# Redactioneel

## *Tijdschrift voor Blockchainrecht*

*mr. H.A.J. de Jong*

Het internet is fascinerend! Voor juristen en ongetwijfeld ook voor vele andere professionals zoals beveiligingsexperts en marketeers. En zeker ook voor ondernemers. Door de elkaar snel opvolgende technologische mogelijkheden, het internationale karakter en de vele schakels die vaak betrokken zijn blijft het voor de praktijkjurist voortdurend een uitdaging om doorwrochte juridische antwoorden te vinden op concrete vragen die ook uitvoerbaar zijn in de praktijk.

Om goed te kunnen adviseren, te begeleiden bij het sluiten van contracten en bij te staan in conflicten is in enige mate inzicht in de technologie naar mijn mening onontbeerlijk. Niet dat met dat inzicht alles kan worden opgelost, maar zonder voldoende kennis van de techniek missen juridische analyses veelal de aansluiting met de praktijk. En praktijk zonder juridische kaders is minimaal onwenselijk.

Tot dusver lijkt het voor juristen gelukkig mogelijk om een redelijke voorstelling te maken van begrippen als de cloud, digitale handtekeningen en profiling. Hoewel dit laatste een goed voorbeeld zou kunnen zijn van het spanningsveld tussen de juridische werkelijkheid en de feitelijke realiteit kijkend naar bijvoorbeeld de (on)mogelijkheid om op de juridisch correcte wijze toestemming te verlangen van een bezoeker van een website voordat een advertentie wordt geplaatst.

Voldoende kennis van de techniek is echter steeds lastiger doordat de technische mogelijkheden zich razendsnel blijven ontwikkelen en de resultaten daarvan steeds complexer en lastiger te doorgronden worden. Dat geldt zeker voor de opkomst van blockchaintechnologie en de daarop gebaseerde toepassingen zoals smart contracts. Hoe werkt het ongeveer? Is het echt zo betrouwbaar als wel wordt beweerd? Welke (juridische) risico's zijn eraan verbonden? Voor welke toepassingen is het geschikt? Enzovoort.

Eenduidige antwoorden op deze vragen die een jurist ook zou kunnen begrijpen blijven vooralsnog echter uit. Dit fascineert omdat er tegelijkertijd advocaten zijn die blockchain zien als een nieuw verdienmodel voor de advocatuur (en een bedreiging voor het bestaande verdienmodel). Advocaten die er teams voor hebben samengesteld of zelfs een heel kantoor voor hebben opgericht.

Blockchain wordt als innovatie vergeleken met de spectaculaire opkomst van het internet. Tot voor kort was ik ervan overtuigd dat het internetrecht in enigerlei vorm een ontmoetingsplaats is voor de allernieuwste technologieën en het recht. Sinds ik mijn hoofd gebroken heb over blockchaintechnologie en toepassingen zoals smart contracts ben ik deze overtuiging kwijt. Dit zou een teleurstelling zijn en een geruststelling. Het niet begrijpen en het niet hoeven te begrijpen. Is blockchain en alles wat daarmee samenhangt een aanstormend nieuw rechtsgebied?

Voordat het mogelijk zover komt, doet het mij goed u te kunnen melden dat in dit nummer zowel een artikel staat waarin wordt uitgelegd wat smart contracts zijn als een noot over bitcoins, beide toepassingen van blockchaintechnologie. We hebben als internetjuristen de aansluiting nog niet definitief gemist.

# Cybersecurityregulering in de praktijk, van wetgeving naar technoregulering

*drs. M. Bolhuis*[1]

**De afgelopen jaren heeft de politieke en maatschappelijke aandacht voor regulering van cybersecurity in Nederland en in Europa een grote vlucht genomen. Bij de voorgestelde aanpak wordt zwaar geleund op wetgeving die zich richt op aanbieders van vitale en essentiële diensten, zoals de Europese Richtlijn voor de Beveiliging van Netwerk- en Informatiesystemen, de Wet Gegevensverwerking en meldplicht cybersecurity en de Cybersecuritywet. Mede naar aanleiding van de opkomst van het Internet-of-Things heeft de Europese Commissie in de herfst van 2017 het cybersecurity pakket gepubliceerd, waarin een voorstel is opgenomen voor een Europees kader voor cybersecurity certificeringsschema's. Ook in Nederland is toenemende aandacht voor regulering van Internet-of-Things. In dit artikel zullen deze initiatieven nader worden besproken. Duidelijk wordt dat naast wetgeving veel wordt verwacht van certificering als instrument om de cybersecurity van ICT-producten en diensten in Europa te verbeteren. Dat kan worden aangeduid als technoregulering.**

## 1. Toenemende aandacht voor regulering van cybersecurity

Zowel in Europa als in Nederland is de afgelopen jaren de aandacht voor regulering van cybersecurity toegenomen.[2] Zo is op 19 juli 2016 de Europese Richtlijn voor de Beveiliging van Netwerk- en Informatiesystemen (hierna: de NIB-Richtlijn) gepubliceerd.[3] In Nederland is op 1 oktober 2017 de Wet Gegevensverwerking en meldplicht cyber security (hierna: Wgmc) gedeeltelijk in werking getreden.[4] Als onderdeel van deze wet is op 1 januari 2018 een meldplicht voor grote digitale veiligheidsincidenten in werking getreden.[5] In februari 2018 is een voorstel voor een Cybersecuritywet door de Minister van Justitie en Veiligheid naar de Tweede Kamer gestuurd.[6] Naast bovengenoemde wetsvoorstellen zijn er ook andere maatregelen genomen waaronder de aankondiging van de oprichting van een Digital Trust Centre in het najaar van 2017.[7] Daarnaast is de afgelopen jaren door het Nederlandse kabinet meer budget beschikbaar gesteld voor cybersecurity, in totaal 95 miljoen euro per jaar.[8] Recent is de in het Regeerakkoord aangekondigde Nederlandse Cybersecurity Agenda (NCSA) door de Minister van Justitie en Veiligheid aan de Tweede Kamer der Staten-Generaal toegezonden.[9]

Recent is zowel in Nederland als in Brussel een aantal rapporten en wetsvoorstellen gepubliceerd om de risico's die samenhangen met de opkomst van het Internet-of-Things te reguleren.[10] Zo heeft

1. Machiel Bolhuis is werkzaam als Adviseur Regulatory Affairs bij EnecoGroep. Dit artikel is op persoonlijke titel geschreven. Het artikel is bijgewerkt tot en met 7 mei 2018.
2. Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan. Definitie is overgenomen uit de Nederlandse Cybersecurity Agenda, Nederland digitaal veilig (2018).
3. Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, *PbEU* 2016, L 194/1.
4. Wet van 25 juli 2017, houdende regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity), *Stb*. 2017, 316. Artikel 1.
5. Besluit van 4 december 2017 tot aanwijzing van aanbieders, producten en diensten ten aanzien waarvan een plicht geldt om ernstige ICT-incidenten te melden (Besluit meldplicht cybersecurity), *Stb*. 2017, nr. 476.
6. Regels ter implementatie van richtlijn (EU) 2016/1148 (Cybersecuritywet), Voorstel van Wet, *Kamerstukken II* 2017/18, 34 883, nr. 2.
7. Informatie- en Communicatietechnologie, brief van de Minister van Economische Zaken aan de voorzitter van de Tweede Kamer der Staten-Generaal, Den Haag, 23 september 2017, *Kamerstukken II* 2017/18, 26 643, nr. 488.
8. 'Vertrouwen in de toekomst', Regeerakkoord 2017 - 2021, VVD, CDA, D66 en Christenunie, 10 oktober 2017.
9. Nederlandse Cybersecurity Agenda, Nederland digitaal veilig. Deze agenda is op 20 april 2018 door de Minister van Justitie en Veiligheid aangeboden aan de voorzitter van de Tweede Kamer der Staten-Generaal, Informatie- en communicatietechnologie (ICT), *Kamerstukken II* 2017/18, 26 643, nr. 536.
10. Het Internet-of-Things is een netwerk van 'slimme'

op 19 september 2017 de Europese Commissie het cybersecuritypakket gepubliceerd.[11] Dit pakket omvat onder andere een Verordening met een voorstel voor een Europees kader voor cybersecurity certificeringsschema's.[12] In Nederland is in het Regeerakkoord 'Vertrouwen in de toekomst' opgenomen dat er standaarden moeten komen voor Internet-of-Things-apparaten[13] en is het bevorderen van digitaal veilige hard- en software als ambitie opgenomen in de Nederlandse Cybersecurity Agenda[14]. Daarnaast heeft de Nederlandse Cyber Security Raad eind 2017 een advies gepubliceerd over de cybersecurity van het Internet-of-Things. In dit advies wordt gepleit voor certificering van Internet-of-Things-apparaten en productaansprakelijkheid voor fabrikanten.[15] Ook in de Nederlandse politiek gaan stemmen op om het Internet-of-Things te reguleren. Op 7 maart van dit jaar is een motie door de Tweede Kamerleden Paternotte, Verhoeven en Van Den Berg ingediend waarin de regering wordt verzocht om in de Europese raad te pleiten voor verplichte certificering van de op internet aangesloten apparaten.[16] In reactie hierop heeft de Staatssecretaris toegezegd dat zij nog voor de zomer van 2018 met een roadmap komt op het gebied van Internet-of-Things.[17] Deze roadmap is op 23 april 2018 aan de Tweede Kamer der Staten-Generaal toegezonden.[18]

## 2. Regulering van cybersecurity

Uit voorgaande introductie blijkt dat in Nederland en Europa verschillende instrumenten worden voorgesteld om cybersecurity te reguleren. De keuze voor deze instrumenten sluit aan bij de indeling van modaliteiten voor regulering van cyberspace die professor Lawrence Lessig onderscheidt in zijn boek Code.[19] Lessig definieert vier modaliteiten die als beperkingen ('constraints') kunnen worden gebruikt om gedrag in cyberspace te reguleren: de markt, de wet, normen en architectuur.[20] Met de modaliteit markt wordt geduid op bijvoorbeeld de marktprijs van virusscanners of beveiligde software die het gedrag van consumenten kan beïnvloeden, terwijl de wet refereert aan cybersecurity wet- en regelgeving, normen aan de maatschappelijke normen die van toepassing zijn (bijvoorbeeld altijd een virusscanner installeren) en architectuur aan bijvoorbeeld het technische ontwerp van hard- en software. Dit laatste wordt ook wel aangeduid als technoregulering.[21] Toepassing van technologie is derhalve niet neutraal, maar speelt – net als bijvoorbeeld wetgeving – een normatieve rol bij het bepalen van menselijk gedrag.[22] In de woorden van Lawrence Lessig: Code is Law.[23] Technoregulering kan daarmee worden gedefinieerd als de bewuste inzet van technologie om gedrag van mensen te reguleren.[24] In het kader van dit artikel zal allereerst nader worden ingegaan op het wetgevingsinstrument als middel om cybersecurity in Nederland en Europa te reguleren. In het vervolg van het artikel zal blijken dat ook technoregulering een grote rol toebedacht krijgt bij het verbeteren van cybersecurity in Nederland en in Europa.

apparaten, sensoren en andere objecten die (vaak verbonden met het Internet), gegevens verzamelen over hun omgeving, deze kunnen uitwisselen en op basis daarvan (semi)autonome beslissingen en/of acties nemen die van invloed zijn op hun omgeving. Deze definitie is overgenomen uit het advies van de Cyber Security Raad, 'Naar een veilig verbonden digitale samenleving', Advies inzake de cybersecurity van het Internet of Things (IoT), december 2017.

11. Staat van de Unie 2017 - Cyberbeveiliging: Commissie versterkt EU-respons op cyberaanvallen, Europese Commissie, Persbericht, Brussel, 19 september 2017, http://europa.eu/rapid/press-release_IP-17-3193_nl.htm.
12. European Commission, Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act'), Brussels, 13.9.2017, COM(2017) 477 final 2017/0225 (COD).
13. Regeerakkoord 'Vertrouwen in de toekomst', Regeerakkoord 2017 - 2021, VVD, CDA, D66 en Christenunie, 10 oktober 2017, p. 3.
14. Nederlandse Cybersecurity Agenda, Nederland digitaal veilig (2018). Bladzijde 27 tot en met 29.
15. Cyber Security Raad, "Naar een veilig verbonden digitale samenleving", Advies inzake de cybersecurity van het Internet of Things (IoT), december 2017.
16. Raad voor Concurrentievermogen, motie van het lid Paternotte, Verhoeven en Van Den Berg, voorgesteld 7 maart 2018, *Kamerstukken II* 2017/18, 21501-30, nr. 422.
17. Raad voor Concurrentievermogen, Verslag van een Algemeen Overleg, vastgesteld 28 maart 2018, *Kamerstukken II* 2017/18, 21 501-30, nr. 427. VAO Raad voor Concurrentievermogen (formeel) op 12 en 13 maart 2018, 7 maart 2018, TK 58.
18. Roadmap Digitaal Veilige Hard- en Software. Deze roadmap is op 23 april 2018 door de Staatssecretaris van Economische Zaken en Klimaat aangeboden aan de voorzitter van de Tweede Kamer der Staten-Generaal, Informatie- en communicatietechnologie, Kamerstukken 2017/18, 26 643, nr. 535.
19. Lawrence Lessig, *Code, Version 2.0*, Basic Books 2006.
20. Ibid. Bladzijde 123.
21. R.E. Leenes, *Harde lessen Apologie van technologie als reguleringsinstrument, Inaugurele rede*, Rede, in aangepaste vorm uitgesproken bij de openbare aanvaarding van het ambt van hoogleraar regulering door technologie aan de Universiteit van Tilburg op 16 april 2010 door prof. dr. Ronald Leenes, versie 1.0, 22 maart 2010.
22. Ronald Leenes, 'Framing Techno-Regulation; an Exploration of State and Non-state Regulation by Technology', *Tilburg Law School Legal Studies Research Paper Series No. 10/2012*, Tilburg University, p. 145.
23. Lawrence Lessig, Code and other laws of cyberspace, Basic Books, 1999.
24. R.E. (Ronald) Leenes, Harde lessen Apologie van technologie als reguleringsinstrument, Inaugurele rede, Rede, in aangepaste vorm uitgesproken bij de openbare aanvaarding van het ambt van hoogleraar regulering door technologie aan de Universiteit van Tilburg op 16 april 2010 door prof. dr. Ronald Leenes, versie 1.0, 22 maart 2010, p. 19 en 20.

## 3. Wet gegevensverwerking en meldplicht cybersecurity (Wgmc)

Op 1 oktober 2017 is de Wgmc in werking getreden.[25] De Wgmc legt taken van het Nationaal Cyber Security Centrum (hierna: NCSC) vast, de bevoegdheden om ten behoeve daarvan persoonsgegevens te verwerken en regelt de vertrouwelijkheid ten aanzien van bij het NCSC berustende gegevens van vitale marktpartijen. Daarnaast bevat art. 6 lid 1 Wgmc een meldplicht voor grote digitale veiligheidsincidenten. Dat artikel stelt dat de vitale aanbieder de minister onverwijld kennis geeft van een inbreuk op de veiligheid of een verlies van integriteit van zijn informatiesysteem waardoor de beschikbaarheid of betrouwbaarheid van een product of dienst in belangrijke mate wordt of kan worden onderbroken. Van een inbreuk op de veiligheid kan bijvoorbeeld sprake zijn in het geval dat een niet-geautoriseerd persoon zich ongeoorloofd toegang heeft verschaft, of zelfs onopzettelijk toegang heeft verkregen, tot het computersysteem of netwerk van de vitale aanbieder. Van een verlies van integriteit kan bijvoorbeeld worden gesproken wanneer een derde in staat is geweest om, ongeoorloofd, informatie die een belangrijke rol speelt in een vitale dienst of een vitaal product toe te voegen, aan te passen of te verwijderen.[26] Die inbreuk of dat verlies van integriteit heeft geleid of kan leiden tot een onderbreking van de beschikbaarheid of de betrouwbaarheid van het product of de dienst. Die feitelijke of potentiële onderbreking moet belangrijk zijn, dus substantieel.[27] Met vitale aanbieder wordt volgens de Wgmc een aanbieder bedoeld van een product of dienst waarvan de beschikbaarheid en betrouwbaarheid van vitaal belang zijn voor de Nederlandse samenleving.[28] De meldplicht is op 1 januari 2018 in werking getreden op basis van het Besluit meldplicht cybersecurity waarin is vastgesteld voor welke vitale aanbieders en producten en diensten zij gaat gelden.[29] Dat zijn drinkwaterbedrijven, netbeheerders in de energiesector, nucleaire bedrijven, financiële instellingen, aanbieders van elektronische communicatienetwerken of -diensten met minimaal 1 miljoen eindgebruikers, een aanbieder van een internetknooppunt met een totale poortcapaciteit van minimaal 8 terabits per seconde, Mainport Rotterdam, Mainport Schiphol en waterkeringen. Over deze meldplicht is eerder in het *Tijdschrift voor Internetrecht* een artikel gepubliceerd.[30]

## 4. Europese Richtlijn voor Beveiliging van Netwerk- en Informatiesystemen (NIB-Richtlijn)

Op 19 juli 2016 is de NIB-Richtlijn gepubliceerd.[31] Deze richtlijn is gericht is op het creëren van een gemeenschappelijk niveau van netwerk- en informatiebeveiliging binnen Europa. Om dit doel te bereiken bevat de NIB-Richtlijn in art. 7 de verplichting voor lidstaten om een nationale strategie voor de beveiliging van netwerk- en informatiesystemen vast te stellen waarin de strategische doelstellingen en passende beleids- en regelgevingsmaatregelen worden vastgesteld met het oog op het tot stand brengen en handhaven van een hoog niveau van beveiliging van netwerk- en informatiesystemen. Daarnaast stellen art. 8 en 9 NIB-Richtlijn dat elke lidstaat een of meerdere Computer Security Incident Response Teams (hierna: CSIRT's) en bevoegde autoriteiten aan moet wijzen, alsmede een centraal contactpunt. Deze CSIRT's, ook wel aangeduid als Computer Emergency Response Teams (CERT's), hebben als taak om te reageren op incidenten en risico's met betrekking tot netwerk- en informatiesystemen en deze zo mogelijk te voorkomen, op te sporen en te verlichten.

