



UvA-DARE (Digital Academic Repository)

De zeven privacytrends van 2017

van Daalen, O.

Publication date

2018

Document Version

Final published version

Published in

Mediaforum

[Link to publication](#)

Citation for published version (APA):

van Daalen, O. (2018). De zeven privacytrends van 2017. *Mediaforum*, 30(1), 2-5.
https://www.ivir.nl/publicaties/download/Mediaforum_2018_1.pdf

General rights

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

De zeven privacytrends van 2017

Rechtspraak

Ot van Daalen*

Het is drie jaar geleden dat Mediaforum een overzicht van tien privacytrends publiceerde.¹ Toen was de Algemene Verordening Gegevensbescherming (AVG) nog niet aangenomen, lag Snowden nog fris in het geheugen en heette de Autoriteit Persoonsgegevens (AP) nog het College Bescherming Persoonsgegevens. Privacyrecht was ook toen al best belangrijk, maar de aandacht voor dit vakgebied is in de afgelopen jaren behoorlijk gegroeid.² Dus laten we de vraag opnieuw stellen: wat is er de afgelopen tijd gebeurd op privacygebied, en vallen daarin grote lijnen te ontwaren?

Organisaties én de AP bereiden zich voor op de AVG

De AVG is gepubliceerd op 4 mei 2016 en is van toepassing vanaf 25 mei 2018. Organisaties hebben dus twee jaar de tijd gekregen om hun compliance op orde te krijgen. Getuige het aantal privacyvacatures doen veel bedrijven ook hun best om op tijd te zijn, al is het door de krapte op de arbeidsmarkt de vraag of het ze gaat lukken. Nederland heeft ook twee jaar de tijd gekregen om nationale wetgeving tot stand te brengen die invulling geeft aan de ruimte die de AVG lidstaten laat. Ook daar is het de vraag of het wel gaat lukken: de Uitvoeringswet AVG is medio december 2017 aan het parlement aangeboden, en is medio februari van dit jaar nog in behandeling in de Tweede Kamer.³

Aan de Autoriteit Persoonsgegevens zal het in ieder geval niet liggen: ook die is zich aan het voorbereiden op de AVG. Dat betekent onder meer dat de organisatie opnieuw is ingedeeld, in verschillende directies: Klantcontact en Controlerend Onderzoek; Systeemtoezicht, Beveiliging en Technologie; Juridische Zaken en Wetgevingsadvisering; en Beleid, Internationaal, Strategie en Communicatie.⁴ Ook zijn de nieuwe directeuren van deze afdelingen aangenomen, waarbij opvalt dat geen van hen voorheen actief was in het privacyveld.⁵

Ondertussen wordt het budget van de AP uitgebreid. Een bureau heeft in opdracht van de AP geadviseerd dat de organisatie een omvang moet krijgen van tussen 185 en 270 fte (afhankelijk van verschillende groeiscenario's). Dat is nogal wat, vergeleken met de iets meer dan 70 fte uit 2016 (het jaarverslag over 2017 is op dit moment nog niet gepubliceerd).⁶ Het Ministerie van Justitie en Veiligheid heeft naar aanleiding hiervan besloten het huidige budget in 2017 van € 7,7 miljoen

te laten groeien: in 2018 met € 5 miljoen en vanaf 2019 met structureel € 7 miljoen per jaar.⁷ Daarmee zit het budget iets onder het middelgrote scenario van € 16 miljoen uit het advies.

