Mr. N.M. Brouwer[1]

Cyberverzekeringen vanuit rechtsvergelijkend perspectief: privacyregelgeving in de VS en de Europese AVG

AV&S 2018/19

In de Verenigde Staten vormt specifieke privacyregelgeving met meldplichten en boetes een belangrijke beweegreden voor organisaties om zich tegen cyberrisico's te verzekeren. In Europa blijft de vraag naar deze specifieke cyberverzekering evenwel achter. De verwachting is dat de onlangs in werking getreden Europese Algemene verordening gegevensbescherming ('AVG') daarin verandering zal brengen. In deze bijdrage wordt aan de hand van een rechtsvergelijking onderzocht of die verwachting gezien de inhoud van de AVG terecht is en in hoeverre de thans in Nederland aangeboden cyberverzekeringen op de AVG aansluiten.

1. Inleiding

Cyberverzekeringen zijn in de Verenigde Staten al tientallen jaren op de markt.[2] In de VS is de privacyregelgeving met haar meldplichten en boetes voor een belangrijk deel de motor achter de vraag naar verzekeringsdekking voor cyberrisico's.[3] De voornaamste reden om deze verzekering af te sluiten is gelegen in (compliance)[4] kosten rondom een 'datalek'.[5]

Inmiddels zijn cyberverzekeringen ook in Europa op de markt gebracht.[6] De Amerikaanse oorsprong is daarin in sterke mate terug te zien.[7] De afname van de cyberverzekering blijft in Europa evenwel achter ten opzichte van de VS.[8] De verwachting is dat de Europese Algemene verordening gegevensbescherming ('AVG'), die op 25 mei 2018 is getreden, een aanzienlijke stijging van de vraag naar cyberverzekeringen in Europa zal veroorzaken.[9] Deze verordening bevat immers, net als de Amerikaanse privacyregelgeving, een meldplicht bij datalekken en forse handhavingsboetes.

Het Amerikaanse privacyrecht verschilt evenwel sterk van de Europese regelgeving. Dit artikel zal aan de hand van een rechtsvergelijking tussen beide stelsels in kaart brengen of de AVG in dezelfde mate als in de Amerikaanse privacyregelgeving een juridische stimulans vormt voor het afsluiten van een cyberverzekering. De vragen die in dit onderzoek centraal staan, luiden derhalve: (1) creëert de inhoud van de AVG dezelfde behoefte aan specifieke cyberverzekeringsdekking als de Amerikaanse privacyregelgeving;[10] en (2) in hoeverre sluit de thans in Nederland aangeboden cyberverzekering op de AVG aan?[11]

Om deze vragen te beantwoorden geef ik een beknopt overzicht van de achtergrond van de cyberverzekering (paragraaf 2). Daarnaast ga ik in op de specifieke Amerikaanse regelgeving die de behoefte aan een cyberverzekering oproept en geef ik de inhoud van de cyberverzekering beknopt weer (paragraaf 3). In paragraaf 4 geef ik een overzicht van de voor de cyberverzekering relevante aspecten van het Europese privacyrecht en onderzoek ik op welke punten de AVG met de Amerikaanse regelgeving overeenkomt en/of verschilt. Aan de hand van die bevindingen kan het antwoord op bovenstaande onderzoeksvragen worden geformuleerd (paragraaf 5 en 6).

---

1 Mr. N.M. Brouwer is advocaat bij Dirkzwager advocaten & notarissen en buitenpromovenda bij het Onderzoekcentrum Onderneming & Recht van de Radboud Universiteit. Citeerwijze: N.M. Brouwer, 'Cyberverzekeringen vanuit rechtsvergelijkend perspectief: privacyregelgeving in de VS en de Europese AVG', *AV&S* 2018/19.

2 R.P. Majuca e.a., 'The Evolution of Cyberinsurance', ACM Computing Res. Repository (https://arxiv.org/abs/cs/0601020), 2006. Zie ook A. Marotta e.a., 'Cyber-insurance survey', *Computer Science Review* 2017-24, p. 35-61.

3 R. Betterley, 'Cyber/privacy insurance market survey – 2017', *The Betterley Report* 2017, p. 8-9. Zie ook O. Ralph, 'Cyber insurance market expected to grow after WannaCry attack', *Financial Times* 16 mei 2017 en ENISA, *Cyber insurance: recent advances, good practices and challenges*, november 2016.

4 In dit artikel wordt met 'compliance' bedoeld: het (treffen van maatregelen om te) voldoen aan de vereisten in de toepasselijke regelgeving.

5 K. Middleton & M. Kazamia, 'Cyber Insurance: Underwriting, Scope of Cover, Benefits and Concerns', in: P. Marano e.a. (eds.), *The dematerialized insurance: distance selling and cyber risk form an international perspective*, Switzerland: Springer 2016, p. 187-191; M. Camillo, 'Cyber risk and the changing role of insurance', *Journal of Cyber Policy* 2017-2 (1), p. 54; A. Marotta 2017, p. 39. In dit artikel wordt de term 'datalek' gebruikt als verzamelterm voor verschillende aanduidingen van hetzelfde: *data breach*, *data security breach*, en inbreuk in verband met persoonsgegevens.

6 Bijvoorbeeld door AIG, Chubb (Ace), CNA Hardy, Catlin XL, Hiscox, Axa en Allianz. Zie uitgebreid over de verschillen in (een aantal van) deze polissen: B.F.H. Nieuwesteeg, L.T. Visscher & B.R.J. de Waard, 'De rechtseconomie van cyberverzekeringen', *Verzekeringsarchief* 2017/3, p. 155-160.

7 P. Hartman, 'Cyberrisico's bieden ongekende kansen!', *TAV* 2017/6-141. Zie ook W.C.T. Weterings, 'Verzekering van cyberschade en -aansprakelijkheid: voorziet de cyberverzekering (voldoende) in een behoefte van organisaties?', *AV&S* 2015/2.

8 OECD, *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing: Paris 2017, p. 60.

9 *Ibid*. Zie ook bijvoorbeeld M. Camillo 2017, p. 60; ENISA 2016, p. 5. Tevens ENISA, *Commonality of risk assessment language in cyber insurance*, ENISA Europe november 2017, p. 7. ENISA spreekt deze verwachting ook uit als effect van de NIB-richtlijn, waarin meldplichten voor ernstige inbreuken op de digitale veiligheid zijn opgenomen. Deze meldplichten gelden echter voor een beperkt aantal sectoren (overheden en kritieke infrastructuur). Ik deel deze visie van ENISA ten aanzien van de cyberverzekering derhalve niet zonder meer en betrek de NIB-richtlijn verder ook niet in dit artikel.

10 De inwerkingtreding van de AVG kan een groter effect hebben dan de inhoud *an sich* oproept, bijvoorbeeld door media- of commerciële aandacht. In dit artikel staat enkel (het effect van) de inhoud van de AVG centraal.

11 Dit onderzoek richt zich op (informationele) privacyregelgeving en cybersecurity. Andere aspecten van cybersecurity, zoals de bedrijfscontinuïteit en bescherming van bedrijfsprocessen, worden buiten beschouwing gelaten.

2. Technologie, privacyregelgeving en de cyberverzekering: een beknopt historisch overzicht van de Amerikaanse ontwikkeling

2.1 *De opkomst van de cyberverzekering in de Verenigde Staten*

De eerste cybergerelateerde verzekering is te vinden in de criminaliteitsverzekering van banken. Vanaf de jaren '70 van de vorige eeuw ontstonden daarop uitbreidingen om banken te beschermen tegen criminelen die zich fysieke toegang tot de computersystemen konden verschaffen. In de jaren '90 kwam de eerste 'hackerpolis' op de markt, waarbij technologiebedrijven en verzekeraars de handen ineensloegen.[12]

Deze verzekeringen boden als *first party* polissen dekking voor de *eigen* schade die bedrijven konden lijden door digitale aanvallen en inbreuken, bijvoorbeeld directe '*hacker damage*' en bedrijfsstagnatie. Verzekerden waren verplicht om diensten zoals veiligheidsscans en monitoring af te nemen bij de technologiebedrijven waarmee hun verzekeraar samenwerkte.[13] De eerste polis met zowel *first party* als *third party* dekking verscheen in 2000.[14] Onder de dekking viel bijvoorbeeld aansprakelijkheid voor inbreuken, smaad, laster, privacy-inbreuken en beroepsfouten ('*errors and omissions*').

Enige jaren later werd in de VS de wetgeving met betrekking tot het gebruik en de opslag van persoonsgegevens aangescherpt. Nadat in California in 2003 de eerste 'meldplicht datalekken' in werking was getreden, ontstond er een grote stijging in de vraag naar cyberpolissen.[15] Inmiddels hebben vrijwel alle staten deze regelgeving overgenomen.[16]

Naast deze (statenrechtelijke) meldplichten kennen de VS een aantal federale wetten waarin scherpe (compliance-) eisen worden gesteld ten aanzien van de omgang met (elektronische) gegevens, zoals financiële informatie, medische informatie en andere persoonlijke gegevens.

In de jaren die volgden hebben zeer grote inbreuken plaatsgevonden die in de media breed zijn uitgemeten. Denk daarbij aan de incidenten bij TJX in 2007, Sony Playstation in 2011, Target in 2013, eBay en JP Morgan Chase in 2014 en zorgverzekeraar Anthem in 2015.[17] Deze gebeurtenissen leidden tot verschillende schadeposten, zoals vergoedingen wegens aansprakelijkheid en kosten voor juridische bijstand, schade in verband met bedrijfsstilstand, boetes en reputatieschade.[18] Risicobeheersing alleen bleek niet meer voldoende. De behoefte aan verzekeringen om het restrisico af te dekken, nam toe. Bovendien bleek uit verschillende juridische procedures dat deze schade door het opnemen van standaarduitsluitingen voor 'cyberschade' in de AVB-verzekeringen, vaak niet was gedekt onder de algemene aansprakelijkheidsverzekering voor bedrijven (AVB).[19] De noodzaak om een apart verzekeringsproduct voor deze risico's af te sluiten werd daarmee steeds groter.[20]

De vraag naar en ontwikkeling van de cyberverzekering in de VS is dus voor een belangrijk deel ingegeven door regelgeving en de (mede daardoor) toegenomen aandacht voor inbreuken en schade die daaruit voortvloeit. Zodoende is de cyberverzekering uitgegroeid van een eenvoudige en relatief beperkte aanvullende verzekering tot een steeds meer gespecialiseerde, in de VS volop aangeboden *stand-alone* verzekering.[21]

2.2 *Privacy en gegevensbescherming in de Verenigde Staten: benadering en regelgeving*

Voor een goed begrip van de achtergrond waartegen de cyberverzekering tot stand is gekomen, is het van belang om te constateren dat er tussen de VS en Europa een significant verschil in benadering van het concept privacy bestaat. In deze paragraaf bespreek ik deze Amerikaanse benadering. In paragraaf 4 ga ik nader in op het Europese kader.

