Tien privacytrends van 2014

*Ot van Daalen**

Het privacyrecht is inmiddels een serieus specialisme met jaarlijks tientallen beschikkingen, vonnissen en richtsnoeren. Een overzicht daarvan is nuttig, maar kan je daarin ook bredere ontwikkelingen ontdekken? Het afgelopen jaar in tien privacytrends.

De Snowden-onthullingen blijven relevant, maar anders dan Snowden had gehoopt

Het is alweer anderhalf jaar geleden dat Edward Snowden voor het eerst naar buiten trad. De beleidsimpact van de onthullingen valt op het eerste gezicht nogal tegen. Nederland, Europa en de Verenigde Staten hebben ongerichte surveillance niet in de ban gedaan. Sterker nog: veel landen, waaronder Nederland, willen de bevoegdheden van geheime diensten juist uitbreiden (waarover later meer).

Toch zijn z'n onthullingen nog steeds belangrijk. Een paar ontwikkelingen zijn een direct gevolg van de lekken: de toegenomen aandacht voor security en de zorgen over gegevensoverdracht naar Amerika bijvoorbeeld. Bovendien halen Snowden's documenten nog steeds het nieuws – zo bleek alleen in januari 2015 al dat de Canadese afluisterdienst filesharingverkeer op grote schaal doorzoekt en werd bevestigd dat Belgacom is gehackt met software van de NSA.[1]

Maar die voortdurende media-aandacht, al anderhalf jaar lang, heeft waarschijnlijk ook een meer subtiele impact. Zo dragen de lekken bij aan een extra gevoeligheid voor privacyinbreuken bij het publiek, en – daarmee samenhangend – een breed gedeeld gevoel dat het internet onveilig is en onder permanente surveillance staat.

Ter illustratie: een groot deel van mijn kennissen – en niet alleen *nerds* – hebben hun laptopcamera afgeplakt met een pleister. Dat doen ze niet omdat ze per se bang zijn voor de NSA, maar omdat ze zich kwetsbaar voelen op internet. En minder anekdotisch: uit onderzoek van afgelopen jaar blijkt dat mensen na de Snowden-onthullingen merkbaar minder controversiële zoektermen intypen.[2] De grootschalige surveillance die Snowden onthulde heeft dus een *chilling effect*.

Ik vermoed verder dat de rest van de trends in 2014 op zijn minst gekleurd zijn door die onthullingen. Ik stel me zo voor dat het Europese Hof in de twee baanbrekende privacy-zaken van het afgelopen jaar geregeld aan Snowden dacht terwijl het tot zijn stevige overwegingen kwam. Ook denk ik dat de reactie op de ING-affaire (waarover hieronder meer) minder heftig was geweest als Snowden geen boekje over de veiligheidsdiensten had opengedaan.

Er blijken ook ongeschreven privacyregels te bestaan

Maar wat ook de oorzaak is, die ING-affaire zal nog lang zijn schaduw vooruitwerpen. ING's plannen om klantgegevens commercieel te benutten met gerichte advertenties leken juridisch in orde: ING zou toestemming vragen van klanten die wilden meedoen aan de pilot. Tóch kreeg ING na aankondiging stevige kritiek vanuit de politiek, financiële toezichthouders en NGO's. Zij besloot de plannen voorlopig in de koelkast te doen.

De cynicus concludeert waarschijnlijk dat communicatie belangrijk is: ING had de maatschappelijke impact van haar plannen beter moeten inschatten en beter moeten communiceren. En daar zit wat in. Eén les van de ING-affaire is dat álle *big data*-besluiten op bestuursniveau moeten worden goedgekeurd, vergezeld van een duidelijk communicatieplan.

Maar het zou zonde zijn als dat de enige conclusie was. De ING-affaire bewijst naar mijn mening ook dat er ongeschreven privacyregels zijn – ongeschreven regels die soms werken in aanvulling op de geschreven regels. Overtreding van die ongeschreven regels leidt niet tot boetes, maar kan wel dodelijk zijn voor je reputatie. Privacybeoefenaren moeten die ongeschreven regels de komende jaren in kaart brengen.

Een les van de ING-affaire is bijvoorbeeld dat de maatschappelijke functie van een organisatie, de gevoeligheid van de gegevens, de onvermijdelijkheid van de dienst en de prijs van de dienst een rol spelen bij de 'maatschappelijke privacytoets'. (Die onvermijdelijkheid zou trouwens ook een haakje bieden voor het meer juridische argument dat toestemming in zo'n geval niet vrij kan worden gegeven, maar dat terzijde.) En deze les is weer relevant voor andere 'nutsbedrijven'. Telecom- en energiebedrijven, met een goudmijn aan onbenutte klantgegevens, doen er verstandig aan eventuele *big data*-plannen langs die maatschappelijke meetlat te leggen.