De Artikel 29 Werkgroep geeft uitleg over de AVG

Ook de Artikel 29 Werkgroep (WP29), het Europese samenwerkingsverband van nationale privacytoezichthouders, heeft niet stilgezeten in aanloop naar de inwerkingtreding van de AVG. De WP29 heeft het afgelopen jaar behoorlijk wat opinies aangenomen. Een aantal van die opinies gaat over nieuwe begrippen – begrippen die in de Richtlijn gegevensbescherming nog niet echt bestonden. Dat zijn allereerst de opinies over dataportabiliteit (het recht van gebruikers om hun persoonsgegevens van de ene naar de andere dienstverlener te laten overhevelen) en de functionaris gegevensbescherming (het aanspreekpunt voor de toezichthouder die moet zorgen dat een organisatie *compliant* is). Dat zijn ook opinies over de leidende toezichthoudende autoriteit (het mechanisme waarmee toezichthouders samenwerken bij grensoverschrijdende zaken) en boetes. En dat zijn tot slot opinies over de gegevensbeschermingseffectbeoordeling (DPIA – de verplichting om de privacyimpact van plannen van tevoren te beoordelen), profileren en de meldplicht datalekken.⁸ Twee opinies die nu in consultatie zijn gaan over begrippen die al bestonden, maar in de AVG verder zijn ingevuld: toestemming en transparantie.⁹ En drie *working documents* gaan over onderwerpen die vooral voor de internationale praktijk van belang zijn: de adequaate bescherming (waarmee wordt bepaald of een land een voldoende hoog beschermingsniveau heeft om ongehinderd gegevens uit te wisselen) en *binding corporate rules* voor verantwoordelijken en verwerkers (dit zijn afspraken binnen inter-

* Mr. O.L.van Daalen is onderzoeker bij het IViR en advocaat te Amsterdam.

1 Zie O.L. van Daalen, 'Tien privacytrends van 2014', *Mediaforum* 2015-2, p. 50-54.

2 Zo zijn de zoektermen 'GDPR' en 'gegevensbescherming' exponentieel gegroeid in Google Trends.

3 Zie *Kamerstukken II* 2017/18, 34851.

4 Zie Besluit houdende wijziging van het Besluit mandaat en machtiging Autoriteit Persoonsgegevens, *Stcrt.* 70149, 28 december 2017.

5 Zie AP 10 januari 2018, 'Autoriteit Persoonsgegevens benoemt nieuwe directeuren', <https://autoriteitpersoonsgegevens.nl/nl/nieuws/autoriteit-persoonsgegevens-benoemt-nieuwe-directeuren>.

6 Zie Bijlage Jaarverslag Autoriteit Persoonsgegevens 2016, te vinden op https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_bijlage_2016.pdf.

7 Zie *Kamerstukken II* 2016/17, 32 761, nr. 112, en *Kamerstukken II* 2017/18, 34 775 VI, nr. 2 en nr. 17, vraag 45.

8 Zie WP242 (dataportabiliteit), WP243 (FGs), WP244 (Lead Supervisory Authorities), WP248 (DPIA), WP253 (boetes), WP250 (meldplicht datalekken) en WP251 (profilering).

9 Zie WP259 (toestemming) en WP260 (transparantie).

nationale concerns om in alle landen een voldoende hoog beschermingsniveau te waarborgen).¹⁰

Bij sommige Nederlandse privacyjuristen is er wat scepsis over het opgetuigde AVG-circus: is die aandacht voor de AVG allemaal terecht? Inderdaad, de AVG introduceert een meldplicht datalekken – maar die kenden we in Nederland al. En ja, de AVG introduceert een boetebevoegdheid – maar de AP kan ook nu al serieuze boetes opleggen. En zeker: de territoriale reikwijdte wordt uitgebreid – maar ook onder de Wbp kon via de ‘middelen’-route al vaak jurisdictie worden geclaimd.¹¹

