Consument en cybersecurity

Verbruggen, Paul; Wolters, P.T.J.

Published in:
Tijdschrift voor consumentenrecht & handelspraktijken

Publication date:
2017

Document Version
Publisher's PDF, also known as Version of record

Mr. dr. P.W.J. Verbruggen en mr. dr. P.T.J. Wolters***

Consument en cybersecurity

Een agenda voor Europese harmonisatie van zorgplichten

Cybersecurity – de beschikbaarheid, integriteit en vertrouwelijkheid van ICT-toepassingen – is van groot belang voor onze maatschappij. In deze bijdrage wordt onderzocht of en in hoeverre Europese harmonisatie van civielrechtelijke zorgplichten voor cybersecurity van ICT-toepassingen aangeboden aan consumenten wenselijk is. Mede gelet op het grensoverschrijdende karakter van de ICT-sector en de thans bestaande onduidelijkheid over de invulling van zorgplichten op dit terrein, wordt betoogd dat het wenselijk is om op deelterreinen van het consumentenrecht via wetgeving en jurisprudentie helderheid en uniformiteit te creëren over het bestaan en de omvang van dergelijke zorgplichten. De bijdrage schetst de mogelijkheden die daartoe bestaan ten aanzien van open normen geldend voor precontractuele informatieplichten, conformiteit bij consumentenkoop en productaansprakelijkheid.

1. Inleiding

Informatie- en communicatietechnologie (ICT) vormt een belangrijke pijler van onze samenleving. Zij biedt mogelijkheden tot marktinnovatie door bedrijven, tot het inspelen op snel veranderende consumentenbehoeften en tot het aanpakken van maatschappelijke problemen.[1]
De voorname economische en maatschappelijke functie die op ICT gebaseerde goederen of diensten (zoals informatiesystemen, infrastructuren, netwerken, hardware, firmware, software en digitale inhoud) thans hebben, leidt echter ook tot een toename van de risico's en kosten die gemoeid zijn met het misbruik, de verstoring of de uitval van ICT.[2] Dit maakt duidelijk dat de beschikbaarheid, integriteit en vertrouwelijkheid van ICT-toepassingen – hier aangeduid onder het overkoepelende begrip *cybersecurity* – van groot belang zijn.[3]
De vraag is echter waartoe consumenten gerechtigd zijn als blijkt dat de cybersecurity van de door hen aangeschafte ICT-toepassingen tekortschiet.[4] De beantwoording van deze vraag vereist een analyse van diverse open normen in het consumentenrecht, het algemene verbintenissenrecht en het persoonsgegevensrecht. Rechtspraak over de invulling van deze normen in het kader van cybersecurity is tot nu toe spaarzaam.[5] Dit leidt tot rechtsonzekerheid. Gecombineerd met onder meer de verregaande exoneratieclausules die aanbieders van ICT-toepassingen (onder andere verkopers, producenten, dienstverleners, softwareontwikkelaars) plegen te hanteren en de complexe en ondoorzichtige ketens en netwerken waarbinnen deze toepassingen worden aangeboden, maakt deze onzekerheid dat consumenten de kosten van cyber*in*security veelal zelf dragen.[6]
De ICT-sector is in sterke mate geïnternationaliseerd en wordt gekenmerkt door marktleiders die wereldwijd actief zijn.[7] Gelet op dit grensoverschrijdende karakter kunnen nationale initiatieven om rechtszekerheid te scheppen over de reikwijdte van zorgplichten voor cybersecurity slechts gedeeltelijk een oplossing bieden. Een nationale aanpak zal immers tot fragmentatie van regelgeving leiden indien deze niet strak gecoördineerd wordt. Dit doet de vraag rijzen of en in hoeverre Europese harmonisatie van zorgplichten voor de beschikbaarheid, integriteit en vertrouwelijkheid van ICT-toepassingen aangeboden aan consumenten wenselijk is.
Beantwoording van deze vraag stond centraal in het rapport *Towards Harmonised Duties of Care and Diligence in Cybersecurity*, opgesteld in opdracht van de Cyber Security Raad in het kader van het Nederlandse voorzitterschap van de Europese Unie (EU) in de eerste helft

* Universitair docent Privaatrecht, Tilburg University en redacteur van dit tijdschrift
** Universitair docent Burgerlijk Recht en onderzoeker bij het Onderzoekcentrum Onderneming & Recht van de Radboud Universiteit

1. Voorbeelden zijn onlineplatforms voor de deeleconomie (Airbnb, Uber), consumentenproducten geschakeld aan het internet (smartphones, auto's, slimme thermostaten), persoonlijke gezondheidapps (MyFitnessPal, Runkeeper en Strava) en het gebruik van 'big data' in het kader van maatschappelijke thema's zoals criminaliteitsbestrijding, natuurrampen en vergrijzing.
2. De kosten van cybersecurityincidenten zoals Distributed Denial-of-Service-aanvallen (DDoS-aanvallen), datalekken, botnets, phishing of besmettingen met malware of ransomware zijn omvangrijk. De opbrengst van ransomware wordt bijvoorbeeld tussen de € 2770 en € 83 000 per dag geschat. Zie *Cybersecuritybeeld Nederland*, Den Haag: Nationaal Cyber Security Centrum 2014, p. 85, www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-4.html. Zie in het algemeen over de becijfering van de kosten van cybersecurityincidenten: R. Anderson e.a., 'Measuring the costs of Cybercrime', in: R. Böhme (red.), *The Economics of Information Security and Privacy*, Berlijn: Springer 2013, p. 265-300.
3. Hiermee sluiten wij aan bij de door de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) gebruikte definitie. Deze omschrijft cybersecurity als 'het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan. De schade kan bestaan uit: aantasting van de betrouwbaarheid van ICT, beperking van de beschikbaarheid en schending van de vertrouwelijkheid en/of de integriteit van in ICT opgeslagen informatie.' *Nationale Cybersecurity Strategie 2. Van bewust naar bekwaam*, Den Haag: NCTV 2013, p. 13, www.ncsc.nl/organisatie/nationale+cybersecurity+strategie.
4. Zie over deze vraag reeds P.W.J. Verbruggen, 'Consumentenrecht en cybersecurity' (redactioneel), *TvC* 2016, afl. 3, p. 97-98.
5. Uitzonderingen in Nederland vormen de recente uitspraken van Rb. Amsterdam (vzr.) 8 maart 2016, ECLI:NL:RBAMS:2016:1175 (*Consumentenbond/Samsung*) en Rb. Midden-Nederland 30 maart 2016, C/16/344721 / HA ZA 13-387 (*Politie/Movit IT Masters*). Zie uitgebreid: P.T.J. Wolters & P.W.J. Verbruggen, 'De verplichting tot het bijwerken van onveilige software', *WPNR* 2016, afl. 7123 (hierna: Wolters & Verbruggen 2016), p. 832-839.
6. Zie in meer detail paragraaf 2.
7. Forbes, 'World's largest tech companies', www.forbes.com/pictures/fi45ejkeig/1-apple/#2ec85b9810fe.

van 2016.[8] Deze bijdrage vormt een weerslag van de in dit rapport gesignaleerde problematiek en oplossingsrichtingen. Zij beantwoordt de normatieve vraag naar de wenselijkheid van Europese harmonisatie op dit terrein en beziet in dat kader in hoeverre bestaande regelgeving bescherming biedt aan consumenten (par. 2 en 3). Vervolgens identificeert zij een drietal deelterreinen voor Europese harmonisatie ter verbetering van de rechtspositie van de consument (par. 4). Ter beantwoording van deze vragen wordt het geldende Europese en Nederlandse privaatrecht, meer in het bijzonder het consumentenrecht, kritisch geanalyseerd. Tevens wordt acht geslagen op de aanstaande hervormingen binnen het Europese persoonsgegevensrecht, te weten de Algemene verordening gegevensbescherming,[9] en de recente richtlijnvoorstellen van de Europese Commissie betreffende de levering van digitale inhoud en inzake online en op afstand verkoop van zaken.[10] De selectie van de te bespreken deelterreinen voor harmonisatie is tot stand gekomen op basis van een analyse van de bestaande privaatrechtelijke regelgeving en haar toepassing in de praktijk. Zeer dienstbaar hiervoor waren twee groepsdiscussies met vertegenwoordigers van de vraag- en aanbodzijde van de Nederlandse ICT-sector, overheidsinstanties, de Consumentenbond en onafhankelijke juridische dienstverleners op het gebied van ICT, die in het kader van de begeleiding van bovengenoemde rapportage werden georganiseerd.[11]