In bijlage II van de NIB-Richtlijn zijn de sectoren en deelsectoren opgenomen, waarvoor de lidstaten op basis van art. 5 uiterlijk op 9 november 2018 aanbieders van essentiële diensten (hierna: AED's) met een vestiging op hun grondgebied moeten aanwijzen. Dit zijn de sectoren energie (met deelsectoren elektriciteit, aardolie en gas), vervoer (met deelsectoren luchtvervoer, spoorvervoer, vervoer over water en vervoer over de weg), bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, levering en distributie van drinkwater en digitale infrastructuur. Laatstgenoemde omvat de Internetknooppunten, DNS-dienstverleners en register voor topleveldomeinnamen. Om binnen deze sectoren door een lidstaat als een AED te worden aange-

25. Besluit van 20 september 2017 tot vaststelling van het tijdstip van inwerkingtreding van enkele bepalingen van de Wet gegevensverwerking en meldplicht cybersecurity, *Stb.* 2017, nr. 347.
26. Regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity), Memorie van Toelichting, *Kamerstukken II* 2015/16, 34388, nr. 3, p. 4.
27. Nationaal Cyber Security Centrum, Ministerie van Veiligheid en Justitie, Informatiesheet Wet gegevensverwerking en meldplicht cyber security, september 2017.
28. Wet van 25 juli 2017, houdende regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity), *Stb.* 2017, 316, art. 1.
29. Besluit van 4 december 2017 tot aanwijzing van aanbieders, producten en diensten ten aanzien waarvan een plicht geldt om ernstige ICT-incidenten te melden (Besluit meldplicht cybersecurity), *Stb.* 2017, nr. 476.
30. Mr. S.E.M.A. Abbady en mr. A.P. Koburg, 'De meldplicht cybersecurity', *IR* 2017, nr. 5/6.
31. Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, *PbEU* 2016, L 194/1.

merkt, moet een aanbieder voldoen aan drie criteria die zijn opgenomen in art. 5 lid 2 NIB-richtlijn. Ten eerste moet een entiteit een dienst verlenen die van essentieel belang is voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten. Ten tweede moet de verlening van die dienst afhankelijk zijn van netwerk- en informatiesystemen en ten derde moet een incident aanzienlijke verstorende effecten hebben voor de verlening van die dienst.

Naast aanbieders van essentiële diensten is de NIB-Richtlijn ook van toepassing op digitaledienstverleners (hierna: DSP's), dat wil zeggen aanbieders van online marktplaatsen, online zoekmachines en cloudcomputerdiensten zoals opgenomen in bijlage III van de NIB-Richtlijn. De AED's en DSP's moeten volgens art. 14, respectievelijk art. 16 NIB-Richtlijn passende en evenredige technische en organisatorische maatregelen nemen om hun netwerk- en informatiesystemen te beveiligen tegen inbreuken van buitenaf. Verder moeten zij passende maatregelen treffen om incidenten te voorkomen en, als zich toch incidenten voordoen, de gevolgen daarvan zo veel mogelijk te beperken. Voor AED's is in art. 14 de plicht opgenomen om incidenten met aanzienlijke gevolgen voor de continuïteit van de door hen verleende essentiële diensten onverwijld aan de bevoegde autoriteit of CSIRT te melden. Om te bepalen of een incident aanzienlijke gevolgen heeft, moeten op basis van art. 14 lid 4 met name de volgende parameters in aanmerking worden genomen: het aantal gebruikers dat door de verstoring van de essentiële dienst wordt getroffen, de duur van het incident en de omvang van het geografische gebied dat door het incident is getroffen.
DSP's moeten op basis van art. 16 NIB-Richtlijn ieder incident onverwijld aan de bevoegde autoriteit of CSIRT melden dat substantiële gevolgen heeft voor de verlening van een door hen in de Europese Unie aangeboden dienst(en). Om te bepalen of een incident aanzienlijke gevolgen heeft, moeten volgens de NIB-Richtlijn met name de volgende parameters in aanmerking worden genomen: het aantal gebruikers dat door het incident wordt getroffen, in het bijzonder gebruikers die de dienst nodig hebben voor de verlening van hun eigen diensten, de duur van het incident, de omvang van het geografische gebied dat door het incident is getroffen, de omvang van de verstoring van de werking van de dienst en de omvang van de impact op de economische en maatschappelijke activiteiten. Ten slotte bevatten art. 15 respectievelijk art. 17 bepalingen inzake de uitvoering en handhaving van de aan en AED's en DSP's opgelegde verplichtingen. Voor DSP's heeft de Europese Commissie inmiddels een uitvoeringsverordening gepubliceerd waarin meer specifiek de beveiligingseisen voor deze aanbieders zijn omschreven, alsmede een nadere duiding wanneer er sprake is van incidenten met substantiële gevolgen.[32]

## 5. Cybersecuritywet

Op 14 februari 2018 is een voorstel inzake de Cybersecuritywet naar de Tweede Kamer gestuurd.[33] Het voornaamste doel van de Cybersecuritywet is de implementatie van de NIB-Richtlijn. Eerdergenoemde verplichtingen uit de NIB-Richtlijn zijn overgenomen in het wetsvoorstel voor de Cybersecuritywet. Zo is in art. 5 opgenomen dat aanbieders van een essentiële dienst of categorieën van zodanige aanbieders en andere vitale aanbieders of categorieën van zodanige aanbieders, bij algemene maatregel van bestuur of bij besluit van een bij die maatregel genoemd bestuursorgaan worden aangewezen. Bij de toepassing van deze bepaling moeten art. 5 en 6 NIB-Richtlijn en bijlage II van die richtlijn in acht worden genomen. Voor wat betreft de definitie van DSP's wordt verwezen naar art. 4 NIB-Richtlijn, waarin is vastgelegd dat het online marktplaatsen, online zoekmachines en cloudcomputerdiensten betreft. De reikwijdte van de Cybersecuritywet omvat alle vitale aanbieders, dus zowel AED's als aanbieders van een andere dienst waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving. AED's zijn dus een subgroep van de vitale aanbieders, zoals bedoeld in de Wgmc. Sommige aanbieders zijn geen AED, maar bieden wel een dienst aan waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving. Een voorbeeld hiervan is de Minister van Infrastructuur en Waterstaat als beheerder van waterkeringen.[34]
Vanwege de inhoudelijke samenhang en overlap met de Wgmc wordt deze wet in de Cybersecuritywet geïncorporeerd en ingetrokken. Incidenten met aanzienlijke gevolgen voor de continuïteit van de verleende diensten moeten door vitale aanbieders op basis van art. 10 lid 1 aan het NCSC worden gemeld. Hetzelfde geldt voor de uit de Wgmc overgenomen bepaling dat vitale aanbieders ook inbreuken moeten melden die aanzienlijke gevolgen *kunnen* hebben voor de continuïteit van vitale dienstverlening ('bijna-ongelukken'). In aanvulling

32. European Commission, Commission Implementing Regulation (EU).../... of 30.1.2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact, Brussels, 30.1.2018 C(2018) 471 final.
33. Regels ter implementatie van richtlijn (EU) 2016/1148 (Cybersecuritywet), Voorstel van Wet, *Kamerstukken II* 2017/18, 34 883, nr. 2.
34. Regels ter implementatie van richtlijn (EU) 2016/1148 (Cybersecuritywet), Memorie van Toelichting, *Kamerstukken II* 2017/18, 34 883, nr. 3, p. 7.

hierop bepaalt art. 10 lid 2 dat incidenten met aanzienlijke gevolgen door AED's (en DSP's op basis van art. 13) zowel bij het NCSC/CSIRT als de bevoegde autoriteit moeten worden gemeld. In art. 16 Cybersecuritywet is de mogelijkheid opgenomen van vrijwillige melding van incidenten die aanzienlijke gevolgen hebben en die niet onder de meldplicht voor vitale aanbieders of DSP's vallen.

In de Cybersecuritywet is de Minister van Justitie en Veiligheid als het centrale contactpunt voor Nederland aangewezen. De functies van het CSIRT (advies en bijstand) en de bevoegde autoriteit (toezicht en sancties) zijn in de wet gescheiden waarbij bevoegde autoriteiten per sector worden aangewezen. Het is in eerste instantie aan AED's en DSP's zelf om te bepalen welke concrete beveiligingsmaatregelen voor hen passend en evenredig zijn. Art. 9 geeft de bevoegdheid om desgewenst, bij of krachtens algemene maatregel van bestuur, voor AED's of DSP's nadere regels te stellen over de te treffen beveiligingsmaatregelen. In hoofdstuk 6 van de Cybersecuritywet zijn handhavingsbepalingen opgenomen. Dit betreft de mogelijkheid voor de bevoegde autoriteit om een onafhankelijke beveiligingsaudit te laten uitvoeren, een bindende aanwijzing te geven of een last onder dwangsom of bestuurlijke boete op te leggen. Deze handhavingsbepalingen zijn alleen van kracht voor AED's en DSP's.

Voor vitale aanbieders die niet onder de NIB-Richtlijn vallen, gelden op grond van het wetsvoorstel geen beveiligingseisen en geen toezicht en sancties. Om te bepalen wanneer er sprake is van incidenten met aanzienlijke gevolgen voor vitale diensten, kan de Minister van Justitie en Veiligheid, in overeenstemming met de vakdepartementen en na overleg met de sector, nadere richtsnoeren opstellen. Daarbij wordt aangesloten bij de criteria die in de NIB-Richtlijnen zijn opgenomen.[35] De Minister van Justitie en Veiligheid verwacht dat met betrekking tot AED's niet meer dan 10 tot 20 incidenten per jaar onder de meldplicht zullen vallen. Voor DSP's gaat het volgens de Minister om 15 meldplichtige incidenten per jaar.[36] Inmiddels heeft de Minister van Justitie en Veiligheid de Nota naar aanleiding van het Verslag aan de Tweede Kamer toegezonden, samen met een Nota van Wijziging om gefaseerde inwerkingtreding van het wetsvoorstel mogelijk te maken.[37] In reactie hierop heeft de Vaste Commissie voor Justitie en Veiligheid besloten om het wetsvoorstel aan te melden voor plenaire behandeling.[38]

35. Ibid, p. 41.
36. Ibid, p. 30-31.
37. Regels ter implementatie van richtlijn (EU) 2016/1148 (Cybersecuritywet), Nota naar aanleiding van het Verslag en Nota van Wijziging, *Kamerstukken II* 2017/18, 34 883, nr. 6 en 7.
38. Vaste Commissie voor Justitie en Veiligheid, Besluitenlijst van de procedurevergadering van donderdag van donderdag 26 april 2018.

## 6. Europees kader voor cybersecurity certificeringsschema's

Op 19 september 2017 heeft de Europese Commissie het cybersecurity pakket gepubliceerd.[39] Dit pakket bestaat uit een vijftal voorstellen, te weten (i) de gezamenlijke mededeling weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de Europese Unie,[40] (ii) de mededeling met richtlijnen voor de implementatie van de Europese richtlijn voor Netwerk- en Informatiebeveiliging,[41] (iii) de aanbeveling voor een blauwdruk voor gecoördineerde crisesrespons in het geval van een grootschalige en grensoverschrijdende cyberincident,[42] (iv) de Verordening voor het mandaat voor het Europees agentschap voor netwerk- en informatiebeveiliging (hierna: ENISA) en het Europees kader voor cybersecurity certificering (hierna: Verordening)[43] en (v) het richtlijnvoorstel over de bestrijding van fraude en vervalsing in verband met niet-chartale betaalmiddelen.[44] De Verordening bevat een voorstel voor een Europees kader voor cybersecurity certificeringsschema's. Met dergelijke schema's wordt geduid op een overzicht van regels, technische eisen, standaarden en procedures die zijn gedefinieerd op Europees niveau en betrekking hebben op de certificering van Informatie en Communicatie Technologie (hierna: ICT) producten en diensten.[45] Dergelijke producten en diensten kun-

39. Staat van de Unie 2017 - Cyberbeveiliging: Commissie versterkt EU-respons op cyberaanvallen, Europese Commissie, Persbericht, Brussel, 19 september 2017, http://europa.eu/rapid/press-release_IP-17-3193_nl.htm.
40. European Commission, Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defense: Building strong cybersecurity for the EU, Brussels, 13.9.2017, JOIN(2017) 450 final.
41. European Commission, Communication from the Commission to the European Parliament and the Council, Making the most of NIS - towards the effective implementation of Directive (EU) 2016/ 1148 concerning measures for a high common level of security of network and information systems across the Union.
42. European Commission, Commission Recommendation of 13.9.2017 on Coordinated Response to Large Scale Cybersecurity Incidents an Crises, Brussels, 13.9.2017, C(2017) 6100 final.
43. European Commission, Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act'), Brussels, 13.9.2017, COM(2017) 477 final 2017/0225 (COD).
44. European Commission, Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, Brussels, 13.9.2017, COM(2017) 489 final 2017/0226 (COD).
45. European Commission, Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Com-

nen zowel kritische infrastructuur omvatten als consumentenapparatuur.[46] Een directe aanleiding voor een dergelijk Europees cybersecurity certificeringskader is de opkomst van tientallen miljarden Internet-of-Things apparaten die aan het Internet verbonden zijn en waarvan cybersecurity bij het ontwerp nog geen prioriteit heeft.[47]

*Doelen cybersecurity certificeringsschema's*

Het doel van certificeringsschema's is het vergroten van het vertrouwen in de Europese digitale markt door middel van het verstrekken van transparante informatie over het beveiligingsniveau van ICT-producten en diensten.[48] In aanvulling hierop stelt art. 43 dat Europese cybersecurity certificeringsschema's er voor moeten gaan zorgen dat de ICT-producten en diensten die zijn gecertificeerd op basis van het schema, met een bepaalde mate van zekerheid weerstand kunnen bieden aan: a) acties die tot doel hebben om de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte data te compromitteren en b) acties die erop gericht zijn om functies of diensten te compromitteren die worden aangeboden of toegankelijk worden gemaakt via die producten en diensten. Meer in het bijzonder zijn in art. 45 van de Verordening de veiligheidsdoelen opgenomen die dienen te worden bereikt met behulp van de Europese cybersecurity certificeringsschema's. Het gaat dan met name om het beschermen van data tegen onopzettelijke of ongeautoriseerde opslag, verwerking, vernietiging, verlies en wijziging, het garanderen dat alleen geautoriseerde personen toegang hebben tot data, diensten en functies, het kunnen bieden van een overzicht wie en wanneer toegang heeft gehad tot deze categorieën, het bieden van tijdig herstel van de beschikbaarheid en toegang tot data, diensten en functies in het geval van een fysiek of technisch incident en ten slotte het garanderen dat ICT-producten en diensten zijn voorzien van up-to-date software en van mechanismen voor veilige software updates.

*De aan ICT-producten en diensten gestelde eisen*

De technische vereisten voor ICT-producten en diensten zijn niet in detail opgenomen in de Verordening. Volgens de Europese Commissie zijn ICT-producten en diensten en daaraan gerelateerde cybersecurity-eisen zo divers dat het heel moeilijk is om algemene cybersecurity vereisten te definiëren die geldig zijn voor alle ICT-producten en diensten. Door de Europese Commissie wordt verwezen naar de in art. 43 en 45 opgenomen algemene doelen als richtinggevend kader. De wijzen waarop dergelijke doelen kunnen worden bereikt voor specifieke ICT-producten en diensten moeten dan verder worden gespecificeerd op het niveau van de individuele certificeringsschema's die worden vastgesteld door de Europese Commissie bijvoorbeeld door middel van referentie aan standaarden of technische specificaties.[49] Wel is in art. 47 Verordening een overzicht opgenomen van de elementen die moeten worden opgenomen in de Europese cybersecurity certificeringsschema's. In art. 46 Verordening worden drie beveiligingsniveaus gedefinieerd die kunnen worden opgenomen in een Europees cybersecurity certificeringsschema: basis niveau, substantieel niveau en hoog niveau. Het gaat dan om de zekerheid waarmee de ICT-producten en diensten weerstand kunnen bieden aan acties die tot doel hebben om de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van data, functies of diensten te compromitteren.

*Procedure voor de vaststelling van een Europees cybersecurity certificeringsschema*

In art. 44 Verordening is de procedure opgenomen die moet worden gevolgd bij de voorbereiding en uitvoering van de Europese cybersecurity certificeringsschema's. De eerste stap is dat ENISA, op verzoek van de Europese Commissie, een kandidaat Europees cybersecurity certificeringsschema opstelt. Ook de Europese Cybersecurity Certificering Groep (hierna: ECCG)[50] en individuele lidstaten kunnen een voorstel voor een kandidaat Europees cybersecurity certificeringsschema indienen bij de Europese Commissie. Bij het opstellen van het kandidaat schema moet ENISA alle relevante stakeholders consulteren en nauw samenwerken met de ECCG. Consultatie van de stakeholders zal plaatsvinden via de Permanente Stakeholders Groep waaraan vertegenwoordigers kunnen deelnemen vanuit de ICT-industrie, telecommunicatiesector, consumentengroeperingen, wetenschap, telecommunicatie-toezichthouders en opsporings- en privacy-autoriteiten. De bevoegdheden en samenstelling van de Permanente Stakeholders Groep is opgenomen in art. 20 Verordening. Nadat ENISA

munication Technology cybersecurity certification ('Cybersecurity Act'), Brussels, 13.9.2017, COM(2017) 477 final 2017/0225 (COD). Art. 2, onder (9).

46. European Commission, Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels, 13.9.2017 JOIN(2017) 450 final, p. 4.
47. Ibid, p. 2.
48. European Commission, Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act'), Brussels, 13.9.2017, COM(2017) 477 final 2017/0225 (COD). Overweging 5.
49. European Commission, Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act'), Brussels, 13.9.2017, COM(2017) 477 final 2017/0225 (COD), p. 32.
50. In art. 53 Verordening is opgenomen dat de Europese Cybersecurity Certificering Groep (ECCG) is samengesteld uit nationale certificeringstoezichthouders. De ECCG heeft een adviserende en ondersteunende rol voor de Commissie en kan voorstellen doen aan de Commissie voor de ontwikkeling van een schema.

het voorstel voor een Europees cybersecurity certificeringsschema aan de Europese Commissie heeft toegezonden, kan de laatstgenoemde zogenaamde uitvoeringsverordeningen vaststellen. Ook kan de Europese Commissie algemene of sectorspecifieke cybersecurity richtlijnen publiceren, bijvoorbeeld op het gebied van goede cybersecurity praktijken of verantwoordelijk cybersecurity gedrag.[51] Nadat certificeringsschema's zijn vastgesteld, kunnen fabrikanten van ICT-producten en diensten een verzoek voor certificering van hun producten en diensten indienen bij de zogenaamde nationale conformiteitsbeoordelingsinstantie die het verzoek zal beoordelen. Het aanvragen hiervan gebeurt op vrijwillige basis. Nationale certificeringstoezichthouders zullen toezicht houden op de nationale conformiteitsbeoordelingsinstanties. De taken en bevoegdheden van beide instanties zijn opgenomen in art. 51 respectievelijk art. 50 Verordening. Wanneer er voor een product of dienst een Europees certificeringsschema wordt vastgesteld zullen bestaande nationale schema's vervallen.[52]

*ICT-producten en diensten die onderdeel kunnen zijn van een schema*

In de gezamenlijke Mededeling worden ten aanzien van de producten, diensten en systemen drie prioriteitsgebieden benoemd.[53] Ten eerste kritische of hoge risico applicaties, dat wil zeggen systemen, waarvan we afhankelijk zijn in onze dagelijkse activiteiten. Dit zijn bijvoorbeeld auto's en machines in fabrieken, variërend van grote systemen zoals vliegtuigen en energiecentrales tot kleine systemen zoals medische apparaten. Deze apparaten worden steeds meer digitaal en met het internet verbonden. ICT-componenten in dergelijke producten en systemen moeten derhalve worden onderworpen aan rigoureuze veiligheidstesten. Ten tweede breed uitgerolde producten, netwerken, systemen en diensten die worden gebruikt in de publieke en private sector ter verdediging tegen cyberaanvallen zoals email encryptie, firewalls en virtual private networks. Het is volgens de Europese Commissie belangrijk dat de verspreiding en het gebruik van dergelijke instrumenten niet leidt tot nieuwe bronnen van risico's of kwetsbaarheden. Ten slotte het gebruik van 'Security by Design'-methoden in goedkope, digitale, aan het internet verbonden massa consumenten apparaten die onderdeel vormen van het Internet-of-Things. Certificeringsschema's kunnen worden gebruikt om te zorgen dat de producten die worden ontworpen, gebruikmaken van state of the art ontwikkelingsmethodes, dat ze onderhevig zijn geweest aan adequate veiligheidstesten en dat de verkopers instemmen met het updaten van hun software in geval van nieuw ontwikkelde kwetsbaarheden of dreigingen. 'Security by Design' zou ook onderdeel kunnen zijn van een zorgplicht voor aanbieders van dergelijke producten, diensten of systemen. Hierbij zou ook productaansprakelijkheid een rol kunnen spelen.[54]

## 7. Conclusie: van wetgeving naar technoregulering

De afgelopen jaren is een aantal wetsvoorstellen gepubliceerd om zowel in Nederland als in Europa de cybersecurity te reguleren. Deze wetten richten zich met name op aanbieders van vitale en essentiële diensten. Aangezien cyberspace geen grenzen kent, zouden ook wereldwijd afspraken gemaakt moeten worden over de cybersecurity regulering van dergelijke aanbieders. Soortgelijke afspraken zijn wereldwijd al wel in gang gezet op het gebied van cyber oorlogsvoering,[55] maar nog niet op het gebied van vitale infrastructuur of van aanbieders van vitale diensten. Het aanwijzen van aanbieders van vitale en/of essentiële diensten blijft daarmee vooralsnog een nationale aangelegenheid, omdat de NIB-richtlijn de bevoegdheid daartoe op basis van art. 5 lid 1 neerlegt bij de lidstaten.

