E.F.D. Engelhard[1]

Immateriële schade als gevolg van data-inbreuken: het ondergeschoven kindje van de AVG

NTBR 2019/30

Bij schending van de Algemene Verordening Gegevensbescherming (AVG) geeft art. 82 AVG de benadeelde recht op schadevergoeding van de materiële en immateriële schade. Hiermee biedt de AVG een zekere waarborg om de toegenomen vrijheid van gegevensuitwisseling en -opslag die het internet biedt, te beschermen. Maar wat in dit verband onder immateriële schade wordt verstaan, is verre van duidelijk en veelal is de schade bij AVG-schendingen van geringe omvang. De kernoverwegingen van het *EBI*-arrest van 15 maart 2019 bieden, indien doorgetrokken naar het onderhavige terrein van data-inbreuken, op een drietal punten verbetering, maar kennen ook serieuze beperkingen voor de positie van de benadeelde.

1. Inleiding

In de gedigitaliseerde samenleving deelt vrijwel iedereen voortdurend – gewild, maar ook ongewild – allerlei gegevens over zijn persoon en identiteit en gegevens over andere personen. Als dit zuivere privéactiviteiten betreft, dan wordt de aansprakelijkheid die daar eventueel voor kan ontstaan, beheerst door het aansprakelijkheidsregime van het Burgerlijk Wetboek.[2] Maar voor zover het de verwerking van persoonsgegevens betreft door bijvoorbeeld sociale media (*Facebook, Instagram,* e.d.), werkgevers (voor wat betreft hun personeelsadministratie), verenigingen (de ledenadministratie), winkels (klantenbestanden), *et cetera,* gelden strikte regels ingevolge de Algemene verordening gegevensbescherming (AVG),[3] die op 25 mei 2018 van kracht is gegaan.[4]

De begrippen persoonsgegevens[5] en verwerking[6] worden daarbij ruim uitgelegd. Persoonsgegevens moeten 'worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is' en verwerking is gebonden aan hetgeen noodzakelijk is voor 'welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden'.[7] Ook moeten persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor deze doeleinden noodzakelijk is. Door het nemen van maatregelen dient passende beveiliging te zijn gewaarborgd.[8] Doel van de AVG is dat zij 'de grondrechten en fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens' waarborgt.[9] Bij schending van de AVG geeft art. 82 lid 1 AVG personen die daardoor materiële of immateriële schade hebben geleden, jegens de verwerkingsverantwoordelijke[10] en jegens de verwerker[11] recht op schadevergoeding.[12]

Typische inbreuken op persoonsgegevens (hierna: data-inbreuken) ontstaan bij *hacking, phishing* en andere vormen van *cybercrime* (in combinatie met inadequate bescherming), maar dan zal er veelal geen identificeerbare en solvabele dader zijn. De gepubliceerde rechtspraak laat vooral inbreuken zien door slordigheid en kennisgebrek: organisaties (denk naast de hiervoor genoemde voorbeelden aan gemeenten, het Uitvoeringsinstituut Werknemersverzekerin-

1 Citeerwijze: E.F.D. Engelhard, 'Immateriële schade als gevolg van data-inbreuken: het ondergeschoven kindje van de AVG', *NTBR* 2019/30, afl. 9/10. Esther Engelhard is universitair hoofddocent en verbonden aan het Utrecht Centre for Accountability and Liability Law (Ucall), Universiteit Utrecht en raadsheer-plaatsvervanger bij het gerechtshof 's-Hertogenbosch.

2 De hierna te noemen AVG geldt (o.m.) niet voor de (beperkte) informatie die mensen bijv. op hun *Facebook, Twitter* of *Instagram*-account zetten, zie art. 2 lid 2, sub c AVG (mits dit 'zuiver persoonlijke of huishoudelijke' activiteiten zijn); zie in dit verband E.R. de Jong & E. Steendam Visser, 'Sharenting & aansprakelijkheid: wanneer is de delende ouder aansprakelijk?', *AA* 2019, p. 642-645.

3 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betr. de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, L/119, 4 mei 2016. Momenteel ligt een voorstel voor de *E-Privacy* verordening (ePV) voor bij de Raad van de EU met regels voor nieuwe internet-telecomdiensten, zoals *Whatsapp* en *Facebook Messenger*, ter aanvulling van de AVG (en ter vervanging van richtlijn 2002/58/EG, waar de Telecommunicatiewet op berust). *Proposal for a Regulation on Privacy and Electronic Communications* 10 januari 2017, COM(2017) 10. Zie de geconsolideerde versie in het Raadsdocument van 26 juli 2019, nr. 11291/19 (2017/0003(COD)).

4 Tot 25 mei 2018 gold de Richtlijn 95/46/EG, L/119, 4 mei 2016 (de Privacyrichtlijn) en ter uitvoering daarvan de Wet bescherming persoonsgegevens (Wbp).

5 Art. 4, onder 1 AVG: 'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon'. 'Identificeerbaar' zijn gegevens doordat ze bestaan uit de 'naam, identificatienummer, locatiegegevens, een online identificator of één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke personen', bijv. ook internetprotocol (IP)-adressen en identificatie (tracking) cookies (aldus onderdeel 30 van de Considerans) en dit ziet dus ook op belgedrag en locatiegegevens in smartphones.

6 Art. 4, onder 2 AVG: het 'verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens'.

7 Art. 5 lid 1, sub a AVG.

8 Art. 5 lid 1, sub e en f AVG.

9 Art. 1 lid 2 AVG, waarbij het vrije verkeer van persoonsgegevens niet mag worden beperkt/verboden (lid 3).

10 D.i. een natuurlijke persoon of rechtspersoon die, alleen of met anderen, 'het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt' (art. 4, onder 7 AVG); dit begrip wordt ruim uitgelegd, aldus het HvJ EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317, *Google v. Spain* en zie ook HvJ EU 5 juni 2018, C-210/16, ECLI:EU:C:2018:388, *Wirtschaftsakademie;* HvJ EU 10 juli 2018, C-25/17, ECLI:EU:C:2018:551, *Jehovan todistajat* en HvJ EU 29 juli 2019, C-40/17, ECLI:EU:C:2019:629, *Fashion ID*.

11 Degene die 'ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt' (art. 4, onder 8). Voor de verwerker geldt een minder strikt regime, zie de tweede volzin van art. 82, tweede lid AVG.

12 In hoeverre daarnaast of in plaats daarvan een vordering uit onrechtmatige daad mogelijk is, is niet helemaal duidelijk; vgl. ontkennend ten aanzien van de verhouding tussen art. 6:162 BW en het *termijn*voorschrift van art. 35 AVG, Rb. Den Haag 28 februari 2019, ECLI:NL:RBDHA:2019:1988, *Eiser/Rabobank e.a.,* r.o. 3.9.

gen (UWV),[13] banken,[14] scholen, enz.) ontvangen, verwerken en bewaren talloze persoonsgegevens van hun werknemers en van klanten en/of bezoekers, doch lang niet altijd conform de AVG. Denk aan het abusievelijk extern openzetten van het administratiesysteem of het onversleuteld versturen van bestanden naar de verkeerde geadresseerde.[15] Persoonsgegevens worden zo onterecht beschikbaar gesteld aan derden en er kunnen verdere nadelige gevolgen ontstaan: ze worden oneigenlijk gebruikt (denk aan vormen van uitsluiting, discriminatie, identiteitsfraude, enz.) en worden, eventueel met *datamining*-technieken, gebruikt voor ongewenste advertenties, beïnvloeding of manipulatie, *microtargeting,*[16] enzovoort. Het verbaast dan ook niet dat 94% van de Nederlanders zich, volgens een peiling eerder dit jaar, grote zorgen maakt over de veiligheid van persoonsgegevens.[17] Dat versterkt het wantrouwen in het digitaal verkeer en bevordert *'social cooling'*.[18]

Dit kan ingrijpende gevolgen hebben voor de betrokkene; hij voelt zich 'bespied' of aangetast in de menselijke vrijheid om over eigen informatie te beschikken. Hij kan dan, waar dit voor hem (nog) relevant kan zijn, een vordering tot ongedaanmaking instellen of tot verwijdering of andere vormen van een rechterlijk gebod of verbod, maar ook of daarnaast kan hij schadevergoeding vorderen. De schadevordering kan betrekking hebben op 'harde kosten' waarvan rechtens vaststaat dat die het gevolg zijn van de data-inbreuk (denk aan identiteitsfraude waarbij de frauduleuze schulden hoog oplopen). Maar in het merendeel van de gevallen gaan schadeclaims over data-inbreuken daar niet over. Afgaande op gepubliceerde rechtspraak zien schadeclaims vooral op immateriële schade.[19] Hierbij kan onder meer worden gedacht aan angstgevoelens en leed/verdriet als gevolg van het feit dat de privégegevens onrechtmatig zijn verkregen en/of verwerkt of 'op straat liggen' en eventueel gevolgschade, bijvoorbeeld verband houdend met gevolgen van de inbreuk in de relationele sfeer.