2. Probleemanalyse

De toenemende rol van ICT vergroot het belang van cybersecurity. De Europese Commissie onderstreept de betekenis van cybersecurity voor de economische groei in Europa in de *Digital Single Market*-strategie die zij in mei 2015 bekendmaakte.[12] In dit beleidsprogramma doet de Commissie voorstellen tot introductie van nieuwe wetgeving ter verbetering van de concurrentiepositie van de Europese digitale economie. Zij legt daarbij tevens de nadruk op het belang van de veiligheid van digitale dienstverlening en de verwerking van persoonsgegevens voor het vertrouwen van burgers in onlineactiviteiten en de digitale economie in het algemeen. Meer in het bijzonder stelt zij:

'Er zijn nog steeds bepaalde lacunes in de zich snel ontwikkelende sector van technologieën en oplossingen voor online netwerkbeveiliging. Er moet dan ook een samenhangender aanpak komen om de ontwikkeling van veiligere oplossingen door de EU-bedrijfstak te stimuleren en te zorgen dat bedrijven, overheden en burgers die ook toepassen.'[13]

2.1. Marktfalen

Tegenover deze ambitie van de Europese Commissie staat dat de markt voor cybersecurity in Europa op dit moment niet optimaal functioneert. Dit leidt tot een lager niveau van bescherming dan efficiënt is.[14] Een van de redenen hiervoor is gelegen in een gebrek aan capaciteit aan de vraagzijde van de retailmarkt. Consumenten en het MKB missen dikwijls informatie over en inzicht in het gerealiseerde niveau van cybersecurity, de relevante bedreigingen voor cybersecurity, de gevolgen van een incident en de mogelijke oplossingen. Zo bestaat er de neiging onder consumenten om zich enkel te richten op de prijs van op ICT gebaseerde goederen en diensten of helemaal geen beveiliging in te kopen.[15] Aanbieders kunnen ook geneigd zijn om een nieuwe toepassing als eerste in de markt te zetten, ongeacht het (lage) niveau van beveiliging dat zij bieden.[16] Het is in sommige gevallen bovendien efficiënter voor individuele aanbieders om kwetsbaarheden pas te dichten nadat de ICT-toepassing in de markt is gezet.[17] In deze gevallen treden er negatieve externe effecten op: de aanbieder neemt de negatieve gevolgen van zijn onveilige ICT-toepassingen voor gebruikers niet mee in de beslissing om te investeren in (betere) cybersecurity. Het gevolg is dat ICT-toepassingen met suboptimale beveiliging hun weg naar de markt vinden.

2.2. Rechtsonzekerheid

Bestaande regulering op het niveau van de lidstaten en de EU ondervangt deze vormen van marktfalen slechts gedeeltelijk en geeft zelfstandig te weinig prikkels aan de ICT-sector tot het investeren en verbeteren van cybersecurity. Dat houdt verband met een aantal elementen. Ten eerste bestaat er onduidelijkheid over het bestaan van een zorgplicht voor cybersecurity en de mate van bescher-

8. P.W.J. Verbruggen e.a., *Towards Harmonised Duties of Care and Diligence in Cybersecurity*, European Foresight Cyber Security Meeting 2016, Den Haag: Cyber Security Council 2016 (hierna: Verbruggen e.a. 2016), p. 78-108.
9. Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming), *PbEU* 2016, L 119/1.
10. Europese Commissie, Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud, COM(2015)634 final en Europese Commissie, Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende bepaalde aspecten van overeenkomsten voor de online-verkoop en andere verkoop op afstand van goederen, COM(2015)635 final.
11. Zie voor een overzicht van de betrokken stakeholders: Verbruggen e.a. 2016, p. 80.
12. Europese Commissie, Strategie voor een digitale eengemaakte markt voor Europa, COM(2015)192 final.
13. Ibid, p. 13.
14. *Risicorapportage Cyberveiligheid Economie* (CPB Notitie van 6 juli 2016), Den Haag: Centraal Planbureau 2016, p. 16, www.cpb.nl/sites/default/files/omnidownload/CPB-Notitie-6juli2016-Risicorapportage-cyberveiligheid-economie.pdf.
15. Ibid, p. 15-16.
16. Dit speelt in het bijzonder bij toepassingen waarvan de waarde afhankelijk is van de gebruikersbasis, zoals bijvoorbeeld social-media-platforms. Zie T. Moore & R. Anderson, *Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research*, Computer Science Group, Harvard University 2011, www.cl.cam.ac.uk/~rja14/Papers/moore-anderson-infoeconsurvey2011.pdf, p. 3 en E. Tjong Tjin Tai e.a., 'Duties of Care and Diligence against Cybercrime', report for the Dutch National Coordinator for Security and Counterterrorism (maart 2015), www.gccs2015.com/sites/default/files/documents/Bijlage%202%20-%20Duties%20of%20care%20and%20diligence%20against%20cybercrime%20(1).pdf (hierna: Tjong Tjin Tai e.a. 2015), p. 34 en 166.
17. A. Arora, J.P. Caulkins & R. Telang, 'Sell First, Fix Later: Impact of Patching on Software Quality', *Management Science* 2006, afl. 3, p. 465-471.

ming die op grond van een dergelijke plicht mag worden verwacht.[18] De invulling van die plicht zal aan de hand van open normen in het consumentenrecht, het algemene verbintenissenrecht en het persoonsgegevensrecht moeten geschieden. Zij is afhankelijk van de omstandigheden van het specifieke geval. In geval van een (consumenten)koop van een ICT-toepassing speelt de norm van 'conformiteit' een centrale rol. Hier is het met name de vraag welke cybersecurity de consument op grond van de koopovereenkomst alsmede het normale gebruik van de zaak mag verwachten. Bij buitencontractuele verhoudingen zal moeten worden bepaald of de aanbieder 'maatschappelijk onzorgvuldig' of 'oneerlijk' handelt in de zin van artikel 6:162 BW respectievelijk artikel 6:193b lid 2 BW als hij bijvoorbeeld een toepassing in de markt zet die kwetsbaar is voor een hack zonder consumenten daarover te informeren.[19] Voor zover de aanbieder persoonsgegevens verwerkt, legt artikel 13 Wet bescherming persoonsgegevens (Wbp) in dit verband de verplichting op tot het nemen van 'technische en organisatorische maatregelen' die een 'passend beveiligingsniveau' garanderen.[20]

Er bestaat weinig tot geen (gepubliceerde) rechtspraak over de vraag of deze open normen een zorgplicht voor ICT-aanbieders in het leven roepen en zo ja, welke omvang die zorgplicht heeft. Een in potentie zeer relevante zaak betreft het geschil tussen de Consumentenbond en Samsung. In juli 2015 werd bekend dat in het besturingssysteem Android een beveiligingslek (een 'bug') genaamd Stagefright zat. Deze bug maakte het mogelijk om smartphones die draaien op dit systeem te hacken waardoor de hacker zich toegang kon verschaffen tot de data op de telefoon. Ook zouden de microfoon en camera op deze toestellen op afstand kunnen worden bediend om zo gebruikers te bespioneren.[21] De smartphones van Samsung draaien op het Android-besturingssysteem, als gevolg waarvan alle Samsung-smartphones kwetsbaar zouden zijn voor cyberaanvallen. Hoewel Google (de ontwikkelaar van Android) reeds een aantal 'patches' ter beschikking stelde om de kwetsbaarheid te verhelpen, voerde Samsung die patches niet door op al zijn toestellen. Met name de wat oudere, maar nog steeds verkochte Samsungmodellen zouden niet gepatcht zijn. Samsung informeerde zijn Nederlandse consumenten zelfs niet over de bug.