De ING-affaire illustreert ook dat klanten prima begrijpen wanneer hun een rad voor ogen wordt gedraaid. Ze begrijpen dat gerichte advertenties vooral de adverteerder en het advertentiemedium ten goede komen, terwijl de klant er vooral armer van wordt. Die wordt met gerichte advertenties immers

* Mr. O.L. van Daalen is oprichter van privacy- en securityadvocatenkantoor Digital Defence. Hij werkt ook als onderzoeker bij het IViR.

1 Zie R. en G. Greenwald, 'Canada Casts Global Surveillance Dragnet Over File Downloads', *The Intercept* 28 januari 2015 en M. Rosenbach, H. Schmundt en C. Stöcker, 'Source Code Similarities: Experts Unmask "Regin" Trojan as NSA Tool', *Der Spiegel* 27 januari 2015.

2 Zie A. Marthews en C. Tucker, *Government Surveillance and Internet Search Behavior*, beschikbaar via SSRN: http://ssrn.com/abstract=2412564.

nog beter verleid om dingen te kopen. Een plan om klantgegevens te analyseren moet dus allereerst bedoeld zijn die klant te helpen, wil het de maatschappelijke privacytoets passeren.

Toezichthouders in Europa leggen de nadruk op waarborgen

Gelukkig kent het privacyrecht zelf ook flexibiliteit. Een manier waarop het gelijke tred probeert te houden met de maatschappij is via de opinies van de Europese samenwerkingskoepel van privacytoezichthouders: de Artikel 29 werkgroep. CBP-voorzitter Jacob Kohnstamm droeg in februari 2014 het voorzitterschap van de werkgroep over aan Isabelle Falque-Pierrotin, president van de Franse privacytoezichthouder (de CNIL). Falque-Pierrotin ziet voor de werkgroep de komende jaren twee uitdagingen: de nieuwe *governance* tussen toezichthouders zoals die mogelijk in de Europese Privacyverordening komt te staan, en de samenwerking tussen toezichthouders op internationaal niveau.

Wat er ook zij van haar plannen: de opinies uit 2014 zijn nog de erfenis van het werk dat is verricht onder het voorzitterschap van Kohnstamm. De belangrijkste opinie van 2014 is die over de invulling van de 'gerechtvaardigd belang'-grondslag.[3] Van alle verwerkingsgrondslagen is die grondslag het meest open: het belang van de verwerker moet worden afgewogen tegen het belang van de betrokkene. De toepassing van de bepaling liep echter nogal uiteen in de verschillende lidstaten, problematische verwerkingen zouden kunnen profiteren van deze grond en bovendien circuleerden bij de onderhandelingen over de Privacyverordening amendementen die deze flexibiliteit zouden inperken.

In april 2014 probeerde de werkgroep daarom duidelijkheid te scheppen over de toepassing hiervan. In de opinie somt de werkgroep de belangrijkste wegingsfactoren op. Die zijn niet zo verrassend: de aard van het belang van de verwerker, de impact op de betrokkene, de verwachtingen van de betrokkene en de aard van de gegevens zijn belangrijk. Ook, en dat zal in de toekomst meer gewicht krijgen in online-omgevingen waar de markt erg geconcentreerd is door netwerkeffecten, kan de dominantie van een verwerker een rol spelen.

De werkgroep onderstreept vervolgens dat de eerste twee hordes van de toets – of sprake is van te wegen belangen aan de zijde van de verwerker en de betrokkene – makkelijk genomen kunnen worden. De weging zelf vergt een serieuze poging om de verschillende factoren tegen elkaar af te zetten – ook dat is niet verrassend.

Wat wél vermeldenswaardig is, en illustratief is voor een bredere trend, is dat bij grensgevallen de genomen waarborgen om het belang van de betrokkene te beschermen vaak de doorslag zullen geven. Die trend tekende zich in Nederland al af in de zaak over Google Streetview, toen het CBP in 2011 akkoord ging met een opt-outmogelijkheid voor het in kaart brengen van wifi-netwerken.[4] De werkgroep legt ook in haar opinie veel nadruk op het bieden van een opt-out mogelijkheid, maar noemt verder beveiligingsmaatregelen, *privacy by design* en *chinese walls* als maatregelen die de weging positief beïnvloeden.