Tóch is zelfs in Nederland deze aandacht terecht en heeft de AVG veel meer dan symbolische waarde. Het voert te ver om hier in te gaan op alle wijzigingen, al is het maar omdat die door anderen uitgebreid zijn besproken.¹² Maar één rode draad in de AVG zal in ieder geval voor de AP heel belangrijk worden: hoe de *accountability*-verplichtingen in de praktijk werken. Onder de AVG wordt van organisaties namelijk niet alleen verwacht dat ze in overeenstemming handelen met de AVG, maar ook dat ze kunnen *aantonen* dat ze hiermee in overeenstemming handelen (art. 5 lid 2 van de AVG). Die gedachte is bovendien verder uitgewerkt in specifieke bepalingen van de AVG. Zo is bepaald dat als toestemming de rechtsgrond is, de verantwoordelijke moet “aantonen” dat de betrokkene toestemming heeft gegeven (art. 7 lid 1 AVG). Ook wordt toestemming “geacht” niet vrijelijk te zijn verleend als die een voorwaarde is voor het afnemen van producten of diensten, terwijl toestemming niet noodzakelijk is voor die producten of diensten (dit suggereert een omkering van de bewijslast).¹³ Bovendien moet de verantwoordelijke maatregelen nemen om te kunnen aantonen dat de verwerking in overeenstemming met de AVG plaatsvindt (artikel 24 lid 1 AVG).

Het verdient nader onderzoek wat dit betekent voor de bewijslastverdeling in bestuursrechtelijke procedures, en welke eisen worden gesteld aan het bewijs dat een verantwoordelijke moet overleggen. Hoe kan een verantwoordelijke bijvoorbeeld aantonen dat hij in overeenstemming handelt met de verplichting om begrijpelijk te informeren? Moet dat via gebruikersonderzoeken, zoals de WP29 suggereert?¹⁴ Deze bewijslastverdeling zal mogelijk vergaande impact hebben in handhavingprocedures – afhankelijk van hoe de toezichthouders en de rechter de bepaling uitleggen.

De rechter geeft opheldering over de handhavingplichten van de AP

Dat is extra belangrijk omdat juist handhaving door de AP het afgelopen jaar onderwerp was van een aantal procedures. Zo boog de rechter zich over de vraag of de AP handhavend had moeten optreden tegen het gebruik van afvalpassen door de Gemeente Arnhem.¹⁵ Ook oordeelde de rechter over de vraag in hoeverre de AP had moeten motiveren waarom ze niet

optrad tegen inmiddels beëindigde onrechtmatige verstrekking van medische persoonsgegevens door de NZa.¹⁶ En de rechter deed uitspraak in een handhavingverzoek over de verwerking van medische persoonsgegevens door zorgverzekeraars.¹⁷

Eén voor de AP belangrijke uitspraak in die reeks kwam in oktober 2017 van de Afdeling bestuursrechtspraak van de Raad van State.¹⁸ Daarin bevestigde de Afdeling het handhavingsbeleid van de AP in grote lijnen. De zaak ging over de publicatie door de overheid van faillissementsverslagen waarin ook persoonsgegevens waren opgenomen. Iemand vroeg de AP om te verbieden deze persoonsgegevens te publiceren.

De Afdeling bespreekt in die uitspraak het handhavingsbeleid van de AP. Dit bestaat blijkens de uitspraak uit vier fasen: eerst wordt getoetst of het verzoek aan de formele eisen uit de Awb voldoet en wordt een “globaal bureauonderzoek” naar een mogelijke overtreding verricht (fase 1). Dan toetst de AP het verzoek aan het prioriteringsbeleid, en wordt bezien of een “uitgebreid onderzoek” in de zin van artikel 60 Wbp moet worden gedaan (fase 2). In fase 3 *doet* de AP vervolgens dat onderzoek en in fase 4 handhaaft de AP. De Afdeling concludeert dat deze aanpak in overeenstemming is met de Richtlijn bescherming persoonsgegevens.

Een open vraag is vervolgens hoe *diepgaand* dat bureauonderzoek moet zijn. De Afdeling overweegt namelijk specifiek dat een handhavingverzoek niet het bewijs van een overtreding hoeft te bevatten, en dat het op de weg van de AP ligt om eventueel ontbrekend of extra bewijs te vergaren. Helaas scheidt ook de AVG daarin geen duidelijkheid: daarin is aan de toezichthouders uitdrukkelijk opgedragen om klachten te behandelen en de inhoud van de klacht te onderzoeken *in de mate waarin dat gepast is* (artikel 57 lid 1 sub f AVG). Hoe dan ook: als het aan de voorzitter van de AP ligt, zullen in de toekomst alle klachten van burgers worden behandeld: “*Als wij dan zeggen: u hebt gelijk, u heeft uw klacht op goede gronden ingediend, dan gaan we optreden. Dan geven we een aanwijzing, een berisping, leggen we een boete op.*”¹⁹ Een lovenswaardig streven, al is het wel de vraag hoe dat zich verhoudt tot de beperkte capaciteit van de AP.