Voor wat betreft de Nederlandse cybersecurity wetgeving is opvallend dat, vooruitlopend op de definitieve publicatie van de Europese NIB-Richtlijn in de zomer van 2016, het Nederlandse kabinet reeds in het begin van 2016 heeft besloten om de Wgmc naar de Tweede Kamer te sturen. Als gevolg hiervan zijn er in korte tijd twee soortgelijke wetsvoorstellen naar de Tweede Kamer gezonden. Ten eerste de Wgmc die reeds in werking is getreden en voor een aantal door Nederland gedefinieerde vitale

51. European Commission, Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act'), Brussels, 13.9.2017, COM(2017) 477 final 2017/0225 (COD), p. 34.
52. European Commission, Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act'), Brussels, 13.9.2017, COM(2017) 477 final 2017/0225 (COD), p. 12 en 33.
53. European Commission, Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels, 13.9.2017 JOIN(2017) 450 final, p. 5.
54. Ibid, p. 6.
55. Zie onder andere de Talinn Manual, een academische, niet bindende studie over de toepassing van internationaal recht ten aanzien van cyberconflicten en cyberoorlogsvoering (https://en.wikipedia.org/wiki/Tallinn_Manual). Ook heeft een werkgroep van de Verenigde Naties in 2013 een rapport gepubliceerd over de toepassing van internationaal recht op cyberaanvallen ('Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, General Assembly of United Nations, Sixty-eighth session, item 94 of the provisional agenda, Developments in the field of information and telecommunications in the context of international security, 24th June 2013').

aanbieders de verplichting bevat om ernstige inbreuk op de veiligheid van informatiesystemen bij het NCSC te melden, gevolgd door een voorstel voor een Cybersecuritywet die soortgelijke verplichtingen omvat voor een grotere groep vitale aanbieders, waaronder AED's en DSP's, zoals in de Europese NIB-Richtlijn gedefinieerd. Nederland had kunnen wachten met het indienen van de Wgmc totdat de NIB-Richtlijn zou zijn vastgesteld, zodat de bepalingen van de Wgmc en Cybersecuritywet in een gezamenlijk wetsvoorstel aan de Tweede Kamer zouden kunnen worden voorgelegd. De reden dat het wetsvoorstel Wgmc in het voorjaar van 2016 toch naar de Tweede Kamer is gestuurd, is waarschijnlijk dat dit wetsvoorstel reeds lange tijd in voorbereiding was. Een meldplicht voor inbreuken op de veiligheid en/of integriteit van informatiesystemen is namelijk reeds in 2012 aangekondigd door de Minister van Veiligheid en Justitie.[56] De toezegging volgde op een eerder verzoek hieromtrent vanuit de Tweede Kamer.[57] Ook is begin 2015 een eerdere versie van het wetsvoorstel reeds onderwerp geweest van een internetconsultatie. Bovendien bevat de Wgmc bepalingen ten aanzien van de taken van het NCSC en het uitwisselen van vertrouwelijke gegevens met vitale marktpartijen, die de Minister van Veiligheid en Justitie waarschijnlijk zo snel mogelijk in werking wilde laten treden.

Daarnaast is opvallend dat als reactie op de opkomst van het Internet-of-Things veel waarde wordt gehecht aan certificering van ICT-producten en -diensten. Zo is in het Europese cybersecurity pakket een voorstel opgenomen voor een Verordening inzake een Europees kader voor cybersecurity certificeringsschema's. Onduidelijk is hoe dit voorstel zich verhoudt tot de reeds bekende ISO-standaarden op het gebied van cybersecurity en risicomanagement.[58] In de Verordening wordt namelijk niet verwezen naar deze ISO-standaarden. Het gebruik van deze cybersecurity certificeringsschema's kan worden beschouwd als technoregulering, in de zin dat technische eisen ten aanzien van de producten en diensten, opzettelijk worden gebruikt om menselijk gedrag te reguleren. Deze aanpak sluit aan bij het concept van 'Security by Design' dat ook expliciet als maatregel wordt genoemd door de Europese Commissie als onderdeel van een gezamenlijk initiatief tussen de Europese Commissie en de industrie.[59] Het voorstel voor certificering van Internet-of-Things is ook terug te vinden in het recente advies van de Nederlandse Cyber Security Raad. Opvallend is dat de Nederlandse politiek op dit punt nog een stap verder gaat dan de Europese Commissie en de certificering *verplicht* wil stellen voor alle ICT-producten en -diensten. De Staatssecretaris van Economische Zaken en Klimaat heeft deze wens overgenomen.

Ten slotte resteert nog de vraag hoe het voorstel voor cybersecurity certificeringsschema's in de praktijk vorm zal krijgen. Ten eerste zullen per lidstaat conformiteitsbeoordelingsinstanties (voor Nederland waarschijnlijk NEN) en nationale certificeringstoezichthouders moeten worden aangewezen. Dat roept ten eerste de vraag op welke procedure dient te worden gevolgd bij de door de nationale beoordelingsinstanties afgegeven goedkeuringen voor ICT-producten en -diensten die onder een door de Europese Commissie vastgesteld cybersecurity certificeringsschema vallen. De reikwijdte van de goedkeuringen beslaat de gehele Europese Unie, dat wil zeggen dat bijvoorbeeld een door een Franse conformiteitsbeoordelingsinstantie afgegeven goedkeuring ook geldig is in Nederland. Indien in Nederland een klacht wordt ingediend over het desbetreffende product of dienst bij de nationale certificeringstoezichthouder, kan deze dan toezicht uitoefenen of moet de Nederlandse toezichthouder in dat geval doorverwijzen naar zijn Franse collega, ook als Nederlandse consumenten zijn getroffen? Daarnaast zal moeten worden bepaald voor welke waarschijnlijk miljoenen ICT-producten en -diensten in Europa certificeringsschema's dienen te worden opgesteld. Dat lijkt een ambitieus project. Daarbij is ook de vraag of het Europese kader ruimte biedt aan de nu breed geaccepteerde praktijk van bedrijven om zogenaamde beta-versies ('testversies') van softwareprogramma's op de markt te brengen. Ook is nog onduidelijk of voor elke nieuwe release van een softwareprogramma een nieuw certificaat moet worden aangevraagd. Daarnaast vraagt het tegengaan van illegale, dat wil zeggen niet-gecertificeerde, ICT-producten en -diensten die wel onder een schema vallen, een aanzienlijke nationale en Europese handhavingsinspanning. Ook en met name voor wat betreft de import van dergelijke illegale ICT-producten en -diensten in Europa.

Enerzijds schept het Europese kader voor cybersecurity certificeringsschema's het beeld van een zeer ambitieus (administratief) project. Anderzijds geldt certificering nu reeds voor een groot aantal producten en diensten in onze samenleving en is er dus niets nieuws onder de zon. Ook de Europese Algemene Verordening Gegevensbescherming (hierna: AVG) die met ingang van 25 mei 2018 in werking zal treden, kent in art. 42 de mogelijkheid van certificering. Met een AVG-certificaat kan een verantwoordelijke of verwerker aantonen dat de

56. Informatie- en communicatietechnologie (ICT), Brief van de Minister van Veiligheid en Justitie aan de Tweede Kamer der Staten-Generaal, Den Haag, 6 juli 2012, *Kamerstukken II* 2011/12, 26 643, nr. 247.
57. Informatie- en communicatietechnologie (ICT), Motie van het Lid Hennis-Plasschaert C.S., voorgesteld 13 oktober 2011, *Kamerstukken II* 2011/12, 26 643, nr. 202.
58. Zie bijvoorbeeld NEN-ISO/IEC 27001: Managementsystemen voor informatiebeveiliging, NEN-ISO/IEC 27002: Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging, NEN-ISO/IEC 27005: Information security risk management en NEN-ISO 31000 Risicomanagement – Richtlijnen.
59. European Commission, Joint Communication to the European parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels, 13.9.2017, JOIN(2017) 450 final, p. 12.

persoonsgegevens, die worden verwerkt door de verantwoordelijke of de bewerker volgens de regels van de AVG worden verwerkt.[60] Het voorstel voor cybersecurity certificeringsschema's sluit derhalve aan bij soortgelijke initiatieven op Europees niveau. Vanuit dat perspectief ligt het voor de hand dat het wiel niet helemaal opnieuw hoeft te worden uitgevonden en met beperkte administratieve inspanningen een separaat kader voor cybersecurity certificeringsschema's kan worden opgesteld en uitgevoerd. Als eerstvolgende stap zal in elk geval de Verordening waarin het voorstel voor cybersecurity certificeringsschema's is opgenomen, door het Europees Parlement worden besproken. Dat zal waarschijnlijk nog tot de nodige wijzigingen leiden. Wordt vervolgd.

60. Regels ter uitvoering van 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) (Uitvoeringswet Algemene verordening gegevensbescherming), Nota naar aanleiding van het verslag, ontvangen 14 februari 2018, *Kamerstukken II* 2017/18, 34 851, nr. 7, p. 53.

# Het recht geketend: Smart contracts: dé oplossing voor gezeur, gedoe en onzekerheid?

*mr. M. van der Linden*[1]

## 1. Inleiding

Smart contracts: dé oplossing voor alle problemen? Wie wil dat nou niet. Of is het alleen maar 'gekkigheid', waar een paar enthousiastelingen veel aandacht mee genereren en geld mee verdienen? Of iets daar tussenin: het heeft bepaalde voordelen en soms is het handig? Als oudere jongere neig ik naar dat laatste; bekijk ik dit soort nieuwe ontwikkelingen met de nodige scepsis. Lijkt het niet verdacht veel op oude wijn in nieuwe zakken? Ik wil het eigenlijk tot op het bot begrijpen voordat ik me aan een oordeel waag.

In dit artikel wil ik de lezer meenemen in mijn zoektocht naar wat ik nou moet vinden van zogenaamde smart contracts, geïmplementeerd op de blockchain. Ik probeer door alle ronkend enthousiaste praatjes, ongefundeerde claims en in mooie woorden vermomde onwetendheid te achterhalen wát het nou écht is en hoe het nou écht werkt. Vervolgens wil ik proberen te bedenken waarom contractspartijen hun overeenkomst op deze manier vorm zouden willen geven. En wat mogelijke andere bruikbare manieren kunnen zijn om deze technologie te gebruiken. Onvermijdelijk stuiten we op vragen die we samenvegen onder de noemer 'uitdagingen voor het recht'. Die zal ik in dit artikel alleen aanduiden, in een volgend artikel probeer ik ze in kaart te brengen.

## 2. Hoe werkt het

Een smart contract is een blockchain-toepassing. Dus om te kunnen begrijpen hoe het werkt moeten we de techniek van de blockchain induiken.

Zoals ieder stuk over privacy begint met Warren en Brandeis, zo begint een blockchain-verhandeling altijd met het verhaal van Satoshi Nakamoto. En daar hebben we meteen een kenmerk te pakken: anonimiteit. Satoshi Nakamoto is een pseudoniem, en niemand (behalve de persoon of personen in kwestie zelf natuurlijk) weet zeker wie erachter zit.

Satoshi Nakamoto schreef in 2008 een paper dat beschouwd kan worden als het eindpunt van de jarenlange zoektocht naar een manier om anoniem en betrouwbaar via internet te kunnen betalen,[2] en het beginpunt van de ontwikkeling van blockchain.[3] Betalen via internet werd eigenlijk pas verrassend laat mogelijk met diensten als PayPal en (in Nederland) iDeal. Daarvoor was er alleen de betaling met een creditcard – ontoegankelijk (want niet iedereen heeft zomaar een creditcard), duur en riskant voor beide partijen. Een tussenpersoon (bank of andere financiële dienstverlener) was dus altijd nodig: een zogenaamde trusted third party (TTP). Die trust in die third party was niet altijd van harte, maar je moest wel, er was immers geen keuze. En in 2008 bleek dat dat vertrouwen niet altijd terecht was – en de ruggegraat van onze economie moest in het algemeen belang, en dus met publieke middelen, overeind gehouden worden. En bovendien is een TTP kwetsbaar voor hacken en dDos aanvallen en zo.

In de fysieke wereld kunnen we contant betalen: snel, efficiënt,[4] anoniem. Zoals we uit de privacy literatuur weten is anonimiteit niet alleen nuttig als je iets te verbergen hebt, maar ook als jouw identiteit niet relevant is. En door de fysieke verschijningsvorm van contant geld (munten of bankbiljet-

1. Tina van der Linden is universitair docent Law Ethics and Technology aan de Vrije Universiteit Amsterdam en redacteur van dit blad.

2. Zie onder andere: R.C. Merkle, 'Protocols for public key cryptosystems', in: *Security and Privacy*, 1980 IEEE Symposium on (p. 122-122). IEEE. (https://www.researchgate.net/profile/Ralph_Merkle/publication/220713913_Protocols_for_Public_Key_Cryptosystems/links/00b495384ecda07784000000/Protocols-for-Public-Key-Cryptosystems.pdf); D. Chaum, (1983) 'Blind Signatures for Untraceable Payments', in: D. Chaum, R.L. Rivest & A.T. Sherma. (eds), *Advances in Cryptology*, Boston: Springer, MA (https://doi.org/10.1007/978-1-4757-0602-4_18); W. Dai, 'b-money,' http://www.weidai.com/bmoney.txt, 1998; F.D. Garcia & J.H. Hoepman (2005), 'Off-Line Karma: A Decentralized Currency for Peer-to-peer and Grid Applications', in: J. Ioannidis, A. Keromytis & M. Yung (eds), *Applied Cryptography and Network Security*, ACNS 2005. Lecture Notes in Computer Science, vol 3531. Berlin: Springer, Heidelberg (https://doi.org/10.1007/11496137_25).
3. S. Nakamoto,(2008), *Bitcoin: A peer-to-peer electronic cash system*, https://bitcoin.org/bitcoin.pdf.
4. Lage transactiekosten behalve als je grote hoeveelheden muntjes op je bankrekening wilt zetten.

ten) kun je hetzelfde geld niet twee keer uitgeven. Dit 'double spending problem' was de grote uitdaging voor internetgeld: natuurlijk kun je reeksen van codes maken en afspreken om daar een bepaalde waarde aan toe te kennen, maar hoe weet je zeker dat de codes die jij ontvangt niet al eerder door dezelfde persoon uitgegeven zijn om bij iemand anders ook iets te kopen? Tom Poes verzin een list. Satoshi Nakamoto verzon de blockchain door drie al langer bestaande technieken te combineren: peer-to-peer technologie, asymmetrische encryptie en hashing.

Peer-to-peer technologie is vooral bekend uit de file-sharing wereld: er is geen centraal knooppunt maar een netwerk van deelnemers, zogenaamde peers, die allemaal potentieel met elkaar verbonden zijn. In theorie zijn alle peers gelijkwaardig.

Asymmetrische encryptie maakt gebruik van een briljante wiskundige truc: een manier om gegevens te versleutelen met de ene sleutel, waarbij die gegevens uitsluitend met de andere sleutel te ontsleutelen zijn, en tegelijkertijd die twee sleutels (die uiteraard wel aan elkaar gerelateerd zijn) niet uit elkaar te herleiden zijn.

Hashing is een manier om gegevens te verzegelen. Door een bewerking op een verzameling van gegevens los te laten wordt een zogenaamde hash gecreëerd, een code. Elke wijziging in de gegevens, ook al is die nog zo miniem, resulteert in een totaal andere hash-code. Kortom een correcte hash garandeert dat de gegevens ongewijzigd zijn.

Het werkt dan conceptueel als volgt. De transacties in het netwerk van deelnemende peers worden bloksgewijs vastgelegd in een traditioneel grootboek, in digitale vorm natuurlijk. Alle peers hebben de complete versie van dit grootboek op hun computer staan. Dat is de uitgangspositie.

Dan vinden er transacties plaats tussen de peers. De ene peer betaalt aan de andere door een bericht het netwerk in te sturen (dus naar alle peers), versleuteld met asymmetrische encryptie, met als inhoud dat zij een bepaald bedrag aan die ander betaalt. Dat kan natuurlijk alleen als zij ook minimaal over dat bedrag beschikt. En dat kan aan de hand van het grootboek door alle peers in het netwerk geverifieerd worden.

Een aantal geverifieerde (en dus goedgekeurde) transacties wordt samengevoegd tot een nieuw blok, dat aan het grootboek wordt toegevoegd. Dát is wat 'minen' genoemd wordt: een nieuw blokje 'vinden' en vastklikken als de nieuwe schakel aan het al bestaande grootboek. Dat houdt in dat je een nieuwe hash moet vinden. De gegevens voor die nieuwe hash omvatten: de hash van het vorige blok (zo weet je zeker dat het 'past'), de verzameling van goedgekeurde transacties van dit blok, én een getal genaamd 'nonce', number used once. De resulterende hash moet onder een bepaald maximum uitkomen, die steeds lager wordt, zodat het steeds moeilijker wordt om er nog onderdoor te komen. Minen komt dus neer op het eindeloos uitproberen van getallen als nonce, totdat je er eentje hebt die, samen met de andere gegevens uit het blok, resulteert in een hash die laag genoeg is. Het is net als met het oplossen van een Sudoku: het vinden van de oplossing is lastig en vergt veel doorzettingsvermogen en een beetje geluk, maar het vaststellen dat de gevonden oplossing de juiste is, is een eitje. Minen kost dus veel, en steeds meer, rekenkracht, en daarmee elektriciteit: 'proof-of-work'. Maar het levert ook wat op: een beloning in de digitale valuta van de desbetreffende blockchain.