Het begrip 'privacy' komt in de Amerikaanse grondwet niet voor.[22] Het recht op privacy kan weliswaar zijdelings worden afgeleid uit een aantal Amendementenbij de grondwet, maar dit ziet slechts op bescherming tegen overheidshandelen. Voor bescherming tegen inbreuken op de privacy door burgers en private partijen bieden de Amendementen

12 Majuca e.a. 2006, p. 5.

13 *Ibid*.

14 *Ibid*.

15 Marotta e.a. 2017, p. 38. Zie ook Camillo 2017, p. 54.

16 Slechts Alabama en South Dakota kennen een dergelijke wet niet; I. Jolly, 'Data protection in the United States: overview', *Thomson Reuters Practical Law* 2017, p. 4. Zie ook B. Nieuwesteeg, 'Van Silicon Valley via Den Haag naar Brussel: de invoering van de meldplicht datalekken', *AV&S* 2016/24 (p. 133-134).

17 'TJX Says Theft of Credit Data Involved 45.7 Million Cards', *New York Times* 30 maart 2007; L. Baker, 'Sony PlayStation suffers massive data breach', *Reuters* 27 april 2011; N. Perlroth, 'Target Struck in the Cat-and-Mouse Game of Credit Theft', *New York Times* 19 december 2013; A. Peterson, 'eBay asks 145 million users to change passwords after data breach', *Washington Post* 21 mei 2014; 'JPMorgan hack exposed data of 83 million, among biggest breaches in history', *Reuters* 3 oktober 2014; R. Abelson, 'Millions of Anthem Customers Targeted in Cyberattack', *New York Times* 5 februari 2015.

18 A. Lorraine e.a., 'The evolution of cyber coverage law: A survey of critical decisions and the market's response, *American Bar Association* 21 november 2016 <www.americanbar.org/publications/litigation-committees/insurance-coverage/articles/2016/fall2016-cyber-coverage.html>, laatst bezocht 13 oktober 2017. Het datalek bij Target leidde destijds tot een miljoenenschade en het ontslag van de CEO, zie bijvoorbeeld www.theguardian.com/business/2014/may/05/target-chief-executive-steps-down-data-breach, laatst bezocht 13 oktober 2017.

19 *Ibid*.

20 A. Zelle & S. Whitlead, 'Cyber Liability: It's Just a Click Away', *Journal of Insurance Regulation* 2014, vol. 33, p. 160.

21 *Stand-alone* verzekering: een zelfstandig, op zichzelf staand verzekeringsproduct, in tegenstelling tot het integreren van aanvullende dekking in bestaande polissen.

22 Pas in 1967 wordt het recht op privacy geconstrueerd/ingelezen in de Grondwet; US Supreme Court in *Katz/US*, 389 US 347, 350 (1967). Zie ook *Roe/Wade*, 410 US 113, 93, S.Ct. 705, 35 L.Ed.2d.147 (1973).

geen grondslag.[23] In 1890 werd het begrip in de *Harvard Law Review* voor het eerst expliciet genoemd en gekwalificeerd als '*the right to be let alone*'.[24]

Met de opkomst van de informatiemaatschappij is de nadruk bij 'privacy' steeds meer komen te liggen op het informationele aspect daarvan: de bescherming van persoonlijke gegevens.[25] Ondanks dat Europese landen en de VS als lidstaten van de OESO[26] in 1980 de '*Privacy Principles*' hebben onderschreven,[27] zijn deze *Principles* in de VS op andere wijze geïmplementeerd dan in Europa.

Het recht op privacy wordt in de VS gezien als een '*commodity*', een handelsartikel.[28] Illustratief daarvoor is de uitspraak van Ambassador Aaron tijdens het Safe Harbor debat in 2001:

> "In America, we believe that privacy is a right that inheres in the individual. We can trade our privacy – our private information for some benefit if we choose."[29]

Het recht op privacy is iets wat een individu toekomt, en omvat bovendien ook de vrijheid van de individu om zijn eigen beslissingen te maken. De individu, de 'eigenaar' van het recht op privacy, kan dit recht dus inruilen voor iets anders als hij dat wil.

Daarnaast hechten de VS veel waarde aan de aloude liberale gedachte van '*laissez-faire*': de overheid moet zich niet te veel met regelgeving bemoeien, maar dient dat over te laten aan de private sector.[30] In de VS bestaat daardoor geen algemene, federale en overkoepelende privacywetgeving. De Amerikaanse privacywetgeving is voor een groot deel vormgegeven door zelfregulering in de private sector, door zowel federaal als statenrecht en door rechtspraak. Dit resulteert in uitgebreide regelgeving die Loring omschrijft als "*decentralized, fragmented, ad hoc, and narrowly tailored to target specific sectors*",[31] oftewel: een "*patchwork quilt*".[32]

3. De invloed van de Amerikaanse regelgeving op de behoefte aan een cyberverzekering

De Amerikaanse privacyregelgeving kent dus een grote omvang en sterke variatie en fragmentatie. Een complete schets daarvan valt buiten het bestek van dit artikel. De te bespreken regelgeving heb ik ingekaderd aan de hand van de door wetgeving ingegeven beweegredenen voor het afsluiten van cyberverzekeringen. In de paragrafen 4 en 5 onderzoek ik of en in hoeverre de Europese AVG eenzelfde stimulans biedt.

Deze beweegredenen zijn grofweg onder te verdelen in (compliance)kosten rondom meldplichten, aansprakelijkheid en boetes.[33] Deze componenten komen in meerdere Amerikaanse wetten naar voren. Ik zal mij beperken tot een aantal in het oog springende federale privacywetten. Op statelijk niveau bespreek ik de beveiligingsverplichtingen en de meldplicht uit het Californische recht, omdat deze wetgeving model heeft gestaan voor vrijwel alle andere Amerikaanse staten.[34]

In verband met de sectorale verdeling van deze wetgeving ga ik achtereenvolgens in op regels voor consumenten, financiële instellingen en medische instellingen.

3.1 *Consumentenbescherming*

De *Federal Trade Commission Act* ('FTCA') beoogt consumenten te beschermen tegen oneerlijke en misleidende praktijken en is van toepassing op bedrijven en particulieren die handelen in de VS. De wet bevat geen bepaling ten aanzien van specifieke (categorieën van persoons)gegevens, maar kent een algemeen verbod op '*unfair or deceptive acts or practices in or affecting commerce*'.[35] Onder '*unfair of deceptive acts*' valt bijvoorbeeld ook de onvoldoende bescherming van klantgegevens waardoor deze worden blootgesteld aan cyberrisico's,[36] verandering van de *privacy policies* zonder dat de klanten daarvan op de hoogte worden gesteld en het niet voldoen aan de eigen privacy policy.[37] De *Federal Trade Commission* ('FTC') handhaaft deze wet.

Ook de *Fair Credit Reporting Act* ('FCRA'), gericht op *credit reporting agencies*,[38] beoogt de belangen van consumenten

23 A. Loring, 'An analysis of the informational privacy protection afforded by the European Union and the United States', *Texas International Law Journal* 2002, vol. 37.421, p. 427.

24 S. Warren & L. Brandeis, 'The right to privacy', *Harvard Law Review* 1890, vol. 4-5.

25 Deze vorm van privacy werd door het *U.S. Supreme Court* in 1977 erkend in de zaak *Whalen/Roe* (429 U.S. 589 (1977), waarin de vraag voorlag of het verstrekken van kopieën van medicijnrecepten door artsen aan de Staat een inbreuk op de privacy vormde.

26 Organisatie voor Economische Samenwerking en Ontwikkeling.

27 De Principles zijn te raadplegen op www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

28 B. Custers e.a. (reds.), *De bescherming van persoonsgegevens. Acht Europese landen vergeleken*, Den Haag: Sdu Uitgevers 2017, p. 15. Een andere duiding van het verschil in benadering is te vinden in J. Whitman, 'The two western cultures of privacy: Dignity versus Liberty', *The Yale Law Journal* 2004/113, p. 1151-1221.

29 D.L. David, Prepared Witness Testimony. *The EU Data Protection Directive: Implications for the U.S. Privacy debate*, The House Committee on Energy and Commerce. Washington D.C., 8 maart 2001 www.gpo.gov/fdsys/pkg/CHRG-107hhrg71497/html/CHRG-107hhrg71497.htm, laatst bezocht 13 oktober 2017.

30 D. Bach, 'The New Economy: transatlantic policy comparison. Industry self-regulation in the E-conomy', *Berkeley Roundtable on the International Economy (BRIE)*, 2001.

31 Loring 2002, p. 425.

32 Movius & Krup, 'U.S. and EU privacy policy: comparison of regulatory approaches', *International Journal of Communication* 2009-3, p. 175.

33 Betterley 2017, p. 8-9.

34 Zie ook § 2.1 van dit artikel. Zie op dit punt ook Nieuwesteeg 2016.

35 Afdeling 5, § 45 van de FTCA.

36 Zie *FTC/Wyndham Worldwide Corporation*, 299 F. 3d 236, US Court of Appeals 3rd Circuit 2015; zie ook FTC, 'Privacy & Data Security Update: 2016', p. 4 (te raadplegen op www.ftc.gov/reports/privacy-data-security-update-2016, laatst bezocht 20 april 2018).

37 Jolly 2017. Het hebben van een privacy policy is overigens niet verplicht, wat illustreert dat de FTCA in beginsel niet is geschreven met het oog op gegevensbescherming, maar op de bescherming van de consument tegen misleidende praktijken.