Het Europese Hof moet zijn eigen arresten ophelderen

Niet alleen de Nederlandse rechter heeft de afgelopen jaren een aantal belangwekkende uitspraken gedaan op privacygebied: ook de hoogste Europese rechter liet van zich horen. Het Hof vestigde zijn reputatie als hoeder van de grondrechten toen het de Bewaarplichtrichtlijn ongeldig verklaarde in 2014.²⁰ Vervolgens creëerde het in 2015 een verstrekkend *right to be forgotten* uit de Richtlijn bescherming persoonsgegevens. En datzelfde jaar verklaarde het de Safe Harbour-regeling, die

10 Zie WP254 (adequacy referential), WP256 (BCR-C) en WP257 (BCR-P).

11 Zie bijv. Rb. Den Haag 22 november 2016, ECLI:NL:RBDHA:2016:14088 (WhatsApp/AP).

12 Zie o.m. G.-J. Zwenne en L. Mommers, ‘De tien belangrijkste veranderingen die de algemene verordening gegevensbescherming gaat brengen (in minder dan vijfduizend woorden)’, *Tijdschrift voor Compliance* 2016/4, p. 182-189.

13 Zie ook WP259 (consent), p. 10.

14 Zie WP260 (transparantie), p. 8.

15 V.zr. Rb. Gelderland 13 juli 2017, ECLI:NL:RBGEL:2017:3665 (X/AP/Arnhem).

16 Zie Rb. Midden-Nederland 7 juli 2017, ECLI:NL:RBMNE:2017:3422 (X/AP).

17 Zie Rb. Midden-Nederland 7 juli 2017, ECLI:NL:RBMNE:2017:3421 (X/AP).

18 ABRvS 19 oktober 2017, ECLI:NL:RVS:2016:2743 (X/AP). Zie ook ABRvS 20 september 2017, ECLI:NL:RVS:2017:2555 (Handhaving OV-chipkaart).

19 Zie *Nu.nl* 7 oktober 2016, “Nieuw jasje voor Autoriteit Persoonsgegevens: ‘De boetes komen’”, te vinden op: <https://www.nu.nl/weekend/4332953/nieuw-jasje-autoriteit-persoonsgegevens-de-boetes-komen.html>. Zie ook *Trouw* 4 oktober 2016, ‘Aleid Wolfsen ombudsman van de privacy’: “Nu kun je daar als burger nog weinig mee – anders dan een melding maken bij de Autoriteit Persoonsgegevens.” Dat gaat veranderen, belooft Wolfsen. “Mensen kunnen straks een officiële klacht indienen, die de privacywaakhond altijd zal behandelen”, te vinden op: <https://www.trouw.nl/home/aleid-wolfsen-ombudsman-van-de-privacy~ab366oc6/>.

20 Zie HvJ EU 8 april 2014, zaak C-293/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland*).

de Europese doorgifte van persoonsgegevens naar Amerikaanse bedrijven mogelijk maakte, ongeldig.²¹

