Aansprakelijkheid bij datalekken

Tjong Tjin Tai, Eric

Published in:
WPNR: Weekblad voor privaatrecht, notariaat en registratie

Publication date:
2016

Document Version
Peer reviewed version

T.F.E. Tjong Tjin Tai, 'Aansprakelijkheid bij datalekken', WPNR 7110 (2016), p. 459-464.

Aansprakelijkheid bij datalekken

T.F.E. Tjong Tjin Tai[1]

1. Inleiding

Sinds 1 januari 2016 is de algemene meldplicht datalekken in Nederland geldend recht.[2] Art. 34a Wet bescherming persoonsgegevens (Wbp) bepaalt thans dat de voor de dataverwerking verantwoordelijke organisatie ingeval van een datalek het College bescherming persoonsgegevens (Cbp)[3] en de betrokken personen onverwijld op de hoogte moet stellen. Dit roept de vraag op naar eventuele aansprakelijkheid.

Overigens is inmiddels een Algemene Verordening gegevensbescherming aangenomen,[4] waarin een meldplicht datalekken, die ertoe zal leiden dat de Wbp te zijner tijd wordt ingetrokken.[5] Nu de verordening niet de civielrechtelijke aansprakelijkheid zal regelen zal het onderhavige betoog naar verwachting zijn waarde behouden onder dat regime.

2. Achtergronden[6]

De meldplicht datalekken is afkomstig uit de Verenigde Staten van Amerika. De staat Californië heeft in 2002 als eerste een 'security breach notification law' aangenomen, en werd spoedig gevolgd door vele andere staten. Op dit moment zijn er diverse federale sector-specifieke regelingen en algemene regelingen voor individuele staten. Deze regelingen vallen op doordat zij geen sanctie opleggen, alleen een verplichting tot melding. De gedachte, die door de praktijk bevestigd lijkt te worden, is dat een meldplicht toch leidt tot voorkoming van datalekken. Cass Sunstein heeft dit

---

[1] Hoogleraar privaatrecht, Tilburg University, onderzoeker bij het Tilburg Instituut voor Privaatrecht, en redacteur van het WPNR.
[2] Wet van 4 juni 2015, Stb. 2015/230, iwtr. Stb. 2015/281. Hierover ook G.J.C. Lekkerkerker en J.W. van Ee, 'De notaris in een digitale wereld, twee invalshoeken', WPNR 7070 (2015).
[3] Deze organisatie wordt thans volgens art. 51 lid 4 Wbp 'in het maatschappelijk verkeer' aangeduid als 'Autoriteit Persoonsgegevens'. Eenvoudigheidshalve zal ik in dit artikel blijven spreken over de wettelijke benaming, zijnde Cbp.
[4] Aangenomen op 14 april 2016: http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm, op moment van schrijven nog niet gepubliceerd. Over het voorstel: J.P. de Jong, 'De Algemene verordening gegevensbescherming', RegelMaat 2015, p. 6-18.
[5] EK 2014-2015, 33 662, nr. C, p. 11.
[6] Nader T.F.E. Tjong Tjin Tai, D.J.B. op Heij, K.K. e Silva, I. Skorvanek en B.J. Koops, *Duties of care and diligence against cybercrime*, rapport (https://pure.uvt.nl/portal/files/5733322/Tjong_Tjin_Tai_cs_Duties_of_Care_and_Cybercrime_2015.pdf), par. 5.3.4, ook T.F.E. Tjong Tjin Tai en B.J. Koops, 'Zorgplichten tegen cybercrime', NJB 2015/16, p. 1065-1072, par. 4.c.

mechanisme aangeduid als 'regulation through disclosure'.[7] Bedrijven vrezen reputatieverlies door datalekken, nu dit kan leiden tot klantenverlies en daling van aandelenkoersen, naast eventuele aansprakelijkheidsrisico's. Zij kiezen daarom voor cyber-insurance polissen.[8] De verzekeraars die dergelijke polissen aanbieden beoordelen doorgaans het huidige beveiligingsniveau en eisen zonodig aanvullende maatregelen. Op elegante wijze wordt aldus, zonder nadere overheidsinterventie, een hoger beveiligingsniveau bereikt op kosten van de betrokken bedrijven.

In navolging van het Amerikaanse voorbeeld hebben de Europese Unie en de nationale wetgever inmiddels diverse meldplichten in het leven geroepen.[9] Art. 2 sub 4(c) Richtlijn 2009/136[10] voerde voor telecommunicatiedienstverleners een notificatieplicht voor datalekken in. In Nederland is dit geïmplementeerd per 5 juni 2012 in art. 11.3a van de nieuwe Telecommunicatiewet.[11] Per 24 juni 2013 is de Verordening notificatie datalekken aangenomen, die per 25 augustus 2013 van kracht werd. Deze gaf preciezere regels voor deze meldplicht.