Hoewel zich in schadeprocedures over data-inbreuken natuurlijk ook andere vormen van schade en schadevragen voordoen, ligt de focus in de onderhavige bijdrage bij schade van immateriële aard. De centrale vraag luidt: op welke gronden en in hoeverre heeft de benadeelde recht op schadevergoeding voor immateriële schade respectievelijk het verlies van controle over zijn persoonsgegevens die/dat het gevolg is van data-inbreuken onder de AVG (waarbij wordt verondersteld dat aansprakelijkheid voor de inbreuk vaststaat)?[20]

2. Art. 82 AVG: een onduidelijk schadebegrip

Opvallend is dat de AVG over het schadebegrip weinig helder is. Uitgangspunt is dat de eiser dient te stellen en zo nodig te bewijzen dat hij schade lijdt. Maar art. 82 AVG volstaat met de zinsnede dat het recht op schadevergoeding op materiële én immateriële schade ziet en geeft daarbij dus *niet* aan wat onder 'schade' dient te worden verstaan of hoe zij dient te worden gewaardeerd.

Wel wijst de considerans van de AVG erop dat 'schade' ruim moet worden uitgelegd, 'in het licht van de rechtspraak van het Hof van Justitie, op een wijze die ten volle recht doet aan de doelstellingen van deze verordening' en dat zij 'volledig en daadwerkelijk' moet worden vergoed.[21] Ook staat er dat data-inbreuken kunnen leiden tot *'lichamelijke, materiële of immateriële schade voor natuurlijke personen, zoals verlies van controle over hun persoonsgegevens of de beperking van hun rechten,* discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, ongeoorloofde ongedaanmaking van pseudonimisering, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, *of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie'*.[22] Maar deze passage is destijds voorgesteld en is in de considerans geplaatst met het oog op de notificatieplicht en de passende maatregelen die vereist zijn door de verwerkingsverantwoordelijke.[23] Zij heeft niet het karakter van een juridisch-technische specificatie over schade; zo worden het verlies van controle en 'de beperking van rechten' gelijkelijk genoemd met klassieke schadeposten, zoals financiële verliezen en reputatieschade. Hier lijkt bijvoorbeeld niet reeds uit te kunnen worden afgeleid dat de opstellers al 'het in andere handen geraken van persoonsgegevens' zonder meer als schade in de zin van art. 82 AVG aanmerken. De bedoeling van deze opsomming is kennelijk niet om aan te geven wat als vergoedbare 'schade' heeft te gelden, maar slechts om een scala aan gevallen te noemen waarin de notificatieplicht en/of de verplichting tot het nemen van passende maatregelen gelden of kunnen gelden. Voor de invulling van

13 Zie bijv. Rb. Amsterdam 2 september 2019, *JAR* 2019/241, ECLI:NL:RBAMS:2019:6490, *UWV*.

14 Die gegevens verder verwerken, *De Volkskrant* 3 juli 2019. De AP waarschuwt de Nederlandse Vereniging van Banken (NVB), maar zij treedt (vooralsnog) niet op, https://www.autoriteitpersoonsgegevens.nl/nl/nieuws.

15 P.A. Nabben & E.C. Post Uiterweer, 'De AVG: hoe heet wordt de soep gegeten?', *AR* 2019, p. 19-25 (p. 24).

16 Zie bijv. J.M. Benning, 'The average online consumer', *TC&H* 2018, nr. 5, p. 218-227.

17 Dit blijkt uit een enquête die in opdracht van de Autoriteit Persoonsgegevens (AP) werd uitgevoerd tussen 12 en 17 januari 2019, laatstelijk geraadpleegd op 23 april 2019: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/resultaten_enquete_privacyzorgen_jan_2019.pdf.

18 Dat is het remmend effect (*chilling effect)* dat erop neerkomt dat mensen zich – doordat zij zich minder vrij voelen – onthouden van deelname aan het dataverkeer, zie bijv. https://www.socialcooling.com/.

19 Zie o.m. Rb. Noord-Nederland 3 mei 2017, ECLI:NL:RBNNE:2017:1700, *WSNP-gegevens*; Rb. Amsterdam 31 januari 2019, ECLI:NL:RBAMS:2019:645, *MMP*; Rb. Den Haag 28 februari 2019, ECLI:NL:RBDHA:2019:1988, *BKR-registraties;* Rb. Overijssel 28 mei 2019, ECLI:NL:RBOVE:2019:1827, *Email Wob-verzoeken*; en Rb. Amsterdam 2 september 2019, ECLI:NL:RBAMS:2019:6490, *UWV*.

20 Ook causaliteitsvragen vallen buiten het kader van dit bestek. Zie daarover Walree 2017, p. 923-924.

21 Onderdeel 146 van de considerans van de AVG.

22 Onderdeel 85 (cursief toegevoegd, EE).

23 Raadsdocument 14901/13, ADD 2, 30 oktober 2013, p. 24. Dit en het bijbehorende Raadsdocument bieden weinig toelichting, noch overige raadsdocumenten die ik heb kunnen achterhalen via het register van de Raad van de Europese Unie (https://www.consilium.europa.eu/register/en).

het schadebegrip moeten wij het dus stellen met de aanwijzing in de considerans dat die dient te worden gegeven op een wijze die ten volle recht doet aan de doelstellingen van deze verordening. Daarom zal hier in het navolgende eerst meer aandacht aan worden besteed.

3. Welke betekenis, if any, komt hierbij toe aan doelstellingen van de AVG?

3.1 *Rechtsbescherming en normhandhaving*

De vraag wat als schade wordt aangemerkt in de zin van art. 82 AVG, kan zoals gezegd niet los worden gezien van de doelstellingen van de AVG. Die doelstelling houdt in dat zij 'de grondrechten en fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens' waarborgt.[24] De AVG dient dus eerst en vooral de burger, hetgeen ook blijkt uit de diverse rechten waarmee de AVG hem toerust, zoals het recht op rechtmatige verwerking en diverse specifieke rechten, zoals het recht op vergetelheid en het recht om geïnformeerd te worden indien men is g*ehackt*. Dit wordt in de considerans in verband gebracht met een economisch belang: de AVG zou het vertrouwen in digitaal dataverkeer bevorderen, en daarmee het dataverkeer en de digitale economie.