Dat wil niet zeggen dat het Hof nu klaar is. Het Hof heeft zich twee keer gebogen over de reikwijdte van het begrip persoonsgegevens, met weinig verrassende uitkomsten.²² Interessanter is dat nationale rechters nog worstelen met de toepassing van de eerdere verstrekkende uitspraken. Zo heeft de *Google/ Spanje*-zaak tot vragen over de reikwijdte van het *right to be forgotten* geleid. Het eerste probleem van rechters is dat als Google bijzondere persoonsgegevens verwerkt, het verwerkingsverbod van toepassing is, terwijl Google van geen van de excepties lijkt te kunnen profiteren. Dit leidt tot inconsistente rechtspraak, zoals blijkt uit het overzicht van de Autoriteit Persoonsgegevens.²³ Zo oordeelde de rechter in Overijssel in januari dat het verwerkingsverbod inderdaad in de weg staat aan indexing door Google, maar de rechter in Den Haag oordeelde in dezelfde maand juist het tegenovergestelde.²⁴ De Franse Raad van State heeft juist over dit probleem in februari 2017 een prejudiciële vraag aan het Europese Hof gesteld.²⁵ Zij heeft in juli 2017 vervolgens een prejudiciële vraag gesteld over de territoriale reikwijdte van vergeetrecht – of dit zich bijvoorbeeld alleen uitstrekt tot het .eu-domein of ook het .com-domein omvat.²⁶

Ook na het stevige oordeel in de *Safe Harbour*-zaak – aangewend door privacyactivist Max Schrems – was het nog lang niet rustig rond internationale doorgifte. De WP29 heeft stevige bedenkingen bij de opvolger van *Safe Harbour*, het Privacy Shield, en dreigt zelfs met procedures als die niet worden opgelost vóór 25 mei 2018.²⁷ De Ierse toezichthouder voert ondertussen onder druk van Schrems een zaak over de nieuwe afspraken, en in die zaak heeft het High Court in oktober 2017 prejudiciële vragen gesteld.²⁸ En twee partijen starten een zaak bij het Gerecht van Eerste Aanleg over het Privacy Shield, waarvan er nu nog één aanhangig is.²⁹

Zelfs de uitspraak rond de Bewaarplichtrichtlijn was blijkbaar niet duidelijk genoeg. In dat arrest somde het Hof een paar omstandigheden op die, “gelet op een en ander”, tot de conclusie leidden dat de regeling disproportioneel was. Volgens sommige lidstaten zou uit dat “een en ander” volgen dat de toelaatbaarheid van nationale algemene bewaarplichtwetten afhankelijk is van de in die wet bepaalde toegangscriteria, beveiligingsmaatregelen en de bewaartermijn. Het Hof werd daarom in *Tele2/Watson* gevraagd om te verduidelijken dat het *beginsel* van een ongerichte opslagverplichting onverenigbaar is met het Handvest. En in die zaak bevestigt het Hof inderdaad dat een “algemene en ongedifferentieerde bewaring van alle verkeersgegevens en locatiegegevens van alle abonnees en

geregistreerde gebruikers betreffende alle elektronische communicatiemiddelen” te ver gaat.³⁰ Zelfs met beperkte toegang, adequate beveiliging en kortere bewaartermijn is de verplichte opslag van verkeersgegevens van *iedereen* niet toelaatbaar.

Het Hof geeft in *Tele2/Watson* ook aan hoe een nationale wet er dan wel moet uitzien. De wet moet onder meer “duidelijke en nauwkeurige regels voor de draagwijdte en de toepassing” bevatten, waaronder “in welke omstandigheden en onder welke voorwaarden” gegevens bewaard moeten worden. Daarbij moet die opslag steeds voldoen aan “objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel” (r.o. 109). Deze maatstaf lijkt op de maatstaf van het EHRM in zaken over grootschalige surveillance.³¹ In de latere zaak over de PNR-overeenkomst verwijst het Hof ook naar een zaak van het EHRM, waarbij het benadrukt dat waarborgen tegen misbruik extra belangrijk zijn wanneer de persoonsgegevens “geautomatiseerd” worden verwerkt.³²

Het maatschappelijk debat over de aftapwet nadert een hoogtepunt

De regering lijkt zich er weinig van aan te trekken, getuige de herziene Wet op de Inlichtingen- en Veiligheidsdiensten. Al in 2011 adviseerde de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) de minister om onderzoek te doen naar de herziening van de toenmalige Wet op de Inlichtingen- en Veiligheidsdiensten, onder meer omdat het onderscheid in bevoegdheden tussen kabelgebonden en niet-kabelgebonden interceptie wat “gedateerd” aanded.³³ Dit advies heeft uiteindelijk, meer dan zes jaar later, geresulteerd in de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten, die op 11 juli 2017 is aangenomen.