Twee andere opinies van het afgelopen jaar gaan vooral over de vraag óf de privacyregels van toepassing zijn. Zo is in april de opinie over anonimisering gepubliceerd, met als belangrijkste conclusie dat écht anonimiseren van gegevens heel moeilijk is. Het pseudonimiseren van gegevens kan een beveiligingsmaatregel zijn, maar is volgens de werkgroep geen maatregel die gegevens hun persoonlijk karakter ontneemt. Ook de opinie over *device fingerprinting* – de herkenning van computers via een unieke combinatie van kenmerken, zoals geïnstalleerde lettertypes, schermformaat en browserversie – past in die opvatting. Mochten bedrijven er nog over twijfelen of *fingerprinting* een minder gereguleerd alternatief is voor cookies: dat is volgens de werkgroep niet zo.

Die drie opinies zijn naar mijn mening tekenend voor de aanpak van privacytoezichthouders zoals het CBP: de toepasselijkheid van regels wordt al snel aangenomen, en de meeste aandacht gaat naar vragen over proportionaliteit, subsidiariteit en, daarmee samenhangend, de waarborgen.

Naast deze meer fundamentele opinies heeft de werkgroep ook een aantal thematische opinies gepubliceerd. Een daarvan is het vermelden waard: de opinie over de *internet of things*.[5] De opinie komt goed op tijd: dit fenomeen wordt waarschijnlijk pas binnen een paar jaar volwassen. In de opinie past de werkgroep dezelfde techniek toe als in haar opinie over apps: ze ontwart de verschillende schakels in de 'waardeketen' en identificeert per schakel de mogelijke problemen. De werkgroep sluit verder aan bij de technologie: ze benadrukt dat ook kleine sensoren zonder beeldscherm en met weinig rekenkracht de gebruiker goed moeten informeren, fijnmazige toestemmingsopties moeten bieden en gegevens goed moeten beveiligen.

Het CBP schrikt niet terug voor nieuwe, maatschappelijk relevante ontwikkelingen

Ook de Nederlandse toezichthouder schrikt er niet voor terug om nieuwe, maatschappelijk relevante ontwikkelingen aan te snijden. De beschikking over de tablets van Snappet is hiervan een mooi voorbeeld.[6] Snappet levert tablets met onderwijssoftware aan meer dan 400 scholen in Nederland. Via die software verzamelt het bedrijf gedetailleerde gegevens over de vorderingen van leerlingen tussen de 7 en 9 jaar. Die gebruikt zij voor de scholen (zodat docenten bijvoorbeeld de resultaten van leerlingen ten opzichte van de klas kunnen volgen). Zij gebruikt die informatie ook voor doeleinden die anderen dan de school ten goede komen: zo hoopt Snappet in de toekomst dyslexie vroegtijdig te kunnen signaleren.

De belangrijkste vraag in deze beschikking was in hoeverre Snappet zelf verantwoordelijke in de zin van de Wbp was (en zich dus aan de belangrijkste regels van de Wbp moest houden). Volgens het CBP is dat het geval. Hoewel de scholen op papier wellicht verantwoordelijke leken, waren ze dat in de praktijk niet. Daarbij staat centraal dat, willen de scholen hun rol als verantwoordelijke kunnen uitoefenen, zij hiervoor voldoende informatie van Snappet moeten krijgen. Die informatie kregen ze nu niet.

3 Zie Artikel 29 werkgroep 9 april 2014, *Opinion 06/2014 on the 'Notion of legitimate interests of the data controller' under Article 7 of Directive 95/46/EC*. Zie verder Artikel 29 werkgroep 10 april 2014, *Opinion 05-2014 on Anonymisation Techniques onto the web* en Artikel 29 werkgroep 25 november 2014, *Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting* voor de hieronder besproken opinies.

4 Zie CBP 15 november 2011, 'Google kondigt opt-out mogelijkheid aan voor verwerking wifi-gegevens' (persbericht), te vinden op: http://bit.ly/1MejOox.

5 Zie Artikel 29 werkgroep 16 september 2014, *Opinion 8/2014 on the on Recent Developments on the Internet of Things.*

6 Zie CBP 14 juli 2014, Onderzoek CBP naar de verwerking van persoonsgegevens door Snappet, z2013-00795.

De situatie die het CBP in de beschikking bespreekt is niet beperkt tot het onderwijs. Waar verschillende schakels in de waardeketen de beschikking hebben over gegevens die binnen de keten worden verwerkt – iets dat je vaak in cloudomgevingen ziet – zal al snel de vraag rijzen in hoeverre die schakels ook verantwoordelijke zijn. De beschikking geeft een begin van een antwoord op de vraag waar de scheidslijn tussen de verantwoordelijke en de bewerker in zo'n geval moet worden getrokken.