Het nieuwe blok wordt toegevoegd aan de ketting, het grootboek wordt bijgewerkt, alle peers ontvangen de nieuwe versie en het verhaal kan van voren af aan beginnen. Blockchain is dus: een manier om data op te slaan, gedistribueerd in een peer-to-peer netwerk met asymmetrische encryptie en hashing als beveiliging. En het kan gebruikt worden voor toepassingen waarbij het gaat om overdracht van zaken die een bepaalde waarde vertegenwoordigen: niet alleen cryptocurrencies (digitale valuta), maar ook andere handelsobjecten – en dan hebben we het over smart contracts.

En zo zijn de grote uitdagingen van betalen via internet opgelost. Het kan anoniem, althans pseudoniem, via een account in het netwerk – dat natuurlijk aan het IP-adres van een computer gekoppeld is maar dat is vrij eenvoudig te maskeren. Het double spending-probleem is opgelost omdat alleen geverifieerde transacties doorgang vinden. Trusted third parties zijn niet meer nodig: in het netwerk van peers wordt het vertrouwen gecreëerd door de onomstotelijkheid van waterdichte encryptie en hashes. Iedereen blij. Of toch niet?

Nakamoto introduceerde met zijn paper de eerste toepassing van blockchain-technologie: de Bitcoin. Een op de internet-infrastructuur gebaseerde manier om peer-to-peer, anoniem en wereldwijd waarde over te dragen. Waar wordt dat, natuurlijk, in eerste instantie en vooral voor gebruikt? Natuurlijk voor transacties die het daglicht niet kunnen verdragen (drugs, wapens, kinderporno), voor afpersing (Wannacry), voor witwassen van crimineel geld. Er zijn geen banken bij betrokken, het is anoniem en wereldwijd, dus er is niet echt een aanknopingspunt voor handhaving van een nationaal rechtssysteem of financieel toezicht. Grillig koersverloop trekt speculanten aan waardoor Bitcoin tot een soort piramidespel wordt. Bitcoin exchanges (wisselkantoren) en handelsplatformen op het Dark Web worden opgerold, verdwijnen in het niets – criminelen zijn niet te vertrouwen.[5] En natuurlijk, de Bitcoin blockchain is pas de eerste toepassing van deze techniek, dus de techniek is ook nog lang niet uitontwikkeld en kan op veel punten gewijzigd en verbeterd worden.

*Verdere ontwikkeling*

Op het basisidee van gedistribueerde gegevensopslag van versleutelde transacties die via hashes rotsvast aan elkaar gelinkt zijn, zijn natuurlijk variaties en daarmee andere toepassingen mogelijk.

5. D. Gerard, 'Attack of the 50 Foot Blockchain: Bitcoin, Blockchain', *Ethereum & Smart Contracts, CreateSpace*: Independent Publishing Platform 2017.

Om te beginnen hoef je natuurlijk niet zomaar iedereen toe te laten tot jouw blockchain. Je kunt best een eigen clubje oprichten, met een eigen blockchain en een toelatingsprocedure voor nieuwe peers. Je kunt de blockchain dan precies zo inrichten als voor de door jou beoogde toepassing ideaal is, sommigen mogen de blockchain alleen raadplegen, anderen mogen ook wijzigingen aanbrengen die door andere peers goedgekeurd moeten worden. Een poging om het beste van twee werelden te combineren: niet de totale chaos van anonimiteit die de bescherming van het recht moet ontberen, maar wel het voordeel van robuuste gedistribueerde gegevensopslag. Dat is een permissioned blockchain, het tegenovergestelde van een permissionles of openbare blockchain.

Er zijn ook alternatieven bedacht voor het energie-slurpende en daardoor niet meer ecologisch verantwoorde proof-of-work minen, zoals proof-of-stake. Niet de rekenkracht maar de hoeveelheid cryptocurrency die een peer al heeft is dan bepalend voor het kunnen toevoegen van een nieuw blok.

En via een blockchain kun je niet alleen betalingen in en saldi van cryptocurrency bijhouden, maar op het grootboek kunnen ook rechten op allerlei zaken geregistreerd, bijgehouden en eventueel overgedragen worden. En zo gaan we naadloos over naar wat 'smart contracting' genoemd wordt: het gebruik van blockchaintechnologie voor het bijhouden van rechten op waardevolle zaken en voor het afhandelen van transacties met betrekking tot die waardevolle zaken.

*Smart contracts*

De term 'smart contracts' is volgens mij misleidend en onjuist. Het gaat volgens mij niet over contracten, maar over de geautomatiseerde uitvoering van eerdere afspraken tussen partijen. Of het gaat over een soort openbaar aanbod, dat je kunt aanvaarden door een bepaalde actie te verrichten (normaal gesproken: betalen). Vergelijkbaar met een frisdrankautomaat.[6] De overeenkomst ontstaat dan door de actie (acceptatie) van de wederpartij.

En in mijn optiek is er niets 'smarts' aan de ijzeren-heinige, rücksichtslose uitvoering van een computerprogramma – zeker niet in vergelijking mensen die met goedschiks of kwaadschiks gebruik van hun gezonde verstand al dan niet aan hun contractuele verplichtingen voldoen. Maar goed, het is een inmiddels ingeburgerde term en hij bekt lekker, dus daar houden we het maar bij.[7]

Een smart contract is een computerprogramma. Zo'n programma is opgebouwd uit een aantal regels in een 'als - dan' vorm: als aan bepaalde condities voldaan is volgt een bepaalde actie. Bijvoorbeeld: als een betaling ontvangen is, wordt een bepaalde zaak geleverd (of andersom). Dat programma 'is' dan een account op een blockchain. Het account heeft een bepaald bedrag in de valuta van de desbetreffende blockchain en handelt precies zoals het geprogrammeerd is. Voor gebeurtenissen die een bepaalde conditie moeten triggeren die niet door het programma zelf vastgesteld kunnen worden kunnen zogenaamde Oracles gebruikt worden: instanties of mensen die geautoriseerd zijn om bepaalde feitelijke vaststellingen te doen (daar zijn ze weer: deTTP's!).

Eenmaal losgelaten op de blockchain is de executie van zo'n programma niet te stoppen. Als de condities zich voordoen, dan zal de actie volgen, wat er ook verder aan de hand is. Voor foutjes en fouten, wilsgebreken, gewijzigde omstandigheden, voortschrijdend inzicht en al dat soort flauwekul is geen plaats. Tenuitvoerlegging is automatisch en dus gegarandeerd. Zo kun je met onbekende partijen over de hele wereld zaken doen, zonder bankgaranties of bemoeienis anderszins van TTP's.

## 3. Waarom zou je 't doen?

Dat zijn meteen de voordelen: ouderwetse, dure en inefficiënte tussenpersonen zoals banken, notarissen en andere juristen zijn overbodig. Nakoming is gegarandeerd, het is in zekere zin veilig en transparant. De nadelen zijn het spiegelbeeld hiervan: er is ook geen derde partij meer om op terug te vallen, nakoming kan niet worden tegengehouden.

Bij smart contracts wordt door de term alleen al in de eerste plaats gedacht aan privaatrechtelijke toepassingen, in de sfeer van de uitvoeringen van overeenkomsten. Maar als het gaat over het bijhouden van rechten op zaken, of het triggeren van verplichtingen door bepaalde gebeurtenissen, dan zijn er misschien ook nuttige publiekrechtelijke toepassingen. Ik denk aan het bijhouden van het kadaster, of het ontstaan van betalingsverplichtingen (bijvoorbeeld belasting of heffingen) die ontstaan bij bepaalde feitelijke handelingen (parkeren, afval genereren). Dat opent misschien de mogelijkheid voor bepaalde bestuursrechtelijke toepassingen?

We hebben deze discussie, zij het in iets andere termen, eerder gehad. In de jaren '90 van de vorige eeuw waren er bij sommigen hooggespannen verwachtingen van gebruik van zogenaamde juri-

6. Een vergelijking die ook Nick Szabo, die de term smart contract voor het eerst gebruikte, maakt. Zie Nick Szabo, The Idea of Smart Contracts, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html.
7. Smart Contract Werkgroep, Smart contracts als specifieke toepassing van de blockchain-technologie, Dutch Blockchain Coalition, (https://www.dutchdigitaldelta.nl/uploads/pdf/Smart-contract-rapport-DBC.pdf). Can smart contracts be legally binding contracts? An R3 and Norton Rose Fulbright White paper, http://www.nortonrosefulbright.com/files/r3-and-norton-rose-fulbright-white-paper-full-report-144581.pdf. Whitepaper Juridische aspecten van Blockchain, Pels Rijcken, aan te vragen via https://www.pelsrijcken.nl/actueel/publicaties/whitepaper-juridische-aspecten-van-blockchain/. E. Tjong Tjin Tai, 'Smart contracts en het recht', *NJB* 2017, 92(3), 176-183. [146].

dische kennissystemen of expertsystemen.[8] Juridisch redeneren zou gereduceerd kunnen worden tot toepassing van vergelijkbare als .. dan regels. Rechtsregels zouden geformaliseerd kunnen worden in deze zogenaamde productieregels, en de jurisprudentie waarin deze regels uitgelegd en toegepast worden zou als grondstof voor zelflerende systemen op basis van deze regels gebruikt kunnen worden zodat ze mee kunnen evolueren met de rechtsontwikkeling.[9] Ook toen werd door sommigen betoogd dat het recht zich niet laat vangen in productieregels, dat er zogenaamde hard cases zijn die een menselijke beoordeling vergen, en dat het onderscheid tussen clear en hard cases niet door een geautomatiseerd systeem zelf gemaakt kan worden.[10] Met verwijzing naar de discussie tussen Hart en Dworkin over de bepaaldheid van het recht en de rol van morele argumenten (die wel of niet tot het rechtssysteem zelf behoren) bij de toepassing van rechtsregels.[11]

Hoewel de overspannen verwachtingen over juridische expertsystemen niet helemaal waargemaakt werden, hebben computerprogramma's natuurlijk toch hun intrede gedaan in de rechtstoepassing.[12] Niet alleen ter ondersteuning van administratieve processen, maar ook om beslissingen te nemen met rechtsgevolgen. Tegenwoordig wordt daar ook weer voorzichtig de term AI bij gebruikt, en de fancy newspeak term is dan 'legal tech'.

Maar dan hebben we het nog steeds 'gewoon' over het inzetten van een computerprogramma bij het uitvoeren of toepassen van regels – hetzij publiekrechtelijke regels hetzij regels zoals die voortkomen uit een privaatrechtelijke overeenkomst. Waarom zou je het computerprogramma dat die regels uitvoert dan wel toepast in hemelsnaam als smart contract op een blockchain implementeren?

Omdat de voordelen die implementatie als smart contract met zich meebrengt voor sommige toepassingen belangrijk zijn. De voordelen kwamen hierboven al even aan de orde: geen afhankelijkheid van een TTP, transparantie, nakoming is gegarandeerd. Je kunt dan denken aan toepassingen als verzekeringen,[13] peer-to-peer lending,[14] crowdfunding,[15] vastgoedbeleggingen,[16] IE-licenties,[17] en bijhouden van zorg-administratie.[18] Misschien zijn er voor dat soort toepassingen inderdaad goede redenen om smart contracts te gebruiken – al vraag ik me soms wel af of het niet beter en gemakkelijker zonder blockchain zou kunnen. Maar goed, dat is aan de vrije markt om uit te proberen – wellicht een uitgelezen kans voor slimmeriken met een briljant idee om snel rijk te worden?

Een moeilijk punt bij smart contracts is de verbinding met de fysieke wereld. Als er Oracles nodig zijn om een bepaalde actie te triggeren, ben je in zekere zin toch weer overgeleverd aan TTP's met risico's van fraude en hacking. Maar als de verbinding met de fysieke wereld nou met behulp van apparaten gelegd kan worden die tegenwoordig met de term 'Internet of Things' (IoT) aangeduid worden, dan opent zich wellicht wel een scala aan mogelijkheden. We pakken onze glazen bol erbij.

Het standaardvoorbeeld van IoT dat meteen bij mij opkomt is de smart koelkast die op het moment dat de voorraad van een of ander artikel (bier of cherrytomaatjes) onder een bepaald minimum komt (en dat weet de koelkast omdat alle verpakking zijn uitgerust met een RFID-chip) automatisch een bestelling doorgeeft zodat later die dag de bezorgdienst van de supermarkt (jongeman op een vrachtwagen òf wellicht een automatisch bezorgkarretje of drone) zorgt dat alles weer goed komt. Prima, leuk – maar waarom zou je zoiets op een blockchain doen? Spreek dat gewoon lekker af met je plaatselijke supermarkt.[19]

De blockchain komt van pas als je ook met onbekenden zaken wilt kunnen doen, via zo'n openbaar-aanbod-smart contract. In plaats van een schaarse parkeerplaats bezet te houden kan de

8. A.W. Koers, *Juridische Informatica, Spelen met de computer, of spelen met het recht, Inaugurele Rede*, Alphen aan den Rijn: Samsom H.D. Tjeenk Willink 1987; H.J. van den Herik, *Kunnen computers rechtspreken? Inaugurele Rede*, Arnhem: Gouda Quint 1991.
9. Zie onder andere A. van der Lieth Gardner, *An Artificial Intelligence Approach to Legal Reasoning*, Cambrigdge, Massachusetts: The MIT Press 1987; J.C. Hage, 'Themis als robot, Juridische expertsystemen tussen trivialiteit en onbetrouwbaarheid', *RM Themis* 1987, pp. 238-248; H. Prakken, *Logical tools for modelling legal arguments*, proefschrift VU Amsterdam, 1993; Arno R. Lodder, DiaLaw, On legal justification and dialog games, proefschrift Universiteit Maastricht, 1998; M.C.M. Weusten, *De bouw van juridische kennissystemen: Building legal knowledge based systems: KRT: methodology and tools: KRT: methodologie en gereedschap*, proefschrift Universiteit Utrecht 1999.
10. Tina Smith, *Legal Expert Systems: Discussion of Theoretical Assumptions,* proefschrift Universiteit Utrecht, 1994.
11. H.L.A. Hart, *The Concept of Law*, Oxford: Clarendon Press 1961, R. Dworkin, *Law's Empire*, Cambridge, Massachusetts: Belknap Press 1986.
12. C.N.J. de Vey Mestdagh, *Juridische kennissystemen, rekentuig of rekenmeester? Het Onderbrengen van Juridische Kennis in een Expertsystem voor het Milieuvergunningenrecht*, Deventer: Kluwer Academic Publishers 1997; T. van der Linden-Smith, *Een duidelijk geval: Geautomatiseerde afhandeling*. Vol. 41, Iter-reeks 2001; Marlies van Eck, *Geautomatiseerde ketenbesluiten & rechtsbescherming. Een onderzoek naar de praktijk van geautomatiseerde ketenbesluiten over een financieel belang in relatie tot rechtsbescherming*, proefschrift Tilburg 2018.
13. https://blog.jincor.com/smart-contract-examples-can-it-really-improve-your-business-4a5821575fe9.
14. https://lendoit.com/.
15. https://www.uitlegblockchain.nl/category/crowdfunding/.
16. https://www.blandlord.com/.
17. http://www.ie-forum.nl/artikelen/bin-du-de-knock-auteursrechtdebat-blockchain-voor-bij-de-hype-hardwells-blockchain-release.
18. https://www.istandaarden.nl/izo/innovaties/blockchain-mijn-zorg-log.
19. En ook zoiets hebben we (veel) eerder gezien, in de vorm van de aan Electronic Data Interchange ten grondslag liggende interchange agreements.

zelfrijdende auto die jou op je werk afgezet heeft, zichzelf anderszins nuttig maken. Andermans kinderen naar de opvang brengen, bestellingen afleveren, verzin maar iets.[20] Een smart contract maakt de organisatie en de afhandeling van dit soort transacties mogelijk. Een sharing economy zonder tussenpersonen als AirBNB en Uber, maar ècht peer-to-peer. Sharing economy tussenpersonen zijn tenslotte ook TTP's, die zich bemoeien met de inhoud van de overeenkomst, die gelden doorsluizen (en een deel zelf inpikken), die fraude kunnen plegen, failliet kunnen gaan en gehackt kunnen worden.

Dàn ziet de wereld er anders uit. Fysiek, en ook juridisch. De mogelijkheden om wanprestatie te plegen zijn (veel) beperkter en dus zijn de risico's (veel) lager. Door het wegvallen van de tussenpersonen zijn de transactiekosten ook (veel) lager.

We maken gauw een screenshot van het beeld uit de glazen bol voordat het vervaagt. En we blijven in verwarring achter.

## 4. Uitdagingen voor het recht

Is er bij gebruik van smart contracts nog wel plaats voor ons goede oude verbintenissenrecht, met z'n verworven subtiele correctiemechanismen als goede trouw, redelijkheid en billijkheid, opgewekte verwachtingen en schijn, gegaste uien,[21] Haviltex?[22] Of is dat overrated folkore?

Zoals altijd: dat hangt ervan af. Bijvoorbeeld van wie je contractspartijen zijn en of zij goed geïnformeerd hebben gekozen voor een smart contract. Gaat het om grote internationale business-contracten? Dan niet piepen: Mark = Mark.[23] Maar anonimiteit maakt dat je niet weet met wie je te maken hebt. Moeten we zwakke partijen zoals consumenten beschermen? Moeten we mensen tegen hun eigen hebzucht en/of dommigheid beschermen?

Wat zijn bestuursrechtelijke haken en ogen van gebruik van smart contracts door overheden? Wie zijn de peers van de betreffende blockchains? Kan de burger nog wel tegenbewijs leveren als de 'blockchain says no'? Is dat wel behoorlijk besturen?

Hoe gaan we ooit compliant zijn met de AVG als 'op' de blockchain persoonsgegevens verwerkt worden?[24] Of staan er op de blockchain alleen links naar persoonsgegevens die elders in de cloud versleuteld opgeslagen zijn? En is dat dan wel AVG-proof?

Tja, het recht. Waarom hebben we dat ook al weer? Het recht moet zorgen voor rechtvaardigheid (maar wat dat inhoudt is onderwerp van voortdurende discussie), misdaad bestrijden (op straffe van verlies van legitimiteit), de democratische rechtsstaat beschermen (of sowieso de staat – hoe gaan we nog belasting heffen?), en natuurlijk mensenrechten zoveel mogelijk verwezenlijken: non-disriminatie, privacy om maar 's wat te noemen. Hoe gaan we dat doen op de Blockchain?

Ik weet het niet. Is dit nu echt iets nieuws onder de zon dat noopt tot heroverweging of misschien zelfs tot aanpassing van het bestaande juridisch instrumentatium? Of gaat het slechts om schaalvergroting van issues zoals anonimiteit, grensoverschrijdendheid, consumentenbescherming, waar we op ons goeie ouwe Internet ook al zo goed en zo kwaad als het gaat mee dealen? Dan is er nog het fenomeen dat 'scale matters',[25] een kwantitatief verschil kan zo groot worden dat het een kwalitatief verschil wordt.