In Nederland was kort tevoren al een concept-wetsvoorstel opgesteld tot wijziging van de Wet bescherming persoonsgegevens voor invoering van een algemene meldplicht aan het Cbp.[12] Dit voorstel is kort daarna ingediend[13] en de resulterende wet per 1 januari 2016 van kracht. Hierna ga ik alleen in op deze algemene meldplicht.

3. De algemene meldplicht

De Wet bescherming persoonsgegevens gaat uit van het begrip 'verantwoordelijke' als degene die verantwoordelijk is voor zorgvuldige gegevensverwerking (art. 1 sub d en 11 lid 2 Wbp). Ingeval van een inbreuk op de beveiliging die ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens dient de

---

[7] C.R. Sunstein, 'Information Regulation and Information Standing: Akins and Beyond', *University of Pennsylvania Law Review* 1999, 147/3, p. 613-675.
[8] W.T.C. Weterings, 'Verzekering van cyberschade en -aansprakelijkheid', AV&S 2015/2, C.M.C. van Tetterode, 'Het verzekeren van Cybersecurity', Bb 2015/54, E.M.I. Wolper, 'Privacy-risico's verzekerd', P&I 2015/2, ook Tjong Tjin Tai e.a. 2015, par. 6.6.2, en R.M. Peters, 'So You've Been Notified, Now What? The Problem With Current Data-Breach Notification Laws', *Arizona Law Review* 2014, 56/4, p. 1171-1202.
[9] Zie voor een overzicht EK 2014-2015, 33 662, nr. C, p. 12-14.
[10] Op p. L 337/30, strekkende tot wijziging van art. 4(3) Richtlijn 2002/58/EG. Implementatietermijn liep ingevolge art. 4 af op 25 mei 2011.
[11] F. van der Jagt, 'Iets te melden?', NJB 2012/1415, p. 1713-1719 en F.J. Zuiderveen Borgesius, 'De meldplicht voor datalekken in de Telecommunicatiewet', *Computerrecht* 2011-4, p. 209-218.
[12] Hierover Van der Jagt 2012.
[13] Wetsvoorstel 33 662, hierover J.M. van Essen, 'Nieuwe meldplichten in privacyland', P&I 2013/176.

verantwoordelijke een melding van dit lek te doen aan het Cbp en de betrokkenen, degenen om wier gegevens het gaat (art. 34a Wbp).

De meldplicht geldt wanneer sprake is van doorbreken van de beveiliging (of afwezige beveiliging), niet voor gevallen zoals lekken door klokkeluiders of als gevolg van een brand.[14] De meldplicht geldt ongeacht of er passende technische of organisatorische maatregelen zijn getroffen.[15] De enkele melding is derhalve geen bewijs dat er is tekortgeschoten in de beveiliging.

De drempel van ernstige gevolgen is bedoeld opdat niet voor elk wissewasje een melding wordt gedaan. "Het zoekraken of hacken van de ledenadministratie van een sportvereniging zal doorgaans leiden tot het nodige ongemak voor vereniging en leden, maar zal niet snel aanleiding geven tot een melding bij het Cbp. De gevolgen van een dergelijk datalek blijven doorgaans beperkt en ook van betrokkenen kan worden gevergd dat zij een zekere mate van risico aanvaarden. Dat is nu eenmaal onlosmakelijk verbonden met het normaal vertrouwen in maatschappelijke verhoudingen. Maar een datalek bij, bijvoorbeeld, de Belastingdienst of de Sociale Verzekeringsbank (SVB) of een commerciële bank of verzekeraar is doorgaans van geheel andere orde. Een datalek bij dergelijke instellingen kan leiden tot financieel nadeel bij de betrokkene of tot de compromittering van gegevens die beschermd worden door een geheimhoudingsplicht."[16] Ook is melding niet nodig bij adequate versleuteling van kwijtgeraakte gegevens.[17] Dan zijn er immers geen ernstige gevolgen.

Het Cbp hanteert beleidsregels voor de toepassing van art. 34a Wbp.[18] Organisaties zullen hoe dan ook toereikend moeten reageren.[19] Het Cbp kan een boete opleggen bij een datalek als de meldplicht is verzaakt of de beveiliging ontoereikend blijkt te zijn.[20] Dit valt buiten de privaatrechtelijke aansprakelijkheid.

4. Aansprakelijkheid: algemeen

---

[14] EK 2014-2015, 33 662, nr. C, p. 2-3.
[15] Beleidsregels voor toepassing van artikel 34a van de Wbp, p. 20, TK 2013-14, 33 662, nr. 6, p. 4.
[16] TK 2012-13, 33 662, nr. 3, p. 7.
[17] EK 2014-2015, 33 662, nr. C, p. 5.
[18] 'Beleidsregels voor toepassing van artikel 34a van de Wbp', op https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken
[19] Zie ook H. Candel, S. Nouwt, 'Help, een datalek! Een procedure voor het omgaan met datalekken', P&I 2016/3.
[20] Art. 66 lid 2 Wbp junto art. 34a en 13 Wbp. Nader TK 2014-15, 33 662, nr. 9, p. 7-23.