38 Instellingen vergelijkbaar met het Bureau Krediet Registratie. Zie 15 U.S.C., § 1681a(f).

te beschermen. Deze wet bestaat al sinds 1970 en wordt wel gezien als de eerste Amerikaanse privacywet.[39] Dat kredietbureaus al vrij vroeg aan dergelijke (informationele) privacyregels zijn onderworpen, heeft volgens Winn te maken met het feit dat Amerikanen in grote mate afhankelijk zijn van krediet om hun levensstandaard te behouden:

> "[…] *he American public's dependence on credit allows them to act as gatekeepers of the 'American Dream'.*"[40]

De FCRA bepaalt onder welke omstandigheden kredietbureaus de verzamelde gegevens mogen delen, dat de verzamelde gegevens enkel mogen worden gebruikt voor de in de wet bepaalde doeleinden en dat er redelijke maatregelen moeten worden getroffen om de vertrouwelijkheid, accuraatheid, de relevantie en het gebruik van de gegevens te waarborgen.[41] Bovendien voorziet de FCRA consumenten van rechten op de accuraatheid van hun gegevens (bijvoorbeeld inzage en correctie). Overtreding van de FCRA betekent een *unfair practice* in de zin van de FTCA. Daarnaast bepaalt de FCRA zelf dat overtreders van de wet aansprakelijk zijn voor daaruit voortvloeiende schade, waaronder *punitive damages*.[42]

Sinds 2002 heeft de FTC meer dan zestig handhavingsprocedures gevoerd tegen bedrijven waarbij zich een (digitaal) beveiligingsprobleem voordeed. Geen van deze zaken is uitgeprocedeerd; zij zijn allemaal geschikt. De hoogste schikking die tot nu toe werd getroffen, was met LifeLock, een bedrijf dat zich (ironisch genoeg) richt op bescherming tegen identiteitsfraude: $ 100 miljoen.[43] Het meest recente schandaal waarnaar de FTC een onderzoek is gestart is het datalek bij Facebook en Cambridge Analytica.[44]

De FTCA en de FCRA bevatten geen meldplicht bij datalekken.

3.2 *Financiële instellingen*

De FTC is eveneens de handhavende instantie voor de Gramm Leach Bliley Act ('GLBA').[45] Deze federale wet heeft betrekking op financiële gegevens en is van toepassing op financiële instellingen, banken, verzekeraars en andere financiële dienstverleners. De GLBA bevat regels over het verzamelen, gebruiken, delen en openbaar maken van niet-openbare[46] financiële gegevens. Daarnaast is in de GLBA het transparantiebeginsel terug te zien in de verplichting voor financiële instellingen om hun klanten[47] minstens één keer per jaar te informeren over de gegevens die worden gedeeld, met welke partijen wordt gedeeld en op welke wijze de gegevens worden beschermd.[48] Bovendien moeten financiële instellingen hun klanten een (begrijpelijke en uitvoerbare) *opt-out* mogelijkheid bieden voor het geval zij het niet eens zijn met het delen van informatie.[49]

In de *Safeguards Rule*, onderdeel van de GLBA, is nader uitgewerkt welke beveiligingsmaatregelen financiële instellingen moeten treffen.[50] Zij moeten onder andere een informatiebeveiligingsprogramma ontwikkelen, implementeren en bijhouden. Daarin moeten administratieve, technische en fysieke waarborgen zijn opgenomen. Deze waarborgen dienen passend te zijn voor de aard en omvang van de financiële instelling en haar activiteiten, en recht te doen aan de aard van de verwerkte gegevens.[51]

Naast de FTC speelt ook de *Security Exchange Commission* ('SEC') een actieve rol in de handhaving van de privacyregelgeving. De SEC ontleent haar bevoegdheid aan de GLBA. Haar taak is om privacyregelgeving te ontwikkelen voor een specifieke groep bedrijfstakken en deze regelgeving te handhaven.[52]

De SEC heeft deze regels – die grotendeels gelijk zijn aan de voornoemde *Safeguards Rule* – opgenomen in de *Regulation S-P*.[53] Zij heeft deze al meermaals strikt gehandhaafd. Zo betaalde R.T. Jones in 2015 na een datalek waarbij de persoonsgegevens van circa 100.000 betrokkenen werden buitgemaakt een forse afkoopsom aan de SEC. Ook Morgan Stanley koos in 2016 voor betaling van een bedrag van één miljoen dollar nadat een werknemer gegevens van duizenden personen had gestolen.[54] Zeker dit laatste geval, waarin Morgan Stanley in feite slachtoffer werd van haar eigen personeel, illustreert de strenge lijn die de SEC hanteert.

39 J. Delionado e.a., 'Efficacy of FCRA Claims Based on Stolen Data In Data Breach Cases', *Westlaw Journal* 2015, vol. 33-5.

40 J. Winn, 'Can a Duty of Information Security Become Special Protection for Sensitive Data Under US Law?', 9 september 2008, p. 3. Beschikbaar op SSRN: https://ssrn.com/abstract=1265775. Laatst bezocht op 6 juli 2018.

41 15 U.S.C., § 1681e.

42 15 U.S.C., § 1681n en 1681o.

43 www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated, laatst bezocht op 27 oktober 2017). Zie ook V. Semendyai, 'Due Process and the FTC's Fair and Reasonable Approach to Data Protection', *George Washington Law Review, Arguendo* 2016, vol. 84:51.

44 H. Kuchler, 'FTC to question Facebook over Cambridge Analytica data scandal', *Financial Times* 20 maart 2018.

45 15 U.S.C., § 6801-6827 (ook wel '*Financial Services Modernization Act*'), in werking getreden op 11 november 1999. Het verhaal gaat dat de catalogus van Victoria's Secret een cruciale rol heeft gespeeld in het opnemen van de privacy restricties in deze wet: een van de Afgevaardigden meende dat zijn creditcardmaatschappij zijn gegevens aan Victoria's Secret had verkocht, waarop hij ongewild de catalogus ontving, met allerlei huwelijkse problemen tot gevolg (zie het bericht van het Electronic Privacy Information Centre op https://epic.org/privacy/glba/victoriassecret.html, laatst bezocht op 20 oktober 2017).

46 Nonpublic: "*personally identifiable financial information – (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or(iii)otherwise obtained by the financial institution*". 15 U.S.C., § 6809 (4).

47 De GLBA maakt een onderscheid tussen *consumers* en *customers*. Met 'klant' wordt in dit artikel *customer* bedoeld: een consument die een duurzame relatie heeft met de financiële instelling.

48 15 U.S.C., § 6803.

49 15 U.S.C., § 6802. Van deze mogelijkheid zou overigens slechts 5-7% gebruik maken, zie J. Winn 2008, p. 5.

50 16 CFR Part 134, 36484 Federal Register, vol. 67, no 100, May 23, 2002.

51 16 CFR Part 134, § 314.3 (a).

52 15 U.S.C., § 6804 en 6805 (section 504 GLBA).

53 17 CFR, § 248, subpart A – Regulation S-P.

54 'SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach', press release 22 september 2015 (www.sec.gov/news/pressrelease/2015-202.html); 'SEC: Morgan Stanley Failed to Safeguard Customer Data', press release 8 juni 2016 (www.sec.gov/news/pressrelease/2016-112.html).

De GLBA en de Regulation S-P kennen beide geen meldplicht bij datalekken.

3.3 *Medische gegevens*

Een derde belangrijke federale wet is de *Health Insurance Portability and Accountability Act* ('HIPAA'). De wet is van toepassing op vrijwel alle instellingen die met medische gegevens in aanraking komen[55] en wordt gehandhaafd door de *Office of Civil Rights*, onderdeel van de *U.S. Department of Health & Human Services* ('HHS'). In de HIPAA staan bepalingen omtrent de verzameling en het gebruik van '*protected health information*' ('PHI'): medische en gezondheidsgegevens die individueel identificeerbaar zijn.[56]

Onderdelen van de HIPAA zijn de *HIPAA Privacy Rule*,[57] waarin medische instellingen worden beperkt in het gebruik van PHI; en de *HIPAA Security Rule*,[58] die medische instellingen verplicht om beveiligingsmaatregelen te nemen op administratief, technisch/fysiek en organisatorisch niveau. Vergeleken bij de FTCA en de GLBA zijn de privacybepalingen in de HIPAA vrij uitgebreid. Deze wet omvat bijvoorbeeld meer bepalingen over de rechten van betrokkenen dan de FTCA en de GLBA, zoals het recht op inzage en correctie van de gegevens.[59] Tevens komt het vereiste dat de betrokkene toestemming voor de verwerking verleent sterker naar voren in de HIPAA dan in de FTCA en de GLBA.[60]

Anders dan de FTCA en de GLBA bevat de HIPAA wel een meldplicht bij datalekken.[61] De medische instelling waarbij PHI als gevolg van een inbreuk (naar redelijk vermoeden) toegankelijk is, is verkregen, gebruikt of geopenbaard,[62] moet dit zonder onredelijke vertraging doch uiterlijk binnen zestig dagen na de ontdekking daarvan melden aan iedere afzonderlijke betrokkene.[63] Raakt het datalek meer dan vijfhonderd ingezetenen van de VS, dan moet de inbreuk bovendien ook worden gemeld aan prominente media, bijvoorbeeld door middel van een persbericht.[64] Tot slot dienen dergelijk grote datalekken gemeld te worden aan de *Secretary* van de HHS.[65] De meldplicht geldt op grond van de wet bovendien ook voor contractpartijen ('*business associates*') van de medische instellingen.[66]

In de HIPAA is expliciet opgenomen dat de bewijslast dat alle notificatieverplichtingen zijn nagekomen, of dat het voorval niet kan worden gekwalificeerd als een inbreuk zoals bedoeld in de wet, op de medische instelling rust.[67] Bij een overtreding van de wet kan de HHS boetes opleggen tot anderhalf miljoen dollar.[68]

3.4 *California Civil Code: Security of Information[69] en Security Breach Notification Law[70]*

Op grond van de *California Civil Code* zijn bedrijven die gegevens van Californische ingezetenen bezitten of anderszins onder zich houden[71] verplicht om redelijke beveiligingsprocedures te implementeren en te onderhouden. De te treffen beveiligingsmaatregelen moeten passen bij de aard van de persoonsgegevens en dienen bescherming te bieden tegen onbevoegde toegang tot de gegevens, alsook vernietiging, wijziging en openbaarmaking daarvan.[72] Bedrijven zijn gehouden om deze verplichting contractueel 'door te leggen' op een derde partij waarmee de gegevens worden uitgewisseld.[73] Wat deze 'redelijke' maatregelen inhouden, blijkt niet uit de wet en volgt evenmin duidelijk uit de jurisprudentie.[74]

Naast deze beveiligingsvoorschriften kent de *California Civil Code* een bepaling waarmee California in 2003 de wereldprimeur had: de verplichting voor bedrijven en overheidsorganen om ingezetenen van California op de hoogte te stellen van datalekken.[75] Het gaat daarbij om *personal information*, een begrip dat in de wet expliciet en limitatief wordt gedefinieerd. *Personal information* houdt in een (voor- en achter) naam, gecombineerd met een ander element zoals een *social security number*, rijbewijsnummer, medische informatie of creditcardnummer mét code.[76]

55 In dit artikel wordt voor al deze instellingen de term 'medische instellingen' gebruikt. Voor een totaaloverzicht zie 45 CFR part 160. Voor instanties die niet onder de HIPAA vallen, bijvoorbeeld websites waarop medische gegevens kunnen worden ingevuld, geldt de *Health Breach Notification Rule* die wordt gehandhaafd door de FTC.