In een voorgenomen vervolgartikel wil ik proberen om deze uitdagingen voor het recht in kaart te brengen. Volgens mij zijn er voorlopig geen zorgen over werkgelegenheid voor juristen. We moeten hiermee aan de gang, en ik vermoed dat we juristen nodig hebben die de code van een smart contract kunnen lezen en schrijven. Conclusie: dit is volgens mij ècht een technologische ontwikkeling die nu nog onvermoede mogelijkheden biedt – en waar juristen zich hoognodig mee moeten bemoeien. Misschien om vast te stellen dat het allemaal wel meevalt. Maar ook om die conclusie te kunnen trekken is het nodig om je er goed in te verdiepen. Wordt vervolgd!

20. Voorbeeld ontleend aan de reactie van Oelfier op 16 januari 2018 op het blog van Arnoud Engelfriet: Welke rol gaan smart contracts spelen in het recht?, https://blog.iusmentis.com/2018/01/12/welke-rol-gaan-smart-contracts-spelen-recht/#comments.
21. HR 7 maart 1969, *NJ* 1969, 249 (*Gegaste uien*)
22. HR 13 maart 1981, *NJ* 1981/635 (*Haviltex*). Zie ook: J.B. Schmaal & E.M. van Genugten, 'Smart contracts en de Haviltex-norm', *Tijdschrift voor Internetrecht* 2017-1, pp. 12-17.
23. HR 2 januari 1931, *NJ* 1931, 274 (*Mark = Mark*)
24. V.I. Laan, 'Privacy en blockchain: wanneer is er voor wie privacywerk aan de winkel?' *IR* 2017, nr. 1, pp. 4-11.
25. D. Post, 'Against "Against Cyberanarchy"' (2002) 17 *Berkeley Technology Law Journal* 1-23.

# Tien jaar Tijdschrift voor Internetrecht

*mr. R.J.J. Westerdijk*[1]

Zoals u heeft kunnen zien in de eerste aflevering van dit jaar, is het *Tijdschrift voor Internetrecht* inmiddels begonnen aan zijn tiende jaargang. Een kleine mijlpaal die we niet ongemerkt voorbij willen laten gaan. Daarom deel ik in deze opinie graag een paar observaties met u over 10 jaar ontwikkeling van het internetrecht en dit tijdschrift.

Een eerste observatie is dat de hoofdonderwerpen van destijds dat nog steeds zijn. Vraagstukken rond de privacy van internetgebruikers spelen een voorname rol in de begindagen van dit tijdschrift, en dat is uiteraard niet minder geworden. Zeker met de op handen zijnde inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) is de aandacht voor privacy de laatste jaren flink toegenomen, en dat zal de komende tijd ook niet minder worden. Maar ook 10 jaar geleden dus, met toen bijvoorbeeld aandacht voor een onderwerp als anonieme gegevensverzamelingen.[2] Artikelen in dit tijdschrift die aan privacyrechtelijke onderwerpen zijn gewijd worden ook relatief veel geraadpleegd.
Een mooi privacyrechtelijk onderwerp dat de gemoederen blijft bezighouden, is natuurlijk het vergeetrecht. Geïntroduceerd door het Hof van Justitie in de bekende *Google/Costeja*-uitspraak[3] is deze clash tussen de vrijheid van meningsuiting en de bescherming van de persoonlijke levenssfeer een voortdurende en interessante bron van jurisprudentie. Helaas keerde de Hoge Raad zich vorig jaar niet tegen het mijns inziens onjuiste standpunt van het Hof van Justitie dat aan het recht op bescherming van de persoonlijke levenssfeer voorrang toekomt vergeleken met andere grondrechten.[4] Maar dat betekent tegelijk ook niet dat elk beroep op het vergeetrecht zo maar wordt gehonoreerd: de verzoeker zal toch moeten aantonen dat de gepubliceerde informatie irrelevant is en dat lukt lang niet altijd.[5] Ook overigens zijn er nog enige interessante open einden in de vergeetrecht jurisprudentie, met name betreffende de vraag of zoekmachines bijzondere gegevens mogen verwerken.[6] De rechtbank Amsterdam heeft hier zeer recent een interessante uitspraak in gewezen.[7] Hierin laat de rechtbank de mogelijkheid open dat Google als zoekmachine bijzondere persoonsgegevens, in dit geval strafrechtelijke persoonsgegevens, mag verwerken door deze toegankelijk te maken aan internetgebruikers: '*De essentiële functie van zoekmachines in de huidige, wereldwijd door het internet verbonden, samenlevingen, zou immers onaanvaardbaar worden beperkt als het voor exploitanten van zoekmachines categorisch zou zijn verboden aan het publiek koppelingen ter beschikking te stellen naar publicaties waarin wordt bericht over strafrechtelijke verdenkingen tegen, of strafrechtelijke veroordelingen van medeburgers.*'[8] Na toetsing van de belangen aan de hand van eerdergenoemd arrest van de Hoge Raad kiest de rechtbank in dit geval vóór toepassing van het vergeetrecht, maar de discussie over waar de grens precies ligt gaat ongetwijfeld verder. Niet in het minst doordat uit deze uitspraak ook blijkt dat (in een andere zaak) inmiddels prejudiciële vragen zijn gesteld aan het Hof van Justitie over de principiële vraag of het Google is toegestaan bijzondere persoonsgegevens, zoals strafrechtelijke persoonsgegevens, te verwerken. Wordt vervolgd, ook in dit tijdschrift.

Ook de aansprakelijkheid van internet service providers en platforms is al lang onderdeel van discussie. Dit is een mooi voorbeeld van een onderwerp waar zich de afgelopen 10 jaar een behoorlijke ontwikkeling heeft voorgedaan. De e-commerce richtlijn introduceerde in 2004 een aansprakelijkheid voor verschillende soorten internetproviders, waarvan in de praktijk met name die van hosting providers aan de orde komt. In een overzichtsartikel beschrijft De Wit nog dat toezichts- en onderzoeksverplichtingen in beginsel niet door de rechtspraak worden gehonoreerd (met uitzondering van de toen toch wat uitzonderlijke uitspraak inzake de vereniging Martijn).[9] Maar dit uitgangspunt, gebaseerd op de e-commerce richtlijn, is meer en meer onder druk komen te staan, zoals al werd opgemerkt in het destijds opvolgende nummer van

1. Reinoud Westerdijk is advocaat bij Kennedy Van der Laan en hoofdredacteur van dit tijdschrift.
2. T. Wisman en M. van der Linden-Smith, *IR* 2008, p. 86.
3. Hof van Justitie EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317.
4. Vgl. Hoge Raad 24 februari 2017, ECLI:NL:HR:2017:316.
5. Zie voor een recent voorbeeld Rechtbank Limburg 20 maart 2018, ECLI:NL:RBLIM:2018:2751.
6. Vgl. ook L. Mourcous & M. Weij, 'Drie jaar het recht om vergeten te worden: een analyse van de Nederlandse rechtspraak', *IR* 2017, p. 1525-160.
7. Rechtbank Amsterdam 15 februari 2018, ECLI:NL:RBAMS:2018:1644.
8. Zie r.o. 4.9 in genoemde uitspraak.
9. A.P. de Wit, 'De civielrechtelijke aansprakelijkheid van internetproviders (Deel I)', *IR* 2009, 37 e.v.

dit tijdschrift.[10] Die trend heeft zich doorgezet, in de richting van een steeds verdergaande aansprakelijkheid voor wat via internetdiensten wordt gepubliceerd. Dat is geen gelukkige ontwikkeling wat mij betreft; ik heb nog steeds sympathie voor het voorstel van Engelfriet om een inspanningsverplichting tot moderatie op te nemen maar dan vervolgens wel tot vrijwaring van aansprakelijkheid te komen.[11] Grappig genoeg kent het onderwerp van de aansprakelijkheid van internetdienstverleners ook zo zijn klassiekers: al in 2009 werd in dit tijdschrift geschreven over The Pirate Bay[12], een dienst/site die tot de dag vandaag aanleiding geeft tot diverse procedures – en publicaties.

Gelukkig is het fascinerende van het internet dat er zich voortdurend interessante nieuwe ontwikkelingen blijven voordoen. Zo wordt ook in deze aflevering aandacht besteed aan het hot topic van het moment, te weten *blockchain*.[13] Het aardige van deze terugblik is om te constateren dat dit onderwerp tien jaar geleden nog niet aan de orde was, maar dat er al wel over iets vergelijkbaars werd geschreven. Wat immers te denken van een artikel met als titel 'Financieel toezicht op virtuele valuta'.[14] Echter, dat artikel ging over de toepassing van de Wft op virtuele valuta zoals deze voorkomen in virtuele werelden zoals Second Life. Zeker een interessant onderwerp, maar toch niet een dat vandaag de dag nog erg tot de verbeelding spreekt. En zo zal het vermoedelijk ook de komende 10 jaar gaan: nieuwe technische ontwikkelingen zullen aanleiding geven tot interessante en diepgravende juridische beschouwingen. Maar de tijd zal leren welke onderwerpen blijvertjes zijn, en welke technische ontwikkelingen weer snel in de (relatieve) vergetelheid zullen raken. Met blockchain zal dat vermoedelijk niet gebeuren, net zo min als met het Internet of Things en kunstmatige intelligentie (AI). We gaan het zien, en de redactie van dit tijdschrift blijft u er met veel plezier over berichten.

10. Vgl. A.P. Engelfriet, 'Naar een passend beschermingsregime voor forumbeheerders en bloggers', *IR* 2009, p. 77 e.v.
11. Engelfriet, a.w., p. 79.
12. B.W. Schermer, 'De Pirate Bay uitspraak: aansprakelijkheid van internetdienstverleners opgehelderd?', *IR* 2009, p. 68-71.
13. Zie in deze aflevering M. van der Linden, Het recht geketend - Smart contracts: dé oplossing voor gezeur, gedoe en onzekerheid? En al eerder J.B. Schmaal en E.M. van Genuchten, 'Smart contracts en de Haviltex-norm', *IR* 2017, p. 12-17.
14. H. de Jong en R. Wever, 'Financieel toezicht op virtuele valuta', *IR* 2009, p. 32-36.

# Ruis in de ether en de juridische kwalificatie(s) van cryptovaluta

## *Noot bij Rechtbank Midden-Nederland 7 december 2017, ECLI:NL:RBMNE:2017:6646*[1]

*mr. W. Weij en mr. M.C. Landerbarthold*[2]

**Opnieuw is vonnis gewezen in een zaak met betrekking tot een cryptovaluta. Waar eerdere jurisprudentie zag op de cryptovaluta 'Bitcoin', gaat het in de onderhavige zaak om 'Ether', eveneens een cryptovaluta, en dus niet te verwarren met de radiosignalen waarmee men het woord doorgaans associeert. Door het recent door de rechtbank Midden-Nederland gewezen vonnis is echter wel wat ruis ontstaan, want hoe vallen cryptovaluta zoals Bitcoin en Ether nu te kwalificeren en wordt dat duidelijker aan de hand van dit vonnis?**

De feiten zijn als volgt: eiser exploiteert een onderneming die zich bezighoudt met het *minen* ('produceren') van cryptovaluta, waaronder Ethers. Gedaagde exploiteert een onderneming die een datacentrum beheert met daarin computers van haarzelf en haar klanten. Eiser heeft 20 computers van gedaagde gekocht, welke in het datacentrum van gedaagde zijn gepositioneerd en waarmee gedaagde Ethers voor eiser *minet*. De geminede Ethers komen in eerste instantie in de *wallet* ('virtuele portemonnee') van gedaagde terecht en worden vervolgens *doorgeboekt* naar eiser, met aftrek van 10% commissie. Na verloop van tijd boekt gedaagde geen Ethers meer door naar eiser en ontstaat het onderhavige geschil. In kort geding, vordert eiser onder meer afgifte van de *mining computers* en overboeking van de niet-doorgeboekte Ethers. Gedaagde verweert zich door te stellen dat zij ook eigen Ethers aan eiser heeft overgemaakt en bovendien haar 10% niet heeft ingehouden, waardoor zij feitelijk 150 Ethers te veel aan haar betaald zou hebben.

De voorzieningenrechter gaat hier echter niet in mee. Om te beginnen, wijst zij de vordering tot afgifte van de mining computers toe, alsmede de daaraan verbonden dwangsom. Vervolgens wijst zij de vordering tot afgifte van de *geminede* Ethers eveneens toe. In het kader van de dwangsom, stelt de voorzieningenrechter voorop dat deze niet zou kunnen worden toegewezen, indien sprake zou zijn van een *veroordeling tot betaling van een geldsom* in de zin van art. 611a Wetboek van Burgerlijke Rechtsvordering (hierna: 'Rv'). In dit artikel is immers het volgende opgenomen: '*De rechter kan op vordering van een der partijen de wederpartij veroordelen tot betaling van een […] dwangsom […] voor het geval dat aan de hoofdveroordeling niet wordt voldaan […]. Een dwangsom kan echter niet worden opgelegd in geval van een veroordeling tot betaling van een geldsom.*'

Vervolgens oordeelt de rechtbank – onder verwijzing naar het *Hedqvist*-arrest[3] – dat in de onderhavige kwestie geen sprake is van een geldsom als bedoeld in art. 611a Rv en dat de dwangsom daarom dient te worden toegewezen. Dit aangezien door partijen niet was gesteld, noch gebleken, dat Ethers evenals Bitcoins als betaalmiddel wordt gebruikt en met dat doel door sommige marktdeelnemers wordt geaccepteerd. De voorzieningenrechter gaat er *daarom* vanuit (en beargumenteert dit overigens niet) dat Ether een 'goed' is, zodat aan het overmaken van Ethers een dwangsom kan worden verbonden. Onzes inziens rijzen er twee vragen uit het onderhavige vonnis, die we in het hiernavolgende zullen bespreken; de vraag of een cryptovaluta als 'geld' is aan te merken en de vraag welke goederenrechtelijke status zij dient te hebben.

1. In het vervolg ook wel aangeduid als '*Ether*-zaak'.
2. Menno Weij en Mike Landerbarthold zijn respectievelijk als advocaat/partner en legal counsel verbonden aan SOLV. Advocaten te Amsterdam.
3. HvJ EU 22 oktober 2015, zaak C-264/14, ECLI:EU:C:2015:498.

## 1. Bitcoin: geld of geen geld?

In de *Ether*-zaak verwijst de rechtbank naar het *Hedqvist*-arrest, waarin het HvJ eerder een oordeel velde over de cryptovaluta Bitcoin. In deze zaak gaf het HvJ antwoord op de (prejudiciële) vraag of een onderneming die Bitcoins inwisselde voor traditionele valuta en andersom btw af diende de dragen. Kort gezegd, was dat niet het geval, aangezien de diensten van de Bitcoin-onderneming van de btw-richtlijn vrijgestelde handelingen – zoals daarin opgesomd – vormden.

In twee andere zaken, waarin een vonnis in eerste aanleg en vervolgens een arrest in hoger beroep is gewezen[4] (hierna: '*Bitcoin*-zaak' of '*Bitcoin*-zaken'), ging het om de aankoop van 2.750 Bitcoins. Gedaagde zou deze aan eiser verkopen voor een bedrag van EUR 8,05 per Bitcoin. Nadat het totaalbedrag aan gedaagde was voldaan, werden vervolgens maar 990 Bitcoins aan eiser geleverd. Levering van de resterende Bitcoins bleef vervolgens uit. Eiser ontbond de overeenkomst hierop partieel voor het gedeelte dat niet was nagekomen en vorderde bij de rechtbank een verklaring voor recht dat Bitcoin als geld in de zin van afdeling 6.1.11 BW dient te worden gezien.

Tevens vorderde eiser een schadevergoeding à EUR 132.792,- voor de niet-geleverde Bitcoins, welke bestond uit de toegenomen waarde van deze niet-geleverde Bitcoins ná ontbinding. De rechter oordeelde in eerste aanleg – op grond van de Memorie van Toelichting bij het BW – dat de Bitcoin niet als 'gangbaar geld' dient te worden gezien (maar als 'ruilmiddel') omdat alleen de Euro de status van wettig betaalmiddel heeft in Nederland. Tevens oordeelde zij dat de schade gevorderd ná ontbinding van de overeenkomst niet voor vergoeding in aanmerking kon komen. Wel kwam de schade à EUR 1.760.- die was geleden in de periode tussen het sluiten van de overeenkomst en de ontbinding voor vergoeding in aanmerking. In hoger beroep werd het voornoemde vonnis door het hof bekrachtigd.

Uit de voornoemde jurisprudentie leiden wij af dat cryptovaluta vooralsnog niet als geld gekwalificeerd kan worden, hetgeen overigens ook buiten de rechtspraak wordt bevestigd. Immers, ook in de (Europese) politiek wordt cryptovaluta doorgaans niet als 'geld' aangemerkt: zo gaf (toenmalig) Minister van Financiën Dijsselbloem reeds in 2013 aan dat Bitcoins als ruilmiddel dienen te worden bestempeld en kwalificeerde de G20 cryptovaluta Bitcoins onlangs 'eerder als een *asset*', dan als een valuta.[5] Kortom, we kunnen op dit moment slechts concluderen dat cryptovaluta niet als geld kan worden gezien. Hoewel er wel aanknopingspunten zijn voor een andere conclusie, zullen wij deze niet verder bespreken in deze annotatie.

4. Rb. Overijssel 14 mei 2014, ECLI:NL:RBOVE:2014:2667 en Hof Arnhem-Leeuwarden 31 mei 2016, ECLI:NL:GHARL:2016:4219.
5. https://bit.ly/2qQixTz.

## 2. Aard cryptovaluta?

Naast de vraag of cryptovaluta kan worden bestempeld als 'geld', is ook de vraag welke goederenrechtelijke kwalificatie men aan cryptovaluta kan verbinden een interessante. Wij merken op dat, vanuit technisch oogpunt, een cryptovaluta niet te beschouwen is als – bijvoorbeeld – een losse euro, die je aan een ander kunt geven, waardoor jouw 'saldo' automatisch met 1 Euro verlaagd wordt en het saldo van de ander met hetzelfde bedrag verhoogd. Een Bitcoin is immers niet 'tastbaar' en bovendien wordt de Blockchain aan informatie, die ten grondslag ligt aan cryptovaluta decentraal op verschillende *nodes* ('computers') opgeslagen.

In dat opzicht moet je eigenlijk vaststellen dat een cryptovaluta als zodanig niet bestaat; er bestaan in de blockchain immers enkel wallets met bijbehorende saldi en (geldige) transactiehistories. Een cryptovaluta is daarmee niet individualiseerbaar, laat staan voor menselijke waarneming vatbaar. Dit maakt onzes inziens dat cryptovaluta, in het licht van art. 3:1 en 3:2 BW, als een goed kan worden gezien, maar in ieder geval niet als zaak.[6]

Deze lijn volgt de HvJ dan ook in *Hedqvist*: zij stelt in r.o. 24 immers (vrij uitdrukkelijk) voorop dat Bitcoins geen *lichamelijke zaak* zijn. In de *Bitcoin*-zaak in hoger beroep lijkt het Hof (in r.o. 4.6 en 4.8) daarentegen te suggereren dat zij Bitcoins als 'goed', en in het bijzonder als 'gekochte zaak' ziet, hetgeen dus in strijd zou zijn met het eerder door het HvJ gevelde oordeel in *Hedqvist*. In de *Ether*-zaak bestempelt de rechter de geminede Ethers echter niet als *zaak*, maar als *goed*, zonder verder te oordelen of het dan een zaak of een vermogensrecht zou betreffen.