De Consumentenbond startte derhalve een kort geding.[22] Daarin vorderde hij onder meer dat Samsung de gebruikers van zijn kwetsbare smartphones informeert over de Stagefright bug, dat hij de veiligheidsupdates die Google als kritisch beschouwt, doorvoert en dat hij alle smartphonemodellen die in de laatste twee jaar in Nederland zijn verkocht en die in de toekomst nog worden verkocht, van beveiligingsupdates zal voorzien. De Consumentenbond baseert deze vorderingen op de zojuist besproken gronden van conformiteit bij (consumenten)koop, oneerlijke (misleidende) handelspraktijken, onrechtmatige daad en artikel 13 Wbp. De voorzieningenrechter komt echter niet tot een inhoudelijke beoordeling van de vorderingen. Hij oordeelt dat de Consumentenbond onvoldoende heeft aangetoond dat er sprake is van spoedeisend belang en wijst de vorderingen derhalve af.[23] Onduidelijk blijft welke civielrechtelijke grondslagen onder welke voorwaarden toepassing vinden in geval van cybersecurityincidenten en mogelijkerwijs een verplichting tot het bijwerken van onveilig gebleken software behelzen. Inmiddels heeft de Consumentenbond een bodemprocedure gestart waarin deze vragen centraal staan.[24]

Praktische bezwaren staan eraan in de weg dat de bestaande rechtsonzekerheid op korte termijn wordt weggenomen door een verdere kristallisatie van relevante open normen door middel van jurisprudentie.[25] Consumenten worden vaak afgeschrikt door de kosten en duur van procederen, zeker als de aanbieder een grote internationale marktspeler is. Ook het financiële belang van consumenten zal doorgaans relatief klein of verspreid over een grote groep zijn, waardoor zij eerder afzien van individuele procedures.[26] Om helderheid te krijgen rondom zorgplichten op het gebied van cybersecurity zullen zij voornamelijk aangewezen zijn op collectieve acties of zogenaamde *public interest litigation*, zoals gevoerd door de Consumentenbond tegen Samsung.[27]

2.3. Beperkende contractsvoorwaarden

Ook het wijdverbreide gebruik van exoneratieclausules en andere beperkende (algemene) voorwaarden in contracten betreffende op ICT gebaseerde goederen en diensten zet een rem op de kristallisatie van zorgplichten voor cybersecurity. Deze voorwaarden bevatten vaak verstrekkende verplichtingen en beperkingen voor con-

18. Zie over zorgplichten in het kader van cybercrime in het algemeen Tjong Tjin Tai e.a. 2015, p. 17-22.
19. Zie uitgebreid Wolters & Verbruggen 2016, p. 837-838.
20. Ook artikel 32 Algemene verordening gegevensbescherming, dat artikel 13 Wbp per 25 mei 2018 zal vervangen, spreekt van de verplichting voor de verantwoordelijke om 'passende technische en organisatorische maatregelen' te treffen 'om een op het risico afgestemd beveiligingsniveau te waarborgen'.
21. www.theguardian.com/technology/2015/jul/28/stagefright-android-vulnerability-heartbleed-mobile.
22. Rb. Amsterdam (vzr.) 8 maart 2016, ECLI:NL:RBAMS:2016:1175 (*Consumentenbond/Samsung*).
23. Het blijkt namelijk dat de kwetsbaarheid als gevolg van de Stagefright-bug in de praktijk zeer moeilijk uit te buiten valt. Androidsmartphones zijn nog slechts in een testomgeving gekraakt en niet 'in the wild'. Het risico dat de consument volgens de Consumentenbond aldus loopt, is onvoldoende om de toets van spoedeisend belang in kort geding te doorstaan.
24. Zie voor meer informatie, inclusief de betekende dagvaarding: www.consumentenbond.nl/nieuws/2016/bodemprocedure-tegen-samsung-van-start.
25. Dit neemt niet weg dat jurisprudentie over zorgplichten voor cybersecurity in commerciële verhoudingen kan bijdragen aan een nadere invulling van deze open normen. Zie bijvoorbeeld Rb. Midden-Nederland 30 maart 2016, C/16/344721 / HA ZA 13-387 (*Politie/Movit IT Masters*).
26. Zie in het algemeen M.G. Faure & L.T. Visser, 'Een rechtseconomische visie op collectieve acties', in: *Collectieve acties* (Preadviezen Vereniging voor Burgerlijk Recht), Zutphen: Uitgeverij Paris 2015, p. 9-12.
27. Zie over de achtergronden en functies van *public interest litigation* L. Enneking & E. de Jong, 'Regulering van onzekere risico's via public interest litigation?', *NJB* 2014/1136, p. 1542.

sumenten en worden gebruikt om verwachtingen rondom cybersecurity te temperen en iedere vorm van aansprakelijkheid uit te sluiten.[28] Een veel gebruikte (Engelstalige) formulering is 'any exclusions, disclaimers or limitation of liability provisions will apply to the extent permitted by local laws'.[29] Recent empirisch onderzoek[30] naar de algemene voorwaarden gebruikt door grote onlineplatformaanbieders en mobiele apps zoals Dropbox, Google, Facebook, LinkedIn, Instagram, Snapchat en Twitter, wijst uit dat deze aanbieders voorwaarden bezigen die mogelijk oneerlijk zijn in de zin van Richtlijn 93/13/EEG.[31] Deze voorwaarden betreffen onder meer de mogelijkheid tot het eenzijdig wijzigen van contractsverplichtingen van de aanbieder en de diensten voor de consument, het eenzijdig beëindigen van contracten door de aanbieder, exoneraties en rechts- en forumkeuzes. Ook de Europese Commissie stelt vast dat algemene voorwaarden op de markt van grensoverschrijdende clouddiensten worden gebruikt om aansprakelijkheid te beperken of uit te sluiten voor het geval dat gegevens in de cloud niet beschikbaar of bruikbaar zijn.[32] Daar waar het consumentenovereenkomsten betreft, kan de rechtmatigheid van de diverse contractsvoorwaarden in het licht van Richtlijn 93/13/EEG sterk worden betwijfeld. Niettemin werpt deze praktijk een extra barrière op voor consumenten en anderen om gerechtelijke actie te ondernemen tegen aanbieders van ICT-toepassingen en zo bij te dragen aan een verdere kristallisatie van zorgplichten voor cybersecurity.

2.4. Ketens, netwerken en het internet der dingen

Een ander element dat de vaststelling van de (omvang van de) zorgplichten voor cybersecurity bemoeilijkt, betreft de complexiteit van de ketens en netwerken via welke op ICT gebaseerde goederen of diensten worden aangeboden. In geval van een smartphone kunnen beveiligingsproblemen ontstaan bij de producent van de hardware of firmware, bij de aanbieder van het besturingssysteem, bij de ontwikkelaar of verkoper van de verschillende apps, software en andere digitale inhoud *embedded* of gedownload op het toestel (door de verkoper, producent of gebruiker zelf) of bij de aanbieder van de netwerkverbinding zoals een telecomaanbieder of wifi-operator. De complexiteit wordt bovendien vergroot doordat de smartphone gekocht kan worden bij verschillende (online)verkopers of onderdeel uitmaakt van een huur- of huurkoopcontract met een telecomaanbieder. Iedere schakel in de keten baseert zijn goederen of diensten op een voorgaande of parallelle schakel, waarbij zij via contracten hun (interne) aansprakelijkheden verdelen. Deze onderlinge verwevenheid van goederen en diensten en de daarmee gepaard gaande fragmentatie van verantwoordelijkheden, maakt het voor de consument bijzonder moeilijk te bepalen wie hij succesvol aansprakelijk kan stellen voor de schade die hij lijdt als gevolg van een cybersecurityincident.

De onderlinge afhankelijkheid en complexiteit in de ICT-distributieketen zal met de verdere ontwikkeling van het *Internet of Things* (IoT) alleen maar groeien. IoT behelst een geïntegreerd netwerk van objecten die onafhankelijk van menselijk ingrijpen met elkaar communiceren, persoonsgegevens verzamelen, delen en verwerken en op deze manier diensten aanbieden aan consumenten.[33] Het aansturen en aanbieden van goederen en digitale diensten wordt aldus nog meer afhankelijk van meerdere onderling geschakelde partijen. Daarmee wordt ook de vraag wie waarvoor verantwoordelijk is moeilijker te beantwoorden.[34] Cybersecurity is in de context van IoT een belangrijk element omdat de beveiligingsrisico's exponentieel kunnen groeien. Een beveiligingslek in een van deze objecten maakt namelijk infiltratie in het gehele netwerk