56 45 CFR, § 160.103. De HIPAA kent overigens een mogelijkheid tot '*de-identification*', 45 CFR, § 164.502(d) en 45 CFR, § 164.514(a)-(b), waarna de PHI toch kunnen worden gebruikt. Volgens Narayanan maakt dit het hele begrip PHI tot een dode letter: A. Narayanan, 'Myths and fallacies of "Personally Identifiable Information"', *Communications of the ACM* 2010, vol. 53-6, p. 24-26.

57 45 CFR, § 160 en 164 (A) en (E).

58 45 CFR, § 160 en 164 (C).

59 45 CFR, § 164.524 en 526.

60 45 CFR, § 164 (E).

61 45 CFR, § 164.404.

62 "*accessed, acquired, used, or disclosed*", 45 CFR, § 164.404(a)(1).

63 45 CFR, § 164.404(b). De wijze waarop moet worden gemeld hangt van de omstandigheden af; dit kan schriftelijk, per e-mail, telefonisch of via een mededeling op de website van het geraakte bedrijf.

64 45 CFR, § 164.406.

65 45 CFR, § 164.408. Op de website van de HHS wordt van grote datalekken een lijst gepubliceerd, wat een zeker schandpaaleffect heeft: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (laatst bezocht op 6 juli 2018).

66 45 CFR, § 160.103.

67 45 CFR, § 164.414.

68 45 CFR, § 160.404. De wet zelf verschaft de betrokkenen niet rechtstreeks een *civil right of action*. In 2014 oordeelde het Supreme Court in Connecticut echter dat de bepalingen in de HIPAA standaarden voor zorgplichten kunnen inhouden die ingezet kunnen worden in *negligence claims* (aansprakelijkheidskwesties); *Byrne/Avery Ctr. for Obstetrics & Gynecology*, P.C., 314 Conn. 433 (2014).

69 Cal. Civ. Code § 1798.81.5.

70 Cal. Civ. Code § 1798.82(a).

71 "*own, license or maintain*", Cal. Civ. Code § 1798.81.5.

72 Cal. Civ. Code § 1798.81.5.(2)(b).

73 Vergelijkbaar met de Europese verwerkingsovereenkomst.

74 Ter verduidelijking heeft de *Attorney General* in 2016 een rapport uitgebracht waarin voorbeelden staan opgenomen, zie: K. Harris, 'California data breach report 2012-2015', *California Department of Justice*, februari 2016 (te raadplegen via https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf).

75 L. Determann, 'New California Data Security and Breach Notification Requirements', *Bloomberg Law* September 2016.

76 Cal. Civ. Code § 1798.81.5(d)(1) en 1798.82.

Er is sprake van een inbreuk indien niet-versleutelde[77] gegevens (naar redelijk vermoeden kunnen) zijn verkregen door een onbevoegd persoon.[78] De melding dient zonder onredelijke vertraging en binnen de meest passende termijn te worden gedaan aan de betrokkenen.[79] Alleen bij een inbreuk met meer dan vijfhonderd betrokkenen dient ook aan de *Attorney General* te worden gemeld.[80] De vorm en inhoud van de melding zijn gedetailleerd omschreven en richten zich op de kenbaarheid en begrijpelijkheid voor de betrokkene.[81] Anders dan in bijvoorbeeld Connecticut en Delaware kent California geen verplichting om schadebeperkende diensten, zoals *credit monitoring*, aan te bieden.[82] Worden deze diensten evenwel vrijwillig aangeboden, dan dient dit gratis te zijn en voor minstens 12 maanden.[83]

In veel Amerikaanse staten is de handhaving, waaronder een boetebevoegdheid, expliciet toegekend aan de *Attorney General*.[84] In California is dit niet het geval. De Californische wet creëert de (civiele) mogelijkheid voor betrokkenen om hun schade te verhalen bij overtreding daarvan.[85] Zij kunnen een *civil penalty* vorderen van $ 500 tot $ 3.000 per overtreding.[86]

Een bedrijf kan aansprakelijk worden gehouden voor een niet-tijdige melding, met dien verstande dat de benadeelde moet aantonen dat de schade is veroorzaakt door de vertraging en niet (enkel) door de inbreuk zelf.[87] Een voorbeeld van een grote *class action* onder (onder andere) de Californische wetgeving is de zaak tegen Yahoo!, waarover het District Court in California zich op 30 augustus 2017 uitsprak.[88] Het District Court nam daarin onder andere aan dat de benadeelden schade hadden geleden doordat Yahoo! een (drietal) datalek(ken) niet direct aan de betrokkenen had gemeld. Het datalek was de oorzaak van onder andere identiteitsfraude, maar door de te late melding was benadeelden de gelegenheid ontnomen om zelf schadebeperkende maatregelen te treffen. Hadden zij die mogelijkheid wel gehad, dan was de schade wellicht in het geheel niet ingetreden.

3.5 *De cyberpolis in het licht van de Amerikaanse privacy- en dataprotectie regelgeving*

Het niet-nakomen van de verplichtingen uit de hiervoor besproken regelgeving kan leiden tot verschillende vormen van schade en aansprakelijkheid. Deze schade kan bestaan uit door de handhavende autoriteiten opgelegde boetes, reputatieschade, claims van betrokkenen en alle daarbij komende kosten (zoals verdedigingskosten).

In deze paragraaf zet ik uiteen hoe de cyberverzekering voor deze risico's dekking biedt. In de VS wordt de cyberverzekering door tientallen maatschappijen aangeboden.[89] Naar de inhoud daarvan is een aantal uitgebreide onderzoeken gedaan.[90] Deze paragraaf is op die onderzoeken gebaseerd.

De (*stand-alone*) cyberverzekering bevat een aantal kenmerkende vormen van dekking die, ondanks de vele verschillen in polissen,[91] in elke polis – in meer of mindere mate – voorkomen.[92] De verzekering heeft een hybride vorm en biedt dus dekking voor zowel *first* als *third party* schade. *First party* schade bestaat bijvoorbeeld uit verlies, beschadiging of diefstal van eigen digitale *assets*, schade wegens bedrijfsstagnatie, notificatiekosten en schade door digitale afpersing. *Third party* schade omvat de kosten die samenhangen met aansprakelijkheidsclaims van derden die schade hebben geleden als gevolg van een cyberincident bij de verzekeringnemer. De cyberverzekering biedt dekking voor kosten van verweer tegen dergelijke claims, kosten van deskundigen en voor de eventueel verschuldigde schadevergoeding of schikkingen.[93]

Daarnaast bestaat de dekking uit bepaalde vormen van dienstverlening: crisismanagement, technische en/of juridische ondersteuning, en communicatiediensten. Dergelijke *response*-diensten zijn vooral wenselijk ter beperking van de eigen schade, al kan ook compliance een rol spelen. Een voorbeeld daarvan is het (al dan niet wettelijk verplicht) aanbieden van schadebeperkende diensten zoals *credit mo-*

77 Als de onderschepte gegevens zijn versleuteld ('*encrypted*'), dan hoeft de inbreuk niet gemeld te worden. Cal. Civ. Code 1798.82(i)(4): "For purposes of this section, "encrypted" means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security."

78 Cal. Civ. Code § 1798.82(a). De wet vereist niet dat die verkregen informatie ook daadwerkelijk moet zijn gebruikt, wat een van de punten is die in deze wet als controversieel worden beschouwd, zie F. Garcia, 'Data protection, breach notification, and the interplay between state and federal law: the experiments need more time', *Fordham Intellectual Property, Media and Entertainment Law Journal* 2007, vol. 17-3, p. 693-727.

79 Cal. Civ. Code § 1798.82(a). Hierop kan een uitzondering worden gemaakt indien de melding een strafrechtelijk onderzoek zou doorkruisen.

80 Cal. Civ. Code § 1798.82(f).

81 Voorbeelden zijn de lettergrootte (minimaal tien), het formaat (zodanig dat het de aandacht trekt), de titel ("*Notice of Data Breach*"), het taalniveau (*plain language*), et cetera., Cal. Civ. Code § 1798.82(d).

82 Connecticut: S.B. 949, sec. 36a-701b(2)(b); Delaware Code 6.II, § 12B 102(e).

83 Cal. Civil Code § 1798.82(d)(2)(G).

84 Bijvoorbeeld in Maine, Massachusetts, New York, Ohio, Oklahoma, Oregon, Utah. De Attorneys General spelen dan ook een grote rol bij het uitzetten van beleid en strategie ten aanzien van gegevensbescherming; zie D. Citron, 'The privacy policymaking of State Attorneys General', *Notre Dame Law Review* 2016/92-2, p. 747-816.

85 Cal. Civ. Code § 1798.84(b): "*Any customer injured by a violation of this title may institute a civil action to recover damages.*" In totaal kennen elf staten een *civil right of action* toe.

86 Cal. Civ. Code § 1798.84(c).

87 *Sony Gaming Networks & Customer Data Sec. Breach Litigation*, 996 F. Supp. 2d 942, 965, 1009-10 (S.D. Cal. 2014), p. 89.

88 *In re: Yahoo! Inc. Customer Data Security Breach Litigation*, U.S. D.C. California, 16-MD02752-LHK.

89 OECD 2017, p. 61.

90 *Ibid;* S. Romanosky e.a., 'Content Analysis of Cyber Insurance Policies. How do carriers write and price cyber risk?', *RAND Justice, Infrastructure, and Environment*, september 2017; Marotta e.a 2017; Betterley 2017.

91 Romanosky e.a. stellen dit uitgangspunt overigens ter discussie: uit hun onderzoek blijkt dat er juist een grote overlap bestaat tussen verschillende cyberpolissen. Dat strookt niet met het beeld dat thans bestaat, namelijk dat er zoveel verschil in polissen is dat dit het afsluiten van de verzekering in sterke mate bemoeilijkt (vgl. bijv. Betterley 2017, p. 3).

92 Marotta e.a. 2017. Ik merk hierbij op dat de polissen op detailniveau nog verschillen vertonen, bijvoorbeeld in de definities van kernbegrippen. Dit kan ertoe leiden dat schade onder de ene polis wel, maar onder de andere polis niet is gedekt.

93 De polis bakent af wat onder 'claims' wordt verstaan. Deze worden vaak onderverdeeld in claims wegens inbreuken op de privacy, onvoldoende netwerkbeveiliging of multimedia aansprakelijkheid.

nitoring, wat in veel polissen is gedekt.[94] Betterley schrijft dat dergelijke diensten ook onverplicht kunnen worden ingezet als middel om de eigen reputatieschade te beperken.[95] Dat uitgangspunt is juist, maar als de dienst louter met dat doel wordt aangeboden, zal niet iedere verzekeraar die kosten dekken.[96]

Schending van de regelgeving creëert het risico op boetes. Gezien de omvang van de boetes die bijvoorbeeld onder de FTCA en de HIPAA kunnen worden opgelegd, is verzekeringsdekking op dit punt zeer waardevol. In veel Amerikaanse polissen blijken *fines, penalties and fees* echter van dekking te worden uitgesloten.[97] De kosten van de juridische verdediging tegen deze boetes zijn vaak wel gedekt.