Een ander voorbeeld van een onderzoek naar een actueel onderwerp, is de beschikking over Okki's Gekkebekkenclub. Kinderen konden met een tandenpoets-app foto's van hun tanden uploaden naar www.gekkebekkenclub.nl. Soms waren foto's gepubliceerd van deels herkenbare kinderen, met naam, leeftijd en woonplaats. De beschikking voelt als prijsschieten voor het CBP, alleen al omdat de website op basale punten niet *compliant* was (er was geen privacybeleid, er werd geen versleuteling toegepast en er werd geen toestemming van de wettelijk vertegenwoordiger gevraagd). De beschikking is daarom inhoudelijk niet zo interessant. Het is wel aardig om te zien dat het onderzoek is gestart naar aanleiding van een rapport van Mijn Kind Online, een kenniscentrum voor jeugd en digitale media. Het bevestigt dat, als een belangrijk deel van het feitenonderzoek al is gedaan, het CBP een onderzoek eerder oppakt.

De meest gewaagde acties van het CBP kwamen echter op de valreep van 2014. In december legde het Google een last onder dwangsom op, als *follow up* van het eerdere onderzoek naar het privacybeleid van Google. Google moet voor het combineren van persoonsgegevens uit haar verschillende diensten (zoals YouTube en Search) ondubbelzinnige toestemming krijgen. Daarnaast moet zij gebruikers beter informeren. Als Google niet vóór 27 februari 2015 voldoet aan deze last verbeurt ze een dwangsom van € 20.000,– per dag, met een maximum van € 5 miljoen.

Daarnaast stelde het CBP een onderzoek in naar het nieuwe privacybeleid van Facebook.[7] Omdat Facebook van plan was gegevens en foto's uit Facebook-profielen per 1 januari 2015 voor commerciële doeleinden te gebruiken, heeft het CBP gevraagd te wachten met de uitrol tot de resultaten van haar onderzoek bekend zijn. Opmerkelijk is dat Facebook al vóór implementatie had besloten andere voorwaarden toe te passen voor Duitse Facebook-gebruikers.[8] Facebook heeft overigens op eerste kerstdag de inwerkingtreding van de voorwaarden uitgesteld tot 30 januari 2015, omdat volgens de woordvoerder nog niet alle gebruikers één maand van tevoren waren geïnformeerd.[9] Het CBP hoopte voor die termijn de eerste conclusies van haar onderzoek met Facebook te kunnen delen, maar hierover is op dit moment nog niets bekend.

Die Amerikaanse internetreuzen zullen zich deze kerst dus ongetwijfeld achter hun oren hebben gekrabd. Maar een échte verrassing kan het niet zijn. Nederland heeft zich de afgelopen jaren ontpopt tot één van de Europese landen waar het debat over privacy en communicatievrijheid op het scherpst van de snede wordt gevoerd. Bovendien geeft de *Google/Spanje*-uitspraak van het Europese Hof van Justitie, waarin een brede toepassing van de territoriale reikwijdte van de nationale privacywetten wordt omarmd, nationale toezichthouders een steun in de rug.

Het Europese Hof van Justitie neemt stelling vóór privacy...

Want dat is nog iets wat is veranderd: in 2014 heeft het Europese Hof van Justitie zich op het gebied van privacy ontpopt tot een serieuze tegenstrever van het Europees Hof voor de Rechten van de Mens. Ik bedoel niet het arrest van december 2014 over de toepassing van de 'privé-exceptie' van de Richtlijn bescherming persoonsgegevens, waarin het Hof oordeelde dat als een surveillancecamera deels gericht is op een publieke weg, die exceptie niet van toepassing is.[10] Nee: in april verklaarde het Hof van Justitie de Europa-brede, ongerichte opslagverplichting van telecomgegevens op grond van de Bewaarplichtrichtlijn ongeldig.[11] En in mei oordeelde het Hof in *Google/Spanje* vervolgens dat zoekmachines geen irrelevante zoekresultaten mogen tonen als een betrokkene daarom verzoekt.[12]

Dat arrest over de relevantie van zoekresultaten is een fundamenteel en mediageniek arrest. Het Hof bespreekt de geografische toepasselijkheid van nationale wetgeving (die is al snel van toepassing) en de uitleg van het begrip 'verantwoordelijke' (die uitleg is breed). Het arrest haalde echter de media met de invulling die het Hof geeft aan het recht op verwijdering en verzet: zoekresultaten die 'ontoereikend, niet of niet meer ter zake dienend of bovenmatig' zijn, moet Google op verzoek niet meer tonen bij een zoekopdracht naar die persoon. Het Hof wijdt in dat verband een aantal stevige overwegingen aan de verhouding tussen de vrijheid van meningsuiting en het grondrecht op privacy (zoals neergelegd in artikel 7 en 8 van het Handvest). Volgens het Hof krijgt het recht op verzet in beginsel voorrang op het economische belang van de zoekmachine-exploitant en het belang van het publiek om informatie te vinden. Dat kan anders zijn als publicatie van de informatie waarnaar wordt verwezen in de zoekresultaten in het publiek belang is.