Vanuit deze doelstelling wordt getracht om paal en perk te stellen aan data-inbreuken; bijgevolg richt de AVG zich tot de potentiële overtreder: ondernemingen met een vestiging in de EU en ondernemingen daarbuiten die de gegevens verwerken van betrokkenen in de EU. Zij zijn belast met regels over de rechtmatige verwerking van persoonsgegevens. Daarnaast regelt de AVG het toezicht op, de aansporing tot en het afdwingen van naleving van deze regels. In zoverre richt zij zich tot de nationale toezichthouders, zoals onze Autoriteit Persoonsgegevens (AP) en tot de Europese toezichtcoördinator, de *European Data Protection Board* (EDBP, voorheen de Artikel 29-werkgroep). De AP kan overtreders berispen en hoge administratieve geldboeten opleggen, die op afschrikking gericht zijn.[25] Benadeelden kunnen bij (mogelijke) inbreuken op de AVG een klacht indienen bij de toezichthouder, maar niet is gezegd dat de AP ook wil[26] en kan optreden. Dat de AVG naast en in het verlengde van het streven naar rechtsbescherming (wat dan weer het vertrouwen in het digitaal verkeer moet bevorderen), de normstelling aanscherpt en normhandhaving wil bevorderen, is logisch; het ontbreken daarvan was vóór haar komst juist de 'Achilleshiel' van het databeschermingsrecht.[27]

Mede onder invloed hiervan is het in de doctrine echter gangbaar geraakt om óók de civielrechtelijke aansprakelijkstelling als een vorm van *private action* aan te merken die publiekrechtelijke *norm*handhaving via het toezicht van de AP kan aanvullen en ondersteunen.[28] Handhaving *van de (gedrags)regels* van gegevensbescherming via het aansprakelijkheidsrecht kan bijdragen aan een effectieve gegevensbescherming. Dat *het vooruitzicht van schadeplichtigheid* op dossier-overstijgend niveau inmiddels enige sturende en preventieve functie heeft of zou kunnen hebben,[29] lijkt mij best overtuigend waar het gaat om de 'bewuste profijttrekkers', zoals *Facebook* en *Google*. Hiervoor is nodig dat de omvang van de verschuldigde vergoeding in een reële verhouding staat tot de verwachte opbrengsten van AVG-overtredingen.[30] In veel gevallen die tot claims leiden, berust de inbreuk echter op slordigheid en is de schade juist beperkt, waardoor substantiële prikkelwerking ontbreekt. Bij ernstige of gecalculeerde overtredingen is het bovendien zeer de vraag of potentiële overtreders van de AVG niet afdoende tot adequate normnaleving worden bewogen door het inmiddels steviger aangescherpte boetebeleid van de AP (en haar andere handhavingsmiddelen).[31]

3.2 *Spanning tussen het streven naar regelhandhaving en rechtsbescherming: de VS*

De aandacht voor regelhandhaving – ook waar het civielrechtelijke claims betreft – is belangrijk, maar die kan doorschieten en afleiden van de voornoemde doelstelling (en daardoor niet noodzakelijk strekken ten voordele van de rechthebbenden). Precies vanuit die gedachte is er in de VS momenteel een storm van kritiek op de *California Consumer Privacy Act* (CCPA), die in juni 2018 onder het mom van het bevorderen van effectiever gegevensbescherming werd afgekondigd,[32] en die op 1 januari 2020 in werking zal treden. Deze CCPA toont een zekere gelijkenis met de AVG,[33] zij het dat de CCPA een beperkter toepassingsbereik heeft.[34]

24 Art. 1 lid 2 AVG, waarbij het vrije verkeer van persoonsgegevens niet mag worden beperkt/verboden (lid 3).

25 Art. 83, lid 4 resp. lid 5 AVG: boetes kunnen tot 10 resp. 20 miljoen Euro bedragen dan wel, indien dit cijfer hoger is, 2% resp. 4% van 'de totale wereldwijde jaaromzet in het voorgaande boekjaar'.

26 Zie haar jaarverslag 2018 (via https://www.autoriteitpersoonsgegevens.nl/nl/nieuws): de AP was tot dusverre nog terughoudend met het inzetten van zwaardere middelen dan waarschuwingen. Wel zal dit in de loop van 2019 en in 2020 vermoedelijk meer gaan gebeuren (op p. 19).

27 M.L. Rustad & Th.H. Koenig, 'Towards a Global Data Privacy Standard', *Florida Law Review* 2018, p. 59.

28 O.m. Walree 2017, p. 921 en vgl. O'Dell 2017, p. 1 *('Claims for compensation are an important part of the enforcement architecture of the GDPR. Private enforcement will help to discourage infringements').*

29 O.m. E. Truli, 'The General Data Protection Regulation and Civil Liability', in: *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, M. Bakhoum *et al.* (red.), Springer-Verlag, 2018, p. 304-329 (op p. 310): *'any sanctioning of data breaches [through liability law,* EE/BV *also has a preventive effect'.*

30 Die gedachte is op verschillende plaatsen terug te vinden in de totstandkomingsgeschiedenis van de AVG, o.a. in het Raadsdocument 5833/12, 27 januari 2012, op p. 115.

31 Waarbij ook met de inbreuk gemaakte winst kan meewegen, *Stcrt.* 2019, 14586. Ook relevant zijn het EDPB-beleid en dat van andere nationale toezichthouders. Door de Franse Commission Nationale de l'Informatique et des Libertés (CNIL) werd begin 2019 50 miljoen opgelegd aan *Google LLC* wegens schending van de informatieverplichtingen van art. 12 en 13 AVG en de Britse Information Commissioner's Office (ICO) heeft honderden miljoenen opgelegd aan *Facebook Ireland Ltd, Uber* en *Yahoo UK Services Ltd.,* en aangekondigd te overwegen *British Airways* (omgerekend) ruim 200 miljoen Euro op te leggen vanwege het datalek in 2018.

32 AB-375, SB-1121.

33 Zie uitvoeriger W.G. Voss & K.A. Houser, 'Personal Data and The GDPR: Providing a Competitive Advantage For U.S. Companies', *American Business Law Journal* 2019, Vol. 56, p. 287-342 (p. 294, met verwijzingen).

34 Zij geldt voor winstgerichte bedrijven met een bruto-jaaromzet van meer dan $ 25 miljoen, terwijl de AVG voor alle (ook non-profit) publieke en private organisaties geldt, met uitzonderingen (zie o.m. r.o. 13 AVG).

Een fundamenteel verschil is dat de CCPA *publiek*rechtelijke handhaving nadrukkelijk boven *private enforcement* plaatst door de *Attorney General (AG)* mede te belasten met het vorderen en innen van schadevergoeding respectievelijk boetes, hetgeen slechts beperkt mogelijk is. De Californische AG zelf, Xavier Becerra, hekelt juist dit aspect van de CCPA en steunt het herzieningsvoorstel van senator Jackson dat consumenten alsnog zelf de actie laat instellen en hun aanspraak op schadevergoeding uitbreidt.[35] Dit herzieningsvoorstel is in juni 2019 gestuit op conservatieve weerstand en vooralsnog 'geblokkeerd': het voorstel zou vooral kleinere ondernemingen duperen en in de weg staan aan innovatie. De CCPA houdt de meningen op dit punt sterk verdeeld. Een andersluidend (ontwerp)voorstel in de staat New York, dat in maart 2019 werd gedaan om burgers aldaar juist wél zelf schadeclaims te laten instellen *to sue companies over privacy violations,*[36] is eveneens verworpen. Er wordt thans gestreefd naar een federale regeling, teneinde te voorkomen dat bedrijven in het digitaal verkeer volgens afzonderlijke wetgeving op statelijk niveau aan uiteenlopende normen moeten voldoen. Dat is koren op de molen van de Amerikaanse businesslobby, de *U.S. Chamber of Commerce*, die Amerikaanse ondernemingen tracht te beschermen tegen het risico van (in haar ogen) *frivolous litigation*. Normhandhaving zou zijn voorbehouden aan publieke toezichthouders.[37] In februari 2019 heeft de *Chamber* een voorstel, de *Federal Consumer Privacy Act 2019*, gepubliceerd, waarin ondernemingen zijn gevrijwaard van aansprakelijkheid voor *privacy*-schendingen. Dit voorstel dan wel de CCPA zal, naar het zich laat aanzien, als modelregeling gaan fungeren voor zo'n nieuwe federale wet.

Wat deze ontwikkelingen goed laten zien, is het gevaar van normhandhavingsretoriek bij de uitleg en toepassing van aansprakelijkheidsvragen over gegevensbescherming: zou bij de AVG de nadruk liggen op handhaving van de AVG-gedragsregels en slechts in mindere mate op vermogensrechtelijke rechtsbescherming voor benadeelden, dan kan dit in de meest vergaande vorm betekenen dat het belang van de individuele burger moet wijken voor het publieke belang. De publieke handhaver krijgt in de VS zelfs het laatste woord bij de vraag of claims aanhangig worden gemaakt. Dit laatste zou je je nog wel kunnen voorstellen bij zaken waarin het geschonden belang primair een algemeen of publiek belang betreft, zoals het klimaat, zij het dat belangenorganisaties dan veelal reeds het voortouw zullen nemen om claims in te dienen (zoals bij de thans aanhangige *Milieudefensie e.a./Shell*-zaak over gevolgen van Shell's CO2-uitstoot voor het klimaat). Maar bij schadeclaims wegens schending van de AVG gaat het erom rechtsbescherming/rechtsherstel te bieden om zo (kort gezegd) het fundamentele recht op gegevensbescherming te waarborgen. Het is dat belang, dat ook bij de uitleg en de interpretatie van het schadebegrip onder de AVG leidend zou moeten zijn.