28. Een extreem geval betreffen de algemene voorwaarden die de speelgoedfabrikant VTech introduceerde na een volgens hackersbronnen relatief eenvoudige hack van zijn 'Learning Lodge Portal', waarbij miljoenen gebruikersgegevens van kinderen en families buit werden gemaakt (zie motherboard.vice.com/read/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids). De voorwaarden bevatten de volgende clausule: 'YOU ACKNOWLEDGE AND AGREE THAT **YOU ASSUME FULL RESPONSIBILITY** FOR YOUR USE OF THE SITE AND ANY SOFTWARE OR FIRMWARE DOWNLOADED THEREFROM. YOU ACKNOWLEDGE AND AGREE THAT ANY INFORMATION YOU SEND OR RECEIVE DURING YOUR USE OF THE SITE **MAY NOT BE SECURE** AND MAY BE INTERCEPTED OR LATER ACQUIRED BY UNAUTHORIZED PARTIES (vetgedrukt PV/PW).' VTech Electronics Europe plc, 'Terms and Conditions' Learning Lodge Support (update 24 December 2015), contentcdn.vtech-da.com/data/console/GB/1668/SystemUpgrade/FirmwareUpdateTnC_GBeng_V2_20160120-170000.txt. Met deze clausule probeert VTech te bewerkstelligen dat zij geen verantwoordelijkheid draagt voor de beveiliging van haar diensten.
29. Van deze clausules stelt de Competition and Markets Authority, de overheidstoezichthouder op het gebied van mededinging en consumentenbescherming van het Verenigd Koninkrijk, dat een dergelijke brede formulering oneerlijk en niet transparant is. Competition and Markets Authority, 'Unfair contract terms guidance. Guidance on the unfair terms provisions in the Consumer Rights Act 2015', 31 July 2015 (CMA37), paragraaf 2.54-2.55, www.gov.uk/government/uploads/system/uploads/attachment_data/file/450440/Unfair_Terms_Main_Guidance.pdf.
30. Zie M. Loos & J. Luzak, 'Wanted: a Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers', *Journal on Consumer Policy* 2016, afl. 1, p. 63-90 en Forbrukerrådet (de Noorse consumentenbond), 'Appfail. Threats to Consumers in Mobile Apps', maart 2016, fbrno.climg.no/wp-content/uploads/2016/03/Appfail-Report-2016.pdf.
31. Richtlijn 93/13/EEG van de Raad van 5 april 1993 betreffende oneerlijke bedingen in consumentenovereenkomsten, *PbEG* 1993, L 95/29.
32. Zo observeert zij: 'In overeenkomsten wordt de contractuele aansprakelijkheid van de cloudaanbieder voor niet-beschikbaarheid of onbruikbaarheid van de gegevens echter vaak uitgesloten of sterk beperkt, of wordt beëindiging van de overeenkomst bemoeilijkt. Daardoor zijn de gegevens in feite niet overdraagbaar.' Europese Commissie, 'Strategie voor een digitale eengemaakte markt voor Europa', COM(2015)192 final, p. 16.
33. Zie in het algemeen over deze ontwikkeling C. Prins, 'Mijn intelligente koelkast', *NJB* 2015/1090, afl. 23, 1519.
34. De beantwoording van die vraag zal in grote mate afhankelijk zijn van het contractuele regime op basis waarvan de diensten worden geleverd. Op basis van hun analyse van het contractuele regime betreffende de slimme Nest-thermostaat, een van de populaire toepassingen van het internet der dingen, stellen Noto La Diega en Walden dat Nest-gebruikers dertien verschillende documenten met een veelvoud aan pagina's moeten doornemen om een compleet beeld te hebben van hun rechten en verplichtingen tegenover verkopers, dienstverleners, licentiehouders en andere derden betrokken bij de werking van de thermostaat en aanverwante diensten. Zie G. Noto La Diega & I. Walden, 'Contracting for the "Internet of Things": Looking into the Nest', Queen Mary University of London, School of Law, Legal Studies Research Paper No. 219/2016, p. 3-4, papers.ssrn.com/sol3/papers.cfm?abstract_id=2725913 (hierna: Noto La Diega & Walden 2016).

mogelijk.[35] Bovendien beschikken de objecten waarover het in IoT gaat, zoals slimme thermostaten, koelkasten en *wearables*, vooralsnog niet altijd over voldoende energie- en computercapaciteit om een hoog niveau van veiligheid te waarborgen, waardoor cyberaanvallen uiterst effectief kunnen zijn.[36] Hoewel deze problematiek te ondervangen is door technieken als versleuteling, is het alarmerend dat geconstateerd wordt dat 70% van de meest populaire IoT-objecten de door hen verzamelde (persoons)gegevens niet versleutelt wanneer die via het internet of lokale verbindingen (zoals wifi of bluetooth) worden verzonden.[37]

3. Noodzaak tot harmonisatie

Cybersecurity zal in toenemende mate van belang zijn voor de ontwikkeling van onze maatschappij. Veelvuldige hacks, bugs of datalekken ondermijnen het vertrouwen in goederen en diensten gebaseerd op ICT en kunnen een rem zetten op hun verdere ontwikkeling. Hoewel het garanderen van 100% veilige ICT-toepassingen technologisch haalbaar noch maatschappelijk wenselijk is,[38] zou een verduidelijking en aanscherping van de bestaande zorgplichten voor aanbieders van ICT-toepassingen kunnen bijdragen aan een hoger niveau van cybersecurity. Dergelijke wijzigingen zouden, gelet op de grensoverschrijdende aard van de ICT-sector en de hier gesignaleerde problematiek, op EU-niveau moeten worden gerealiseerd. Het wetgevingskader betreffende zorgplichten voor cybersecurity in EU-lidstaten en de aldaar bestaande remedies in het geval van onveilige ICT-toepassingen zijn thans slechts gedeeltelijk geharmoniseerd. De Algemene verordening gegevensbescherming zal voor consumenten een recht op schadevergoeding garanderen voor het geval dat hun persoonsgegevens zonder passende technische en organisatorische beveiligingsmaatregelen zijn verwerkt.[39] Buiten het terrein van persoonsgegevens gaat de bestaande EU-wetgeving echter niet expliciet in op de vraag waartoe consumenten jegens aanbieders gerechtigd zijn als de aan hen aangeboden ICT-toepassingen niet beschikbaar, integer of vertrouwelijk blijken. Zij zijn dan aangewezen op het nationale privaatrecht, dat wat betreft deze materie tot op heden nog zeer gefragmenteerd is.[40]

Verdere harmonisatie van zorgplichten voor cybersecurity op Europees niveau kan bijdragen aan de verbetering van cybersecurity en onduidelijkheid over het bestaan van dergelijke zorgplichten en hun omvang wegnemen. Het voeren van een discussie over harmonisatie op dit terrein lijkt tijdig te zijn gelet op de *Digital Single Market*-strategie die de Europese Commissie in mei 2015 lanceerde. In dat kader deed zij twee voorstellen voor nieuwe richtlijnen betreffende de levering van digitale inhoud en de online en op afstand verkoop van zaken.[41] Zoals hierna zal blijken, zullen deze voorstellen in hun huidige vorm niet tot een hoger niveau van cybersecurity leiden.

4. Deelterreinen van harmonisatie

Verschillende deelterreinen van het consumentenrecht en het algemene verbintenissenrecht lenen zich voor (verdere) Europese harmonisatie van zorgplichten voor cybersecurity ter verbetering van de rechtspositie van consumenten van op ICT gebaseerde goederen en diensten. De drie hier te bespreken deelterreinen sluiten nauw aan bij reeds bestaande EU-regelgeving en de recent gepresenteerde richtlijnvoorstellen betreffende de levering van digitale inhoud en de online en op afstand verkoop van zaken.[42] Het gaat in de kern om het verduidelijken en aanpassen van bestaande concepten en open normen in het licht van cybersecurityproblemen.

4.1. Precontractuele informatieverplichtingen

Consumenten moeten over betrouwbare en begrijpelijke informatie kunnen beschikken om een weloverwogen beslissing te nemen over het aangaan van een contract. Zoals besproken (par. 2.1) ontbreekt het consumenten echter vaak aan goede informatie over en inzicht in de mate van cybersecurity van ICT-toepassingen. Op EU-niveau bestaat allerhande regelgeving waarin bedrijven verplicht worden om informatie over de aangeboden goederen en diensten aan de consument te verschaffen voorafgaande aan een overeenkomst. De informatie die moet worden verschaft betreft onder meer de belangrijk-

35. Ernst & Young schrijft hierover treffend: 'The security of the "thing" is only as secure as the network in which it resides: this includes the people, processes and technologies involved in its development and delivery.' EY, *Cybersecurity and the Internet of Things*, 2015, p. 11, www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf.
36. Zo waarschuwt het onafhankelijke advies- en overlegorgaan van Europese privacytoezichthouders, de Artikel 29-werkgroep, dat: 'As their components use wireless communications infrastructures and are characterised by limited resources in terms of energy and computing power, devices [connected in the Internet of Things – IoT] are vulnerable to physical attacks, eavesdropping or proxy attacks. Most common technologies currently in use – i.e. KPI infrastructures – are not easily ported on IoT devices since most of the devices do not have the computing power needed to cope with the required processing tasks.' Artikel 29-werkgroep, 'Opinion 8/2014 on the recent developments on the Internet of Things', 14/EN, WP 223, Opinie van 16 september 2014.
37. Hewlett Packard, *Internet of Things research study*, november 2015, p. 5, h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en. Hewlett Packard, een van de ICT-marktleiders, constateert tevens dat 80% van de meest populaire IoT-objecten het gebruik van onveilige paswoorden toestaat en dat 60% een onveilige gebruikersinterface heeft.
38. Zie ook Centraal Planbureau 2016, p. 20.
39. Artikel 32 en 82 Algemene verordening gegevensbescherming.
40. Zie voor rechtsvergelijkende opmerkingen in het kader van digitale consumentengoederen en diensten: H. Beale, *Scope of application and general approach of the new rules for contracts in the digital environment* (briefing paper voor het Europees Parlement), PE 536.493, 2016 (hierna: Beale 2016), p. 7, www.europarl.europa.eu/committees/nl/ events-workshops.html?id=20160217CHE00181.
41. COM(2015)634 final en COM(2015)635 final. Zie voor een bespreking V. Mak, 'Op weg naar een Europese "Digital Single Market"', *NJB* 2016/397, afl. 8, p. 518-524 (hierna: Mak 2016) en M. Loos, 'Europese harmonisatie van online en op afstand verkoop van zaken en de levering van digitale inhoud', *NtER* 2016, afl. 3 en 4, p. 114-120 en 148-156 (hierna: Loos 2016).
42. Zie voor een volledig overzicht van deelterreinen waarom Europese harmonisatie ter verbetering van de rechtspositie van consumenten zou kunnen plaatsvinden: Verbruggen e.a. 2016, p. 89-104.