Ingeval een datalek is gemeld staat niet vast dat dit ook te wijten is aan onzorgvuldigheid. De meldplicht staat los van de vraag of de veiligheid toereikend was (par. 3). Omgekeerd hoeft niet ieder datalek dat onzorgvuldig is veroorzaakt te worden gemeld: indien de risico's gering zijn, is melding niet nodig (par. 3). In dat geval zullen betrokkenen hier overigens waarschijnlijk niet van op de hoogte raken en blijft de aansprakelijkheidsvraag theoretisch.[21]

Voor aansprakelijkheid is vereist dat sprake is van een onrechtmatige daad of wanprestatie. Schending van de verplichtingen van de Wbp is op zichzelf onrechtmatig op grond van art. 6:162 BW: schending van een wettelijke plicht. Aan het relativiteitsvereiste zal ingeval van een datalek jegens de betrokkene zijn voldaan. Daarnaast bepaalt art. 49 lid 1 juncto 3 Wbp dat de verantwoordelijke aansprakelijk is voor schending van de bepalingen van de Wbp, behalve voorzover de schade hem niet kan worden toegerekend (art. 49 lid 4 Wbp). Dit vormt een tweede grondslag voor aansprakelijkheid: deze is in beginsel overbodig naast art. 6:162 BW, behalve dan dat een specifieke partij wordt aangewezen (de verantwoordelijke). Naast de verantwoordelijke kan overigens ook de bewerker van de data aansprakelijk zijn als hij een fout heeft gemaakt bij de beveiliging (art. 49 lid 3, slot, Wbp). Eventueel kan de verantwoordelijke regres nemen.[22] Daarnaast is er discussie of de bestuurders van de verantwoordelijke en/of concrete werknemers die fouten hebben gemaakt zijn aan te spreken. Voor bestuurders gelden de gewone regels inzake bestuurdersaansprakelijkheid.[23] Voor werknemers geldt in contractuele situaties art. 6:257 BW (het verbod op de 'paardesprong', waardoor werknemers de door de werkgever overeengekomen exoneraties kunnen inroepen jegens de wederpartij). Bij acties op basis van onrechtmatige daad is persoonlijke aansprakelijkheid echter wel mogelijk.[24]

Ingeval van een datalek zou de schending moeten zijn gelegen in tekortschieten in de ex art. 13 Wbp vereiste veiligheid: dit vereist in essentie een 'passend beschermingsniveau' gelet op de aard van de te verwerken gegevens. Het

[21] Tenzij op een later moment misbruik van de gegevens wordt gemaakt en alsnog blijkt dat de gegevens door een datalek zijn verspreid.
[22] TK 2012-13, 33 662, nr. 3, p. 9, ook TK 1997-98, 25 892, nr. 3, p. 176-177 over art. 49 Wbp.
[23] Waarover A.J.P. Schild, 'Ontwikkelingen bestuurdersaansprakelijkheid: een overzicht', WPNR 7087 (2015). Daarnaast heeft de wetgever aangegeven dat het Cbp onder omstandigheden ook een boete aan de bestuurders van de verantwoordelijke kan opleggen (TK 2014-15, 33 662, nr. 9, p. 15, EK 2014-15, 33 662, nr. C, p. 20-21).
[24] Algemeen (kritisch): C.J.M. Klaassen, *Schadeveroorzakend handelen in functie*, oratie Nijmegen, Deventer 2000.

Cbp heeft beleidsregels opgestelt voor de te nemen veiligheidsmaatregelen.[25] Het blijft echter mogelijk dat de rechter in een concreet geval tot hogere eisen komt dan deze beleidsregels (op grond van uitleg van art. 13 Wbp), dan wel oordeelt dat los van deze wettelijke verplichtingen sprake is van schending van de algemene zorgvuldigheidsnorm van art. 6:162 BW. Het is mogelijk dat een zekere handeling onder de beleidsregels is toegelaten maar in de verhouding tot de betrokkene toch van onvoldoende zorg voor diens belangen getuigt.[26] De rechter zal bij zijn oordeel vermoedelijk moeten teruggrijpen op algemene gezichtspunten die zijn ontwikkeld in andere context van beveiliging tegen risico's, zoals de Kelderluikcriteria.[27]

Daarnaast zou ook een contractuele basis verdedigbaar zijn. Bewaring van gegevens zal in beginsel een rechtsverhouding zijn die doorgaans als contractueel kan worden gekenmerkt. Er zal immers toestemming moeten zijn gegeven voor de verwerking, en dit zal meestal slechts zijn gebeurd omdat daar iets tegenover stond voor betrokkenen. Zelfs als betrokkenen geen voordeel hebben gehad bij de toestemming mag – gelet op de regeling van de Wbp – worden aangenomen dat deze toestemming is gegeven onder de veronderstelling dat de data toereikend beschermd zou worden. Die bescherming vormt dus (een deel van) de tegenprestatie voor de toestemming. Het is echter de vraag of deze exercitie veel toegevoegde waarde heeft. Ofschoon in sommige contractuele verhoudingen een hogere mate van zorg kan worden verwacht dan buiten contract, lijkt dat in dit geval, gelet op de strekking van de Wbp, niet passend. Dit kan anders zijn als in de contractuele verhouding zelf nadere afspraken zijn gemaakt over de beveiliging.