3.3 *Rechtsherstel, compensatie en collectivisering van claims*

Leidend voor de positionering en interpretatie van het schadebegrip van art. 82 AVG is dus, zo blijkt uit het voorgaande, dat dáár niet, althans *niet primair,* mee wordt beoogd om te bevorderen dat gedragsregels worden nageleefd (*regel*handhaving), maar om te bevorderen dat de schending van het recht op bescherming van persoonsgegevens wordt 'goedgemaakt' ofwel hersteld.[38] Zeker hebben potentiële benadeelden en veelal degenen die al getroffen zijn door een data-inbreuk, er belang bij dat de AVG-inbreuk een halt wordt toegeroepen en dat er eventueel een sanctie op volgt, bijvoorbeeld in de vorm van een waarschuwing of een boete, maar aan hierdoor ontstane schade verandert zo'n sanctie niets. Hún persoonlijke informatie ligt al op straat. Denk aan het geval waarin een werkgever persoonsgegevens van een werknemer doorgeeft aan een incassobedrijf, dat, naar achteraf blijkt, de verkeerde debiteur najaagt. Mogelijk trekt de werkgever wijze lessen uit dit voorval en maakt het risico van schadeplichtigheid onder de AVG bedrijven al *ex ante* voorzichtig, maar de schadeplichtigheid van de inbreukmaker strekt primair ertoe om fundamentele rechten zoals art. 8 EVRM en art. 8 EU-Handvest grondrechten te waarborgen. Deze doelstelling van constitutionele rechtsbescherming, die door de AVG 'tanden krijgt', onderstreept tevens het belang om het schadebegrip unierechtelijk uit te leggen.[39]

Hiermee is overigens niet gezegd dat, met het oog op individueel rechtsherstel, claims op individueel niveau zouden moeten plaatsvinden. In schadeprocedures spant het veelal om de vraag of een te vorderen vergoeding dermate substantieel is dat procederen de kosten waard lijkt te zijn. Wat de mogelijkheden om het recht op schadevergoeding te effectueren voor benadeelden zal bevorderen, is de invoering van de 'Wet afwikkeling massaschade collectieve actie' die per 1 januari 2020 van kracht gaat:[40] bij massaschade kan hierdoor op de voet van het (hiertoe gewijzigde) art. 3:305a BW voor de rechter één schadebedrag ter compensatie worden gevorderd voor het collectief van benadeelden, door *non-profit* organisaties (zoals *Bits of Freedom* en *Privacy First*) die aan bepaalde voorwaarden voldoen.[41] Een belangrijke gedachte van de wetgever is dat dit een pressiemiddel is om inbreukmakers bereid te vinden om in der minne tot een schikking te komen. Dit maakt een einde aan de regel

35 *Senate Bill* 561 (SB 561). https://advocacy.calchamber.com/2019/02/25, geraadpleegd op 7 juni 2019.

36 https://www.wired.com/story/new-york-privacy-act-bolder/, laatstelijk geraadpleegd op 7 juni 2019.

37 Zie https://www.uschamber.com/sites/default/files/9.6.18_us_chamber_-_ctec_privacy_principles.pdf, geraadpleegd op 7 juni 2019.

38 Ook in de totstandkomingsgeschiedenis staat de compensatiegedachte voorop, zie o.a. Raadsdocument 5833/12, 27 januari 2012, p. 115.

39 Vgl. *Vidal-Hall/Google* [2015], EWCA Civ, 311.

40 *Stb.* 2019/447; zie reeds *Kamerstukken II* 2016/17, 34608, nr. 3 en *Stb.* 2019/130.

41 Mits aan de voorwaarden van het nieuw ingevoerde art. 3:305a BW is voldaan. Bovendien is in beginsel vereist dat het een 'orgaan, organisatie of vereniging zonder winstoogmerk' is 'waarvan de statutaire doelstellingen het openbare belang dienen' en dat/die 'actief is op het gebied van de bescherming van de rechten en vrijheden van de betrokkene in verband met de bescherming van diens persoonsgegevens', aldus art. 80 lid 1 AVG.

dat de rechtsvordering van een stichting of vereniging die strekt tot bescherming van gelijksoortige belangen van benadeelden niet kan strekken tot schadevergoeding in geld, doch slechts tot een gebod of verbod of tot een verklaring voor recht.[42] De AVG biedt nadrukkelijk de mogelijkheid tot een collectieve actie, indien de lidstaten zelf dit toelaten.[43] Thans kan men bij massaschade, zoals bekend, een getroffen schikking over schadeplichtigheid algemeen verbindend (laten) verklaren, waardoor zij ook geldt voor benadeelden die geen contractspartij zijn geweest.[44] Dit laatste staat of valt met de schikkingsbereidheid van de aangesproken en uiteraard de eisende partij. Die bereidheid zal bij een collectieve schadeactie toenemen.[45] Bij vorderingen tot smartengeld, maken groepsacties, zoals die tegen *Facebook* en *Google*,[46] het vermoedelijk juist mogelijk dat een substantieel bedrag kan worden verhaald. Eerder dit jaar beriep *Facebook* zich in de *Cambridge Analytics*-zaak op het ontbreken van schade in de betekenis van *'actionable identity theft, emotional distress, or economic injury'*.[47] Slechts zou sprake zijn van een aantasting van de *privacy* van de *Facebook*-gebruikers.[48] Maar als zovelen zich bekocht voelen, is het moeilijk vol te houden dat de schade onbeduidend is. De schade van individuele eisers mag dan van geringe omvang zijn, maar het optreden als groep of collectief zorgt voor een grotere slagkracht.

Ook in kwesties over incidentele data-inbreuken, laat de gepubliceerde rechtspraak het beeld zien dat de (rechtens relevante) immateriële schade beperkt is:[49] de smartengeldbedragen schommelen over het algemeen onder 1.000 Euro. Waar het oordeel over de schadeomvang in Nederland is voorbehouden aan de feitenrechter, kiest het al genoemde Californisch wetsvoorstel voor een forfaitaire regeling: in deze regeling is bepaald dat de schadevergoeding tussen de 100 en 750 US Dollar per consument bedraagt.[50] Wettelijke standaardbedragen passen bij het Amerikaanse stelsel nu daarin publiekrechtelijke regelhandhaving de boventoon voert; dat is anders als het streven naar rechtsherstel voorop staat, zoals bij de AVG. Bovendien lijkt mij dit voor Nederland een onwenselijke benadering omdat de AVG verlangt dat de benadeelde 'volledige en daadwerkelijke vergoeding' ontvangt van zijn schade.[51] Dat vraagt om differentiatie op basis van zijn concrete omstandigheden en een toereikende rechterlijke motivering.[52]

4. Nationaal recht als leidraad voor smartengeld resp. waardevergoeding

4.1 *Invulling van het schadebegrip langs twee routes*

Voor de invulling van het schadebegrip biedt de vingerwijzing in de considerans van de AVG, zoals hiervoor bleek, slechts beperkt richting. Dat het schadebegrip niet scherp is, is te betreuren, aangezien art. 82 AVG, zoals gezegd, veelvuldig wordt ingeroepen voor schade van *immateriële aard* en het verweer van de aangesprokene daartegen dan al gauw luidt dat er geen schade is. Hoewel dit laatste ook in het kader van de wordingsgeschiedenis is onderkend,[53] blijft in de AVG in het midden wanneer men recht heeft op smartengeld, wat onder immateriële schade wordt verstaan en of voor het stellen en zo nodig bewijzen van schade *voldoende* is dat sprake is van controleverlies of dat sprake moet zijn van concrete hieruit voortvloeiende schade. Hoe dient met deze onduidelijkheid over het schadebegrip te worden omgegaan? Het kan lang wachten zijn op daadwerkelijk richtinggevende uitspraken van het Hof van Justitie en het is niet onwaarschijnlijk dat ook als die uitspraken komen, hierbij de nodige ruimte aan de lidstaten wordt gelaten. Het ligt dan voor de hand om te rade te gaan bij het nationale recht. Dit is ook de heersende benadering: bij het ontbreken van een nadere, unierechtelijke interpretatie van het concept schade, wordt, met inachtneming van de hiervoor genoemde aanwijzingen in de AVG, uitgegaan van het nationale recht.[54]

Als we de blik richten op het schadevergoedingsrecht van afdeling 6.1.10 BW, kunnen mijns inziens (ten minste) twee routes worden verkend (waarbij er telkens van wordt uitgegaan dat de aansprakelijkheid ingevolge art. 82 AVG en/

42 Art. 3:305a BW en art. 50 Wbp. Rb. Oost-Brabant 20 juli 2016, ECLI:NL:RBOBR:2016:3892. Vgl. art. 79 AVG en art. 21 van de geconsolideerde versie van de concept-ePV (Raadsdocument 29 juli 2019).

