodriquez, 'Micro-Targeting and ICT media in the Dutch Parliamentary system: Technological changes in Dutch Democracy', rapport Delft University, http://designforvalues.tudelft.nl/wp-content/uploads/2018/10/Micro-Targeting-and-ICT-media-in-Dutch-Parliamentary-System-public.pdf, p. 32.

52. Art. 3:15e BW; dat art. 6 Richtlijn Elektronische Handel (2000/31/EG) implementeert.

53. Art. 11.1 Nederlandse Reclame Code; www.reclamecode.nl/nrc/.

54. Zie UK Electoral Commission, http://search.electoralcommission.org.uk/Search/Spending.

55. Zie voor een vergelijkbaar voorstel: S. Barocas, 'The price of precision: voter microtargeting and its potential harms to the democratic process', in: PLEAD, *12 Proceedings of the First Edition Workshop on Politics, Elections and Data,* 2012, p. 31-36; C. Prins, 'Politiek profileren', Vooraf, *NJB* 2017/2031, afl. 38.

56. Zie over anonieme politieke uitingen een uitspraak van het Supreme Court in de Verenigde Staten: *McIntyre/Ohio Elections Commission*, 514 U.S. 334, 1995. Zie ook A.H. Ekker, *Anoniem communiceren: van drukpers tot weblog: een onderzoek naar de grondrechtelijke bescherming van anonieme openbare communicatie*, Den Haag: Sdu 2006.

57. Commission nationale de l'informatique et des libertés (CNIL), 'Délibération n° 2012-020 du 26 janvier 2012 portant recommandation relative à la mise en œuvre par les partis ou groupements à caractère politique, élus ou candidats à des fonctions électives de fichiers dans le cadre de leurs activités politiques', 9 februari 2012, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025344843. De Engelse privacytoezichthouder heeft Facebook een boete opgelegd van een half miljoen pond, in verband met het Cambridge Analytica schandaal (24 oktober 2018), https://ico.org.uk/action-weve-taken/enforcement/facebook-ireland-ltd/.

58. https://autoriteitpersoonsgegevens.nl/nl/nieuws/verkennend-onderzoek-naar-gebruik-persoonsgegevens-verkiezingscampagnes

59. D. Kreiss & S. McGregor, 'Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google With Campaigns During the 2016 US Presidential Cycle', *Political Communication* 2018, afl. 2, p. 1-23.

60. J. Roettgers, 'Facebook Wants to Self-Regulate Political Advertising, Provide Russian Ads to Congress', *Variety* 21 september 2017, http://variety.com/2017/digital/news/facebook-political-ads-1202565678/. Google heeft transparantie-bevorderende maatregelen aangekondigd rond de verkiezingen voor het Europees Parlement: 'Supporting the European Union Parliamentary Elections', www.blog.google/around-the-globe/google-europe/supporting-european-union-parliamentary-elections/.

61. www.facebook.com/ads/archive.

62. Centraal Planbureau,'Platforms veranderen de wereld. Beleid voor transparantie', december 2017, www.cpb.nl/sites/default/files/omnidownload/CPB-Policy-Brief-2017-11-Scientia-Potentia-Est-De-opkomst-van-de-makelaar-voor-alles.pdf, p. 3.

63. EHRM 22 april 2013, ECLI:CE:ECHR:2013:0422JUD004887608 (*Animal Defenders International/Verenigd Koninkrijk*), par. 117. Zie voor een uitgebreidere analyse: F.J. Zuiderveen Borgesius, J. Möller, S. Kruikemeier, R.Ó. Fathaigh, K. Irion, T. Dobber, B. Bodo, & C. de Vreese, 'Online political microtargeting: promises and threats for democracy', *Utrecht Law Review*, vol. 14, iss. 1, 2018, p. 82-96.

64. EHRM 22 april 2013, ECLI:CE:ECHR:2013:0422JUD004887608 (*Animal Defenders International/Verenigd Koninkrijk*), par. 122.