Een ander opvallend element uit de cyberzekering, dat evenwel nog in ontwikkeling is,[98] is de mogelijkheid van '*pre-breach services*'. (Cyber)verzekeraars beschikken bij uitstek over de kennis en contacten om de verzekeringnemers bij het afsluiten van de verzekering te voorzien van informatie en diensten of producten. Dit kan aantrekkelijk zijn voor de verzekeringnemers, omdat het kan helpen om aan de regelgeving te voldoen. Ook voor de verzekeraars biedt dit echter een kans. Zij houden immers meer controle over de wijze waarop de verzekeringnemers hun processen inrichten, weten bijvoorbeeld beter wat hun *incident response* plannen inhouden en kunnen derhalve de risico's beter inschatten.

Zetten we de inhoud van de gemiddelde cyberverzekering af tegen de risico's die rechtstreeks uit de Amerikaanse privacyregelgeving voortvloeien, dan is te zien dat de cyberverzekering goed bij die risico's aansluit. De verzekering biedt in de meeste gevallen dekking bij aansprakelijkheid wegens datalekken en de daaraan verbonden kosten van verweer. Bovendien kan een verzekering helpen bij het beperken van de eigen schade en het voorkómen van aansprakelijkheid door het verlenen van *incident response services*, zoals ondersteuning bij notificaties aan betrokkenen. Een uitgebreide verzekering kan zelfs dekking bieden voor boetes (of de kosten van verweer daartegen). De cyberverzekering voorziet daarmee in een specifieke behoefte van verzekeringnemers die uit Amerikaanse privacyregelgeving voortvloeit.

94 Betterley 2017, p. 9.

95 *Ibid*.

96 Een voorbeeld van een dergelijke beperkende omschrijving is: "*such services shall not be covered if notification is not required under applicable Breach Notification Laws*". Freedom Specialty Cyber Insurance Policy CYF-P-1 (12-15), section II, D.2.

97 Betterley 2017, p. 9 en Romanosky 2017, p. 14-15. Uit andere onderzoeken blijkt dat boetes in veel gevallen juist wel onder de dekking vallen. Zie bijvoorbeeld het rapport van OECD, *Enhancing the role of insurance in cyber risk management*, OECD Publishing: Paris 2017, p. 62 en de daarin genoemde bronnen. Een verklaring voor dit verschil kan zijn dat Romanosky enkel Amerikaanse polissen bij zijn onderzoek heeft betrokken, terwijl de OECD zich tevens lijkt te hebben gericht op onder andere de Europese markt, waar de situatie anders is dan in de VS.

98 Betterley 2017, p. 8.

4. Europa: privacyregelgeving

4.1 *Benadering en algemeen Europees juridisch kader*

Hiervoor is al benoemd dat er een cruciaal verschil bestaat tussen de Europese en de Amerikaanse benadering van het begrip 'privacy' en de rol die de overheid speelt bij de regelgeving. In Europa is privacy (zowel relationeel als informationeel) een fundamenteel mensenrecht dat in verschillende mensenrechtenverdragen is opgenomen.[99] In Nederland is het recht op privacy verankerd in de Grondwet.[100]

Het feit dat privacy in Europa een mensenrecht is, maakt de staat verantwoordelijk voor het waarborgen van dit recht. Een dergelijk fundamenteel recht leent zich naar zijn aard bovendien minder voor 'verhandelbaarheid' dan een *commodity*, zoals privacy in de VS wordt gezien. Een typisch verschil tussen het Amerikaanse en het Europese privacy-/gegevensbeschermingsrecht is dan ook dat het verwerken van persoonsgegevens in Amerika in beginsel is toegestaan,[101] terwijl daarvoor in Europa eerst een wettelijke grondslag is vereist.[102]

In Europa heeft de Algemene verordening gegevensbescherming ('AVG') sinds 25 mei 2018 de Europese Privacy Richtlijn 95/46/EG uit 1995 vervangen. Door de rechtstreekse werking van de AVG zijn bij de inwerkingtreding daarvan ook de bestaande uitwerkingen van de eerdere Richtlijn in nationaal recht vervallen, zoals in Nederland de Wet bescherming persoonsgegevens ('Wbp').[103]

In de VS ontbreekt een algemeen overkoepelende, federale regelgeving en is gegevensbescherming sectoraal bepaald. In Europa is de regelgeving voor gegevensbescherming centraal bepaald en geldt deze voor vrijwel alle sectoren.[104]

99 Artikel 8 EVRM, artikel 16 VWEU, artikel 7 en 8 Handvest Grondrechten EU.

100 Artikel 10 Gw. Volgens een aantal auteurs moet de verklaring van dit cruciale verschil in benadering worden gezocht in ingrijpende historische gebeurtenissen die in Europa hebben plaatsgevonden die de VS niet in dezelfde mate hebben beïnvloed. Voorbeelden daarvan zijn de rol van de Gestapo in Duitsland, de KGB in de Sovjet-Unie en de Stasi in de DDR, zie Movius & Krup, 2009, p. 169-187; D. Bach, 'The New Economy: transatlantic policy comparison. Industry self-regulation in the E-conomy', *Berkeley Roundtable on the International Economy (BRIE)* 2001; A. Newman, 'The New Economy: transatlantic policy comparison. Data privacy', *Berkeley Roundtable on the International Economy (BRIE)* 2001; D. Baumer e.a., 'Internet privacy law: A comparison between the United States and the European Union', *Computer & Security* 2004, vol. 23, nr. 5, p. 400-412; A. Loring 2002, p. 423; L. Determann, 'Adequacy of data protection in the USA: myths and facts', *International Data Privacy Law* 2016, vol. 6-3, p. 250.

101 P. Schwartz, *Foreword*, in L. Determann, *California Privacy Law: practical guide and commentary U.S. federal and state law*, San Francisco (CA): The Recorder 2017, p. vii. Zie ook L. Determann 2016, p. 247.

102 Artikel 7 Richtlijn 95/46/EG, artikel 6 AVG, artikel 8 Wbp.

103 Artikel 94 AVG. Zie ook de memorie van toelichting bij het wetsvoorstel Uitvoeringswet AVG, 13 oktober 2017 (pagina 3), te raadplegen op www.rijksoverheid.nl.

104 Opgemerkt zij dat ook in Europa sectorspecifieke regelgeving bestaat, zoals de E-privacy Richtlijn (Richtlijn 2002/58/EG). Deze richtlijn richt zich specifiek op de verwerking van persoonsgegevens in de sector elektronische communicatie en zal binnenkort, net als de Privacy Richtlijn 96/46/EG worden omgezet naar een verordening (Voorstel E-privacy Verordening, COM(2017)10 final, 2017/0003, p. 2). Omdat deze verordening als een *lex specialis* (zie artikel 95 AVG) werkt ten opzichte van de AVG, wordt deze wetgeving in dit artikel verder buiten beschouwing gelaten.

De AVG streeft naar harmonisatie en beoogt een coherente, homogene toepassing van de regels over gegevensbescherming te bewerkstelligen; het niveau van gegevensbescherming dient in iedere EU-lidstaat gelijk te zijn.[105] Door verschillende manieren van implementatie was (en is) dat onder de Richtlijn 95/46/EG niet altijd het geval.[106]

4.2 *De invloed van de Europese privacyregelgeving op de behoefte aan een cyberverzekering*

Uit het voorgaande is gebleken dat de Amerikaanse privacyregelgeving op een aantal punten leidt tot risico's die de behoefte aan de cyberverzekering hebben doen toenemen: compliance en kosten rondom meldplichten bij datalekken, aansprakelijkheid en boetes. In deze paragraaf onderzoek ik in hoeverre de AVG een soortgelijke behoefte in Europa creëert.

4.2.1 *Meldplicht bij datalekken*

De AVG bevat de verplichting om inbreuken in verband met persoonsgegevens te melden aan de toezichthoudende autoriteit (artikel 33 AVG). Dergelijke meldplichten bestonden al in specifieke sectoren, bijvoorbeeld in de telecommunicatie.[107] Een algemene meldplicht ontbrak. Slechts een aantal landen – waaronder Nederland sinds 2016 – kende al een algemene meldplicht voor inbreuken op persoonsgegevens.[108]

Met de introductie van deze meldplicht lijkt de Europese wetgever het Californische voorbeeld te hebben gevolgd.[109] Nadere analyse van de inhoud van de meldplicht laat echter een aantal verschillen zien, bijvoorbeeld in de definities van begrippen, de drempel om te moeten melden, de termijn en de geadresseerde.

Anders dan de *California Civil Code* definieert de AVG het begrip 'persoonsgegevens' niet als een limitatieve lijst van gegevens. De term 'persoonsgegevens' beslaat *alle* informatie over een geïdentificeerde of (direct of indirect) identificeerbare natuurlijke persoon.[110] Door de limitatieve opsomming is in de VS de beoordeling of sprake is van een persoonsgegeven eenvoudiger. De betekenis van het begrip '*personal information*' is bovendien enger. In Europa zal de verwerkingsverantwoordelijke bij een inbreuk moeten onderzoeken of er informatie is vrijgekomen waarmee betrokkenen al dan niet indirect geïdentificeerd kunnen worden. In de VS kan de verantwoordelijke kort gezegd volstaan met het zetten van vinkjes.

Daarnaast is de definitie van het begrip 'inbreuk' onder de AVG breder dan onder de Amerikaanse (statenrechtelijke) regelgeving. Immers, volgens de wetgeving in California is slechts sprake van een inbreuk bij '*acquisition by an unauthorized person*' (zie paragraaf 3.4). Dat is een engere definitie dan in de AVG. Hierin wordt bijvoorbeeld het verlies of de wijziging van persoonsgegevens ook als 'inbreuk' aangemerkt (artikel 4 onder 12 AVG).[111] De brede definitie van 'inbreuk' in de AVG lijkt meer op het ruimere begrip dat in de VS ten aanzien van medische gegevens wordt gehanteerd in de (federale wet) HIPAA. De waarde die in de VS slechts aan dergelijke uiterst gevoelige gegevens wordt toegekend, wordt in Europa kennelijk aan *alle* soorten gegevens toegekend.