Dan rest nog de vraag of cryptovaluta wellicht als vermogensrecht beschouwd zou kunnen worden. In beginsel is dit – naar onze opvatting – mogelijk, gezien de zeer ruime definitie van art. 3:6 BW.[7] Waar Dammers in zijn annotatie echter spreekt over een 'absoluut vermogensrecht'[8], menen wij echter dat je een cryptovaluta in het kader van art. 3:6 BW eerder zou kunnen zien als een vordering die de 'eigenaar' ervan heeft op de volledige cryptovaluta-gemeenschap in de Blockchain.

Dat een cryptovaluta als een vermogensrecht kan worden gezien, is recentelijk door de rechtbank Amsterdam bevestigd.[9] De betreffende rechtbank

6. Art. 3:1 BW bepaalt immers het volgende: '*Goederen zijn alle zaken en alle vermogensrechten*.' En artikel 3:2 BW het volgende: '*Zaken zijn de voor menselijke beheersing vatbare stoffelijke objecten*'.
7. Dit artikel bepaalt immers het volgende: '*Rechten die, hetzij afzonderlijk hetzij tezamen met een ander recht, overdraagbaar zijn, of er toe strekken de rechthebbende stoffelijk voordeel te verschaffen, ofwel verkregen zijn in ruil voor verstrekt of in het vooruitzicht gesteld stoffelijk voordeel, zijn vermogensrechten*.'
8. Mr. W.F. Dammers, *Bitcoins: een vreemde zaak?*, Noot bij Hof Arnhem-Leeuwarden 31 mei 2016, ECLI:NL:GHARL:2016:4219.
9. Rb. Amsterdam 14 februari 2018, ECLI:NL:RBAMS:2018:869 (*Koinz Trading*).

verklaarde Koinz Trading, een onderneming die zich bezighield met de in- en verkoop van Bitcoins, failliet nadat één van haar schuldeisers recht zou hebben op uitbetaling van Bitcoins uit hoofde van een eerder vonnis, te vermeerderen met een dwangsom van maximaal EUR 10.000,-. De rechtbank kwam tot dit oordeel doordat zij de Bitcoin-vordering zag als een te verifiëren vordering, aangezien deze volgens haar een waarde vertegenwoordigt en overdraagbaar is en daarmee *kenmerken vertoont van een vermogensrecht*.

Hoewel het onderhavige *Ether*-vonnis het juridisch raamwerk over cryptovaluta dus wel *iets* duidelijker maakt (immers; we weten nu dat dwangsommen kunnen worden verbonden aan cryptovaluta-vorderingen), brengt het niet veel nieuws met zich mee in het licht van eerdere jurisprudentie en berichten uit de politiek. De kwalificatie van Ether als 'goed', wekt verder eerder verwarring op dan duidelijkheid, gezien de gebrekkige motivering ervan. Hierbij speelt mee dat de rechtbank nalaat te oordelen of zij Ether – bijvoorbeeld – als vermogensrecht beschouwt, hetgeen naar onze mening een gemiste kans is. Wat de achterliggende reden daarvan is, zullen we nooit te weten komen. Wel weten we dat het recente *Koinz Trading*-vonnis wat ruis heeft weggenomen en zijn het van harte eens met de motivering die daarin is geformuleerd door de rechtbank.

# Jurisprudentie

*Onder redactie van mr. M. van der Linden en mr. C.C.M. Kroeks-de Raaij*

## 48. Gerechtshof Arnhem-Leeuwarden 19 december 2017 (BMW), ECLI:NL:GHARL:2017:11216

Domeinnaam, registratie van domeinnaam, onrechtmatige daad, toerekening

*Het hof verwerpt de stellingen van BMW, dat voor het geval niet komt vast te staan dat geïntimeerde de Domeinnamen heeft geregistreerd, deze registratie als onrechtmatige daad aan geïntimeerde kan worden toegerekend. Onvoldoende voor aansprakelijkheid van geïntimeerde is dat de registratie is verricht met het account van Innofab, een vennootschap waarvan geïntimeerde indirect bestuurder en aandeelhouder was, en dat de Domeinnamen op naam van geïntimeerde zijn gezet. Dat geïntimeerde verantwoordelijk is voor het reilen en zeilen binnen Innofab, maakt niet dat hij persoonlijk aansprakelijk is voor een onrechtmatige registratie met behulp van het account van Innofab, ook zonder dat hij betrokken was bij deze registratie. Voor een dergelijke vergaande toerekening is geen plaats. Dat Innofab de facturen voor de registratie van de Domeinnamen heeft betaald, maakt een en ander niet anders. Enerzijds heeft BMW te weinig uitgewerkt, waarom het laten voortduren van een door een ander gecreëerde onrechtmatige situatie in dit geval een onrechtmatige daad van geïntimeerde zou opleveren. Anderzijds heeft BMW ook te weinig uitgewerkt, waarom geïntimeerde aan de hand van de ontvangen facturen had moeten begrijpen dat hij actie moest ondernemen ter beëindiging van deze door een ander gecreëerde onrechtmatige situatie. Daarbij is van belang dat Innofab ongeveer honderd domeinnamen had geregistreerd via TransIP en dat het abonnementsgeld € 6 à € 7 voor het eerste jaar is. Verder heeft BMW haar stelling dat geïntimeerde in zijn hoedanigheid van bestuurder van Innofab persoonlijk een ernstig verwijt ervan kan worden gemaakt dat zoveel personen beschikten over de inlogcode van het account van Innofab bij TransIP, te weinig uitgewerkt, zodat het hof daaraan voorbij gaat. Deze omstandigheid, ook tezamen genomen met het verwijt dat geïntimeerde de inlogcode van het account bij TransIP niet regelmatig heeft*
*gewijzigd, is onvoldoende voor een gegrond beroep op bestuurdersaansprakelijkheid.*
*Niet is komen vast te staan dat geïntimeerde de inbreukmakende domeinnamen heeft geregistreerd, noch dat hij daarvoor verantwoordelijk is.*

## 49. Rechtbank Den Haag 22 december 2017 (namaakwebshops), ECLI:NL:RBDHA:2017:15272

Computercriminaliteit, internetoplichting, nepwebshops, namaakwebshops, phishing, hacken, computervredebreuk, art. 138ab Sr, art. 139d Sr, art. 311 Sr, art. 317 Sr, art. 326 Sr, art. 350a Sr, art. 420bis Sr

*Verdachte heeft in een periode van zestien maanden 18 strafbare feiten gepleegd, waaronder computervredebreuk, diefstal en grootschalige oplichting van consumenten door elektronica aan te bieden via namaakwebshops. Verdachte heeft met gephishte gegevens ingelogd op Admarkt- en reguliere Marktplaatsaccounts en daarop andere advertenties geplaatst, die verwezen naar namaakwebshops. Deze namaakwebshops waren afgeleid van webshops van gerenommeerde bedrijven zoals BCC, Dixons, Simyo en Topprice24. De namaakwebshops zagen er zo goed uit dat ze niet of nauwelijks van de echte webshops van voornoemde bedrijven waren te onderscheiden.*
*Zo hadden ze internetadressen waarin de naam van het gerenommeerde bedrijf voorkwam en werden de merknaam en logo's van het bedrijf gebruikt. Ook werden soms adressen, telefoonnummers, BTW- en KvK-nummers van het reguliere bedrijf overgenomen en altijd bestond er een contactmogelijkheid via e-mail of door middel van een chatfunctionaliteit. De producten werden op professionele wijze gepresenteerd. Consumenten hadden nadat zij via een betrouwbaar ogende advertentie op Marktplaats werden doorgelinkt naar de namaakwebshop, dan ook niet door dat zij op een frauduleuze website waren beland. In tegendeel, zij voelden zich juist veilig bij de gedachte dat ze bij een goed bekend staand bedrijf kochten en dat was ook precies de bedoeling. Ze deden in goed vertrouwen vaak voor honderden euro's aankopen. De koopprijs werd vervolgens betaald op een door verdachte opgegeven rekeningnummer, meestal via iDEAL of een andere betaaldienstverlener. De bestelde producten werden daarna niet geleverd en verdachte heeft ook nooit de intentie gehad die te leveren.*
*Verdachte heeft regelmatig nadat slachtoffers hadden betaald voor hun bestelling, per e-mail laten weten dat er iets was misgegaan bij de betaling en gevraagd om gebruik te maken van een retourlink. Wanneer slachtoffers dat deden, betaalden ze in het gunstigste geval nog een keer en in het ongunstigste geval haalde verdachte hen ook nog over om hem hun bankgegevens te verstrekken en liet hij ze ongemerkt grote bedragen wegschrijven naar door hem uitgekozen rekeningnummers. Volgt veroordeling tot 146 weken gevangenisstraf.*

## 50. Rechtbank Amsterdam 15 januari 2018 (foto van caravan), ECLI:NL:RBAMS:2018:133

Auteursrecht, foto op website, hoogte schadevergoeding

*Geschil tussen eiser Stichting en gedaagde CCC over foto van caravan.*

*Het staat voldoende vast dat de foto zonder toestemming van De Stichting en zonder vermelding van haar naam als maker in juni 2016 op de website is geplaatst en daarmee openbaar is gemaakt. Gelet daarop is sprake van een inbreuk op de auteurs- en persoonlijkheidsrechten van De Stichting en daarmee van onrechtmatig handelen van CCC jegens De Stichting. Eventueel ontbreken van kwade opzet aan de zijde van CCC doet hieraan niet af en ook het onbewust schenden van het auteursrecht komt voor rekening en risico van de inbreukmaker. Dat de foto geen commercieel belang heeft, zoals CCC aanvoert, maakt voor de inbreuk evenmin verschil.*
*De Stichting heeft voor de begroting van haar schade aangeknoopt bij de volgens haar gebruikelijke licentievergoeding en de leveringsvoorwaarden van de Fotografen-Federatie. Gelet op het feit dat de foto niet is gemaakt door een professionele fotograaf en geen commercieel belang is gemoeid met de foto – dat is althans gesteld noch gebleken – kan niet worden ingezien dat het genoemde tarief een redelijke prijs is voor het publiceren van de foto. Gelet verder op de soort foto, de (beperkte) tijd die de foto op de website van CCC heeft gestaan, het feit dat CCC heeft geprobeerd de foto van haar website te verwijderen en het feit dat partijen in onderhavig geding niet zozeer op zakelijk gebied actief zijn, maar clubs (vereniging/stichting) zijn die zich bezig houden met een(zelfde) liefhebberij, wordt geoordeeld dat onvoldoende is komen vast te staan dat De Stichting door de publicatie van de foto op de website van CCC schade heeft geleden. Het gevorderde bedrag wordt dan ook afgewezen.*

### 51. Rechtbank Amsterdam 17 januari 2018 (toeristische verhuur), ECLI:NL:RBAMS:2018:163

Bestuursrecht, advertentie op internet, structurele verhuur aan toeristen

*Bezwaar tegen opgelegde last onder dwangsom in verband met structurele verhuur van een woonboot aan toeristen.*
*Het standpunt van verweerder dat sprake is van structurele toeristische verhuur is onvoldoende deugdelijk gemotiveerd. Uit de advertenties op internet waarin de woonboot zonder tijdsbeperking voor verhuur wordt aangeboden kan deze conclusie niet zonder meer worden getrokken.*

### 52. Rechtbank Limburg 17 januari 2018 (Bralex), ECLI:NL:RBLIM:2018:310

E-commerce, informatie over product, retourtermijn, art. 6:230m BW

*Vaststaat dat gedaagde de door hem bestelde producten buiten de retourtermijn van 14 dagen heeft teruggestuurd.*
*Gedaagde voert verder tegen de vordering aan dat Bralex heeft geweigerd om voor hem essentiële informatie aangaande de geleverde producten te verstrekken. Zo ontbrak bij de levering enige productinformatie en een bijsluiter met informatie op welke wijze de producten in gebruik moesten worden genomen. Met name het ontbreken van deze belangrijke informatie heeft gedaagde aanleiding gegeven de goederen – weliswaar te laat – te retourneren.*
*Tussen partijen is niet in debat dat er in het onderhavige geval sprake is van een koop op afstand. Bralex is dan ook op grond van het bepaalde in art. 6:230m lid 1 onder a BW gehouden om – kort samengevat – aan gedaagde als koper de nodige informatie omtrent het product te verschaffen. In deze zaak is naar het oordeel van de kantonrechter in ontoereikende mate gebleken dat Bralex aan deze verplichting heeft voldaan. Vordering afgewezen.*

### 53. Raad van State 17 januari 2018 (Europacasino), ECLI:NL:RVS:2018:155

Bestuursrecht, gokken op internet, kansspel op internet, online kansspelen, kansspelautoriteit, prioriteringscriteria, art. 1 Wok

*Kansspelautoriteit had appellante boete opgelegd omdat zij zonder vergunning online kansspelen heeft aangeboden.*
*Aangezien het de ksa ontbreekt aan middelen en mankracht om tegen alle aanbieders van online kansspelen zonder vergunning handhavend op te treden, heeft de ksa het prioriteringsbeleid opgesteld. Daarin staat dat de aanbieders die prominent op de Nederlandse markt zijn gericht in eerste instantie voorwerp zijn van haar handhavingsacties. Om te bepalen of een aanbieder zich zodanig op Nederland richt, gebruikt de ksa drie prioriteringscriteria, namelijk of een .nl extensie wordt gebruikt, of op de websites gebruik wordt gemaakt van de Nederlandse taal en of op Nederlandse radio, televisie of in geprinte media reclame wordt gemaakt voor de websites. Deze prioriteringscriteria zijn volgens het prioriteringsbeleid niet cumulatief. Evenals de rechtbank heeft overwogen, komt dit beleid de Afdeling niet onredelijk voor, nu in het bijzonder op Nederland gerichte illegale aanbieders veel schade aan Nederlandse consumenten kunnen berokkenen. Vergelijk ook de uitspraak van de Afdeling van 22 februari 2015, ECLI:NL:RVS: 2017:484. Dat zich in het buitenland Nederlandstaligen bevinden en dat veel Nederlanders Engels kunnen spreken, lezen en schrijven, doet er niet aan af dat een website, door daarop gebruik te maken van de Nederlandse taal, beter toegankelijk wordt voor de Nederlandse consument. Gelet op de hiervoor vermelde reden waarom de Afdeling het prioriteringsbeleid niet onredelijk acht, hoeft de ksa de niet op de Nederlandse markt gerichte websites niet op één lijn te stellen met websites die wel specifiek mede daarop zijn gericht en mag de ksa met voorrang handhavend optreden tegen laatstbedoelde websites.*

### 54. Rechtbank Noord-Nederland 18 januari 2018 (versturen van afbeeldingen), ECLI:NL:RBNHO: 2018:587

Strafrecht, kinderporno, sturen van foto's naar minderjarigen, art. 240a Sr, art. 240b Sr

*Naast het bezit van kinderporno heeft verdachte naar drie minderjarigen foto's van zijn ontblote (stijve) ge-*

*slachtsdeel gestuurd. Volgens verdachte hebben de minderjarigen hem uit nieuwsgierigheid uit eigen beweging benaderd en hebben zij hem tot het sturen van dergelijke foto's aangezet of uitgelokt. De minderjarigen hebben volgens verdachte een eigen verantwoordelijkheid. Verdachte toont hiermee naar het oordeel van de rechtbank aan geen inzicht te hebben in het kwalijke van zijn handelen en in het gegeven dat alleen hij, als volwassene, daarvoor verantwoordelijk is. Daar komt bij dat jeugdige personen beschermd moeten worden tegen het tonen van foto's als de onderhavige.*
*Volgt veroordeling tot 12 maanden gevangenisstraf waarvan 6 maanden voorwaardelijk.*

### 55. Rechtbank Den Haag 24 januari 2018 (ook zusje en moeder), ECLI:NL:RBDHA:2018:1185

Strafrecht, social media, chat, naaktfoto, foto op internet, Facetime, WhatsApp, kinderporno, feitelijke aanranding van de eerbaarheid, sextortion, ontucht met minderjarige art. 240b Sr, art. 246 Sr en art. 248a Sr

*Verdachte heeft aangeefster eerst via social media ontmoet. Daarna hebben zij elkaar verder via WhatsApp gesproken. Het was voor verdachte van meet af aan duidelijk dat zij pas 15 jaar was. In eerste instantie waren het leuke gesprekken en aangeefster werd dan ook verliefd op verdachte.*
*Na enige tijd begon verdachte haar om naaktfoto's te vragen. Dit heeft ze eerst geweigerd. Verdachte bleef aandringen. Toen ze bleef weigeren werd hij boos en schold haar uit. Daarbij liet hij zich zeer grof en vernederend uit jegens dit nog jonge en kwetsbare meisje. Aangeefster deed toen maar wat verdachte wilde omdat ze hem leuk vond en niet wilde dat hij bij haar weg zou gaan. Na zijn vernederend gescheld heeft aangeefster telkens opnieuw haar excuses gemaakt, en zich in elk geval verbaal – zo blijkt uit de apps – geheel ondergeschikt aan hem opgesteld. Dat kon niet voorkomen dat verdachte haar bleef uitschelden en vernederen.*
*Verdachte bedreigde aangeefster bovendien ook en heeft haar vele keren dreigend gezegd dat hij bij haar weg zou gaan of dat hij de van haar gekregen naaktfoto's of de andere naaktfoto's van haar minderjarige zusje en moeder op internet zou zetten als zij bepaalde seksuele handelingen, zichtbaar via de telefoon of Facetime, niet zou doen of laten gebeuren.*
*Daarnaast heeft zij zich gedwongen gevoeld om naaktfoto's en naaktfilmpjes van haar zusje en moeder te maken en aan verdachte te verzenden.*
*Volgt veroordeling tot 12 maanden gevangenisstraf waarvan 6 maanden voorwaardelijk en schadevergoeding aan slachtoffer.*

### 56. Rechtbank Den Haag 24 januari 2018 (WCR vs. TCC), ECLI:NL:RBDHA:2018:500

Domeinnaam, merkenrecht, hyperlink, link, gebruik voor waren en diensten, onderscheidend vermogen, art. 9 UMVo

*Door de Domeinnamen te gebruiken om door te linken naar (de onderhoudspagina van) haar eigen website, gebruikt gedaagde TCC deze voor haar eigen onderhoudsdiensten ten aanzien van warmtewisselaars. Door dit gebruik is een verband ontstaan tussen de tekens (de Domeinnamen) en de aangeboden waren en/of diensten op de onder dat teken gehouden en gepresenteerde website, zodat sprake is van gebruik ter onderscheiding van waren en diensten in het economisch verkeer. De Domeinnamen worden door TCC gebruikt voor waren en diensten die gelijk zijn aan of overeenstemmen met die waarvoor de WCR-merken zijn ingeschreven, te weten (onderhoud van) warmtewisselaars. De door TCC als domeinnamen gebruikte tekens stemmen in grote mate overeen met de WCR-merken. De lettercombinatie 'WCR' vormt het meest kenmerkende aspect van de WCR-beeldmerken en van de Domeinnamen. Het onderdeel Benelux en de domeinnaamextensie zijn slechts beschrijvend van aard. TCC betwist dat de WCR-merken onderscheidende kracht hebben. Dit verweer heeft zij echter niet, althans niet voldoende, toegelicht. Gesteld noch gebleken is dat de lettercombinatie 'WCR' beschrijvend is voor de waren en diensten die onder de WCR-merken worden aangeboden, zodat de WCR-merken naar het oordeel van de rechtbank een normaal onderscheidend vermogen hebben. TCC heeft derhalve diensten aangeboden onder met de WCR-merken overeenstemmende tekens voor diensten die overeenstemmen met de diensten waarvoor de WCR-merken zijn ingeschreven.*
*Het verweer van TCC dat het gebruik van de Domeinnamen – het doorlinken – niet tot verwarring kan leiden, faalt.*
*Een en ander leidt tot de slotsom dat TCC inbreuk op de WCR-merken heeft gemaakt in de zin van art. 9 lid 2 aanhef en onder b UMVo.*