De melding aan de betrokkene heeft tot gevolg dat deze in staat is om zelf maatregelen te nemen om verdere schade te beperken. Voorzover hij hier niet aan voldoet zal hij geen recht hebben op schadevergoeding (art. 6:101 BW).[28] Men kan hierbij denken aan eenvoudige maatregelen als wijzigen van wachtwoorden.[29]

---

[25] Cbp Richtsnoer beveiliging van persoonsgegevens, februari 2013, https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/beveiliging-van-persoonsgegevens

[26] Vgl. ten aanzien van verlening van een vergunning: HR 21 oktober 2005, NJ 2006/418 (Ludlage/Van Paradijs), HR 10 maart 1972, NJ 1972/278 (Vermeulen/Lekkerkerker) en Neerhof, NTBR 2007/4, p. 138-148.

[27] HR 5 november 1965, NJ 1966/136.

[28] TK 2012-13, 33 662, nr. 3, p. 9, Van der Jagt 2012, p. 1716. Als echter ook de verantwoordelijke deze maatregelen had kunnen nemen is mogelijk dat een beroep op eigen schuld faalt, vgl. HR 5 december 2014, NJ 2016/159 m.nt. Lindenbergh.

[29] TK 2012-13, 33 662, nr. 3, p. 22.

Overigens moet de verantwoordelijke bij de melding ook aangeven welke maatregelen getroffen kunnen worden.[30]

5. Vormen van schade[31]

Bij aansprakelijkheid wegens datalekken is het voor het privaatrecht relevant welke belangen zijn geschonden. In de literatuur wordt dit niet altijd zeer concreet gemaakt. De Parlementaire Geschiedenis op de wijziging van de Wbp is gelukkig wat concreter: "Het gaat dan om de gevolgen van het lekken van de persoonsgegevens voor de persoonlijke levenssfeer van de getroffen personen. Burgers kunnen door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. De schade kan van materiële of immateriële aard zijn (zoals bijvoorbeeld onrechtmatige publicatie, aantasting in eer en goede naam, identiteitsfraude, discriminatie)."[32]

Dergelijke risico's doen zich in het bijzonder voor als het gaat om lekken van privacygevoelige gegevens naar malafide derden.[33] Als dergelijke gegevens bij bona-fide, grote partijen belanden mag men er in de regel van uit gaan dat deze geen onrechtmatig gebruik van deze gegevens maken. Als dit anders is, zijn deze partijen zelf aan te spreken. De partij die de data heeft gelekt kan dan buiten schot blijven.

Als het gaat om aansprakelijkheid van de verantwoordelijke is derhalve vooral relevant schade uit onrechtmatig gebruik door malafide partijen, of uit nadelig doch rechtmatig gebruik door derden. Dit omvat zowel vermogensschade (par. 6) als immateriële schade (par. 7). Ik zal de risico's kort uitwerken.

Bij misbruik door malafide partijen wordt vooral gedacht aan identiteitsfraude: het zich voordoen als een ander. Dit kan leiden tot bestellingen op andermans naam, opgeven van valse identiteit waardoor een ander wordt verdacht van misdrijven. Er is echter ook ander misbruik mogelijk: delicten zoals inbraak,[34] leegtrekken van een

---

[30] "de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken." (art. 34a lid 3, slot, Wbp).
[31] Ik beperk mij hier tot schade aan individuele belangen. Onderwerpen als know-how en bedrijfsgeheimen blijven derhalve onbesproken. Onder het EVRM vallen rechtspersonen buiten de reikwijdte van het recht op bescherming van privacy (EHRM 2 februari 2016, 22947/13, Magyar v Hungary, nr. 66).
[32] TK 2013-14, 33 662, nr. 6, p. 19.
[33] Literatuur over privacy ging oorspronkelijk vooral over privacyschending door de overheid ('Big brother') en later door grote bedrijven. Dit valt buiten het bestek van dit artikel.
[34] Denk aan de 'Quote 500-inbraken': slachtoffers van inbraken werden uitgezocht op basis van vermelding in de Quote 500. http://www.nrc.nl/nieuws/2013/09/03/tot-zes-jaar-cel-geeist-tegen-quote-500-inbrekers. Of ook doordat het wachtwoord van een alarminstallatie bekend wordt.

bankrekening,[35] chantage. Gegevens kunnen ook gebruikt worden om toegang te verkrijgen tot andere systemen (wachtwoorden raden of vragen ter identificatie beantwoorden). Bovendien kunnen gegevens, als zij eenmaal gelekt zijn, langdurig bewaard blijven of gaan rondzwerven en veel later alsnog daadwerkelijk misbruikt worden.