Onderdeel van die wet is dat het onder voorwaarden mogelijk is geworden voor de diensten “onderzoeksopdrachtgericht” communicatie te onderscheppen via de kabel. Het is de vraag hoe de vaagheid van die term zich verhoudt tot de eis uit deze hierboven genoemde jurisprudentie dat bevoegdheden duidelijk moeten zijn.

Een groep studenten wilde dat niet afwachten, en verzamelde bijna vierhonderdduizend handtekeningen om hierover een raadgevend referendum te organiseren.³⁴ Dat zal op 21 maart 2018 zal worden gehouden. Een groot succes, met een klein probleem: regeringspartijen CDA en VVD lieten al weten dat ze zullen vasthouden aan de wet.³⁵ En dat onderstreept maar weer het belang van toetsing door een rechter. Een aantal organisaties hebben dan ook aangekondigd dat ze een

21 Zie HvJ EU 6 oktober 2015, zaak C-362/14, ECLI:EU:C:2015:650 (*Facebook/ Schrems*).

22 Zie HvJ EU 19 oktober 2016, zaak C-582/14, ECLI:EU:C:2016:779 (*Breyer*) en HvJ EU 20 december 2017, zaak C-434/16, ECLI:EU:C:2017:994 (*Nowak*).

23 Zie Autoriteit Persoonsgegevens mei 2017, ‘Overzicht bemiddeling Autoriteit Persoonsgegevens bij verwijdering resultaten zoekmachines’, te vinden op: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/overzicht_bemiddeling_ap_bij_verwijdering_resultaten_zoekmachines_mei_2017.pdf.

24 Zie Rb. Overijssel 24 januari 2017, ECLI:NL:RBOVE:2017:278 (*X/Google*) en Rb. Den Haag 12 januari 2017, ECLI:NL:RBDHA:2017:264 (*X/Google*).

25 Zie het persbericht van de Conseil d’Etat van 24 februari 2017, <http://english.conseil-etat.fr/Activities/Press-releases/Right-to-be-delisted>.

26 Zie het persbericht van de Conseil d’Etat van 19 juli 2017, “Portée territoriale du droit au déréférencement”, te vinden op <http://www.conseil-etat.fr/Actualites/Communiqués/Portee-territoriale-du-droit-au-dereferencement>.

27 Zie het rapport van de Artikel 29 Werkgroep na één jaar Privacy Shield (WP255), waarin ze een aantal “significant concerns” beschrijft die vóór 25 mei 2018 moeten worden geadresseerd.

28 Zie <http://www.europe-v-facebook.org/sh2/PA.pdf>.

29 Eén van die zaken, aangespannen door Digital Rights Ireland, is niet-ontvanke-lijk verklaard, GvEA 22 november 2017, T-670/16 en één, van La Quadrature du Net, loopt nog (T-738/16).

30 HvJ EU 21 december 2016, C-203/15 en C-698/15 (*Tele2/Watson*), r.o. 107. Zie O.L. van Daalen, ‘Over waterfilters en bioscoopschermen: het WIV-voorstel en *Tele2/Watson*’, *Mediaforum* 2017-2, p. 41.

31 Zie EHRM 4 december 2015, nr. 47143/06 (*Zakharov/Rusland*), r.o. 247 en EHRM 12 januari 2016, nr. 37138/14 (*Szabó & Vissy/Hongarije*), r.o. 65 en 67.