Ook in het arrest over de Richtlijn bewaarplicht telecomgegevens laat het Hof dat grondrecht op privacy zwaar wegen, al wijdt ze wel een aantal ongelukkige overwegingen aan het 'wezen' van die grondrechten. Het wezen van het grondrecht op gegevensbescherming (artikel 8 Handvest) wordt volgens het Hof niet aangetast, omdat de Bewaarplichtrichtlijn de lidstaten verplicht om beveiligingsmaatregelen te nemen. Het Hof wekt daarmee ten onrechte suggestie dat de kern van gegevensbescherming draait om goede beveiliging van gegevens. Ook het wezen van artikel 7 wordt volgens het Hof niet aangetast, omdat de richtlijn niet ziet op de inhoud van communicatie. Het onderscheid tussen 'verkeer' en 'inhoud' is echter niet altijd goed te maken: een URL (verkeer) met daarin verwerkt een zoekopdracht verraadt al snel de interesse van de bezoeker (inhoud). Belangrijker nog: gedragsgegevens zelf kunnen soms minstens evenveel informatie prijsgeven als de communicatie-inhoud.

7 Zie CBP 16 december 2014, 'CBP onderzoekt nieuwe privacyvoorwaarden Facebook' (persbericht), te vinden op: http://bit.ly/1yY5HC2. Zie verder CBP 17 november 2014, Last onder dwangsom Google Inc., te vinden op: https://cbpweb.nl/sites/default/files/atoms/files/last__onder__dwangsom__google__privacyvoorwaarden.pdf voor de last onder dwangsom van het CBP.

8 Zie https://www.facebook.com/legal/terms/update.

9 Zie NOS 30 december 2014, 'Facebook stelt nieuwe privacyvoorwaarden uit', te vinden op: http://nos.nl/artikel/2011151.

10 HvJ EU 11 december 2014, C-212/13 (*František Ryneš/Úřad pro ochranu osobních údajů*).

11 HvJ EU 8 april 2014, C-293/12 en C-594/12 (*Digital Rights Ireland en Seitlinger e.a*).

12 HvJ EU 13 mei 2014, C-131/12 (*Google Spain SL, Google Inc/Agencia Española de Protección de Datos, Mario Costeja González*).

Gelukkig past het Hof de proportionaliteitstoets wel streng toe. Het gaat in op de ongerichtheid van de opslag en het feit dat de richtlijn de toegang en het gebruik hiervan niet goed regelt. Ook de onbepaaldheid van de bewaartermijn en de beperkte regels rond de beveiliging van de bewaarde gegevens wegen mee. Het Hof concludeert dat de richtlijn ongeldig is, met terugwerkende kracht – dus de richtlijn wordt geacht nooit bestaan te hebben. De vraag is nu wat dit betekent voor de nationale implementatiewetten.

Maar de Nederlandse overheid laat zich daaraan weinig gelegen liggen

Als het aan de Nederlandse overheid ligt: vrijwel niets. En dat is nog een thema dat zich – helaas – scherper aftekent in het afgelopen jaar: de Nederlandse overheid laat zich weinig gelegen liggen aan het grondrecht op privacy. Naar aanleiding van de uitspraak van het Hof heeft de Raad van State de regering geadviseerd dat, omdat de wet ongeveer dezelfde inhoud heeft als de richtlijn, belangrijke delen ongeldig zijn.[13] De Raad van State concludeert voorzichtig dat juist het ongericht karakter van de opslag strijdig is met het noodzakelijkheidscriterium uit het Handvest. Ook andere plannen om gegevens van burgers ongericht te bewaren zouden hierom strijdig kunnen zijn met het Handvest, suggereert de Raad van State.