### 57. Rechtbank Noord-Holland 30 januari 2018 (neefje), ECLI:NL:RBNHO:2018:628

Strafrecht, kinderporno, ontucht met minderjarige, dierenporno, art. 240b Sr, art. 245 Sr, art. 247 Sr, art. 248 Sr, art. 254a Sr

*Verdachte heeft vanaf zijn 29e in een periode van bijna drie jaren meerdere keren seksuele handelingen verricht met zijn neefje. Het seksuele misbruik is begonnen toen het slachtoffer negen jaar oud was. Verdachte heeft tevens foto's en video's gemaakt van de seksuele handelingen die hij verrichtte met slachtoffer, waarmee hij zich ook heeft schuldig gemaakt aan het vervaardigen van kinderpornografie.*
*Uit de verklaringen van verdachte en slachtoffer volgt dat de handelingen niet altijd tegen de zin van slachtoffer waren, maar verdachte heeft met zijn handelen desondanks ernstig inbreuk gemaakt op zowel de lichamelijke als de geestelijke integriteit van het slachtoffer.*
*Daarnaast heeft verdachte zich schuldig gemaakt aan het bezit, het verspreiden en het vervaardigen van kinderporno en heeft hij hier ook een gewoonte van gemaakt.*
*Volgt veroordeling tot 1 jaar gevangenisstraf en dadelijk uitvoerbare terbeschikkingstelling.*

### 58. Rechtbank Amsterdam 30 januari 2018 (Joke Smit-prijs), ECLI:NL:RBAMS:2018:383

Onrechtmatige uiting, perspublicatie, steun in de feiten, publiek figuur, eer en goede naam, misstand

*In dit geval gaat het om beschuldigingen van wangedrag. In de eerste plaats dient te worden onderzocht in hoeverre de uitlatingen steun vinden in het ten tijde van de publicatie beschikbare feitenmateriaal. Anders dan eiser meent, is er voor de gedane uitlatingen voldoende steun te vinden in de feiten. Het artikel bevat onder meer een verkorte weergave van de verklaringen van twee vrouwen die weliswaar niet met naam in de krant zijn genoemd, maar van wie de namen wel bekend zijn bij de redactie. Met de identiteit van één van hen is eiser bekend vanwege de tegen hem gevoerde strafzaak. Dat eiser niet weet wie achter een bepaalde naam schuil gaat, maakt haar verklaring nog niet onbetrouwbaar. De journalist heeft uitvoerig gesproken met beide vrouwen om zich te vergewissen van de geloofwaardigheid van hun beschuldigingen, en heeft daarvan een verslag opgemaakt dat zich onder de stukken bevindt. Beide vrouwen hebben afzonderlijk tegenover hem gedetailleerde verklaringen afgelegd en verteld over gedrag van eiser dat in beide zaken gedeeltelijk van vergelijkbare aard was (strelen van borsten en billen). Dit draagt bij aan de geloofwaardigheid van hun verklaringen. Bovendien zijn – kennelijk letterlijke – transcripten overgelegd van de door de journalist met de vrouwen gevoerde gesprekken, welke transcripten als zodanig niet zijn betwist.*
*De onderzoeksresultaten van de journalist rechtvaardigden in beginsel publicatie daarvan.*
*Seksueel overschrijdend gedrag is immers een misstand die de hele samenleving raakt. Dat geldt te meer wanneer daarbij kwetsbare jongeren betrokken zijn en wanneer dat gedrag zich voordoet in ongelijkwaardige relaties, zoals in dit geval.*
*Daarbij komt dat eiser was genomineerd voor de Joke Smitprijs, een prijs ter beloning van gedrag dat in schril contrast staat met de eiser verweten gedragingen. Door deze nominatie is eiser bovendien, zij het in beperkte mate, een publieke figuur geworden, waardoor hij zich in zoverre meer publiciteit moet laten welgevallen dan de gemiddelde burger.*
*Alles overziende, weegt het belang van TMG bij publicatie van het artikel zwaarder dan het belang van eiser bij bescherming van zijn eer en goede naam.*
*Eis tot verwijdering van het artikel van alle door TMG geëxploiteerde websites en plaatsing van een rectificatie met de in het petitum van de dagvaarding opgenomen tekst, zowel online als in de papieren versie van De Telegraaf wordt afgewezen.*

### 59. Gerechtshof Arnhem-Leeuwarden 30 januari 2018 (SourceLogic), ECLI:NL:GHARL:2018:974

Domeinnaam, registratie, overdracht, email, verzoek via email, privé mailadres, zakelijk mailadres, inloggegevens

*Geschil rond de registratie en overdracht van domeinnamen.*

*A had voor SourceLogic domeinnamen geregistreerd via Deziweb. Vanaf november 2013 was A niet meer vertegenwoordigingsbevoegd voor SourceLogic. C vraagt als nieuwe vertegenwoordiger van SourceLogic aan Deziweb om de domeinnamen over te dragen aan ESP.*
*Afgaande op de e-mailcorrespondentie is naar het oordeel van het hof dan ook goed te begrijpen dat Deziweb in reactie op de verzoeken van C om de domeinen op naam van ESP te zetten bij herhaling een probleem heeft gemaakt van het feit dat deze verzoeken per mail aan Deziweb werden gericht; Deziweb wees op de fraudegevoeligheid van dergelijke verzoeken en verwees telkens naar de beschermde ICT-omgeving voor het doorvoeren van dergelijke wijzigingen, met gebruikmaking van de beschikbaar gestelde inlogtools. Op basis van deze correspondentie ziet het hof niet in dat Deziweb onjuist heeft gehandeld door C in november 2013 mee te delen dat haar contactpersoon tot dat moment, A, bevoegd en in staat was dergelijke handelingen voor SourceLogic te verrichten. Dat Deziweb er in die periode van op de hoogte was of kon zijn dat de bevoegdheden van A als vertegenwoordiger van SourceLogic waren komen te vervallen, blijkt uit het e-mailverkeer namelijk niet - laat staan dat Deziweb duidelijk was dat C als diens opvolger (indien hij al bevoegd was SourceLogic te vertegenwoordigen, wat ook niet uit de correspondentie blijkt) niet beschikte over de inloggegevens van Deziweb. Daarbij verdient opmerking dat C voortdurend gebruikmaakte van een privé-mailadres, en niet van een zakelijk mailadres van SourceLogic (of ESP of IT Management). Niet valt in te zien dat, en waarom, Deziweb onder dergelijke omstandigheden onderzoek had moeten doen naar de positie en bevoegdheden van A en/of C .*

### 60. Rechtbank Den Haag 31 januari 2018 (toestemming tot wederbericht), ECLI:NL:RBDHA: 2018:1079

Auteursrecht, cartoons op website, email, online archief, toestemming, intrekken toestemming, licentie

*Arvy, auteursrechthebbende op cartoon, had aan Doorbraak 'tot wederbericht' toestemming. In het licht van deze maatstaf acht de rechtbank in de eerste plaats van belang dat partijen, zoals hiervoor reeds werd vastgesteld, over de toestemming en de voorwaarde(n) waaronder deze werd verleend uitsluitend per e-mail hebben gecommuniceerd. Deze communicatie bestaat uit niet meer dan drie korte e-mails en vangt aan met twee verzoeken zijdens Doorbraak om toestemming de cartoons van Arvy – met bronvermelding – in de krant 'te plaatsen' en op de website 'te zetten'. Waar deze bewoordingen duiden op eenmalige, actieve handelingen had het voor eiser duidelijk moeten zijn dat de betrokken medewerkers van Doorbraak er onmiskenbaar vanuit gingen dat met het verkrijgen van toestemming voor die handelingen de kous af was, in die zin dat eenmaal met toestemming overgenomen en geplaatste cartoons ook geplaatst konden blijven. De rechtbank neemt daarbij in aanmerking dat Doorbraak geen professioneel medium is en dat haar medewerkers slechts een beperkte kennis van het auteursrecht hebben.*

*Tegen deze achtergrond is de rechtbank van oordeel dat Doorbraak er bij gebreke van enige nadere toelichting van de zijde van eiser niet bedacht op hoefde te zijn dat de aan diens toestemming verbonden voorwaarde 'tot wederbericht' niet alleen inhield dat er vanaf dat moment geen nieuwe cartoons meer mochten worden overgenomen, maar dat ook reeds eerder overgenomen cartoons weer dienden te worden verwijderd. De rechtbank laat daarbij meewegen dat een dergelijke verwijderingsplicht bij het gebruik van cartoons in nieuwsmedia hoogst ongebruikelijk is. Voorts weegt zwaar mee dat eiser, zoals ook uit de overgelegde producties blijkt, al vóór 3 december 2012 een regelmatige en actieve bezoeker van de Doorbraak-website was, zodat ervan uitgegaan mag worden dat hij ermee bekend was dat artikelen en de Doorbraak-kranten volledig beschikbaar bleven via het online archief op die website.*

### 61. Rechtbank Limburg 2 februari 2018 (opruiing via Tweets), ECLI:NL:RBLIM:2018:1073

Strafrecht, Twitter, Tweets, opruiing, art. 131 Sr

*Veroordeling voor opruiende tweets. Oproepen om geweld tegen politieagenten te gebruiken. De rechtbank is van oordeel dat met de door de verdachte in zijn berichten op Twitter gebruikte woorden expliciet wordt opgeroepen tot het plegen van een in Nederland strafbaar feit, namelijk een terroristisch misdrijf en het plegen van geweld tegen het openbaar gezag, namelijk tegen de politie. Door het plaatsen van de berichten roept de verdachte anderen op om agenten van de politie te vermoorden, waarmee de bevolking, of in ieder geval een deel ervan, ernstige vrees zou worden aangejaagd.*
*Volgt veroordeling tot 6 maanden voorwaardelijke gevangenisstraf en 80 uren taakstraf.*

### 62. Rechtbank Den Haag 5 februari 2018 (Regio15),ECLI:NL:RBDHA:2018:1227

Auteursrecht, filmpje op internet, watermerk, persoonlijkheidsrecht, video, hoogte schadevergoeding

*Eiser is maker van een videoreportage gevoegd bij het artikel 'Veel overlast door overvloedige regen' (hierna: de video) op 23 juni 2016 gepubliceerd op regio15.nl. Op 5 august 2016 is heeft eiser geconstateerd dat gedaagde op zijn website welingelichtekringen.nl (beelden van) de video heeft geplaatst. Daarbij heeft gedaagde niet de naam van eiser afgebeeld. Gedaagde heeft voor dit gebruik van de video geen toestemming aan eiser gevraagd.*
*Voor zover in gedaagde' verweer moet worden gelezen dat hij er niet op bedacht had behoeven te zijn dat hij de video niet zonder meer mocht openbaar maken op zijn eigen website, heeft te gelden dat dit niet aan het aannemen van auteursrechtinbreuk in de weg staat. Bovendien had hij door het watermerk in de video kunnen weten dat de rechten op de video bij eiser lagen. Dat er een watermerk in de door NOS openbaar gemaakte video was aangebracht, is door gedaagde onvoldoende gemotiveerd weersproken. Van een partij zoals gedaagde die op zijn website veelvuldig gebruik maakt van beelden van derden, mag worden verwacht dat hij controleert of hij toestemming voor publicatie heeft. Zoals gedaagde naar voren heeft gebracht, heeft hij met ANP en Hollandse Hoogte contracten gesloten voor hergebruik van beeldmateriaal. In dat licht bezien, valt niet goed te begrijpen dat hij er zonder meer vanuit is gegaan dat hij geen toestemming behoefde voor het overnemen van een video.*
*Gedaagde heeft ook watermerk verwijderd en daarmee inbreuk gemaakt op persoonlijkheidsrecht van eiser.*
*Totale toegewezen schadevergoeding € 1875,50.*

### 63. Rechtbank Den Haag 8 februari 2018 (sok met uien), ECLI:NL:RBDHA:2018:1355

Strafrecht, marktplaats-oplichting, identiteitsfraude, art. 231b Sr, art. 326 Sr

*De verdachte heeft zich gedurende een periode van ongeveer zeven maanden schuldig gemaakt aan oplichting. Op de internetsite www.marktplaats.nl heeft de verdachte zich voorgedaan als bonafide verkoper, waarbij hij zich telkens van een valse naam bediende.*
*De geldbedragen voor de gekochte goederen werden telkens op een bankrekening, die aan de verdachte kon worden gekoppeld dan wel die door de verdachte werd gebruikt, overgemaakt. In goed vertrouwen hebben de aangevers de bedragen overgemaakt, in de veronderstelling dat de goederen zouden worden opgestuurd. De verdachte liet hen in die waan. Er zijn geen gekochte en betaalde goederen geleverd. Vaak is er niets ontvangen, soms een pakketje met een steen erin of zelfs ook een sok met daarin twee uien.*
*De verdachte heeft bij de oplichting van de aangevers ook een aantal malen gebruik gemaakt van de identiteit van een ander en zich aldus schuldig gemaakt aan identiteitsfraude.*
*Volgt veroordeling tot 100 uren werkstraf en schadevergoeding aan benadeelde partijen.*

### 64. Rechtbank Limburg 12 februari 2018 (100 personen opgelicht), ECLI:NL:RBLIM:2018:1407

Strafrecht, oplichting, marktplaats, speurders, Facebook, art. 326 Sr

*De verdachte heeft via Marktplaats.nl, Facebook en Speurders.nl ruim 100 personen opgelicht. Zodoende heeft hij de betrokkenen elk tientallen, soms honderden en in totaal duizenden euro's afhandig gemaakt en in teleurstelling achtergelaten. Oplichtingspraktijken als de onderhavige schaden het vertrouwen in eerlijke handel en verstoren de werking van dergelijke toegankelijke en populaire handelsforums. De oplichtingen getuigen van brutaliteit en egoïsme.*
*Volgt veroordeling tot 2 maanden voorwaardelijke jeugddetentie en 150 uren taakstraf, en schadevergoeding aan slachtoffers.*

## 65. Gerechtshof Arnhem-Leeuwarden 13 februari 2018 (kenbaarheid tarieventabel), ECLI:NL:GHARL:2018:1360

Belastingrecht, publicatie op website, overheid.nl, toegankelijkheid, kenbaarheid, heffingsmaatstaf, Legesverordening, art. 139 Gemeentewet, art. 217 Gemeentewet

*Tussen partijen is in geschil of de heffingsmaatstaf overeenkomstig art. 217 Gemeentewet in de Legesverordening is vermeld, aangezien voor de maatstaf van heffing wordt verwezen naar de aannemingssom, bedoeld in paragraaf 1, eerste lid, van de 'Uniforme Administratieve Voorwaarden voor de uitvoering van werken 2012 (UAV 2012)', terwijl deze regeling door de gemeente niet is bekendgemaakt.*
*In art. 139 en 217 Gemeentewet worden eisen gesteld aan de kenbaarheid van de maatstaven waarnaar gemeentebelastingen worden geheven. Door de verwijzing naar de UAV 2012 in de Legesverordening, wordt de UAV 2012 niet zelf een algemeen verbindend voorschrift, waarop art. 139 Gemeentewet van toepassing is. De kenbaarheid van de UAV 2012 dient niettemin voor de belastingplichtige verzekerd te zijn, omdat de belastingplichtige de omvang van zijn belastingschuld moet kunnen afleiden uit de in de Legesverordening genoemde essentialia. De toegankelijkheid en kenbaarheid van de UAV 2012 zijn naar het oordeel van het Hof voldoende gewaarborgd, doordat deze als bijlage bij de genoemde beschikking is gepubliceerd in de Staatscourant en de beschikking is geplaatst op de websites www.officielebekendmakingen.nl en www.overheid.nl. Een belastingplichtige kan aan de hand van de Legesverordening en de UAV 2012 de maatstaf van heffing bepalen, zodat van een onverbindendheid van de Legesverordening op dit punt geen sprake is.*

## 66. Rechtbank Amsterdam 14 februari 2018 (betaling in Bitcoin), ECLI:NL:RBAMS:2018:869

Faillissementsrecht, bitcoin, wallet, vermogensrecht, verificatie, verplichting tot betaling, vorderingsrecht, betalen, art. 1 Fw

*Een bitcoin bestaat, zo begrijpt de rechtbank, uit een unieke, digitaal versleutelde reeks van cijfers en letters opgeslagen op de harde schijf van de computer van de rechthebbende. Bitcoins worden 'geleverd' door het verzenden van bitcoins van de ene wallet naar de andere wallet. Bitcoins zijn op zichzelf staande waarde-bestanden, die bij een betaling rechtstreeks door de betaler aan de begunstigde worden geleverd. Hieruit volgt dat een bitcoin een waarde vertegenwoordigt en overdraagbaar is. Naar het oordeel van de rechtbank vertoont het hiermee kenmerken van een vermogensrecht. Een vordering tot betaling in bitcoin is dus te beschouwen als een vordering die voor verificatie in aanmerking komt.*
*Onbetwist staat vast dat tussen verzoeker en gerekestreerde een verbintenis bestaat die strekt tot betaling van bitcoin, welke verbintenis ook in bitcoins moet worden voldaan. De rechtbank kwalificeert deze rechtsverhouding als een civielrechtelijke verplichting tot betaling. Aan deze verplichting is tot op heden door gerekestreerde niet voldaan. Van een vorderingsrecht is dus summierlijk gebleken. Is echter ook voldaan aan het vereiste dat gebleken is van de toestand dat gerekestreerde opgehouden is te betalen? De term betalen ziet niet alleen op voldoening van een geldvordering, maar meer algemeen op voldoening aan een verbintenis (HR 3 juni 1921, NJ 1921, p. 968). Onbetwist staat vast dat de vordering die verzoeker op gerekestreerde heeft niet door gerekestreerde is voldaan. Ter terechtzitting heeft verzoeker het bestaan van meerdere (steun)vorderingen aangetoond. Uit de door verzoeker overgelegde stukken is gebleken dat meerdere personen vorderingen op gerekestreerde hebben die zien op het uitbetalen van bitcoins of op vorderingen wegens niet nakomen van verplichtingen uit een overeenkomst, met in sommige gevallen daaraan verbonden dwangsommen.*

## 67. Rechtbank Amsterdam 15 februari 2018 (Overstappen), ECLI:NL:RBAMS:2018:821

Auteursrecht, foto op website, hoogte schadevergoeding, watermerk, boete, punitive damages