32 Zie verder HvJ EU 26 juli 2017, Advies 1/15, ECLI:EU:C:2017:592 (*PNR overeenkomst*).

33 CTIVD 23 augustus 2011, *Toezichtsrapport inzake de inzet van SIGINT door de MIVD* (nr. 28).

34 Zie <https://www.referendumovereenwet.nl/wetten/34588>.

35 F. Hendrickx en R. Meijer, ‘Buma: Kabinet zal ‘nee’ bij referendum over “de sleepwet” negeren’, *de Volkskrant* 28 oktober 2017.

rechtszaak beginnen tegen de wet als die na 1 mei 2018 ongewijzigd in werking treedt.³⁶

De eerste schermutselingen rond collectieve privacyvorderingen

Rechtszaken zullen ook op ander vlak een belangrijke rol spelen: namelijk bij collectieve vorderingen. Privacyinbreuken zijn vervelend, maar veroorzaken per stuk meestal niet zoveel schade dat een stap naar de rechter loont – de kosten wegen in de meeste gevallen niet op tegen de baten. Tegelijkertijd zijn de meeste privacyinbreuken tegenwoordig geautomatiseerde inbreuken die juist een grote groep gedupeerden raken. Bij dat soort “strooischade” kan een collectieve actie uitkomst bieden: in één rechtszaak kun je dan vorderingen instellen voor een grote groep mensen.

We kennen die rechtszaken uit de financiële wereld, waar er behoorlijk wat claimstichtingen zijn opgericht, juist met het doel rechtszaken te voeren. In het privacyrecht kenden we dat fenomeen echter nog niet – tot 2016, toen de Stichting Privacy Claim een rechtszaak startte tegen VerzuimReductie die ten onrechte medische persoonsgegevens van werknemers verwerkte.³⁷ De rechtbank verklaarde de stichting niet-ontvankelijk, omdat zij niet voldeed aan de in de Claimcode gestelde eisen aan dit soort organisaties, maar in de toekomst kan een andere stichting natuurlijk wel door deze formele hoepel heen springen.

Ook Max Schrems probeerde een Oostenrijkse variant op de *class action* te voeren: hij startte in 2014 namens een grote groep – in dit geval 25.000 Facebook-gebruikers die hun vordering aan Max Schrems hadden overgedragen – een rechtszaak bij de rechter in Wenen.³⁸ Daarin verweet Schrems dat Facebook het gegevensbeschermingsrecht op verschillende punten overtreedt en claimde € 500 per gebruiker. Facebook stelde dat de Weense rechter niet bevoegd was. Dit is uitgevochten tot het Hof van Justitie, dat onlangs oordeelde dat de Weense rechter wel bevoegd is in de zaak van Max Schrems, maar niet ten aanzien van de vorderingen van anderen.³⁹

Schrems laat zich hierdoor niet weerhouden en heeft ondertussen NOYB – None of Your Business – opgericht: een initiatief met als doel om via collectieve vorderingen privacyrechten te handhaven. In een paar maanden heeft de organisatie meer dan € 300.000 opgehaald via crowdfunding – genoeg om van start te gaan. En deze keer is hij van plan om gebruik te maken van de mogelijkheid onder de AVG om collectieve acties in te stellen.⁴⁰

Het is de vraag of dat in Nederland ook zo makkelijk is. De AVG kent weliswaar de mogelijkheid om een NGO te laten procederen namens een gedupeerde en om zelfs onafhankelijk van een gedupeerde een rechtszaak te voeren, maar alleen als het lidstatelijke recht daarin voorziet (artikel 80). In Nederland bestaat al een mogelijkheid om collectieve acties in te stellen, maar die strekt zich niet uit tot vorderingen tot schadevergoeding.⁴¹ Op dit moment is een wetsvoorstel in behandeling dat dit zou adresseren – het is dus even afwachten of dit in de toekomst wel zal kunnen.⁴²

Meer aandacht voor aandacht door de Dopamine Machine

Het is trouwens geen toeval dat Max Schrems alle pijlen op Facebook richt. Sommige Amerikaanse techbedrijven zijn inmiddels zo groot dat zij vergaande impact op de maatschappij hebben. Sterker nog: de Duitse mededingingstoezichthouder is zelfs een onderzoek gestart naar misbruik van machtspositie door Facebook door toepassing van gebruikersvoorwaarden die in strijd zijn met het gegevensbeschermingsrecht.⁴³