Onder de AVG hoeft niet iedere inbreuk te worden gemeld. Die situatie is als een uitzondering op de hoofdregel omschreven: inbreuken moeten worden gemeld, *tenzij* niet waarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden voor natuurlijke personen inhoudt. Deze omschrijving betekent dat de verwerkingsverantwoordelijke ter beoordeling van haar meldplicht een uitgebreide risico-inventarisatie moet uitvoeren.[112] De wetgeving in de VS kent een dergelijke meldingsdrempel niet. Dit betekent dat iedere inbreuk moet worden gemeld. Een risico-inventarisatie hoeft daarbij niet te worden gemaakt. Dit maakt de beslissing om wel of niet te melden in de VS een stuk eenvoudiger dan in Europa. Enkel indien de gegevens adequaat zijn versleuteld en de sleutel niet is verkregen, hoeft in de VS niet te worden gemeld.[113]

Een meer praktisch verschil tussen de Amerikaanse meldplichten en de AVG is te zien in de meldingstermijn. De AVG bepaalt dat de melding moet plaatsvinden 'zonder onredelijke vertraging' en uiterlijk binnen 72 uur na kennisname van de inbreuk. Indien er aan de betrokkenen dient te worden gemeld, dan moet dit 'onverwijld' gebeuren.[114] Onder de AVG zullen bedrijven worden gedwongen om al vooraf een *incident response plan* gereed te hebben; tijd om nog een uitgebreid plan te maken op het moment na kennisname van de inbreuk, is er niet. Organisaties zullen dus een helder beeld moeten hebben van hun verwerkingen en de getroffen beveiligingsmaatregelen.[115] Dit is ook overigens met het oog op het *accountability*-beginsel (artikel 5 lid 2 en 24 AVG) verplicht.

105 Verordening (EU) 2016/679, cons. 3, 9 en 10.

106 Of de beoogde harmonisatie onder de AVG zal worden gerealiseerd, valt nog te bezien. Zie bijvoorbeeld P.T.J. Wolters, 'De beveiliging van persoonsgegevens. Een geharmoniseerde verplichting of een gedeelde verantwoordelijkheid?', *SEW* 2017/4, p. 144-157.

107 Artikel 4 lid 2 Richtlijn 2002/58/EG.

108 Duitsland kent een dergelijk meldplicht sinds 2009 (artikel 42a BDSG). Zie ook B. Custers (red.) 2017.

109 Zie ook B. Nieuwesteeg 2016.

110 Artikel 4 onder 1 AVG. Toch somt ook de AVG voorbeelden op van identificatoren. Dit wordt echter gekoppeld aan het begrip 'identificeerbaar', niet aan het begrip persoonsgegeven zelf.

111 Onder 'verlies' dient bovendien ook de tijdelijke niet-beschikbaarheid van persoonsgegevens te worden verstaan, zie Article 29 Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679', *18/EN WP250rev01*, p. 7.

112 *Ibid*, p. 22-23. Een dergelijke risico-inventarisatie wordt overigens ook in de HIPAA genoemd, maar wordt daarbij niet gekoppeld aan de vraag of de inbreuk dient te worden gemeld, maar of überhaupt van een inbreuk sprake is. Indien het bedrijf aan de hand van een risico-inventarisatie kan aantonen dat het onwaarschijnlijk is dat de gegevens in gevaar zijn (geweest), is van een inbreuk geen sprake – en dus ook niet van een meldplicht. Zie 45 CFR, § 164.402(2).

113 Vergelijk artikel 32 lid 1 onder a en 33 AVG.

114 Artikel 33 AVG resp. artikel 34 AVG.

115 De andere door de AVG voorgeschreven verplichtingen kunnen hierbij van belang zijn, bijvoorbeeld het verwerkingsregister (artikel 30 AVG) en het beveiligingsbeleid (artikel 30 lid 1 onder g AVG).

De termijn in de Amerikaanse regelgeving verschilt; vrijwel alle staten hanteren uitgangspunten als 'zo snel mogelijk' en 'zonder onredelijke vertraging', maar de uiteindelijke deadlines variëren van dertig, vijfenveertig, zestig tot zelfs negentig dagen.[116] De gemiddelde termijn waarbinnen wordt gemeld, is veertig dagen.[117] De noodzaak om snel te melden is voor Amerikaanse organisaties dus niet zozeer gelegen in compliance, maar in beperking van de eigen reputatieschade en het voorkomen van claims.

Een ander groot verschil tussen de meldplichten in de VS en in Europa is de geadresseerde: waar in de VS de betrokkenen *altijd* moeten worden geïnformeerd en de overheid (de *Attorney General*) eerder niet dan wel, wordt in Europa de melding *op de eerste plaats* aan de overheid (de toezichthoudende autoriteit) gedaan en slechts onder omstandigheden aan de betrokkenen. Een ander verschil is gelegen in aanvullende verplichtingen, zoals het onder omstandigheden verplicht gratis aanbieden van schadebeperkende diensten.[118] In de AVG zijn dergelijke verplichtingen niet opgenomen.

Een verklaring voor deze verschillen kan worden gezocht in het doel van de meldplicht. De Amerikaanse meldplichten lijken zich niet zozeer te richten op bescherming van fundamentele rechten, maar meer op de rechten van 'de consument': voorkoming van financiële schade en (identiteits)fraude.[119] De Europese meldplicht beoogt ook dit soort schade voor natuurlijke personen te voorkomen,[120] maar dit lijkt niet het enige doel te zijn. De Artikel 29-Werkgroep[121] schrijft:

> "The focus of any breach response plan should be on protecting individuals and their personal data. Consequently, breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data."[122]

Hieruit kan worden afgeleid dat het doel van de meldplicht uiteindelijk de bescherming is van natuurlijke personen tegen de aantasting van een fundamenteel recht. De meldplicht waarborgt dus het overkoepelende doel van de AVG.

116 Florida resp. New Mexico, Ohio, Rhode Island, Tennessee, Vermont, Washington en Wisconson, resp. Delaware (vgl. ook HIPAA) resp. Connecticut.

117 K. Harris, 'California data breach report 2012-2015', *California Department of Justice* februari 2016, p. 25 (te raadplegen via https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf).

118 Zie bijvoorbeeld de Breach Notification Law van Connecticut: S.B. 949, sec. 36a-701b(2)(b).

119 Dit blijkt ook uit de wetsgeschiedenis bij de Californische breach notification law: "*to help consumers protect their financial security by requiring that state agencies and businesses* […] *to quickly disclose to consumers any breach of the security of the system, if the information disclosed could be used to commit identity theft.*" (SB1386). Zie ook S. Romanosky, 'Do data breach disclosure law reduce identity theft?', *Journal of policy analyses and management* 2011/30-2, p. 256-286.

120 Overweging 85 AVG.

121 Het onafhankelijke advies -en overlegorgaan van Europese privacytoezichthouders.

122 Article 29 Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679', 18/EN WP250rev01, p. 5.

4.2.2 *Boetes en aansprakelijkheid*

Overtreding van de voorschriften van de AVG kan leiden tot een door de toezichthoudende autoriteit opgelegde boete (artikel 83 AVG).[123] Deze boete kan oplopen tot € 20 miljoen of 4% van de wereldwijde jaaromzet indien dat bedrag hoger is (artikel 83 lid 5 AVG). De boete moet doeltreffend, evenredig en afschrikwekkend zijn en kan worden gecombineerd met corrigerende maatregelen (artikel 83 lid 1-2 AVG jo. artikel 58 lid 2 AVG). Voorbeelden daarvan zijn het opleggen van een verwerkingsbeperking (waaronder een verwerkingsverbod), het gelasten van de verwerkingsverantwoordelijke tot het rectificeren of wissen van persoonsgegevens en het intrekken van certificeringen (artikel 58 lid 2 onder f-h AVG).

In vergelijking met de maximale boetebedragen in bijvoorbeeld de HIPAA (anderhalf miljoen dollar) zijn de maximale boetes in Europa hoog. Dit betekent echter niet dat de Europese toezichthouders ook echt meer of hogere boetes dan hun Amerikaanse collega's zullen gaan opleggen. In geen enkel land ter wereld wordt zoveel geprocedeerd en worden er zo veel boetes uitgedeeld (dan wel schikkingen getroffen) ten aanzien van overtredingen van privacyregelgeving als in de VS.[124]

Naast het opleggen van boetes voorziet de AVG in een mogelijkheid voor betrokkenen om op basis van de AVG een vordering tot schadevergoeding in te dienen (artikel 82 AVG), bijvoorbeeld wegens het schenden van de beveiligingsverplichting (artikel 32 AVG). In de VS wordt regelmatig geprocedeerd over het verkrijgen van schadevergoeding wegens overtredingen van de privacyregelgeving, met name in het geval van datalekken.[125] Daarbij wordt vaak op verschillende grondslagen een beroep gedaan: overtreding van federale wetten (FCRA), statelijke meldplichten voor datalekken en onrechtmatige daad.[126]

In de civiele *class actions* die in de VS worden gevoerd, hebben de benadeelden evenwel regelmatig grote moeite om aan te tonen dat zij ontvankelijk zijn in hun vordering ('*standing*'). Het blijkt bij datalekken moeilijk om aan te tonen dat er daadwerkelijk sprake is van schade ('*injury in fact*'). In de zaak *Spokeo/Robins* oordeelde het U.S. Supreme Court dat de enkele overtreding van regelgeving niet voldoende was voor *standing*, tenzij de benadeelde kon aantonen dat hij ook schade had geleden die '*particularized*' en '*concrete*' was.[127] De jurisprudentie na *Spokeo* is evenwel wisselend.[128]

123 *Ibid.*

124 A. Raul, 'United States', in: A. Raul (ed.), *The privacy data protection and cybersecurity law review*, London: Law Business Research Ltd. 2014, p. 292.

125 In 2017 vonden er bijvoorbeeld al 76 class actions plaats, zie D. Zetoony e.a., '2017 Data breach litigation report', *Bryan Cave* 2017, te raadplegen op www.bryancave.com/en/thought-leadership/2017-data-breach-litigation-report.html (laatst bezocht 6 juli 2018).

126 '*Negligence*'.

127 U.S. S.C. 13.1339, 136 S. Ct. 1540 (24 mei 2016). "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical'."

128 663 Fed. Appx. 384 (6th Cir. 2016), 12 september 2016, *Galaria/Nationwide*; 846 F3d 625 (3d Cir. 2016), 12 juli 2016 (*In re: Horizon Healthcare Services Breach Notification*) resp. 819 F3d 963 (7th Cir. 2016; *Chang's China Bistro*); In alle drie de zaken werd *standing* aangenomen. Anders: 848 F3d 252 (4th Circ. 2017; *Beck/Mcdonald*).