De regering heeft dit advies echter naast zich neergelegd en houdt de wet in stand in afwachting van een wijzigingswet die slechts een aantal waarborgen zou introduceren.[14] Het CBP heeft in februari 2015 korte metten gemaakt met het voorstel voor die wijzigingswet, maar de regering lijkt ook dat oordeel naast zich neer te leggen.[15] Ook ziet de regering in het oordeel van het Hof geen aanleiding om andere plannen, voor de ongerichte kentekenregistratie, door de politie aan te passen. Sterker nog: zij blijft zelfs vasthouden aan haar voornemen om de Wet op de inlichtingen- en veiligheidsdiensten te wijzigen zodat ongerichte kabelgebonden interceptie mogelijk wordt (een grootschalige internettap, dus).[16] Het wordt daarom interessant wat het EHRM in de nu aanhangige *Big Brother Watch*-zaak zal oordelen: daarin staat de toelaatbaarheid van de massale interceptie van internetverkeer via transatlantische kabels centraal.[17] Al is het de vraag of de Nederlandse overheid zich dáár wel wat van aan zal trekken, natuurlijk.

Ten slotte hoort in deze categorie het schokkende nieuws dat de AIVD advocaten van kantoor Prakken d'Oliveira lange tijd heeft afgeluisterd. Het kantoor had hierover een klacht ingediend, en minister Plasterk heeft die klacht deels gegrond verklaard.[18] Hij kondigt echter geen maatregelen aan om dit in de toekomst te voorkomen.

Gelukkig krijgt procederen in Nederland over privacy vorm

Het is dan ook goed om te zien dat er meer wordt geprocedeerd over privacy, juist tegen de Staat. Zo vraagt een coalitie van belangenorganisaties en providers in een kort geding tegen de Staat om de huidige bewaarplichtwet ongeldig te verklaren.[19] De uitspraak volgt waarschijnlijk in 2015.

Dat wil trouwens niet zeggen dat al die procedures tegen de Staat ook een goed einde krijgen. Zo was de Belastingdienst tegen SMSParking een procedure gestart over de weigering om de gegevens van al haar klanten in bulk af te staan omwille van de opsporing van frauderende leaserijders. In eerste instantie kreeg SMSParking nog gelijk: de voorzieningenrechter vond in 2013 zo'n brede vordering in strijd met artikel 8 EVRM.[20] In hoger beroep overweegt het Hof Den Bosch in 2014 echter dat vorderingen in de context van de belastingheffing al snel voldoen aan de proportionaliteitstoets, en concludeert het dat ook in dit geval de vordering evenredig is.[21]

Ook de procedure over het uitwisselen van communicatiedata door de Nederlandse geheime diensten met de NSA, ook wel bekend als 'Burgers tegen Plasterk', is voorlopig niet goed geëindigd. In een uitgebreid gemotiveerd vonnis komt de Rechtbank Den Haag tot de opmerkelijke conclusie dat de uitwisseling van gegevens in bulk minder inbreukmakend zou zijn dan de uitwisseling van gericht verzamelde gegevens.[22] Dat is onwenselijk, omdat het verwerken van méér data juist inbreukmakender is dan het verwerken van mínder data. Ik hoop dan ook dat dit vonnis in hoger beroep wordt vernietigd.

Het *safe harbour*-regime komt verder onder vuur te liggen

Die verliezen weerhouden activisten er ondertussen niet van om rechtszaken te starten. Eén van de meer gewaagde rechtszaken met een maatschappelijk doel, is de zaak van Max Schrems tegen de Ierse privacytoezichthouder.[23] Deze 'data privacy activist' (zijn woorden) heeft naam gemaakt met zijn actiegroep Europe v. Facebook, waarmee hij probeerde inzage te krijgen in zijn gegevens bij Facebook. Nu richt hij zijn pijlen op het *Safe Harbour*-regime: hij had de Ierse toezichthouder gevraagd om te bepalen dat de gegevensoverdracht van Facebook naar de Verenigde Staten onrechtmatig zou zijn, omdat uit de Snowden-onthullingen blijkt dat de VS geen passende bescherming bieden. Het Ierse High Court heeft het Europese Hof van Justitie vervolgens gevraagd of een toezichthouder gebonden is aan de *Safe Harbour*-beschikking van de Europese Commissie, of dat de toezichthouder de vrijheid heeft om zelf in het licht van recente ontwikkelingen te bepalen dat een land desondanks geen passende bescherming biedt.