ste kenmerken van de aangeboden goederen of diensten.[43] Deze regelgeving is echter generiek en ziet derhalve op vrijwel alle consumentengoederen en diensten. De vraag is dan ook hoe zij moet worden toegepast op goederen en diensten gebaseerd op ICT. In hoeverre moeten kernaspecten van cybersecurity, te weten de beschikbaarheid, integriteit en vertrouwelijkheid van ICT, als belangrijkste eigenschappen van ICT-toepassingen worden beschouwd?

Om de markt voor cybersecurity in Europa beter te laten functioneren, is het nodig om consumenten beter te informeren over de mate van veiligheid, de gevolgen van cybersecurityincidenten en de mogelijke oplossingen die aanbieders van ICT-toepassingen bieden. Om dat te realiseren zou de bestaande EU-regelgeving over precontractuele informatieverplichtingen zo moeten worden uitgelegd dat ICT-aanbieders verplicht zijn om consumenten op duidelijke, begrijpelijke en zinvolle wijze van informatie te voorzien over de cybersecurity van de betrokken ICT. Indien ICT onmisbaar is voor de functionaliteit van de consumentengoederen of -diensten, zou de beschikbaarheid, integriteit en vertrouwelijkheid van de ICT als een van de belangrijkste kenmerken daarvan moeten worden aangemerkt. Voor de aanschaf van standaardsoftware zou dan bijvoorbeeld informatie over wanneer, hoe, en voor welke duur aanbieders updates of upgrades van de software verstrekken aan consumenten moeten worden gegeven. Mochten dergelijke updates of upgrades slechts beschikbaar zijn tegen extra betaling of na het aangaan van aanvullende contracten voor dienstverlening (inclusief onderhouds- of zogenaamde *end-user license agreements* – EULAs), zou dat vooraf duidelijk moeten zijn voor de consument. Met deze informatie zijn consumenten beter in staat om een weloverwogen economische transactie aan te gaan.

Ook de Richtlijn oneerlijke handelspraktijken creëert precontractuele verplichtingen voor bedrijven jegens consumenten.[44] Hij verbiedt oneerlijke commerciële communicatie, met inbegrip van reclame en marketing, door een bedrijf (de 'handelaar') verband houdende met de promotie, verkoop of levering van producten aan consumenten. De richtlijn is in Nederland geïmplementeerd in afdeling 6.3.3a BW. Een handelspraktijk is in het bijzonder oneerlijk als hij 'misleidend' is.[45] Hiervan is op grond van artikel 6:193d lid 2 BW sprake als er 'essentiële informatie' die een gemiddelde consument nodig heeft om een geïnformeerd besluit over een transactie te nemen wordt weggelaten.

Informatie over de beschikbaarheid, integriteit en vertrouwelijkheid van ICT zou door consumenten als essentieel kunnen worden beschouwd bij het nemen van een weloverwogen beslissing over bijvoorbeeld de aanschaf van ICT-toepassingen. Cybersecurity is immers, zoals hierboven gesteld, van groot belang voor het functioneren van ICT. De omstandigheid dat de meeste consumenten bij de aanschaf van ICT alleen op de prijs letten (par. 2.1), doet hier niet aan af. Een 'gemiddelde consument' in de zin van de richtlijn wordt immers gezien als 'redelijk geïnformeerd, omzichtig en oplettend'.[46] Handelaren van op ICT gebaseerde goederen en diensten zouden consumenten derhalve inzage moeten bieden in de mate waarin en wijze waarop zij zorg dragen voor cybersecurity.[47] Het beschikbaar maken van dergelijke informatie zou consumenten helpen in het aangaan van weloverwogen economische transacties en zou meer in het algemeen kunnen bijdragen aan een betere marktwerking voor cybersecurity in Europa.

4.2. Conformiteit

Een verkoper is verplicht om een zaak te leveren die de eigenschappen bezit die de koper gelet op de koopovereenkomst mocht verwachten. Krachtens artikel 7:17 lid 2 BW mag een koper in ieder geval verwachten dat de zaak die eigenschappen bezit die voor normaal gebruik daarvan nodig zijn en waarvan hij de afwezigheid – bijvoorbeeld als gevolg van reclame, mededelingen of andere precontractuele informatie – niet behoefde te betwijfelen. Zijn de beschikbaarheid, integriteit en vertrouwelijkheid van ICT eigenschappen van ICT-toepassingen waarvan de consument-koper mag verwachten dat die toepassingen deze eigenschappen in ieder geval bezitten? De generieke Nederlandse regeling van koop noch de Richtlijn consumentenkoop[48] geeft antwoord op deze vraag. Zij zien immers niet specifiek op de koop van ICT. In het geval van standaardsoftware, waarop de titel van koop (Titel 7.1 Boek 7 BW) analoog moet worden toegepast,[49] moet worden aangenomen dat consumenten niet mogen verwachten dat er nooit een beveiligingslek aan het licht zal

43. Over het algemeen betreffen de precontractuele informatieverplichtingen de belangrijkste kenmerken van de goederen of diensten: identiteit van het bedrijf, prijs, wijze van betaling, levering en uitvoering, duur van de overeenkomst, het herroepingsrecht en de mogelijkheid van toegang tot buitengerechtelijke klachten- en geschilbeslechtingsprocedures. Zie bijvoorbeeld artikel 5 en 6 Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ('Richtlijn inzake elektronische handel'), *PbEG* 2000, L 178/1; artikel 22 Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt, *PbEU* 2006, L 376/36 en artikel 5 en 6 Richtlijn 2011/83/EU van het Europees Parlement en de Raad van 25 oktober 2011 betreffende consumentenrechten, tot wijziging van Richtlijn 93/13/EEG van de Raad en van Richtlijn 1999/44/EG van het Europees Parlement en de Raad en tot intrekking van Richtlijn 85/577/EEG en van Richtlijn 97/7/EG van het Europees Parlement en de Raad, *PbEU* 2011, L 304/64.
44. Richtlijn 2005/29/EG van het Europees Parlement en de Raad van 11 mei 2005 betreffende oneerlijke handelspraktijken van ondernemingen jegens consumenten op de interne markt en tot wijziging van Richtlijn 84/450/EEG van de Raad, Richtlijnen 97/7/EG, 98/27/EG en 2002/65/EG van het Europees Parlement en de Raad en van Verordening (EG) 2006/2004 van het Europees Parlement en de Raad ('Richtlijn oneerlijke handelspraktijken'), *PbEU* 2005, L 149/22. De richtlijn is geïmplementeerd in Titel 3A van Boek 6 BW.
45. Artikel 6:193b lid 3 sub a BW.
46. Zie over dit criterium HvJ EG 16 juli 1998, C-210/96, ECLI:EU:C:1998:369 en overweging 18 Richtlijn 2005/29/EG (oneerlijke handelspraktijken). Zie uitgebreid in algemene zin M.Y. Schaub, 'Wie is consument?', *TvC* 2017, afl. 1, p. 30-40.
47. Dit zou door middel van een Nederlands of Europees certificaat voor cybersecurity kunnen worden vormgegeven. Zie ook Centraal Planbureau 2016, p. 16.
48. Richtlijn 1999/44/EG van het Europees Parlement en de Raad van 25 mei 1999 betreffende bepaalde aspecten van de verkoop van en garanties voor consumptiegoederen, *PbEG* 1999, L 304/64.
49. HR 27 april 2012, *NJ* 2012/293 (*Beeldbrigade/Hulskamp*). Zie ook artikel 7:5 lid 5 BW over digitale inhoud.