43 Art. 80, lid 1 AVG; vgl. art. 21 van de geconsolideerde versie van de concept-ePV (Raadsdocument 29 juli 2019); T.E. van der Linden & T.F. Walree, 'De collectieve procedure als oplossing voor het privaatrechtelijke handhavingstekort bij een datalek?', *AV&S* 2018/20, (p. 105-113); N. Vrugt & W.F. Dammers, 'Massaschadeclaims voor betrokkenen onder de AVG volgens Nederlands recht, *Privacy & Informatie* 2018, p. 114-120.

44 Art. 7:907 e.v. BW; *Kamerstukken II* 2016/17, 34608, nr. 3, p. 1 en 4.

45 L. Jančiūtė, 'Data protection and the construction of collectieve redress in Europe: exploring challenges and opportunities', *International Data Privacy Law* 2019, Vol. 9, No. 1, p. 7-8.

46 In juni van dit jaar heeft de Franse consumentengroep UFC-Que Choisir een collectieve actie ingesteld tegen *Google*, na eerdere boetes (waaronder de al genoemde 50 miljoen Euro begin 2019) die de CNILhad opgelegd wegens het gebrek aan transparantie en gemakkelijk toegankelijke informatie voor gebruikers. Deze zaak betreft een gebods- en/of verbodsactie om de exploitatie van persoonsgegevens van gebruikers te laten eindigen, maar ook een vordering van maximaal 1.000 Euro per gebruiker aan schadevergoeding.

47 Zie, uitvoerig hierover, Walree 2018. Er hebben zich, naar verluidt, zo'n honderdduizenden Europeanen aangesloten bij groepsacties tegen *Facebook*.

48 Zie o.a. https://www.marketwatch.com/story/facebook-defends-itself-in-cambridge-analytica-consumer-class-action-case-2019-03-18 (laatst geraadpleegd op 12 april 2019).

49 Mijn beeld van de rechtspraak is niet anders dan reeds verwoord bij Walree 2017, p. 922, mede onder verwijzing naar het preadvies van Tjong Tjin Tai 2016, p. 282. Recenter toegewezen bedragen betreffen 500 Euro (Rb. Overijssel 28 mei 2019, ECLI:NL:RBOVE:2019:1827, *Eiser/College B&W Deventer)* resp. 250 Euro (Rb. Amsterdam 2 september 2019, ECLI:NL:RBAMS:2019:6490.

50 *Section* 11 (1798.150) van de CCPA; *DataGuide* 2018, p. 39-40.

51 Onderdeel 146 van de considerans.

52 In het kader van art. 6:106 BW klinkt hier in algemene zin reeds (los van de AVG) kritiek op, zie de website van Slachtofferhulp Nederland en, mede n.a.v. enkele mediagevoelige kwesties, bijv. *De Volkskrant* 15 oktober 2019, p. 2 en p. 14-15 'Advocaten: grabbelton, Rechters: Maatwerk'.

53 Met name door de (oude) Artikel 29-werkgroep, die een motor was voor (vermelding in art. 82 AVG van) de uitbreiding naar immateriële schade, zie Raadsdocumenten 7375/12 en 8366/12, 8 resp. 30 maart 2012.

54 Walree 2017, p. 930; F.C. van der Jagt-Vink, 'Schadevergoeding onder de Algemene Verordening Gegevensbescherming', *MvV* 2019, p. 286-292 (p. 290); Rb. Overijssel 28 mei 2019, ECLI:NL:RBOV:2019:1827, *Eiser/College B&W Deventer,* r.o. 5 e.v.

of art. 6:162 BW vaststaat).[55] Ten eerste de route waarbij de benadeelde smartengeld vordert voor de immateriële schade die het gevolg is van dat controle- of gebruiksverlies of van die rechtsinbreuk op de voet van art. 6:106 sub b BW. In het bijzonder voor deze route is van belang dat de Hoge Raad eerder dit jaar de mogelijkheid tot het verkrijgen van een smartengeldaanspraak op grond van het slot van die bepaling wat heeft opgerekt, doch tevens heeft beslist dat de enkele rechtsinbreuk daarvoor niet voldoende is. Dit is een belangrijk arrest, zo blijkt ook uit nadien verschenen uitspraken van de Hoge Raad.[56] Ten tweede is er de route waarin de benadeelde het controleverlies zelf en/of de inbreuk op zijn recht op bescherming van persoonsgegevens (dat is neergelegd in art. 8 van het EU-Handvest grondrechten en ook beschermd wordt door art. 8 EVRM, zie par. 4.3) kwalificeert als schade. Dit heeft mijns inziens alleen kans van slagen indien daardoor sprake is van zuivere vermogensschade: het verlies van de monetaire waarde (veelal de marktwaarde) van het gebruik van de persoonsgegevens. Beide routes zullen worden toegelicht.

4.2 *Route 1: smartengeld, i.h.b. via het vangnet van art. 6:106 sub b BW*

De eerstgenoemde route heeft betrekking op de immateriële schade: daarvoor heeft de benadeelde slechts binnen de beperkte kaders van art. 6:106 BW recht op vergoeding.[57] De belangrijkste gronden voor smartengeld volgens deze regeling zijn dat de benadeelde is aangetast in zijn eer of goede naam, lichamelijk letsel heeft of *'op andere wijze in zijn persoon is aangetast'*.[58] Als er van reputatieschade of lichamelijk letsel geen sprake is, dan komt het met name aan op dit gecursiveerde slotstuk.[59] Bij de 'persoonsaantasting op andere wijze' wordt over het algemeen – buiten het terrein van data-inbreuken – veelal gedacht aan gevallen waarin de eiser geestelijk letsel heeft opgelopen; dat is een geestelijke beschadiging in de medische zin. Dit is uitzonderlijk bij data-inbreuken en vraagt om concrete gegevens die ondersteunen dat hij geestelijk letsel heeft, welk oordeel berust op objectieve maatstaven, en in het algemeen pas wordt aangenomen bij een 'in de psychiatrie erkend ziektebeeld'.

Tot de komst van *EBI* was het hebben van geestelijk letsel de hoofdregel voor een beroep op het vangnet van art. 6:106 sub b, slot BW, maar werd deze 'vangnet'-categorie bij wijze van uitzondering ook toegepast bij inbreuken op de *privacy*.[60] In het *EBI*-arrest, dat niet over data-inbreuken ging, herpositioneert de Hoge Raad het criterium van geestelijk letsel – dat is nu niet meer de hoofdregel – en geeft hij verdere richting aan de beoordeling van 'persoonsaantastingen op andere wijze' onder art. 6:106 sub b, slot BW zonder dat sprake is van geestelijk letsel.[61] De Hoge Raad noemt als algemene criteria voor de beoordeling van de 'persoonsaantasting op andere wijze' van art. 6:106 sub b BW: *de aard en ernst van de normschending en van de gevolgen daarvan.* Die zijn beslissend. Het is aan de eiser om dit over het voetlicht te brengen. Ook verlangt de Hoge Raad in *EBI* dat de eiser de immateriële gevolgen van de normschending met voldoende concrete gegevens onderbouwt. Het gegeven dat sprake is van een inbreuk op een fundamenteel recht is hiervoor niet voldoende. Met dit laatste wordt art. 6:106, sub b, slot BW strikt, maar mijns inziens tegelijk ook in drie opzichten ruim geïnterpreteerd.[62] Ten eerste geldt volgens de Hoge Raad niet langer als uitgangspunt dat de benadeelde geestelijk letsel aannemelijk maakt. Dat geestelijk letsel hiermee als feitelijk keurslijf is verlaten, lijkt mij voor data-inbreuken wenselijk, getuige ook de Amerikaanse rechtspraktijk en doctrine. Daar wordt gegoocheld met vage juridisch-medische constructen, zoals *identity harm* en *databreach anxiety,* die leiden tot onnodig ingewikkelde discussies.[63]