Het is één van de manieren waarop het Safe Harbour-regime verder wordt uitgekleed. Ook het Europees Parlement heeft

13 Zie *Kamerstukken II* 2014/15, 31145, nr. AA en de bijlagen.
14 *Idem*.
15 Zie Wetgevingsadvies CBP 10 februari 2015 over de Wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met het aanbieden van openbare elektronisch telecommunicatiediensten, http://bit.ly/1yY5HC2.
16 Zie *Kamerstukken II* 2014/2015, 33 820, nr. 4.
17 Zie Application no. 58170/13 (*Big Brother Watch e.a./Verenigd Koninkrijk*).
18 Zie Prakken d'Oliveira 18 december 2014, 'AIVD luistert advocaten Prakken d'Oliveira af', te vinden op: http://bit.ly/18pWB50.
19 Zie onder meer NVJ 16 januari 2015, 'Kort geding tegen Wet Bewaarplicht Telecommunicatie' (persbericht), te vinden op http://bit.ly/1EWBq8g.
20 Vzr. Rb. Oost-Brabant 26 november 2013, *ECLI:NL:RBOBR:2013:6553* (*Belastingdienst/SMSParking*).
21 Hof Den Bosch 19 augustus 2014, *ECLI:NL:GHSHE:2014:2803* (*Belastingdienst/SMSParking*).
22 Rb. Den Haag 23 juli 2014, *ECLI:NL:RBDHA:2014:8966* (*Burgers/Plasterk*).
23 Zie het verzoek in zaak C-362/14 en http://europe-v-facebook.org/EN/en.html.

een motie aangenomen waarin ze oproept om de *Safe Harbour*-beschikking op te schorten.[24] En het schijnt dat de Duitse toezichthouders in Bremen en Berlijn een onderzoek zijn gestart naar twee Amerikaanse bedrijven die gegevens overdragen in het kader van het *Safe Harbor*-regime.[25]

Security staat in de schijnwerpers

Een ander onderwerp dat mede door de Snowden-onthullingen meer aandacht krijgt is informatiebeveiliging. Zo gaan grote bedrijven communicatie van begin tot eind versleutelen: WhatsApp (overgenomen door Facebook) heeft alle apps *end-to-end* versleuteld en Google ontwikkelt een Gmail-encryptie plugin.[26]

Maar ook het CBP vindt security belangrijk: in 2015 is dit voor het CBP zelfs een van de vijf thema's waarop het zich richt. Het meest opvallende voorbeeld uit 2014 vond ik dat het CBP naar aanleiding van het OpenSSL-lek (bekend als Heartbleed) in de gaten hield of voldoende onveilige beveiligingscertificaten werden ingetrokken.[27] Ook sloot het CBP in 2014 het onderzoek naar de beveiliging bij SWIFT af – een onderzoek dat was gestart omdat uit de Snowden-onthullingen zou blijken dat de NSA dat internationale betalingsnetwerk had gehackt. Het CBP vond geen overtredingen van de Wbp-beveiligingsnorm.[28]

Verder publiceerde het CBP in 2014 haar bevindingen over de beveiliging bij het Groene Hart ziekenhuis. De beschikking is aardig omdat het CBP hierin aangeeft hoe je met legacy-systemen waarop bedrijfskritieke processen draaien moet omgaan: die moeten in een quarantaine-netwerk worden geplaatst.[29] Ook deed het CBP onderzoek naar de beveiliging van Suwinet, een systeem waarin overheidsinstellingen gegevens over werk en inkomen kunnen uitwisselen.[30] Het onderzoek legt de nadruk beveiliging van *toegang*: die moet beperkt zijn, zowel qua *mensen* die toegang krijgen, als *gegevens waartoe* ze toegang krijgen. Zo bleek in dit geval onder meer dat het Ierse Ministerie van Sociale Zaken toegang had tot de gegevens van alle mensen in Suwinet, hoewel zij slechts toegang zou hoeven te hebben tot Ieren die in Nederland hebben gewerkt. Het systeem was dan ook niet goed genoeg beveiligd.

Informatiebeveiliging kreeg ook meer aandacht in de rechtspraak. Zo bespreekt de Rechtbank Amsterdam uitgebreid of de verkoper van Diginotar zijn beveiligingsgarantie, afgegeven in het kader van de verkoop van Diginotar aan een Amerikaanse partij, had geschonden.[31] Dat is zo en de verkoper moet een schadevergoeding betalen, omdat door die slechte beveiliging Diginotar gehackt kon worden en uiteindelijk failliet is gegaan. De Rechtbank Midden-Nederland heeft verder in een procedure over de beveiliging van het LSP (de nieuwe naam van het Elektronisch Patiëntendossier) zich in een civiele procedure gebogen over de vraag wanneer een systeem veilig genoeg is (in de zin van artikel 13 Wbp). De rechtbank sluit aan bij een beveiligingsstandaard en komt tot de conclusie dat aan die standaard is voldaan.[32] Hiertegen is hoger beroep ingesteld.