komen.[50] Volledige veiligheid zal in een markt die gekenmerkt wordt door dynamiek en technologische innovatie immers nooit kunnen worden gegarandeerd. Het enkele feit dat een kwetsbaarheid is ontdekt zal daarom niet betekenen dat de software non-conform is. De relevante eigenschap waarvan de aanwezigheid in een dergelijk geval getoetst moet worden is dan ook niet de beveiliging ten tijde van het sluiten van de koopovereenkomst, maar de geboden ondersteuning of updates die de softwareontwikkelaar na ontdekking van het lek verschaft. De consument zou mogen verwachten dat hij gedurende een redelijke periode ondersteuning krijgt die het product geschikt houdt voor normaal gebruik.[51] Op die wijze wordt ook de kwaliteit van dienstverlening betrokken bij de bepaling van conformiteit van een afgeleverde zaak.[52]

Deze dynamische benadering van conformiteit komt terug in het richtlijnvoorstel betreffende de levering van digitale inhoud (hierna: Richtlijn digitale inhoud), dat samen met het richtlijnvoorstel betreffende online en op afstand verkoop van zaken (hierna: Richtlijn online-verkoop) door de Europese Commissie in december 2015 werd gepresenteerd als onderdeel van de *Digital Single Market*-strategie. De eerste richtlijn ziet op overeenkomsten gesloten tussen leveranciers en consumenten over de levering van digitale inhoud, een verzamelbegrip waar onder meer video, audio, applicaties, digitale games, software en cloud computing onder vallen.[53] De tweede richtlijn betreft koopovereenkomsten gesloten tussen verkopers en consumenten zonder hun gelijktijdige fysieke aanwezigheid, maar door middel van internet, telefoon of andere ICT-toepassingen. Beide richtlijnen voorzien in de introductie van volledig geharmoniseerde regels die beogen een hoog en uniform niveau van consumentenbescherming op het door ieder van hen bestreken terrein te realiseren in de EU.

Artikel 6 lid 1 Richtlijn digitale inhoud formuleert conformiteit als het beantwoorden van de digitale inhoud aan de overeenkomst. Het lid vestigt daarbij de aandacht op aspecten van onder meer functionaliteit, interoperabiliteit en andere prestatiekenmerken zoals de toegankelijkheid, continuïteit en veiligheid van de digitale inhoud, alsmede het updaten daarvan. De Richtlijn digitale inhoud zet daarmee aspecten van cybersecurity in de levering van digitale inhoud en aanpalende dienstverlening op de kaart. Echter, de wijze waarop dat gebeurt is onvolkomen. Objectieve maatstaven voor de beoordeling of de digitale inhoud conform is, zoals het normaal gebruik dat de consument mag verwachten, zijn krachtens artikel 6 lid 2 namelijk alleen van toepassing als partijen niet bij overeenkomst in de in lid 1 genoemde aspecten hebben voorzien. Daarmee schept de richtlijn de mogelijkheid dat leveranciers van digitale inhoud contractueel kunnen bepalen welke conformiteitsverwachtingen consumenten mogen hebben, ook omtrent cybersecurity.

Deze subjectieve invulling van conformiteit heeft op veel kritiek kunnen rekenen in de literatuur.[54] Zij staat toe dat aanbieders iedere verwachting onder consumenten omtrent de beschikbaarheid, integriteit en vertrouwelijkheid van ICT-toepassingen wegschrijven. Ook lijkt het voor aanbieders mogelijk om op voorhand bij overeenkomst uit te sluiten dat ze zorg moeten dragen voor het updaten van software, zelfs als dergelijke updates noodzakelijk zouden zijn voor het normale gebruik van de software of gerelateerde producten. De subjectieve invulling wijkt bovendien af van het bestaande recht. Bij consumentenkoop is de in artikel 7:17 lid 2 BW opgenomen objectieve maatstaf immers van dwingend recht op grond van artikel 7:6 BW.

De voorgestelde subjectieve benadering van conformiteit in de Richtlijn digitale inhoud is ook wegens een andere reden problematisch. Die reden is gelegen in het feit dat de werkingssfeer van de richtlijn in de praktijk lastig te onderscheiden zal zijn van die van de Richtlijn online-verkoop, en dat terwijl die laatste richtlijn, net als de bestaande regelgeving, nu juist uitgaat van een objectief criterium voor conformiteit.[55] De moeilijkheid komt voort uit het gegeven dat in de toekomst steeds meer consumentenproducten digitale inhoud zullen bevatten die de functionaliteit van het product bepalen. Dat is grotendeels al het geval voor *smart devices* (zoals smartphones en tablets), maar zal nog sterker worden bij producten met een verbinding met IoT.[56] Hier kan bijvoorbeeld gedacht worden aan een slimme thermostaat, waarvan kan worden gezegd dat zijn voornaamste functie het aansturen van de verwarming in huis is. Een dergelijke thermostaat kan echter ook met behulp van ingebouwde sensoren, software en een netwerkverbinding andere slimme apparaten (zoals deursloten, lichten, wandcontactdozen, brandalarmen, sprinklers en het beveiligingsalarm) gaan aansturen en aanvullende diensten leveren. Zo verandert zijn functie in een veel bredere, namelijk een controlesysteem voor energieverbruik en beveiliging opererend op basis van gebruikergegenereerde data.[57]

Deze groeiende hybriditeit van fysieke goederen en digitale inhoud maakt dat het onderscheid tussen de verkoop van goederen met geïntegreerde digitale inhoud enerzijds

50. Vgl. Wolters & Verbruggen 2016, p. 835.
51. Vgl. Beale 2016, p. 27 en Loos 2016, p. 153
52. Vgl. Wolters & Verbruggen 2016, p. 835. Zie ook C. Wendehorst, 'Sales of goods and supply of digital content – Two worlds apart? Why the law on sale of goods needs to respond better to the challenges of the digital age', briefing paper voor het Europees Parlement, PE 556.928, 2016, p. 14, www.europarl.europa.eu/committees/nl/events-workshops.html?id=20160217CHE00181 (hierna: Wendehorst 2016).
53. Vgl. artikel 2 lid 1 Richtlijnvoorstel digitale inhoud.
54. Zie o.a. Beale 2016, p. 21; Mak 2016, p. 523 en Loos 2016, p. 151-152.
55. Krachtens artikel 5 Richtlijn online-verkoop dienen goederen 'geschikt te zijn voor ieder gebruik waarvoor goederen van dezelfde omschrijving gewoonlijk dienen' en 'de hoedanigheden en prestatievermogens te bezitten die voor gelijke goederen normaal zijn en die de consument mag verwachten'. Met deze formulering sluit de richtlijn aan bij conformiteit zoals omschreven in de Richtlijn consumentenkoop.
56. IoT wordt in de Richtlijn digitale inhoud thans helemaal buiten de werkingssfeer van de richtlijn geplaatst. Zie overweging 17 Richtlijn digitale inhoud.
57. Deze toepassingen zijn mogelijk met de slimme thermostaat van Nest. Zie voor een uitgebreide beschrijving van zijn mogelijkheden Noto La Diega & Walden 2016.

en de verkoop van goederen en aanvullende levering van digitale inhoud anderzijds steeds moeilijker te maken zal zijn.[58] De afstemming van de werkingssfeer van de twee richtlijnen zoals geformuleerd in de considerans van de Richtlijn digitale inhoud en de Richtlijn online-verkoop zal dan ook niet werkbaar zijn op de lange termijn.[59] Deze constatering nodigt uit tot het denken over een algemeen regime voor koop dat alle overeenkomsten van consumenten betreffende digitale inhoud (al dan niet *embedded* in goederen) omvat, waarbij dan tevens de algemene Europese regeling van consumentenkoop voor 'gewone', fysieke koop zou kunnen worden meegenomen.[60] Bij een herziening, in welke vorm dan ook, zou het uitgangspunt moeten zijn dat conformiteit met een objectieve maatstaf wordt ingevuld en bij de toetsing van die maatstaf eigenschappen als beschikbaarheid, integriteit en vertrouwelijkheid van ICT worden betrokken.