Het koor van ex-Googlers en -Facebookers dat zich zorgen maakt over de gevolgen van het systeem dat ze zelf hebben gecreëerd groeit dan ook. Facebook's *founding president* en miljardair door zijn investeringen in Facebook vindt dat het bedrijf menselijke kwetsbaarheden exploiteert.⁴⁴ De ontwikkelaar van de Like-knop heeft berouw.⁴⁵ En een investeerder in Facebook vergelijkt het bedrijf zelfs met een sigarettfabriek.⁴⁶

De zorgen gaan vooral over hoe systemen als Facebook erop gericht zijn om je aandacht te kapen, een soort Dopamine Machine, zodat je zoveel mogelijk tijd op hun platform doorbrengt – terwijl je eigenlijk betere dingen te doen hebt. Twee ex-Googlers richtten in reactie daarop een NGO op om technologie te helpen ontwikkelen waarmee gebruikers hun tijd goed besteden (“Time Well Spent”).⁴⁷ Technologie, met andere woorden, waarvan het doel is om de intrinsieke wensen van de gebruiker te realiseren.

Het zal nog moeilijk worden om het tij te keren. We leven al zo lang met technologie die de belangen van anderen dient, van adverteerders tot softwareproducenten, dat we ons moeilijk kunnen voorstellen hoe een wereld eruit ziet waarin de gebruiker centraal staat. Laten we hopen dat ook het privacyrecht daaraan een bijdrage kan leveren.

36 Zie website PILP, 'Wet op de Inlichtingen en Veiligheidsdiensten (Wiv)', <https://pilp.njm.nl/dossiers/wet-op-de-inlichtingen-en-veiligheidsdiensten-wiv/>.

37 Rb. Oost-Brabant 20 juni 2016, ECLI:NL:RBOBR:2016:3892 (*Stichting Privacy Claim*), *Mediaforum* 2016-8, p. 236-240, m.nt. O.L. van Daalen.

38 Zie <https://www.fbclaim.com>.

39 HvJ EU 25 januari 2018, C-498/16 (*Schrems/Facebook*).

40 Zie M. Schrems, 'CJEU gives Green Light for Facebook Lawsuit in Vienna', http://www.europe-v-facebook.org/sk/CJEU_en.pdf.

41 Terzijde: er is wel een min of meer recente uitspraak waarin de rechter oordeelde dat door een privacy-inbreuk een immateriële schadevergoeding op zijn plaats was. Een advocatenkantoor gebruikte in *de Staatscourant* gepubliceerde persoonsgegevens van mensen die in de schuldsanering terecht waren gekomen om hun een aanbod voor rechtsbijstand te doen. De rechter kwam tot de conclusie dat er geen grondslag hiervoor was en heeft een schadevergoeding van € 100 toegevoegd. Zie Rb. Noord-Nederland 3 mei 2017, ECLI:NL:RBNNE:2017:1700 (*X/bedrijf*).

42 Zie de kamerstukken met nr. 34608.

43 Zie 'Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules', 2 maart 2016, te vinden op: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html.

44 *The Guardian* 9 november 2017, 'Ex-Facebook president Sean Parker: site made to exploit human "vulnerability"', te vinden op: <https://www.theguardian.com/technology/2017/nov/09/facebook-sean-parker-vulnerability-brain-psychology>.

45 *The Guardian* 6 oktober 2017, "Our minds can be hijacked": the tech insiders who fear a smartphone dystopia', te vinden op <https://www.theguardian.com/technology/2017/oct/05/smartphone-addiction-silicon-valley-dystopia>.

46 *The Guardian* 24 januari 2018, "Facebook should be 'regulated like cigarette industry", says tech CEO", te vinden op: <https://www.theguardian.com/technology/2018/jan/24/facebook-regulated-cigarette-industry-salesforce-marc-benioff-social-media>.

47 Zie <http://www.timewellspent.io/>.