Ten tweede is de smartengeldaanspraak, bij het ontbreken van (aantoonbaar) geestelijk of lichamelijk letsel en van aantasting van de eer of goede naam, niet afhankelijk van het vaak ingewikkelde oordeel of sprake is van een rechtsinbreuk. Hiermee maakt het *EBI*-arrest in feite óók duidelijk dat ook los van de vraag of sprake is van een inbreuk op art. 8 EVRM of art. 8 EU Handvest grondrechten, de stress en de angst die het gevolg zijn van een ernstige schending van de AVG voldoende kunnen zijn voor een aanspraak op smartengeld.[64] Er waren in de feitenrechtspraak in het kader van de oude *Privacy*-richtlijn 95/46/EG al uitspraken in die richting.[65] In meer algemene zin (los van data-inbreuken) werd voor art. 6:106 sub b, slot BW echter aangenomen dat, bij het ontbreken van geestelijk letsel, de benadeelde veelal slechts aanspraak kon maken op smartengeld bij een ernstige inbreuk op een fundamenteel recht. Dit werd te-

55 Overigens kan ook evt. aan aansprakelijkheid op grond van art. 6:75 BW of andere gronden worden gedacht.

56 HR 15 maart 2019, *NJ* 2019/162, m.nt. S.D. Lindenbergh, *Onrechtmatig EBI-verblijf* (hierna ook: *EBI*). De kernoverwegingen van dit arrest werden herhaald in HR 19 juli 2019, ECLI:NL:HR:2019:1278, *Prejudiciële vragen mijnbouwschade* en zie voorts, van de strafkamer: HR 28 mei 2019, ECLI:NL:HR:2019:793, *NJ* 2019/379, m.nt. W.H. Vellinga, *Overzichtsarrest vordering b.p.* en HR 15 oktober 2019, ECLI:NL:HR:2019:1465, *Woninginbraak*.

57 Art. 6:95 BW.

58 Art. 6:106, sub b BW; reputatieschade wordt, zoals hiervoor al werd gezien, ook in de considerans van de AVG genoemd. De gronden van sub a en c zijn nauwelijks relevant en laat ik rusten.

59 De navolgende analyse berust deels op mijn artikel 'Ruimer baan voor smartengeld bij 'persoonsaantastingen op andere wijze' zonder dat sprake is van geestelijk letsel', *AV&S* 2019/37 (nog te verschijnen).

60 C.J. van Zeben e.a. (red.), *Parlementaire geschiedenis van het Nieuwe Burgerlijk Wetboek. Boek 6 algemeen gedeelte van het verbintenissenrecht*, Deventer 1981, p. 397, 380 en 382-383; ECLI:NL:PHR:2019:427, *Woninginbraak*, randnr. 16.

61 HR 15 maart 2019, *NJ* 2019/162, m.nt. S.D. Lindenbergh, *Onrechtmatig EBI-verblijf;* zie kort na het verschijnen mijn bespreking (te raadplegen via https://blog.ucall.nl/index.php/2019/03/ruimer-baan-voor-smartengeld-bij-inbreuken-op-fundamentele-rechten-een-reactie-op-hr-15-maart-2019-eclinlhr2019376/) en, uitvoerig, S.D. Lindenbergh, 'Smartengeld wegens spanning, frustratie, ergernis en (ander) onbehagen?', *NTBR* 2019/20, (p. 122-130).

62 Zie Engelhard 2019 (nog te verschijnen).

63 Zie de rechtspraakanalyse van D.J. Solove & D.K. Citron, 'Risk and Anxiety: A Theory of Data-Breach Harms', *Texas Law Review 2018,* Vol. 96, p. 736-786, die spreken van een *'cramped understanding of harm'* (p. 754), met verdere verwijzingen.

64 Zie hierna, par. 3.3.

65 O.a. Rb. Midden-Nederland 12 augustus 2009, ECLI:NL:RBUTR:2009:BJ5273, *X/Agis*; Rb. Oost-Brabant 22 mei 2014, ECLI:NL:RBOBR:2014:2701, *X/Sûreté;* Rb. 28 december 2016, ECLI:NL:RBNHO:2016:10635, *X/Van Hees*.

ruggevoerd op enkele specifieke arresten, niet in de sfeer van databescherming.[66] De benadering die de Hoge Raad kiest in het *EBI*-arrest biedt rek en ruimte voor rechtsontwikkeling, maar wel met terughoudendheid gelet op het feit dat art. 6:106 BW een gesloten karakter heeft,[67] en (uiteraard) mits dit goed wordt gemotiveerd ter zake van de aard en ernst van de normschending en de aard en ernst van de gevolgen daarvan.

Een derde 'stukje rek' van *EBI* is dat de Hoge Raad overweegt dat de nadelige gevolgen van de normschending in 'voorkomende gevallen', en dus bij uitzondering, 'zo voor de hand liggen, dat een aantasting in de persoon kan worden aangenomen'.[68] Op dit laatste punt verwijst de Hoge Raad naar de arresten inzake *Oudejaarsrellen* en *Wrongful life;* Kwesties die gemeen hebben dat ze gaan over ernstig verwijtbaar gedrag met zo ernstige gevolgen dat ze als een inbreuk op een fundamenteel recht worden gekwalificeerd. Wezenlijk is hier dat het gaat om ernstige aantasting van de persoonlijke veiligheid respectievelijk het zelfbeschikkingsrecht. Niet uitgesloten is echter, lijkt mij, dat bijvoorbeeld ernstige *cyber*aanvallen, die gericht zijn op zeer (persoons)gevoelige informatie, indien dit tot aantasting van de veiligheid of tot andere ernstige persoonlijke gevolgen leidt, daar ook aanleiding toe zouden kunnen geven. Minder in de rede ligt het om, bij wijze van hypothese, de *Cambridge Analytics* kwestie onder deze categorie te scharen. De maatschappelijke aandacht en commotie zijn groot en het vertrouwen van gebruikers in sociale media is geschaad, maar dáármee is de ernst van de normschending nog niet gegeven en de concrete persoonlijke gevolgen veel minder aangrijpend dan in de kwesties die ten grondslag lagen aan de voornoemde arresten van de Hoge Raad. Buiten deze laatstbedoelde (uitzonderings)gevallen, dient de benadeelde zo concreet en uitvoerig mogelijk de precieze immateriële gevolgen van de gestelde normschending toe te lichten en te onderbouwen, om de 'persoonsaantasting op andere wijze' van art. 6:106, sub b, slot BW aannemelijk te maken.