4.3. Productaansprakelijkheid

De zojuist besproken hybriditeit van fysieke goederen en digitale inhoud en daarmee gepaard gaande complexe distributieketens en netwerken in de ICT-sector, betekenen dat het voor consumenten bijzonder moeilijk is om te bepalen wie waarvoor zorg draagt, en dus ook wie zij aansprakelijk moeten stellen ter vergoeding van de schade geleden door een cybersecurityincident. Toepassing van de Richtlijn productaansprakelijkheid[61] op ICT-toepassingen zou deze ondoorzichtigheid van verantwoordelijkheden kunnen doorbreken. De richtlijn, die in Nederland is geïmplementeerd in afdeling 6.3.3 van Boek 6 BW, gebruikt namelijk een ruime definitie van het begrip 'producent'. Het begrip omvat niet alleen de fabrikant van een eindproduct, maar ook andere spelers in de distributieketen van ICT-toepassingen. Zo zou bijvoorbeeld een softwareontwikkelaar als producent kunnen worden gezien van een onderdeel van de ICT-toepassing.[62] Een bedrijf dat ICT-toepassingen gemaakt in China, Japan of de Verenigde Staten invoert in de Europese Economische Ruimte zou eveneens als producent worden gezien.[63] Mocht de werkelijke producent onbekend zijn, kunnen ook als producent worden aangemerkt degene die zich als zodanig presenteert door zijn naam, merk of andere onderscheidingstekens op het product aan te brengen, of onder omstandigheden zelfs de leverancier van de ICT-toepassing.[64]

Om deze spelers op grond van de implementatiewetgeving van de richtlijn te verplichten tot vergoeding van schade geleden door een cybersecurityincident is het echter wel noodzakelijk om ook het concept 'product' breed uit te leggen. Dat concept stelt thans fysieke tastbaarheid centraal: producten zijn roerende zaken, elektriciteit daaronder begrepen.[65] Derhalve lijkt productaansprakelijkheid in beginsel alleen van toepassing bij ICT die onderdeel uitmaakt van een fysieke zaak. In een wereld waarin niet alleen de fysieke eigenschappen van een product, maar ook de ICT de functionaliteit van een product bepaalt, is het echter wenselijk dat dergelijke technologie als zelfstandig product of als inherent onderdeel van een fysiek product wordt beschouwd. Eind jaren tachtig nam de Europese Commissie reeds het standpunt in dat software ook als zelfstandig product in de zin van de Richtlijn productaansprakelijkheid zou moeten worden gezien.[66] Ook diverse schrijvers hebben betoogd dat software onder omstandigheden als product moet worden aangemerkt.[67] Een dergelijke verruiming van het concept 'product' in afdeling 6.3.3 BW zou ook aansluiten bij de positie die de Hoge Raad in het *Beeldbridage*-arrest innam, te weten dat titel 7.1 Boek 7 BW betreffende de koop van roerende zaken analoog moet worden toegepast op de aanschaf van standaardsoftware. Het Hof van Justitie van de EU heeft (nog) geen kans gezien om zich uit te laten over de vraag of software en andere digitale inhoud onder de reikwijdte van de Richtlijn productaansprakelijkheid vallen. Als de Europese wetgever hier geen actie onderneemt, is het Hof de aangewezen instantie om deze verruiming tot stand te brengen.

De producent is op grond van de regeling van productaansprakelijkheid aansprakelijk als de ICT-toepassing gebrekkig is en daardoor schade heeft veroorzaakt bij de consumenten. Een product is volgens artikel 6:186 BW gebrekkig indien het niet de veiligheid biedt die gebruikers daarvan mochten verwachten. Digitale inhoud die kwetsbaar is in de zin van cybersecurity zou als gebrekkig

58. Wendehorst 2016, p. 8. Zie ook Mak 2016, p. 522.
59. Zie overweging 11 Richtlijn digitale inhoud en overweging 13 Richtlijn online-verkoop.
60. Mak 2016, p. 524.
61. Richtlijn 85/374/EEG van de Raad van 25 juli 1985 betreffende de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen der lidstaten inzake de aansprakelijkheid voor producten met gebreken, *PbEG* 1985, L 210, laatst gewijzigd bij Richtlijn 1999/34/EG, *PbEG* 1999, L 141.
62. Artikel 6:187 lid 2 BW.
63. Artikel 6:187 lid 3 BW.
64. Artikel 6:187 lid 2 en 4 BW.
65. Artikel 6:187 lid 1 BW.
66. In 1989 beantwoordde Lord Arthur Cockfield, toenmalig vicepresident van de Commissie en Commissaris Interne Markt, Belastingen en Douane, vragen gesteld door Europarlementariër Gijs de Vries (Liberaal Democraten) over de reikwijdte van de Richtlijn productaansprakelijkheid. Ook vroeg De Vries of computersoftware onder de reikwijdte van de richtlijn viel. Cockfield antwoordde dat de richtlijn op dezelfde wijze van toepassing is op software dan dat zij van toepassing is op handwerk- en artistieke producten. Zie Antwoord op geschreven vraag 706/88, *PbEG* 1989, C 114/42.
67. Zo stelt R.J.J. Westerdijk, *Produktenaansprakelijkheid voor software: beschouwingen over de aansprakelijkheid voor informatieprodukten*, Deventer: Kluwer 1995 dat software geleverd op een fysieke drager onder het regime van de richtlijn zou moeten vallen. Meer recent pleit J.J. Borking, 'Privacy-by-Design, Haute couture of confectie?', *Computerrecht* 2013/117, p. 189 voor productaansprakelijkheid voor fabrikanten en ontwerpers van voor privacy onveilige informatiesystemen. K.A.P.C. van Wees, 'Enkele juridische aspecten van de (deels) zelfrijdende auto', *Computerrecht* 2015/198, p. 318 geeft in het kader van productaansprakelijkheid bij zelfrijdende auto's aan dat software die gericht is op besturing van producten wel onder het regime van de richtlijn valt. S. De Schrijver & M. Maes, 'Aansprakelijkheid in een ambient intelligent-omgeving: Wie heeft het gedaan?', *Computerrecht* 2010/174, p. 290-291 (hierna: De Schrijver & Maes 2010) betogen hetzelfde voor ambient intelligence. Anders Tjong Tjin Tai e.a. 2015, p. 58, die zonder veel discussie stellen dat productaansprakelijkheid niet van toepassing is op software. Zie voor een rechtsvergelijkende analyse: K. Alhelt, 'The Applicability of the EU Product Liability Directive to Software', *Comparative and International Law Journal of Southern Africa* 2001, afl. 2, p. 188-209.

moeten worden beschouwd.[68] Een product zou ook als gebrekkig moeten worden gezien als het voorzienbaar onveilig gebruik door consumenten onvoldoende tegengaat. Bijgevolg worden producenten geprikkeld om te anticiperen op onveilig gebruik door slimme oplossingen in hun ICT-toepassingen in te bouwen; geen standaardwachtwoorden, automatische implementatie van kritische beveiligingsupdates en andere vormen van veiligheid door vormgeving (*security by design*) zouden de regel moeten zijn.[69] De kwetsbaarheid behoeft niet door een aanvaller misbruikt te worden om het product gebrekkig te laten zijn. Het risico dat er misbruik van kan worden gemaakt is voldoende om de gebrekkigheid te laten bestaan.[70] In dat geval komen voor vergoeding in aanmerking de kosten die noodzakelijk zijn om de schadelijke gevolgen te verhelpen en om het veiligheidsniveau dat men mag verwachten te herstellen. Hierbij kan gedacht worden aan de kosten van patches, updates of upgrades.[71]

Artikel 6:190 BW geeft consumenten slechts recht op vergoeding van schade door dood of letsel en schade aan zaken anders dan het gebrekkige product die bestemd zijn voor gebruik in de privésfeer, met toepassing van een franchise van € 500. Een gebrekkige cybersecurity leidt in de meeste gevallen echter niet tot dergelijke schade.[72] Transactieschade en zuivere vermogensschade komen niet voor vergoeding in aanmerking. Onduidelijk is of ook immateriële schade kan worden gevorderd.[73] Omdat een schadevergoeding volgens de rechtspraak van het Hof van Justitie van de EU voor consumenten zinvol en effectief moet zijn,[74] zouden niet alleen letsel- en zaakschade voor vergoeding in aanmerking moeten komen, maar ook zuivere vermogensschade en immateriële schade. Misbruik van een kwetsbaarheid in een ICT-toepassing zal doorgaans schade toebrengen aan de digitale omgeving van de consument, zoals het moeten aanschaffen van nieuwe hard- of software. Ook kunnen (persoons)gegevens verwijderd, veranderd of beschadigd zijn geraakt. Aanvallers kunnen zelfs aan de haal gaan met die gegevens om bijvoorbeeld de bankrekening van de consument leeg te halen. Om consumenten compleet schadeloos te stellen zou ook het verlies van gegevens zonder economische maar wel met emotionele waarde, zoals familie- of vakantiefoto's, voor vergoeding in aanmerking moeten komen.[75] Op die wijze zou beter worden aangesloten op de Algemene verordening gegevensbescherming, die in artikel 82 consumenten het recht geeft op vergoeding van zowel materiële als immateriële schade in geval van schending van de regels inzake de bescherming van persoonsgegevens zoals neergelegd in die verordening.