Verder kan een derde gegevens publiek maken zonder winstoogmerk, en daarmee schade aanrichten. Dit kan leiden tot reputatieschade, wat tot verlies van inkomen naast immateriële schade kan leiden. Ook kan vervolgens sprake zijn van onderscheid op basis van onrechtmatig publiek geworden gegevens: een beoogd werkgever kan bijvoorbeeld iemand afwijzen omdat hij lid is van een bepaalde politieke partij, een zekere seksuele voorkeur heeft, een bepaalde ziekte heeft. Dergelijk handelen van de werkgever kan onrechtmatig zijn, echter is dit niet altijd. De betrokkene lijdt ook bij een rechtmatige afwijzing schade. Daarnaast zal het lastig zijn aan te tonen dat dit speelt.[36]

Gelekte gegevens kunnen ook rechtmatig worden gebruikt op een wijze die nadeel oplevert. Op zichzelf geldt dat een organisatie ingevolge de Wbp gegevens niet zonder toestemming mag verwerken, maar in een civielrechtelijke procedure geldt dat zulke op zichzelf onrechtmatig verkregen gegevens wel tot bewijs kunnen bijdragen en niet principieel zijn uitgesloten.[37] Ingeval de verkrijger een overheidsinstantie is, ligt dit ingewikkelder; ik ga hier niet nader op in, doch merk alleen op dat ook bij overheidsinstanties niet uitgesloten is dat dergelijke data gebruikt mag worden. Dit kan bijvoorbeeld leiden tot naheffingen wegens belastingontduiking,[38] procedures of verlies van uitkering wegens verzwijging bij verzekeringen.[39]

Tot slot kan een betrokkene genoodzaakt zijn kosten te maken, bijvoorbeeld om schade als hierboven beschreven te voorkomen of te beperken (art. 6:96 lid 2 sub a BW), of buitengerechtelijke kosten. Deze komen in beginsel ook voor vergoeding in aanmerking.

---

[35] Men kan contact leggen met een bank e.d. door zich telefonisch vals te identificeren op basis van de gegevens.
[36] Een zeldzaam geval waar de werkgever dit zelf meldde: https://www.om.nl/actueel/nieuwsberichten/@94162/geldboete-1-600/
[37] HR 18 april 2014, NJ 2015/20 en HR 11 juli 2014, ECLI:NL:HR:2014:1632.
[38] Denk aan de LuxLeaks-affaire. In hoeverre in fiscalibus gebruik mag worden gemaakt van 'gelekte' data hoeft hier verder niet te worden uitgewerkt; het gaat om de mogelijkheid dat dit soms zou kunnen en tot nadelige consequenties kan leiden.
[39] Bijvoorbeeld bij verzwijgen van relevante medische of strafrechtelijke gegevens, wat kan leiden tot verval van recht op uitkering (art. 7:928 juncto 7:930 lid 5 BW).

Er zullen ongetwijfeld nog andere vormen van benadeling gaan optreden. Niettemin geeft deze kleine inventarisatie een indruk van de soorten schade die op dit moment voorzienbaar lijken. Deze zullen zich niet in alle gevallen van datalekken voordoen. Dit zal mede afhangen van de aard van de gegevens en de concrete inhoud.

Het zal, lijkt het, vooral gaan om lekken van adresgegevens en andere identiteitsgegevens (BSN), bankgegevens of creditcardgegevens, wachtwoorden, medische gegevens. Daarnaast zal het dan moeten gaan om gegevens die niet alleen naar hun aard maar ook in concreto tot de beschreven soorten nadelen kunnen leiden. Een medisch gegeven als de aankoop van hoestdrank zal bijvoorbeeld niet snel tot schade leiden, ook al is het strikt genomen wel beschermd.