4.3 *Fundamentele rechtsinbreuk is geen schade. Anders: Lloyd/Google (2019)*

In het *EBI*-arrest oordeelt de Hoge Raad verder nog dat de inbreuk op een fundamenteel recht nog niet betekent dat sprake is van een 'persoonsaantasting op andere wijze' in de zin van art. 6:106 sub b, slot BW. Dat is relevant, aangezien het recht op bescherming van persoonsgegevens constitutioneel is gewaarborgd, onder meer onder artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en fundamentele vrijheden (EVRM) en het is een *zelfstandig* grondrecht, neergelegd in artikel 8 van het Handvest van de Grondrechten van de Europese Unie (EU).[69] Deze regelingen brengen mee dat de Staat of andere publieke entiteiten zich van inbreuken moeten onthouden en er op hen positieve verplichtingen rusten.[70] Bij schendingen van art. 8 EU-Handvest en/of de rechten die de AVG biedt, dient de overheid te voorzien in een *'effective judicial remedy'*,[71] met ook procedureel voldoende waarborgen voor de benadeelden.[72]

Bij data-inbreuken schuilt het belang hiervan in de eisen die de Hoge Raad in *EBI* stelt aan de onderbouwing (en de rechterlijke motivering) van het oordeel of de benadeelde recht heeft op smartengeld. Hoewel enkele arresten over andersoortige kwesties onder het oude wetboek in de richting wezen dat *ernstige* schending van het – in die gevallen aan de orde zijnde – recht op eerbiediging van de persoonlijke levenssfeer als bedoeld in art. 8 EVRM reeds een zelfstandige grond vormt voor smartengeld,[73] komt uit latere arresten[74] een genuanceerder beeld naar voren. Daaruit blijkt weliswaar dat de inbreuk op een fundamenteel recht in het algemeen, de persoonlijke levenssfeer in het bijzonder, een grondslag voor het recht op smartengeld *kan* bieden, maar dat 'niet iedere inbreuk op die levenssfeer voldoende is om te spreken van een aantasting in de persoon' in de zin van art. 6:106 sub b, slot BW.[75] Thans, in *EBI,* verduidelijkt de Hoge Raad dat de aard en de ernst van de normschending en van de gevolgen daarvan beslissend zijn en niet de inbreuk op een fundamenteel recht. *EBI* stond weliswaar niet in de sleutel van data-inbreuken, maar lijkt leidend te zijn, zolang de uitleg van art. 82 AVG op nationaal recht berust. Opvallend is dat de Londense *Court of Appeal* in de kwestie *Lloyd/Google LLC* in de uitspraak van 2 oktober jongstleden juist wèl de route koos 'rechtsinbreuk is schade'.[76] In deze procedure vordert Richard Lloyd, kort gesteld, collectief namens 4 miljoen *Apple iPhone* gebruikers schadevergoeding van Google in verband met het zonder toestemming tracken van hun internetactiviteiten. De vraag is enkel of hier plaats is voor een *class action,*[77] maar in het kader van die vraag ligt ter beoordeling voor of naast het controleverlies over persoons-

66 O.a. HR 30 oktober 1987, ECLI:NL:HR:1987:AD0034, *NJ* 1988/277, m.nt. L. Wichers Hoeth, *Naturistengids* en HR 1 november 1991, ECLI:NL:HR:1991:ZC0393, *NJ* 1992/58, *K/Staat*.

67 Zo ook A-G Hostee, in zijn Conclusie van 23 april 2019, ECLI:NL:PHR:2019:427, *Woninginbraak,* randnr. 14.

68 HR 15 maart 2019, *NJ* 2019/162, m.nt. S.D. Lindenbergh, *Onrechtmatig EBI-verblijf*, r.o. 4.2.

69 Naast het algemene recht op privacy, dat is neergelegd in art. 7 van het EU-Handvest grondrechten. Zie uitvoerig H. Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Art. 16 TFEU*, Springer International Publishing Switzerland, 2016, p. 125 e.v.

70 Vgl. EHRM 14 februari 2012, nr. 7094/06, *Romet/Nederland*; HR 21 december 2018, ECLI:NL:HR:2018:2368.

71 HvJ (EU) 19 november 1991, gevoegde zaken C-6/90 en C-9/90, ECLI:EU:C:1991:428, *ECR* 1991, I-05357, r.o. 33, *A. Francovich en D. Bonifaci e.a./Italiaanse Republiek*.

72 Althans EHRM 16 oktober 2008, nr. 39058/05, *Kyriakides/Cyprus,* nr. 45: art. 8 EVRM *'may include the requirement that the State set up a system for the effective protection of an individual's right to privacy'*.

73 HR 1 november 1991, ECLI:NL:HR:1991:ZC0393, *NJ* 1992/58, r.o. 3.5, onder verwijzing naar HR 30 oktober 1987, ECLI:NL:HR:1987:AD0034, *NJ* 1988/277, m.nt. Wichers Hoeth.

74 HR 9 juli 2004, ECLI:NL:HR:2004:AO7721, *NJ* 2005/391, m.nt. J.B.M. Vranken, *Oudejaarsrellen Groningen*; HR 18 maart 2005, ECLI:NL:HR:2005:AR5213, *NJ* 2006/606, m.nt. J.B.M. Vranken, *Wrongful life* en HR 4 oktober 2013, ECLI:NL:HR:2013:851, *NJ* 2013/479, *Het Parool*.

75 A-G Hostee, in zijn Conclusie van 23 april 2019, ECLI:NL:PHR:2019:427, *Woninginbraak*, randnr. 17.

76 *Lloyd/Google LLC* [2019], EWCA Civ 1599. Deze vordering berust op art. 13 van de oude Data Protection Act (DPA) 1998, thans art. 169 DPA 2018.

77 In de zin van CPR Part 19.6.

gegevens afzonderlijk schade dient te worden gesteld en zo nodig bewezen. Die vraag wordt ontkennend beantwoord. Hiervoor is van belang dat Google moedwillig en met het oog op puur winstbejag heeft gehandeld, en dat het niet gaat om triviale schade. Deze factoren komen ook terug bij de Hoge Raad, waar hij in *EBI* de aard en ernst van de normschending en van de gevolgen voorop stelt. Het verschil is echter dat die gevolgen en de schade die hierdoor ontstaat, met concrete gegevens dienen te worden onderbouwd.

4.4 *Concrete onderbouwing*

In *EBI* bevestigt de Hoge Raad, zoals ik al aangaf, ook nog dat de eiser zijn stelling dat hij 'op andere wijze' in zijn persoon is aangetast, voldoende *met concrete gegevens moet onderbouwen*. Hoewel dit evident lijkt en ook voor het *EBI*-arrest al gold, gebeurt dit lang niet altijd toereikend, zo blijkt uit dit arrest zelf (waarin werd volstaan met een uitleg en onderbouwing van de disproportionele vrijheidsberoving) en uit het latere arrest inzake *Identiteitsfraude*. Dat sprake is van een datalek of van de verspreiding van de persoonsgegevens of identiteitsfraude kan wel relevant zijn voor het vaststellen van de normschending, maar de aard en ernst van concrete immateriële gevolgen daarvan dienen concreet te worden onderbouwd en toegelicht. In *Identiteitsfraude* had de eiser volstaan met de onderbouwing dat hij ernstig leed (en psychische schade) had ondervonden van de (wegens misbruik van zijn rijbewijs) ten onrechte opgelegde boetes, resulterend in gijzelingen en gerechtelijke procedures tegen de Rijksdienst voor het Wegverkeer. Die onderbouwing kwam neer op de stelling dat hij jarenlang in zijn 'persoonlijke levenssfeer' was aangetast, onder meer door verlies van werk, problemen met uitkeringsinstanties en relaties.[78] A-G Hartlief mist een concrete toelichting en producties van de concrete immateriële schade, met name over de precieze stappen die de eiser concreet had ondernomen en andere concrete feiten en omstandigheden waaruit bleek dat hij op andere wijze in zijn persoon was aangetast.[79] De immateriële schade dient te worden onderbouwd, bijvoorbeeld met verklaringen over het precieze leed of verdriet, documentatie van consulten hierover bij de huisarts, medicatie, en dergelijke.

4.5 *Route 2: controle- of gebruiksverlies als zuivere vermogensschade – kan dat?*

De tweede route voor het recht op schadevergoeding bij schade van immateriële aard betreft gevallen waarin de benadeelde stelt dat het enkele verlies van de controle over zijn persoonsgegevens schade is. Zoals hiervoor werd gezien, leidt deze route, anders dan in de Engelse zaak van 2 oktober, niet gauw tot smartengeld. Bij de vaststelling van de omvang van de aansprakelijkheid, is het uitgangspunt dat de benadeelde zoveel mogelijk in de toestand moet worden gebracht waarin hij zou hebben verkeerd indien de data-inbreuk zou zijn uitgebleven. Schade wordt in beginsel concreet vastgesteld en gewaardeerd,[80] dat wil zeggen aan de hand van alle feitelijke omstandigheden van het voorliggende geval. Kansrijker is dat de benadeelde die al het enkele gegeven dat zijn persoonsgegevens onrechtmatig in de handen zijn geraakt van de aangesprokene of door diens toedoen (of onder diens verantwoordelijkheid) in die van derden, schade noemt, dit als een verlies van monetaire waarde met concrete gegevens onderbouwt. Dat persoonsgegevens monetaire waarde hebben, is onomstreden. Ze zijn, om met Walree te spreken, de drijvende kracht van de data-gestuurde economie.[81] Die gedachte is ook voelbaar in de richtlijn Digitale inhoud.[82] Het verlies van de exclusiviteit of de beperking van persoonsgegevens, kan zich dan ook, als het *privacy*gevoelige informatie betreft, in een (markt) waarde laten uitdrukken. Walree heeft dit reeds eerder uitvoerig laten zien.[83] Die grondgedachte wordt krachtig ondersteund door het feit dat diensten en *websites* op het internet, zoals *Google* en *Facebook,* 'gratis' worden geleverd omdat er persoonlijke gegevens van klanten worden verzameld, verwerkt en verkocht.[84] Op het internet is gegevensbescherming een 'product' waar een prijskaartje aan verbonden kan worden.[85] Daarmee is echter nog niet gezegd dat alle persoonsgegevens die waarde hebben en hoe die waarde van geval tot geval fluctueert.