Producenten kunnen aansprakelijkheid voor de schade veroorzaakt door onveilige ICT-toepassingen afwenden door onder meer aan te tonen dat het op grond van de wetenschappelijke en technische kennis op het moment waarop het product op de markt werd gebracht, onmogelijk was om het gebrek te ontdekken.[76] In een markt die gekenmerkt wordt door dynamiek en technologische innovatie, is dit ontwikkelingsrisico-verweer een belangrijke troef voor producenten van ICT-toepassingen.[77] Dit verweer zou echter niet zo moeten worden geïnterpreteerd dat daarmee aansprakelijkheid kan worden ontlopen indien ICT-toepassingen in het verkeer worden gebracht met bekende of kenbare kwetsbaarheden. In een dergelijk geval zouden producenten verplicht moeten zijn om de kwetsbaarheden door middel van updates te ondervangen.[78] Indien dat onmogelijk is of indien de kwetsbaarheden onvoldoende ondervangen worden, zou een verplichting tot schadevergoeding moeten bestaan.

Dat de aansprakelijkheid voor schade veroorzaakt door onveilige ICT-toepassingen door de producent moeten worden gedragen, doorbreekt niet alleen de ondoorzichtigheid van verantwoordelijkheden in ICT-distributieketens. Een dergelijke allocatie van het aansprakelijkheidsrisico is ook efficiënter.[79] Ten eerste is de producent als geen ander in staat de gebrekkigheid weg te nemen. Hij ontwikkelt immers het product en heeft de meeste expertise. Bovendien heeft de producent de mogelijkheid tot het verzekeren van het aansprakelijkheidsrisico. De verzekeringskosten kan de producent vervolgens afwikkelen op zijn klanten door de prijs van de ICT-toepassingen iets te verhogen. Het verdisconteren van de verzekeringskosten in de prijs van deze toepassingen is efficiënter dan

68. Dit strookt met hetgeen hierboven betoogd is in het kader van conformiteit bij koop.
69. Best practices betreffende *security by design* worden onder andere opgesteld en gedeeld door de private non-profitorganisatie OWASP, opgericht in 2001 en geïncorporeerd in de Verenigde Staten. Het 'Application Security Verification Standard'-project probeert bijvoorbeeld de standaard voor beveiliging van webapplicaties te normaliseren. Zie: www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project.
70. Vgl. HvJ EU 5 maart 2015, ECLI:EU:C:2015:148, r.o. 40-42 en 49 (*Boston Scientific Medizintechnik*).
71. Idem, r.o. 50. Zie ook HvJ EU 10 mei 2001, C-203/99, ECLI:EU:C:2001:258, r.o. 27-29 (*Veedfald/Arhus Amtskommune*).
72. Soms kan een gebrek echter wel tot deze schade leiden. Een gebrek in de beveiliging van semi-zelfrijdende jeeps maakte het bijvoorbeeld mogelijk om de besturing van deze voertuigen op afstand over te nemen, waardoor een ongeluk met letsel- en zaakschade het gevolg zou kunnen zijn. Zie www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
73. Hoewel artikel 9 van de richtlijn bepaalt dat de richtlijn nationale regels inzake de vergoeding van immateriële schade onverlet laat, benoemt artikel 6:190 BW deze schadesoort niet. Ook de burgerlijke rechter lijkt deze er niet in te willen lezen. Het gevolg is dat de consument aangewezen is op de regeling van onrechtmatige daad om immateriële schade te vorderen. Dit is onnodig complex voor een consument. Zie ook A. Keirse, 'Richtlijn 1985/374/EG inzake de aansprakelijkheid voor producten met gebreken', in: A.S. Hartkamp e.a. (red.), *De invloed van het Europese recht op het Nederlandse privaatrecht. 2: bijzonder deel*, Deventer: Kluwer 2014, p. 33-65.
74. Vgl. HvJ EU 5 maart 2015, ECLI:EU:C:2015:148, r.o. 49 (*Boston Scientific Medizintechnik*). Vgl. HvJ EU 10 mei 2001, C-203/99, ECLI:EU:C:2001:258, r.o. 27-29 (*Veedfald/Arhus Amtskommune*).
75. Vgl. Mak 2016, p. 523.
76. Zie artikel 6:185 lid 1 sub e BW. Een mogelijkheid voor producenten om hun aansprakelijkheid te verminderen of zelfs op te heffen, betreft het eigen schuldverweer in de zin van artikel 6:185 lid 2 BW. Een dergelijk verweer zou doel kunnen treffen indien de kwetsbaarheid van de ICT-toepassing het gevolg is van onverantwoord paswoordgebruik door de consument of het verwijtbaar nalaten van het implementeren van vrijelijk aangeboden patches, updates of upgrades die door de aanbieder als kritiek worden beschouwd.
77. Vgl. De Schrijver & Maes 2010, p. 291.
78. Het laten bestaan van een gevaar of daar onvoldoende effectief voor waarschuwen kan onrechtmatig zijn overeenkomstig HR 5 november 1965, ECLI:NL:HR:1965:AB7079 (*Kelderluik*) en HR 28 mei 2004 ECLI:NL:HR:2004:AO4224 (*Jetblast*).
79. S. Weatherill, *EU Consumer Law & Policy*, Cheltenham: Edward Elgar 2013, p. 174.

het betalen van de (gerechtelijke) kosten gemoeid met het vergoeden van de schade bij een klein aantal gedupeerde consumenten.

5. Tot besluit

Deze bijdrage beoogt inzicht te geven in de rechtspositie van consumenten indien blijkt dat de cybersecurity van de door hen aangeschafte ICT-toepassingen tekortschiet. Het juridisch kader dat op deze materie van toepassing is, wordt gekenmerkt door open normen. Jurisprudentie over hun toepassing is spaarzaam en heeft niet kunnen leiden tot heldere uitgangspunten voor de consument en evenmin voor de ICT-sector. De rechtsonzekerheid die dit meebrengt wordt thans door ICT-aanbieders benut om hun zorgplichten voor cybersecurity van ICT-toepassingen aangeboden aan consumenten te minimaliseren. Verschillende vormen van marktfalen staan bovendien in de weg aan een verbetering van het niveau van bescherming (par. 2). Zoals betoogd in deze bijdrage, is het wenselijk om via wetgeving en jurisprudentie helderheid en uniformiteit te creëren over het bestaan en de omvang van zorgplichten voor cybersecurity. Dergelijke harmonisatie kan aanvullende prikkels genereren voor een gemeenschappelijk hoog niveau van bescherming voor consumenten in Europa (par. 3).

Bij de door ons behandelde grondslagen voor deze zorgplichten hebben wij voorstellen gedaan om bestaande concepten en open normen op het terrein van precontractuele informatieplichten, conformiteit en productaansprakelijkheid te verduidelijken en uit te breiden in het licht van actuele cybersecurityproblemen (par. 4). Deze wijzigingen zouden gelet op de grensoverschrijdende aard van de ICT-sector op EU-niveau moeten worden gerealiseerd. Zo zou het Europese Hof van Justitie een actieve rol kunnen vervullen door bestaande regelgeving extensief te interpreteren en aspecten van cybersecurity kunnen betitelen als 'essentieel' voor consumenten om een weloverwogen beslissing over de aanschaf van ICT-toepassingen te kunnen nemen (par. 4.1). Hetzelfde zou het Hof kunnen doen voor de regels over consumentenkoop door cybersecurity te bestempelen als een 'eigenschap' van ICT-toepassingen die consumenten redelijkerwijs mogen verwachten bij normaal gebruik (par. 4.2) of door software als 'product' in het kader van de Richtlijn productaansprakelijkheid te zien (par. 4.3).

De Europese wetgever kan echter nog een veel duidelijker signaal afgeven door zelf dergelijke wijzigingen te realiseren in het kader van de *Digital Single Market*-strategie. Door expliciete plichten op het gebied van cybersecurity te creëren, kan de Europese wetgever een grotere mate van rechtszekerheid creëren. Bij de uitwerking van deze regels zou aandacht moeten worden geschonken aan aspecten als het doel waarvoor de consument de ICT-toepassing aanschaft en haar normale gebruik, de aard en ernst van het risico dat consumenten door gebruik van de onveilige ICT-toepassing lopen, en de verwachtingen die een consument ten aanzien van de cybersecurity van een ICT-toepassing mag hebben. Harmonisatie van deze materie door middel van een enkel Europees wetgevingsinstrument, ongeacht of het minimum- of maximumharmonisatie betreft, is echter niet haalbaar. De aard van de besproken problematiek en de vele wijzen waarop cybersecurity op bestaande regelgeving voor consumenten betrekking heeft staan daaraan in de weg. Het heeft daarom de voorkeur om aan te sluiten bij het huidige wetgevingskader betreffende precontractuele informatieplichten, conformiteit en productaansprakelijkheid, alsmede de recent gedane richtlijnvoorstellen betreffende digitale inhoud en online-verkoop. Met name de Richtlijn digitale inhoud geeft een uitgelezen mogelijkheid om cybersecurity sterker te verankeren in het huidige Europese consumentenrecht.