6. Causaliteit en bewijs van de (materiële) schade

Deze mogelijke vormen van schade hoeven zich niet zo vaak voor te doen. Het gaat vooral om risico's die pas als zij zich verwezenlijken, uitmonden in voor vergoeding in aanmerking komende schade. De enkele theoretische mogelijkheid op zodanig nadelig gevolg is op zichzelf onvoldoende om als schade aangemerkt te worden: op zijn minst zal het moeten gaan om een vrij serieuze kans.[40] Pas dan is er reden om bijvoorbeeld toekomstige schade te begroten op voet van art. 6:105 BW, of eventueel de leer van verlies van een kans toe te passen.[41]

Voor de diverse vormen van misbruik kan een beletsel zijn dat causaliteit vaak lastig te bewijzen is. Over de Quote-500-inbraken is bijvoorbeeld betoogd dat de inbraken niet door de publicatie (die overigens rechtmatig is) waren veroorzaakt: adressen waren niet medegedeeld, terwijl ook via andere bronnen eenvoudig is te achterhalen welke Nederlanders vermogend zijn.[42] In het algemeen is het niet onmogelijk dat de gegevens langs andere weg zijn bekend geworden of uitgelekt, misschien zelfs door handelen van het betrokken individu zelf. Wel zou misschien de omkeringsregel of een jurisprudentieel vermoeden kunnen worden toegepast, nu het lekken van de gegevens het risico op dergelijk misbruik heeft geschapen.

Bij publiek geworden gegevens kan het gemakkelijker zijn het causaal verband aan te tonen. Alleen zal in veel gevallen geen noemenswaardige schade zijn ontstaan.

---

[40] Vgl. naar Amerikaans recht Peters 2014, p. 1188-1192.
[41] Zie HR 24 oktober 1997, NJ 1998/257 (Baijings) en laatstelijk HR 19 juni 2015, NJ 2016/1 (gem. Zoeterwoude).
[42] http://www.quotenet.nl/Nieuws/Quote-500-geen-routekaart-voor-inbrekers-28079

Dit kan anders liggen bij bekende personen die inkomen verwerven op basis van hun reputatie en bij wie hun reputatie daadwerkelijk wordt aangetast door de publicatie. Een recent (omstreden) voorbeeld is de zaak Bollea v Gawker, waar de beroepsworstelaar Hulk Hogan (de artiestennaam van Bollea) schadevergoeding van $ 55 miljoen voor *economic injuries* aan zijn carrière en $ 60 miljoen voor *emotional distress* verkreeg wegens publicatie van een sextape op de website van Gawker.[43] Hoewel de aanleiding niet een datalek is en de schade volgens Amerikaans recht is beoordeeld, laat het zien dat zeer substantiële bedragen mogelijk zouden kunnen zijn. In Nederland is er een geval geweest waar naaktfoto's van een presentatrice van haar privé-computer waren gehaald; zij heeft vervolgens gesteld opdrachten misgelopen te zijn tot € 330.000.[44] Zij slaagde echter niet in het bewijs van causaal verband; wel werd smartengeld toegewezen tot € 3.000. Dit betrof overigens in beide gevallen beelden of filmpjes, die waarschijnlijk als indringender en gevoeliger worden beschouwd.

Als openbaar geworden gegevens ertoe leiden dat een sollicitant wordt afgewezen zal dit waarschijnlijk praktisch niet te bewijzen zijn, behalve in uitzonderlijke gevallen zoals een verkeerd gestuurde e-mail.[45]

Als er nadeel ontstaat door rechtmatig gebruik van gegevens geeft dit niet zonder meer grond voor schadevergoeding. In de in par. 5 beschreven gevallen houdt het nadeel dan immers verband met eigen onjuist handelen dat aan het licht komt. Het is hoogst onzeker of dergelijk nadeel wel vergoed wordt. Zo is in HR 24 november 2000, NJ 2001/195 geoordeeld dat verlies van zwarte inkomsten niet wit (inclusief over de vergoeding verschuldigde belastingen) vergoed behoefte te worden. Een onrechtmatig voordeel dat verloren is gegaan behoort niet vergoed te worden. Dit wordt ook wel aangeduid als dat schade aan een niet rechtmatig belang niet of minder snel voor vergoeding in aanmerking komt.[46] Als juridisch instrument werkt men met toerekening (art. 6:98 BW) dan wel relativiteit.

---

[43] http://money.cnn.com/2016/03/18/media/hulk-hogan-gawker-jury-deliberations/
[44] Rb Noord-Nederland 18 december 2013, ECLI:NL:RBNNE:2013:8036 en 21 mei 2014, ECLI:NL:RBNNE:2014:2592.
[45] http://www.volkskrant.nl/binnenland/sollicitant-afgewezen-omdat-hij-een-donker-gekleurde-neger-is~a3552293/
[46] I. Haazen, 'Schade in een niet-rechtmatig belang', WPNR 6816 (2009) en S.D. Lindenbergh, *Schadevergoeding: algemeen, deel 1*, Mon. BW B34, 4e dr., Deventer 2014, nr. 46, conclusie A-G Rank-Berenschot, voor HR 22 oktober 2013, ECLI:NL:PHR:2013:BY6104, nr. 2.10.