Ook onder de Europese regelgeving is niet direct helder of de schade die betrokkenen kunnen oplopen na een inbreuk op de AVG wel daadwerkelijk vergoedbaar is.[129] Dat er op het punt van de schade nog de nodige vragen openstaan, neemt evenwel niet weg dat de AVG aan benadeelde betrokkenen wel de expliciete mogelijkheid biedt om gerechtelijke procedures te starten (zie ook artikel 79 AVG), met alle (verdedigings)kosten voor de aangesproken partij van dien. De enkele dreiging van procedures, administratief wegens opgelegde boetes of civiel wegens gestelde aansprakelijkheid, kan dus zeer wel een reden zijn voor bedrijven om zich hiertegen te verzekeren.

4.3 *Tussenconclusie*

Er bestaan grote verschillen in de inhoud, het toepassingsbereik en de achterliggende conceptuele benadering en ratio van de privacyregelgeving in de VS en in Europa. Toch kan met de introductie van de AVG in grote lijnen een trend worden waargenomen die meer neigt naar de Amerikaanse systematiek: meer nadruk op compliance, meldplichten en forse handhavingsbevoegdheden. Met vergelijkbare middelen lijkt in Europa echter een ander doel te worden nagestreefd: bescherming van fundamentele rechten van individuen tegenover bescherming van financiële belangen en posities van consumenten.

5. De cyberpolis in het licht van de Europese privacy- en dataprotectie regelgeving

In Europa wordt de cyberpolis slechts door een select groepje verzekeraars aangeboden.[130] De analyse van de in Europa aangeboden cyberverzekeringen is voor dit artikel beperkt tot de polissen die thans in Nederland openbaar voorhanden zijn.[131] Er is gekozen voor bestudering van de algemene polisvoorwaarden. De specifieke verzekeringsbehoefte is uiteindelijk voor ieder bedrijf anders. Verzekeraars houden daar bijvoorbeeld met aanvullende clausules op het polisblad rekening mee. Omdat dit maatwerk betreft, zijn deze clausules in dit onderzoek niet meegenomen.[132]

De getoetste onderdelen zijn ingekaderd naar de hiervoor benoemde drijfveren: compliance en kosten rondom (de meldplicht) datalekken, boetes en aansprakelijkheid.

5.1 *Compliance en kosten rondom de meldplicht datalekken*

Compliance en verantwoording zijn belangrijke thema's in de AVG. Vertaald naar verzekeringsdekking is dit element met name te zien rondom de meldplicht datalekken. Een voorbeeld daarvan is het feit dat alle getoetste polissen voorzien in *incident response services.* Daarmee kan de aangeboden dekking voor de verwerkingsverantwoordelijke een middel vormen om in geval van een datalek aan de AVG te voldoen.

Verzekerden kunnen aanspraak maken op crisismanagement,[133] juridische ondersteuning bij de beoordeling of de inbreuk meldingplichtig is,[134] of juist voor de communicatie met de overheid.[135] De technische ondersteuning kan bestaan uit forensische of IT-diensten die de oorzaak van de inbreuk vaststellen[136] of herstelwerkzaamheden uitvoeren.[137] Verder bieden alle getoetste polissen dekking voor het opzetten van een callcenter om betrokkenen van informatie te voorzien, al is daar in een enkele polis voorafgaande toestemming van de verzekeraar voor nodig.[138]

Dekking voor deze diensten is met het oog op de 72-uurstermijn uit de AVG in Europa wellicht nog wenselijker dan in de VS. De verzekerde kan gebruikmaken van het netwerk van specialisten van de verzekeraar, wat een grote tijdbesparing kan opleveren. Het wordt daarmee voor hem een stuk beheersbaarder om te voldoen aan de eisen van de AVG rondom het melden van datalekken.

Het merendeel van de onderzochte polissen noemt bij *incident response services* ook diensten zoals (krediet)monitoring.[139] De polissen definiëren dit begrip niet. De AVG kent geen wettelijke verplichting voor verwerkingsverantwoordelijken om deze dienst aan de betrokkenen aan te bieden. De vraag is dan ook hoe dergelijke clausules in het licht van de Europese regelgeving dienen te worden uitgelegd; wanneer is kredietmonitoring bijvoorbeeld 'noodzakelijk', zoals in een aantal polissen als voorwaarde is opgenomen?[140] Is dit in Europa bovendien wel een uitvoerbare en effectieve dienst, waar kredietbureaus veel minder gebruikelijk zijn dan in de VS? Bij gebrek aan een wettelijke verplichting die

129 T.F. Walree, 'De vergoedbare schade bij de onrechtmatige verwerking van persoonsgegevens', *WPNR* 2017/7172, p. 921-930. Zie ook T. Tjong Tjin Tai, 'Een Europees schadebegrip?', *NTBR* 2018/5, p. 31-36.

130 OECD 2017, p. 61.

131 Dat wil zeggen: op internet te raadplegen zonder daarvoor een aanvraag te hoeven doen. De bestudeerde polissen zijn van Chubb/ACE (Cyber 2016), AIG (CyberEdge 01/2017), CNA Hardy (TCNB1115 NetProtect Cyberverzekering) en Hiscox (Cyber en Data Risks by Hiscox 2017/01). De polissen van Allianz, Catlin XL, Delta Lloyd en HDI Gerling zijn niet openbaar beschikbaar. De verzekering van De Goudse is vanwege de nieuwe opzet ('verzekeren zonder polisvoorwaarden') niet in het onderzoek betrokken.

132 In dergelijke clausules kunnen bijvoorbeeld wachttijden bij bedrijfsschade worden aangepast.

133 Hiscox artikel 2.1.2 onder 4, Chubb/Ace artikel 2.5(D)(6), AIG artikel 1.2.1(iii). CNA noemt dit niet in de polis.

134 "*Juridische kosten voor het melden van een inbreuk, nodig om toepasselijke meldingsverplichtingen vast te stellen* […]" (Hiscox, artikel 2.1.2 onder 2); zie in algemenere zin AIG, artikel 1.2.2. "[…] *Response Adviseur voor het verlenen van juridisch advies*."

135 Chubb/Ace artikel 2.5(C): "[…] *een juridisch adviseur* […] *die de communicatie met een overheidsorgaan ter hand kan nemen teneinde de noodzakelijke maatregelen te bepalen* […] *zodat voldaan wordt aan de toepasselijke Privacyregelgeving*."

136 Hiscox artikel 2.1.2, Chubb/Ace artikel 2.5(A) en in algemene zin AIG artikel 1.2.3.

137 CNA rubriek 1 sub 1: "[…] *kosten forensisch onderzoek opgelopen door de verzekerde bij het herstel* […]."

138 Hiscox artikel 2.1.2 (toestemming vereist), AIG artikel 1.2.6, Chubb/Ace artikel 2.5(D)(2) (toestemming vereist), CNA rubriek 1 sub 7.

139 Hiscox artikel 2.1.2 onder 3, Chubb/Ace artikel 2.5(D)(4), AIG artikel 1.2.7, CNA rubriek 1 sub 7(a).

140 AIG: "*De verzekeraar dekt de redelijke en noodzakelijke vergoedingen, kosten en uitgaven voor monitoringsdiensten* […]."

een dergelijke dienst voorschrijft,[141] ligt de noodzaak (dan wel het effect) van het verlenen van een dergelijke dienst eerder in de beperking van de eigen (reputatie)schade van de verzekerde, dan in compliance. Overigens lijkt kredietmonitoring ook als beperking van reputatieschade eerder een Amerikaans dan een Europees fenomeen.[142] Vooralsnog zie ik in dit aspect van de dekking geen directe aansluiting op een uit de AVG voortvloeiende behoefte.

De in Nederland aangeboden polissen bieden net als de polissen in de VS dekking voor notificatiekosten.[143] De waarde die aan deze dekking in Europa zal worden gehecht – en daarmee de vraag of dit voor Europese bedrijven een reden vormt om een cyberverzekering af te sluiten – kan echter van de VS verschillen door het *one-stop-shop* beginsel uit de AVG: er dient te worden gemeld aan één instantie, de toezichthouder. De drempel om ook aan de betrokkenen te melden, ligt hoger en kent verschillende uitzonderingen (bijvoorbeeld als individuele notificatie onevenredige inspanningen zou vergen).[144] In de VS is dit juist andersom: het uitgangspunt is dat melding altijd aan alle betrokkenen wordt gedaan, niet zozeer aan de toezichthoudende autoriteit. Daar komt bij dat er in de Amerikaanse regelgeving, anders dan onder de AVG, geen verdere toetsingsdrempel voor de meldingsplichtigheid van de inbreuk bestaat. Er zal dus sneller moeten worden gemeld aan (veel) meer geadresseerden dan in Europa. De daaraan verbonden kosten zullen in de VS dus hoger zijn dan in Europa.[145] Dat notificatiekosten in de VS een grotere drijfveer vormen voor het afsluiten van verzekeringsdekking dan in Europa is derhalve aannemelijk.

Andere aspecten van compliance, bijvoorbeeld preventieve maatregelen zoals beveiliging, vergen op de eerste plaats een investering van verzekeringnemers zelf. Toch lijkt er net als in de VS ook in Europa een groeimogelijkheid te bestaan in dekking voor zogenoemde *pre-breach services*. Verzekeraars kunnen verzekerden helpen om reeds in de acceptatiefase de beveiliging tegen datalekken op een hoger niveau te brengen, adequate *response* plannen op te stellen en organisatorische maatregelen te treffen, zoals training van het personeel. Indien (een deel van) deze kosten door de verzekeraar wordt vergoed of anderszins in de premie wordt verdisconteerd, dan lijkt dat een aantrekkelijke reden voor organisaties om zich te verzekeren.

5.2 *Boetes*

De AVG blijkt voor veel bedrijven een moeilijk te begrijpen wet, hetgeen onzekerheid en onrust veroorzaakt.[146] Dat de AVG hoge boetes kent, is voor veel bedrijven echter wel heel duidelijk. In het kader van risicomanagement zou een verzekering een oplossing kunnen bieden.

Waar in Amerikaanse cyberpolissen de boete een veelvoorkomende uitsluiting is, valt de handhavingsboete die de toezichthouder (in Nederland de Autoriteit Persoonsgegevens) kan opleggen veelal wel onder de dekking van de in Nederland aangeboden cyberverzekeringen.[147] Sporen van die Amerikaanse uitsluitingen zijn ook terug te zien in de in Nederland aangeboden polissen. Zo is in meerdere polissen opgenomen dat van dekking is uitgesloten 'regulerende boetes' of 'regelgevingsboetes',[148] terwijl de eventuele boete van de AP wel is gedekt.

Ondanks dat het vooralsnog de vraag blijft hoe vaak deze boetes werkelijk zullen worden opgelegd en dus hoe reëel de dreiging daarvan is[149] en of boetes in het licht van artikel 3:40 BW wel verzekerbaar zijn, sluit deze dekking thans goed aan op een behoefte die de AVG creëert.