En het bleef erg stil rond de Privacyverordening

En één trend viel meer op door zijn afwezigheid: de herziening van de Europese gegevensbeschermingregels. Nadat het Europees Parlement op 12 maart 2014 de concept-Privacyverordening in eerste lezing had aangenomen, ligt het concept nu al bijna een jaar bij de Raad van Ministers. *Insiders* maken zich zorgen over de onderhandelingen bij de raad: zo wordt er onderhandeld aan de hand van het beginsel dat over niets een akkoord is bereikt, tot over de hele verordening een akkoord is bereikt. Dat biedt veel ruimte voor verwatering van de regels. Duitsland schijnt zich ondertussen te verzetten omdat zij verwacht dat de verordening onder haar nationale beschermingsniveau zou duiken. En de onderhandelingen over een nieuw handelsverdrag tussen Amerika en Europa gaan door – met waarschijnlijk ook bepalingen over gegevensbescherming – zodat de ruimte voor strenge regels in de nieuwe verordening mogelijk nog verder wordt ingeperkt.

Het is daarom niet slecht dat de Nederlandse regering ondertussen een aantal voorstellen in de pijplijn heeft die het beschermingsniveau in Nederland enigszins zouden verbeteren.[33] Ten eerste komt er een meldplicht datalekken aan. Ten tweede krijgt het CBP – die dan de Autoriteit persoonsgegevens zou gaan heten – de bevoegdheid om een bestuurlijke boete van maximaal € 810.000,– op te leggen. Dit voorstel is in februari 2015 door de Tweede Kamer aangenomen, en wordt nu door de Eerste Kamer besproken.

Tot slot: een *slow motion*-botsing, met horten en stoten

Technologische ontwikkelingen liggen al een paar jaar op ramkoers met het privacyrecht. Er kán steeds meer, maar er mág niet meer (en misschien zelfs minder). Het afgelopen jaar tekenden de breuklijnen van dit conflict zich scherper af. Security is heel belangrijk, zo vindt ook het CBP. Maar zelfs de meest basale beveiligingsmaatregelen worden vaak niet genomen. Het ongericht opslaan van gedragsgegevens is verboden, zo oordeelde het Hof. Maar de Nederlandse regering handhaaft de bewaarplicht en introduceert een nieuwe ongerichte afluisterbevoegdheid. Het commercieel exploiteren van klantgegevens is controversieel, zo blijkt uit de ING-affaire. Maar veel bedrijven werken aan *big data*-plannen.

Het is niet te verwachten dat dit conflict dit jaar wordt beslecht. Dat betekent dat de praktijk en de regels verder uit elkaar zullen groeien. In dat vacuüm zullen ongeschreven, maatschappelijke normen vaak de doorslag geven. Mijn voorspelling voor 2015? Privacyjuristen worden iets minder jurist, en iets meer onderzoeker van die maatschappelijke normen.

24 Zie Europees Parlement 12 maart 2014, 'US NSA: stop mass surveillance now or face consequences, MEPs say' (persbericht), te vinden op http://bit.ly/1iA2YYa.

25 Zie Hunton & Williams 28 januari 2015, 'German DPAs Host Event Regarding U.S.-EU Safe Harbor Framework and Initiate Administrative Proceedings Against Two U.S. Companies', te vinden op http://bit.ly/1A6ASXM.

26 Zie Open Whisper Systems 18 november 2014, 'Open Whisper Systems partners with WhatsApp to provide end-to-end encryption' (blog), te vinden op: https://whispersystems.org/blog/whatsapp/ en Google online security blog 16 december 2014, 'An Update to End-To-End'(blog), te vinden op: http://googleonlinesecurity.blogspot.nl/2014/12/an-update-to-end-to-end.html

27 Zie CBP 18 april 2014, 'Verscherpte aandacht CBP voor OpenSSL', te vinden op: https://cbpweb.nl/nl/nieuws/verscherpte-aandacht-cbp-voor-openssl.

28 Zie CBP 8 mei 2014, 'Privacytoezichthouders constateren geen overtredingen bij SWIFT', te vinden op: http://bit.ly/1DVeKRv.

29 CBP 6 oktober 2014, Onderzoek naar de beveiliging van het netwerk van het Groene Hart Ziekenhuis, z2012-00717.

30 CBP 4 november 2014, Onderzoek Suwinet UWV en Onderzoek Suwinet Gemeente Den Bosch, z2013-00560 en z2014-00238.

31 Rb. Amsterdam 30 juli 2014, *ECLI:NL:RBAMS:2014:4888* (*Ratonigid e.a./Vasco*).

32 Rb. Midden-Nederland 23 juli 2014, *ECLI:NL:RBMNE:2014:3097* (*VPH/VZVZ*).

33 Zie *Kamerstukken II* 2014/2015, 33 662.