Dit ligt echter anders als de gegevens leiden tot nadeel dat geen onjuist handelen betreft. Wellicht is een voorbeeld dat uit privé-postings op Facebook blijkt dat een opdrachtnemer/ZZPer extreme sporten uitoefent in zijn vrije tijd. Als dit uitlekt stelt de opdrachtgever, die dit te riskant vindt, beperkingen of eist garanties ingeval van arbeidsongeschiktheid (omdat anders het project riskeert uit te lopen), of zelfs ervoor kiest de overeenkomst op te zeggen.[47]

Kosten ter beperking of voorkoming van schade zouden wel voor vergoeding in aanmerking komen, mits kan worden aangetoond dat zij de 'dubbele redelijkheidtoets' doorstaan: het maken ervan en de omvang ervan moeten redelijk zijn. Voorbeelden zijn procedures die nodig zijn om te voorkomen dat gegevens verder worden verspreid.[48]

Het lijkt er derhalve op dat slechts in een beperkte categorie van gevallen significante vermogensschade kan worden verhaald. Positief gezegd betekent dit dat er (naast eventuele bewijsproblemen) maar zelden sprake zal zijn van grote schade.

7. Immateriële schade

Voor smartengeld wegens immateriële schade is het voordeel dat causaliteit gemakkelijker kan worden aangetoond: het feit dat bepaalde gegevens zijn gelekt en/of openbaar zijn geworden kan voldoende zijn om de immateriële schade aan te tonen. Er zijn twee soorten immateriële schade relevant. Daarbij geldt dat datalekken waarschijnlijk slechts bij hoge uitzondering tot deze soorten schade leiden.

Ten eerste is er schending van eer en goede naam (art. 6:106 lid 1 sub b BW). De zaak Bollea v Gawker laat zien dat dit in Amerika tot zeer substantiële vergoedingen kan leiden (voor *emotional distress*). In Nederland echter zijn de bedragen veelal aanzienlijk lager.[49] Het enkele bekend worden van persoonlijke gegevens leidt niet vanzelf tot schending van eer en goede naam, het zal wel moeten gaan om gegevens die tot zodanige schending leiden.

Ten tweede is er de aantasting van de persoon 'op andere wijze' (art. 6:106 lid 1 sub b, slot, BW). De Hoge Raad heeft aangegeven dat hiervan sprake is bij hetzij

---

[47] Voor werknemers ligt dit ingewikkeld; het voert te ver diep in te gaan op het arbeidsrecht.
[48] Bijv. Rb Amsterdam 14 juli 2010, ECLI:NL:RBAMS:2010:BN4359, 10 augustus 2011, ECLI:NL:RBAMS:2011:BT1877, en 10 februari 2011, ECLI:NL:RBAMS:2011:BP3926, ook over rechtshandhaving T.F.E. Tjong Tjin Tai, 'The right to be forgotten – private law enforcement', International Review of Law, Computers & Technology, 30/1 (2016), p. 1-8.
[49] Bijv. Rb Noord-Nederland 21 mei 2014, ECLI:NL:RBNNE:2014:2592: € 3.000 voor openbaarmaken naaktfoto's en filmpjes.

ernstig geestelijk letsel, hetzij bij een ernstige inbreuk.[50] Kan dit zich bij datalekken voordoen? Het lijkt dan vooral te gaan om inbreuk op privacy, door het feit van bekend worden van persoonlijke gegevens. Op zichzelf wordt dit immers tamelijk strikt opgevat: in de zaak HvJ EG 6 november 2003, zaak C-101/01 (Lindqvist) betrof het een tamelijk onschuldige website waar een vrijwilligster wat informatie over andere vrijwilligers opnam, zoals hobby's, maar ook werkzaamheden en soms een telefoonnnumer. Dit leidde tot strafrechtelijke vervolging: dit was inderdaad in strijd met de EU-privacyregels. Maar is dit ook voldoende voor privaatrechtelijke schadevergoeding?

In het verleden is wegens inbreuk op privacy wel smartengeld toegekend. Dit betrof veelal onrechtmatige publicatie van portretten/foto's (bedragen van honderden tot tienduizenden gulden/euro).[51] Maar deze rechtspraak lijkt moeilijker toe te passen op het loutere openbaar worden van gegevens die geen foto's zijn en die niet in een tijdschrift maar op een website staan (en daar misschien niet door mensen worden geraadpleegd of gezien). Dit geldt nog sterker als de data wel gelekt is maar niet is gebleken dat deze verder verspreid is. De rechtspraak inzake onrechtmatige publicaties lijkt te veronderstellen dat er tenminste enige concrete schade aanwezig moet zijn, een geschonden belang. Toegegeven zij dat dit mede verklaard kan worden uit het gegeven dat daar dan ook de vrijheid van meningsuiting in het geding is.