5.3 *Aansprakelijkheid*

Alle bestudeerde polissen bevatten bepalingen ten aanzien van aansprakelijkheid. In een aantal polissen wordt onderscheid gemaakt tussen privacyaansprakelijkheid, cyber/media-aansprakelijkheid en aansprakelijkheid wegens onvoldoende netwerkbeveiliging.[150] In een enkele polis wordt onderscheid gemaakt tussen schade bij een privacygerelateerde onrechtmatige daad, die wordt beperkt tot personenschade, en schade voortvloeiend uit een privacyclaim.[151] In de meeste polissen wordt evenwel een algemeen schadebegrip gebruikt ('schade voortvloeiend uit een gedekte aanspraak').[152] Alle polissen bieden dekking voor de kosten van verweer, zowel tegen aansprakelijkheidsclaims als tegen een boetebesluit door de Autoriteit Persoonsgegevens.

141 Dit kan wellicht worden ingelezen in artikel 33 lid 2 onder d AVG als schadebeperkende maatregel.

142 Zie in dit kader Betterley 2017, p. 9. Over de zin en onzin van kredietmonitoring wordt nog gediscussieerd: P. Kemp, 'Credit monitoring services can mitigate effect of data breach, says expert', Out-Law.com, 17 februari 2017, te raadplegen op www.out-law.com/en/articles/2017/february/credit-monitoring-services-can-mitigate-effect-of-data-breach-says-expert/, Dit bericht wordt tegengesproken door K. Kulp, 'Credit monitoring services may not be worth the costs', *CNBC* 30 november 2017, te raadplegen op www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html. Beide websites laatst bezocht op 9 maart 2018.

143 Kosten die gepaard gaan met het maken van de melding van het datalek.

144 Artikel 34 lid 3 onder c AVG.

145 Dat de notificatiekosten in de VS verreweg het hoogst zijn, blijkt ook uit de jaarlijkse bevindingen van het Ponemon Institute. Zie Ponemon Research Report, '2017 Cost of Data Breach Study: global overview', The Ponemon Institute 2017.

146 Zie bijvoorbeeld N. Trappenburg, 'Nieuwe privacyregels hele kluif voor bedrijven', en 'Bedrijven weten iets over privacywet, maar zijn er niet klaar voor', beide *Het Financieele Dagblad* 7 maart 2018.

147 Altijd onder bijkomende voorwaarde dit wettelijk gezien verzekerbaar is, bijvoorbeeld in het licht van artikel 3:40 BW. Hiscox artikel 1.1.5, AIG artikel 1.3, Chubb/Ace artikel 1.2(A)(iv) jo 2.34. CNA noemt de boete niet.

148 Hiscox artikel 3.1 resp. Chubb/Ace artikel 2.34. Het verdient de opmerking dat dit bij werelddekking een bewuste uitsluiting kan zijn om op die wijze claims uit de VS uit te sluiten.

149 Volgens de Minister van Rechtsbescherming zal de AP zich zeker in het begin vooral richten op voorlichting, zie N. Trappenburg, 'Dekker: privacytoezichthouder gaat niet onmiddellijk boetes opleggen', *Het Financieele Dagblad* 9 maart 2018, p. 9. Uit het rapport van Andersson Elffers Felix (uitgevoerd in opdracht van de AP) uit 2017 volgt ook dat de AP veel meer personeel zal moeten aannemen om de taken adequaat te kunnen uitvoeren. Zie Andersonn Elffers Felix, 'Organisatorische vertaling Verordening & Richtlijn gegevensbescherming', eindrapportage 27 maart 2017.

150 Hiscox en Chubb/Ace.

151 Chubb/Ace artikel 1.1(C).

152 Bijvoorbeeld AIG en Hiscox.

Hiervoor is reeds uiteengezet dat het vooralsnog onduidelijk is of en in hoeverre de slachtoffers van een datalek daadwerkelijk in staat zijn om hun schade met een beroep op (schending van) de AVG vergoed te krijgen. Bovendien ontbreekt in de meeste landen in Europa, waaronder Nederland, vooralsnog de mogelijkheid om via een *class action* schadevergoedingen te claimen, zoals dat in de VS wel mogelijk is.[153] Daarin is evenwel een veranderende trend te zien. Zo biedt artikel 80 AVG de mogelijkheid om een orgaan of vereniging als vertegenwoordiger aan te wijzen om het recht op schadevergoeding in de zin van artikel 82 AVG uit te oefenen. In steeds meer lidstaten worden wetten voorgesteld en aangenomen waarin *class actions* op beperkte wijze mogelijk worden gemaakt.[154] In Nederland is al enige tijd een wetsvoorstel aanhangig waarmee een collectieve schadevergoedingsactie in het leven wordt geroepen.[155] Dit voorstel is echter nog niet aangenomen.

Ondanks deze trend zijn de procedurele mogelijkheden om schade te verhalen in Europa beperkter dan in de VS. De druk om te schikken, zoals in de VS veelvuldig gebeurt ('*sue-and-settle*'),[156] is daarom wellicht ook minder groot.[157] Dit neemt echter niet weg dat ook individuele aansprakelijkheidsclaims tot (kostbare) procedures en uiteindelijk een potentieel grote schade kunnen leiden. Een toename van dergelijke claims onder de AVG is, mede gezien de nadruk op de rechten van betrokkenen, bovendien te verwachten. De dekking die de thans in Nederland aangeboden cyberverzekeringen op dit punt bieden, sluit dus op zich aan bij de Europese regelgeving. Nu in Europa echter de druk van massaclaims voorlopig zal uitblijven, valt vanuit juridisch oogpunt te betwijfelen of de AVG een zodanig aansprakelijkheidsrisico creëert dat dit leidt tot een significant grotere belangstelling voor cyberverzekeringen.

6. Conclusie

Het sluiten van een cyberverzekering blijft in Europa achter ten opzichte van de VS. De verwachting is dat de AVG daarin verandering zal brengen. In deze studie heb ik onderzocht of deze verwachting gezien de inhoud van de AVG terecht is.

De vraag naar de cyberverzekering in de VS wordt grotendeels gedreven door zeer specifieke privacyregelgeving, waarin een grote nadruk ligt op het voldoen aan die regelgeving (compliance), meldplichten na datalekken en grote schades door boetes en aansprakelijkheid. Dit creëert een verzekeringsbehoefte waar de cyberverzekering op aansluit, bijvoorbeeld door dekking te verlenen voor aansprakelijkheid, kosten van verweer en kosten rondom datalekken, zoals notificatiekosten.

In de AVG is in grote lijnen een beweging naar het Amerikaanse model te zien. De AVG roept daarmee deels dezelfde behoefte aan specifieke verzekeringsdekking op. De in Nederland aangeboden cyberverzekeringen sluiten daar in beginsel goed op aan. Er bestaat echter een aantal nuanceverschillen, met name rondom (het melden van) datalekken.

In de fase voorafgaand aan een datalek dwingt de AVG door het *accountability*-beginsel tot aantoonbare compliance. Zowel in de VS als in Europa bestaat er op dit punt een groeimogelijkheid voor cyberverzekeraars, door ondersteuning te bieden door middel van *pre-breach services.*

Indien sprake is van een datalek, schrijft de AVG een risicoanalyse voor die de onderneming in zeer korte tijd dient uit te voeren. Niet ieder datalek hoeft immers te worden gemeld. Cyberverzekeringen bieden hierin ondersteuning door middel van *incident response services*. Met het oog op compliance kunnen deze diensten voor verzekeringnemers zeer waardevol zijn. De verzekeringsbehoefte in de VS is op dit punt niet zozeer gelegen in compliance met de regelgeving, maar in beperking van de eigen (reputatie)schade. De Amerikaanse verzekeringnemer heeft daarin dus een keuze die de Europese verzekeringnemer niet heeft. Doordat in de VS bovendien geen meldingsdrempel bestaat en altijd aan alle betrokkenen moet worden gemeld in plaats van enkel aan de toezichthoudende autoriteit, heeft de Amerikaanse verzekeringnemer vanuit compliance meer behoefte aan vergoeding van notificatiekosten. De Europese verzekeringnemer zal meer waarde hechten aan een snelle *incident response*.

De gevolgen van een datalek kunnen bestaan uit aansprakelijkheidsclaims van derden en boetes van handhavende instanties. Door de nadruk op *accountability*, meer verplichtingen en een sterkere positie van betrokkenen valt onder de AVG een stijging van het aantal aansprakelijkheidsclaims te verwachten. Of dit daadwerkelijk tot schadevergoeding zal leiden, is de vraag. Cyberverzekeringen bieden dekking voor deze claims en kosten van verweer. Door de afwezigheid van een mogelijkheid tot een *class action* is de kans dat verzekeringnemers met dezelfde massaclaims zullen worden geconfronteerd als organisaties in de VS echter minder groot.

De dekking die op dit moment in Nederland voor boetes wordt geboden, is waardevol. Deze dekking ontbreekt vaak in Amerikaanse polissen. De kans dat deze boetes in Nederland daadwerkelijk zullen worden opgelegd – zeker in de orde van grootte waarin dit in de VS gebeurt – lijkt vooralsnog echter minder reëel.

153 In Nederland kan, indien aan de vereisten wordt voldaan, met een collectieve actie slechts een verbod, gebod, of verklaring voor recht worden gevorderd (artikel 3:305a BW). Daarnaast kan via de Wet collectieve afwikkeling massaschade (artikel 7:907-910 BW en artikel 1013-1018 Rv) een getroffen schikking voor alle gedupeerden (tenzij gebruik is gemaakt van de *opt-out* mogelijkheid) verbindend worden verklaard.

154 Bijvoorbeeld Frankrijk en Duitsland sinds 2016 en België sinds 2014. Zie ook W. Sapranov, 'Class consciousness: class action arbitration under U.S. and EU privacy laws', *Yearbook on International Arbitration* 2017/5, p. 83-92.

155 *Kamerstukken II* 2016/17, 34608, 2.

156 Vgl. Romanosky e.a 2014, p. 74-76.

157 Het gebrek aan bijvoorbeeld *punative damages* in Europa maakt bovendien de schadebedragen minder hoog.

Gezien al het voorgaande sluit ik zeker niet uit dat de AVG inderdaad een stijging in de vraag naar cyberverzekeringen in Europa zal veroorzaken. Er bestaan echter cruciale verschillen in de Amerikaanse en Europese privacyregelgeving die maken dat de behoefte van de Europese verzekeringnemer niet dezelfde zal zijn als die van de Amerikaanse. Het verschil in benadering van gegevensbescherming speelt daarbij een grote rol: bescherming van consumentenrechten tegenover bescherming van individuen tegen schendingen van een fundamenteel recht. Voor cyberverzekeraars op de Europese markt valt dan ook nog winst te behalen door beter op deze verschillen in te spelen.