In het kader van art. 6:97 BW geldt als uitgangspunt dat de schade in beginsel concreet wordt begroot, dat wil zeggen met inachtneming van alle omstandigheden van het geval. Wat vergoeding voor het waardeverlies van (controle over de eigen) persoonsgegevens problematisch maakt, is dat de benadeelde zal dienen toe te lichten dat hij die zonder de data-inbreuk wél zelf te gelde had kunnen maken.[86] Zijn schade bestaat veeleer uit het verlies van exclusiviteit. Maar wat is dat waard? Dat is in een individueel geval eigenlijk niet of toch zeer moeilijk vast te stellen. Nu biedt het schadevergoedingsrecht over het algemeen, buiten het specifieke terrein van persoonsgegevens, ruimte om op 'praktische gronden en om redenen van billijkheid' in bijzondere gevallen op het uitgangspunt van concrete schadeberekening een uitzondering te aanvaarden door van bepaalde omstandigheden te abstraheren.[87] Bij data-inbreuken die zo'n bijzonder geval opleveren, zou van de complicerende omstandigheid dat de benadeelde de persoonsgegevens niet

78 Aangehaald door A-G Hartlief, ECLI:NL:PHR:2019:561, *Identiteitsfraude,* randnr. 3.17.

79 Conclusie, ECLI:NL:PHR:2019:561, *Identiteitsfraude,* randnr. 3.17.

80 Zie, vrij recent nog, HR 19 juli 2019, ECLI:NL:HR:2019:1278, *Prejudiciële vragen mijnbouwschade,* r.o. 2.11.

81 Walree 2017, p. 926.

82 Richtlijn (EU) 2019/770 van het Europees Parlement en de Raad van 20 mei 2019 betr. bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en digitale diensten, PbEU 22 mei 2019, L 136/1: art. 3 lid 1 laat deze richtlijn ook gelden voor diensten waarvoor persoonsgegevens worden verstrekt (lees: met persoonsgegevens wordt betaald).

83 Zie hierover T.F. Walree, 'Het Cambridge Analytica-schandaal: wat kan de Nederlandse Facebook-gebruiker claimen', *Tijdschrift voor Internetrecht* 2018, p. 134-142, par. 3.2.

84 Vgl. B. van der Sloot, 'De Privacyverklaring als onderdeel van een wederkerige overeenkomst', *P&I* 2010/3.

85 Mits met inachtneming van de AVG; zie art. 3 lid 1 van de richtlijn Digitale inhoud (2019/770).

86 Walree 2018, p. 142.

87 HR 19 juli 2019, ECLI:NL:HR:2019:1278, *Prejudiciële vragen mijnbouwschade,* r.o. 2.11.3.

had gematerialiseerd alsmede van de onzekerheid omtrent de daadwerkelijke, precieze waarde in de concrete omstandigheden, kunnen worden geabstraheerd. Overeenkomstig de constante lijn van arresten over de abstracte berekening van herstelkosten ingeval van zaakschade,[88] zou, met enige moeite,[89] kunnen worden betoogd dat een data-inbreuk al vóór en onafhankelijk van eventuele verdere schadelijke gevolgen, een aantasting is in het vermogen en als zodanig schade oplevert. Maar anders dan over het algemeen bij zaakschade het geval is, lijkt mij ook de *abstracte* begroting van de vermogenswaarde buitengewoon lastig, terwijl Walree heeft laten zien dat de omvang veelal zeer beperkt is. Walree bespreekt diverse wijzen waarop de marktwaarde van de persoonsgegevens in een geldwaarde zou kunnen worden uitgedrukt.[90] Hij merkt daarbij op dat dergelijke begrotingsmethodes een zeer klein financieel bedrag opleveren.[91]

Ook in de gepubliceerde rechtspraak voert concrete schadeberekening de boventoon; er wordt (en werd ook al onder de oude Privacyrichtlijn 95/46/EG) van de eiser voldoende onderbouwing van de daadwerkelijke schade verlangd.[92] Noodzakelijk is om *concreet, feitelijk* aan te geven waar zijn schade precies uit bestaat. Dat geldt, zoals in par. 4.2 al werd gezien, voor immateriële schade, en dus ook voor zuivere vermogensschade. Dit maakt route 2 buitengewoon lastig. Schadeclaims zullen om die reden veelal beperkt blijven tot concreet gematerialiseerde en in zoverre eenvoudiger te onderbouwen gevolgschade. Die kan bijvoorbeeld bij identiteitsfraude bestaan uit onrechtmatige afschrijvingen van de bankrekening van de benadeelde of bij derden openstaande schulden op zijn naam (bijv. boetes en belastingschulden) en kosten van ongedaanmaking.[93]

5. Tot slot

De mogelijkheden tot het verkrijgen van schadevergoeding zijn inmiddels wat verruimd door de aanstaande inwerkingtreding van de collectieve schadeactie en door het *EBI*-arrest over immateriële schade, maar die ontwikkelingen ten spijt blijft het schadebegrip problematisch. Bij verdere invulling van het schadebegrip van art. 82 lid 1 AVG is in beginsel niet leidend in hoeverre schadebedragen preventief of afschrikwekkend kunnen zijn voor potentiële overtreders. Bij smartengeld zijn de aard en de ernst van de concrete normschending en de gevolgen daarvan beslissend alsmede de vraag welk schadebedrag met het oog op adequate rechtsbescherming (waarborgen bij schending van art. 8 EVRM en art. 8 EU-Handvest grondrechten) van de burger opportuun is. Daartoe dient de schade concreet te worden onderbouwd. De toekomst moet uitwijzen hoe de toepassing van het *EBI*-criterium, mede gelet op de doelstellingen van de AVG, tot verfijning en differentiatie zal leiden. Niet valt te verwachten dat de Hoge Raad eenzelfde koers zal volgen als recentelijk in *Lloyd/Google* van het Engelse *Court of Appeal*. Dit betekent dat voor schadeclaims die enkel berusten op controleverlies van persoonsgegevens als gevolg van een AVG-schending ten minste is vereist dat daarbij concreet wordt onderbouwd tot welke monetaire schade dit heeft geleid. Hierin heeft de rechter de nodige vrijheid, die niet te vroeg 'aan banden moet worden gelegd' en waarbij het juist belangrijk is een beter oog te krijgen op de casuïstiek dan thans nog het geval is.

88 O.a. HR 16 juni 1961, *NJ* 1961/444, *Telefoonkabel;* HR 15 januari 1965, *NJ* 1965/197, *Flint/Veldpaus;* HR 19 december 1975, *NJ* 1976/280, *Rijksweg 12.*

89 Want abstracte schadeberekening is uitzonderlijk en het betreft hier, anders dan bij zaakschade, geen fysieke aantasting.

90 Hierover uitvoeriger Walree 2018, p. 925.

91 Walree 2018 spreekt van bedragen tussen 0,25 - 75,80 US Dollar, berustend op economisch onderzoek.

92 Vgl. reeds de Ierse *Court of Appeal* 14 maart 2013, *IEHC* 2013/137, *Collins v. FBD ('evidence of actual loss or damage').*

93 T.F.E. Tjong Tjin Tai, 'Aansprakelijkheid bij datalekken', *WPNR* 2016/7110, p. 463.