Hoe moet er dan met privacyschendingen zonder concrete benadeling worden omgesprongen? Op zichzelf zou men kunnen wijzen op art. 49 lid 2 Wbp: "Voor nadeel dat niet in vermogensschade bestaat, heeft de benadeelde recht op een naar billijkheid vast te stellen schadevergoeding."[52] Dit lijkt echter opnieuw te suggereren dat ten minste sprake moet zijn van *nadeel*. Een 'billijke' schadevergoeding houdt dan niet meer in dan wat art. 6:106 BW reeds toekent.[53]

---

[50] A.J. Verheij, *Vergoeding van immateriële schade wegens aantasting in de persoon*, diss. Amsterdam (VU), Nijmegen 2002, p. 277, verwijzend naar HR 30 oktober 1987, NJ 1987/277 (Naturistengids) en HR 1 november 1991, NJ 1992/58 (K. Staat).

[51] Zie reeds HR 1 juli 1988, NJ 1988/1000 (Vondelpark) voor een op zich onschuldige foto van een zoenend stelletje, waar de publicatie toch tot nadelige gevolgen leidde (uitgaan latere relatie), en analyse van rechtspraak in Spoor/Verkade/Visser, *Auteursrecht*, 3e dr., Deventer 2005, § 6.11 en Verheij 2002, p. 281-287.

[52] Dit is overgenomen van het tot 2001 geldende art. 9 lid 2 Wet Persoonsregistraties (WPR).

[53] De wetgever gaf destijds aan dat art. 9 lid 2 WPR "kan worden beschouwd als een toepassing van artikel 6.1.9.11, eerste lid, onder b, van het Nieuwe Burgerlijk Wetboek. Het betreft hier "schade door aantasting van de persoon", waarvan moet worden betwijfeld of deze reeds onder artikel 1401 B.W. voor vergoeding in aanmerking komt." (TK 1986-1987, 19 095, nr. 6 (MvA), p. 39) Er wordt ook

De tendens in de literatuur lijkt te zijn dat inbreuk op fundamentele rechten op zichzelf, zonder concrete verdere nadelen, grond kan bieden voor smartengeld.[54] Daarbij wordt echter ook aangenomen dat niet de inbreuk per se al leidt tot smartengeld: niet iedere ergenis of onbehagen behoort tot aanspraken te leiden.[55] Bovendien is het mogelijk dat op andere wijze genoegdoening kan worden bereikt,[56] zoals bij de vaststelling van een schending.[57] Mede in het licht van de in par. 3 geciteerde opmerkingen van de wetgever lijkt de enkele privacyschending van te licht gewicht, waarbij men bedenke dat de (al dan niet publieke) melding en eventuele oplegging van boete door het Cbp zou kunnen worden aangemerkt als een vorm van genoegdoening voor geringe schendingen.

Uiteindelijk zal een beoordeling van de concrete omstandigheden nodig zijn. Lindenbergh lijkt hierbij wat terughoudender, Emaus staat positiever tegenover substantiële vergoedingen.[58] Hoe dan ook lijkt ten minste van belang wat voor soort gegevens zijn gelekt en wat er vervolgens mee gebeurd is: hebben alleen de 'inbrekers' de gegevens gezien of is dit openbaar gemaakt? Dit alles overziend lijkt het loutere lekken van data niet op zichzelf al te leiden tot smartengeld, ten minste lijken er enige bijkomende omstandigheden (in het bijzonder concrete benadeling) nodig te zijn.

8. Tot besluit

Deze inventarisatie laat zien dat datalekken soms kunnen leiden tot aanzienlijke schade, maar dat veelal hooguit geringe schade te verwachten is en ook slechts geringe vergoedingen kunnen worden toegewezen.[59] Men zou kunnen betogen dat collectieve actie de handhaving zou versterken, echter dan loopt men nog steeds vast op het gegeven dat de vergoedingen waarschijnlijk zo laag zullen zijn dat het

---

aangegeven dat deze bepaling na invoering van (thans) art. 6:106 BW wellicht zou kunnen vervallen (TK 1986-1987, 19 095, nr. 6, p. 49).

[54] Hierover uitvoerig, naast andere remedies: J.M. Emaus, *Handhaving van ERM-rechten via het aansprakelijkheidsrecht*, diss. Utrecht, Den Haag 2013. Hierbij wordt aansluiting gezocht bij de vaste rechtspraak van het EHRM inzake de noodzaak van een *effective remedy*.

[55] Zie uitvoerig S.D. Lindenbergh, 'Vermogensrechtelijke remedies bij schending van fundamentele rechten', Preadvies VBR 2011, Deventer, p. 89-96.

[56] Lindenbergh, p. 96-100.

[57] Vaste rechtspraak van het EHRM, zie hierover Lindenbergh, p. 83-86 en 97.

[58] Emaus 2013, p. 344-345.

[59] Voor een afwijkende inschatting zie http://dirkzwagerieit.nl/2015/12/16/hoe-de-kosten-bij-een-datalek-al-snel-in-de-miljoenen-kunnen-oplopen/

collectiveren niet de moeite loont.[60] Publiekrechtelijke handhaving is dan ook onontbeerlijk om een handhavingstekort te vermijden.

[60] Vgl. voor Amerikaans recht Peters 2014, p. 1192-1193.