*Geoordeeld wordt dat met het zonder nader onderzoek downloaden en gebruiken van een op het internet circulerende foto Overstappen.nl het risico heeft genomen dat op die foto auteursrecht rustte.*
*Onvoldoende is gesteld om ervan uit te kunnen gaan dat de kopie van de foto zoals door Overstappen.nl van een andere site dan die van Masterfile is gedownload daar bewust door Masterfile zelf is geplaatst om overtreding uit te lokken. Het enkele feit dat foto's zonder meer illegaal (zonder watermerk) van de site van Masterfile zelf kunnen worden gedownload, zoals onbetwist is gesteld, en daardoor makkelijker kunnen worden verspreid is, gelet op de belangen die Masterfile zegt te behartigen, zeker merkwaardig, maar onvoldoende om van uitlokking te kunnen spreken. Deze gang van zaken is dus niet van invloed op de hoogte van de eventueel door Overstappen.nl te betalen schadevergoeding.*
*Voor de hoogte van het bedrag dat Masterfile in rekening had mogen brengen indien toestemming was gevraagd wordt uitgegaan van de door Overstappen.nl uitgevoerde berekening die uitkomt op € 290,00, nu die uitkomst bij de door Overstappen.nl gebruikte variabelen op zichzelf niet door Masterfile wordt betwist.*
*Masterfile vordert een verhoging van de schadevergoeding van 100% van het reguliere tarief, door haar opslag genoemd. Uit haar stelling dat de opslag gerechtvaardigd is omdat het niet aantrekkelijk gemaakt moet worden om een auteursrechtinbreuk achteraf te herstellen door het betalen van het gangbare tarief, kan worden opgemaakt dat zij deze opslag ziet als een boete. Een dergelijke boete kent het Nederlands schadevergoedingsrecht bij onrechtmatige daad evenwel niet, dus op deze grond is het bedrag aan opslag niet toewijsbaar.*
*Een hogere schadevergoeding dan onder 13 genoemd is dan ook alleen toewijsbaar indien vast komt te staan dat deze schade daadwerkelijk door Masterfile is geleden. Zij dient daarvoor feiten en omstandigheden te stellen. Masterfile heeft in dat verband gesteld, kennelijk subsidiair, dat zij kosten maakt voor het opsporen van inbreuk en daartoe derde partijen inschakelt. Deze*

*stelling heeft zij echter niet nader uitgewerkt, zodat hieraan voorbij wordt gegaan.*
*Volgt veroordeling tot € 290 schadevergoeding.*

### 68. Rechtbank Midden-Nederland 15 februari 2018 (bitcoin minen), ECLI:NL:RBMNE:2018:368

Arbeidsrecht, bitcoin minen, bitcoinmachine, ontslag op staande voet, vertrouwen, integriteit, dringende reden

*Geschil over ontslag op staande voet van systeembeheerder die een zogenaamde bitcoinmachine had geïnstalleerd in een serverkast op zijn werk.*
*Rechter: oordeel dat voorgaande gronden alleen niet tot een ontslag op staande voet leiden. Het zwaartepunt in deze zaak ligt in het gebrek aan vertrouwen dat verweerster naar aanleiding van dit incident in verzoeker heeft gekregen. Ook dit heeft zij aan het ontslag ten grondslag gelegd. Verweerster stelt daarbij dat zij volledig wil kunnen vertrouwen op een systeembeheerder en van iemand met een dergelijke functie moet kunnen verwachten dat hij volledig integer handelt. De kantonrechter is met verweerster van oordeel dat verzoeker had moeten aanvoelen dat hij met dit gedrag een grens heeft overschreden, met name nu dit heimelijk is gegaan. Hij heeft hierbij een grote inschattingsfout gemaakt. Van een systeembeheerder moet je kunnen verwachten dat hij integer en betrouwbaar is en het plaatsen van een bitcoinmachine binnen een bedrijfsomgeving voor eigen gebruik valt daar niet onder. Wat in deze zaak zwaar meeweegt is dat verzoeker nooit eerder dergelijk gedrag heeft getoond en dat niet gebleken is dat zijn werkzaamheden er onder hebben geleden. De kantonrechter is van oordeel dat deze gemaakte fout hem niet zodanig zwaar moet worden aangerekend dat het gelet op alle omstandigheden van het geval als een dringende reden kwalificeert.*

### 69. Rechtbank Oost Brabant 19 februari 2018 (ex politieagent), ECLI:NL:RBOBR:2018:735

Strafrecht, computercriminaliteit, schending ambtsgeheim, computervredebreuk, omkoping, witwassen, criminele organisatie, identiteitsfraude, valse reisdocumenten, media-aandacht, sociale media, art. 138ab Sr, art. 140 Sr, art. 231 Sr, art. 272 Sr, art. 362 Sr, art. 420bis Sr, art. 420ter Sr

*Verdachte is, ondanks zijn strikte geheimhoudingsplicht, zonder ambtelijk doel gericht gaan zoeken in het hem uit hoofde van zijn functie ter beschikking staande en voor hem toegankelijke politiesysteem en hij heeft de door hem gevonden informatie veelvuldig gedeeld met medeverdachten.*
*Gezien het grote aantal bevragingen en abonnementen op andere personen dan de medeverdachten, gaat de rechtbank er bij de bepaling van strafmaat van uit dat verdachte ook bij een aanzienlijk aantal andere personen dan de medeverdachten het ambtsgeheim heeft geschonden.*
*Niet alleen heeft verdachte de vertrouwelijk politie-informatie schaamteloos met anderen gedeeld, hij heeft er zich op enig moment ook voor laten betalen in de vorm van een belofte voor een toekomstige zakelijke samenwerking bij de handel van onder andere versleutelde (encrypted) telefoons en diamanten.*
*Het is een feit dat deze zaak en de rol van verdachte daarin breed zijn uitgemeten in de pers en de social media. Deze media-aandacht heeft verdachte echter over zichzelf afgeroepen, immers hij is degene die ernstige strafbare feiten gedurende lange tijd heeft gepleegd. De grote media-aandacht geeft ook aan hoe zeer verdachte de rechtsorde heeft geschokt. Voor strafmatiging om deze reden ziet de rechtbank geen enkele aanleiding.*
*Volgt veroordeling tot 5 jaar gevangenisstraf en ontzetting uit het recht om een publieke functie uit te oefenen voor de duur van 10 jaren.*

### 70. Rechtbank Limburg 21 februari 2018 (fysio), ECLI:NL:RBLIM:2018:1801

Handelsnaamrecht, domeinnaam, bijkomende omstandigheden, verwarring, patiëntgegevens

*Geschil tussen Fysio Roermond en Fysiotherapie Roermond. De kantonrechter is van oordeel dat de handelsnaam van verzoeker (Fysio Roermond) zuiver beschrijvend van karakter is. Immers de aanduidingen 'fysio' beschrijft de diensten die verzoeker aanbiedt terwijl het woord 'Roermond' aanduidt in welke plaats die diensten worden aangeboden.*
*In zijn arrest van 11 december 2015, ECLI:NL:HR:2015:3554 heeft de Hoge Raad geoordeeld dat het in beginsel voor een ieder mogelijk moet zijn zich van een aanduiding te bedienen die beschrijvend is voor zijn diensten of producten en dat het gebruik van een dergelijke aanduiding, ook als dit gevaar voor verwarring veroorzaakt, alleen onrechtmatig is indien bijkomende omstandigheden dat meebrengen.*
*In dat verband heeft verzoeker gesteld dat hij vreest dat patiëntengegevens bij de verkeerde praktijk terechtkomen, wat gelet op het delicate karakter daarvan een zeer ernstige kwestie is. Naar het oordeel van de kantonrechter is dit, zo dit zich al zou voordoen, echter geen bijkomende omstandigheid zoals door de Hoge Raad wordt bedoeld.*

### 71. Rechtbank Oost-Brabant 23 februari 2018 (leraar), ECLI:NL:RBOBR:2018:830

Strafrecht, kinderporno, seksuele verleiding, poging, vrijwillige terugtred, art. 240b Sr, art. 248a Sr

*Verdachte heeft via de privé-accounts van in elk geval twee van de drie in de tenlastelegging genoemde leerlingen aan hen berichten verzonden met de vraag, kort gezegd, of zij bereid waren ontuchtige handelingen te verrichten of van verdachte te dulden. Verdachte heeft daarbij kenbaar gemaakt dat ze daarvoor een hoger cijfer konden krijgen.*
*De drie betrokken leerlingen hebben daar met elkaar over gesproken en waren eensgezind van mening dat verdachte ongepaste seksuele diensten van hen verlangde, zij hebben verdachte daar ook op gewezen (onder meer door verdachte op hun leeftijd te wijzen) en zijn niet ingegaan op het verzoek van verdachte. Zij hebben*

*vervolgens van de app-conversatie melding gemaakt bij de schoolleiding.*
*Toen het voor verdachte duidelijk werd dat de leerlingen niet op zijn aanbod wilden ingaan heeft verdachte die leerlingen verzocht de over en weer verstuurde berichten uit hun telefoon te verwijderen en de berichten ook zelf verwijderd.*
*De rechtbank acht gelet op het voorgaande en gelet op de inhoud van de door verdachte verstuurde berichten en de opbouw daarvan, niet aannemelijk dat aan het verzoek van verdachte om de berichten te verwijderen, een wilsbesluit ten grondslag ligt om zijn voorgenomen gedragingen niet te voltooien.*
*Volgt veroordeling tot 9 maanden gevangenisstraf waarvan 6 maanden voorwaardelijk en 200 uur taakstraf.*

## 72. Rechtbank Den Haag 27 februari 2018 (advies kindertelefoon),ECLI:NL:RBDHA:2018:2285

Strafrecht, sextortion, ontucht, mensenhandel, filmpje op internet, Whatsapp, art. 245 Sr, art. 273f Sr

*De verdachte heeft zich schuldig gemaakt aan mensenhandel ten aanzien van de destijds veertien- respectievelijk vijftienjarige slachtoffer. De verdachte heeft tevens verschillende keren seksueel contact met haar gehad en zich aldus schuldig gemaakt aan het plegen van ontucht met iemand die de leeftijd van twaalf, maar nog niet die van zestien jaren heeft bereikt. Nadat hij het vertrouwen van slachtoffer had gewonnen, heeft de verdachte haar op manipulatieve wijze ertoe aangezet om zich te prostitueren door onder meer te dreigen een seksfilmpje waarop te zien is dat slachtoffer de verdachte pijpt aan haar familie en schoolvriendinnen te sturen. Hierbij moest slachtoffer alle opbrengsten uit de prostitutie aan de verdachte afstaan.*
*Volgt veroordeling tot 5 jaar gevangenisstraf en schadevergoeding aan slachtoffer.*

## 73. Gerechtshof 's-Hertogenbosch 27 februari 2018 (ring met diamant), ECLI:NL:GHSHE:2018:831

E-commerce, verzending, risico van verzending

*Koop gouden ring met diamant via internet. Ring is wel aan de koper verzonden, maar zat bij aankomst van de zending bij de koper niet in de envelop.*
*Bewijswaardering dienaangaande. Dat de ring wel is verzonden maar bij aankomst van de zending niet meer in de envelop zat, komt voor rekening en risico van de verkoper, nu die zich als verkopende partij bij de verkoop van een ring aan een consument van deze methode van verzending heeft bediend.*

## 74. Raad van State 28 februari 2018 (besluitenlijst op internet), ECLI:NL:RVS:2018:702

Bestuursrecht, publicatie op internet, besluitenlijst, persoonlijke levenssfeer, persoonsgegevens, adres, proportionaliteit, art. 60 Gemeentewet, art. 8 EVRM

*Uit de besluitenlijst die het college op internet heeft gepubliceerd kan worden afgeleid dat appellant bezwaar heeft gemaakt tegen een besluit van het college op een door hem ingediend Wob-verzoek en dat het college akkoord is met het voorstel om het bezwaar gegrond te verklaren wat betreft de motivering van het besluit, het bestreden besluit met een verbeterde motivering in stand te laten en appellant geanonimiseerde loonstaten, dan wel salarisstroken, te verstrekken. Hierbij zijn de initialen, achternaam, straat, huisnummer en woonplaats van appellant vermeld.*
*Appellant heeft niet toegelicht waarom zijn persoonlijke levenssfeer ernstig zou worden aangetast doordat zijn initialen, achternaam en woonplaats op internet zijn gepubliceerd en in verband worden gebracht met een door hem ingediend Wob-verzoek over loonstaten, dan wel salarisstroken. Voor zover het deze persoonsgegevens betreft, is de Afdeling dan ook van oordeel dat het belang bij openbaarmaking zwaarder weegt dan het belang van appellant bij eerbiediging van zijn persoonlijke levenssfeer en het college het verzoek in zoverre heeft mogen afwijzen. In deze inmenging in de uitoefening van het recht van appellant op respect voor zijn privéleven als bedoeld in art. 8 EVRM is in de wet, namelijk art. 60 lid 3 Gemeentewet, voorzien. Voorts is de inmenging proportioneel en in een democratische samenleving noodzakelijk in het belang van de bescherming van de rechten en vrijheden van anderen. Er doet zich derhalve geen strijd met art. 8 EVRM voor.*
*Ter zitting van de Afdeling is namens het college desgevraagd toegelicht dat er geen argumenten zijn om ook het adres van een betrokkene te publiceren. Mede gelet op de risico's van het op internet publiceren van persoonsgegevens, is de Afdeling van oordeel dat voor zover het de straat en het huisnummer van het adres van appellant betreft, het belang van het publiceren daarvan op de besluitenlijst op internet niet opweegt tegen het belang van appellant bij eerbiediging van zijn persoonlijke levenssfeer. In zoverre is de verwerking van persoonsgegevens derhalve in strijd met het openbaar belang en dient het college die te verwijderen.*

## 75. Rechtbank Gelderland 2 maart 2018 (cadeaubonnen), ECLI:NL:RBGEL:2018:957

Strafrecht, computervredebreuk, inloggen, digitaal kerstpakket, cadeaubon, art. 138ab Sr, art. 311 Sr, art. 350a Sr

*Verdachte heeft zich schuldig gemaakt aan computercriminaliteit. Als medewerker van een helpdeskafdeling kon hij inloggen in een systeem waarin gegevens stonden van werknemers van verschillende bedrijven die via internet met deze inloggegevens een keuze konden maken voor hun kerstpakket. Hiervoor moesten zij op een speciale website inloggen waarna zij vervolgens onder meer cadeaubonnen van meerdere winkels konden aanschaffen. Verdachte heeft in dit systeem onbevoegd aanpassingen gedaan om zo over vele inloggegevens te kunnen beschikken. Hij deed zich eigenlijk voor als een werknemer die zijn kerstcadeau wilde uitkiezen en schafte op deze manier meer dan 1500 cadeaubonnen aan ter waarde van bijna een ton. Om zijn sporen uit te wissen heeft verdachte de door hem gebruikte gegevens*

*later weer gewist. Met zijn handelen heeft verdachte computervredebreuk gepleegd en digitale gegevens gemanipuleerd. Daarnaast heeft hij zich samen met een ander schuldig gemaakt aan diefstal door de cadeaubonnen te bestellen. Het totale bedrag van die bonnen is namelijk voor rekening gekomen van het bedrijf dat de digitale kerstpakketten aanbood.*
*Verdachte heeft zijn kennis van de digitale wereld misbruikt en daarmee het vertrouwen dat eenieder moet kunnen hebben in het gebruik van interne systemen en het internet geschaad.*
*Volgt veroordeling tot 2 maanden voorwaardelijke gevangenisstraf en 150 uur werkstraf.*

### 76. Rechtbank Noord-Nederland 2 maart 2018 (identiteitsfraude WhatsApp), ECLI:NL:RBNNE:2018:727

Strafrecht, WhatsApp, oplichting, identiteitsfraude, art. 326 Sr, art. 421 Sr

*Verdachte heeft zich schuldig gemaakt aan twaalf gevallen van een geraffineerde manier van oplichting van particulieren. De slachtoffers werden via WhatsApp benaderd waarbij verdachte of een medeverdachte zich voordeed als een familielid of goede bekende van het slachtoffer. Door het meesturen van een foto van die ander en eventueel het noemen van persoonlijke details, werd het vertrouwen gewonnen van het desbetreffende slachtoffer. Het slachtoffer dacht dan ook echt met het familielid of de goede bekende te WhatsAppen. In de loop van het WhatsApp gesprek werd het slachtoffer overgehaald om een (of meerdere) grote geldbedrag(en) over te maken naar bepaalde bankrekeningnummers. Het geld werd vervolgens contant opgenomen van die rekeningen en kwam zo in handen van verdachte en/of zijn mededader(s). Het slachtoffer bleef met lege handen achter.*
*De houders van de bankrekeningen waarnaar het geld werd overgemaakt, kwamen vrij snel in de problemen, hun bankrekening werd geblokkeerd, omdat zij voor de politie (en de banken) gemakkelijk traceerbaar waren. Een deel van deze bankrekeninghouders wist niet dat verdachte hun rekeningnummer zou gebruiken voor het oplichten van mensen.*
*Volgt veroordeling tot 18 maanden gevangenisstraf.*

### 77. Rechtbank Rotterdam 5 maart 2018 (publicatie boetes AFM), ECLI:NL:RBROT:2018:1725

Bestuursrecht, publicatie van boete op internet, schandpaal, reputatieschade, kleine gemeenschap, maatschappelijk belang, art. 198 Wft

*De AFM is in beginsel gehouden de besluiten tot het opleggen van een bestuurlijke boete zo spoedig mogelijk openbaar te maken, tenzij bekendmaking van persoonsgegevens onevenredig zou zijn of betrokken partijen in onevenredige mate schade zou worden berokkend. Daarvan is sprake als het gaat om een individuele, bijzondere situatie, waarin de door verzoekers als gevolg van de publicatie te verwachten schade en/of gevolgen zodanig uitzonderlijk zijn dat het belang van de bescherming van de markt daarvoor moet wijken (vergelijk overweging 12.3 van de uitspraak van het College van Beroep voor het bedrijfsleven (CBb) van 12 oktober 2017, ECLI:NL:CBB:2017:327).*
*Van een dergelijke situatie is in het geval van verzoekers naar het oordeel van de voorzieningenrechter geen sprake. Verzoekers hebben in dit verband aangevoerd dat een publicatie op internet verder verspreid zal worden en niet meer van het internet verdwijnt, dat zij natuurlijke personen zijn, dat zij in een kleine gemeenschap leven en dat reputatieschade voor hen ernstige gevolgen heeft.*
*Dat publicatie zal leiden tot reputatieschade is gelet op de genoemde uitspraak van het CBb van 12 oktober 2017 en de strekking van art. 1:98 lid 1, aanhef en onder a, Wft op zichzelf onvoldoende om publicatie van de boetes onevenredig te achten. Dat wordt niet anders als in aanmerking wordt genomen dat verzoekers naar gesteld in een kleine gemeenschap leven, dat de publicatie op internet verspreid zal worden en niet meer van internet verwijderd zal kunnen worden. Ook deze omstandigheden zijn niet bijzonder, laat staan uitzonderlijk. Dat publicatie van de opgelegde boetes impact zal hebben op de gezinsleden van verzoekers is evenmin uitzonderlijk.*
*Verder heeft de AFM van belang kunnen achten dat de markt wordt voorgelicht over de aan verzoekers opgelegde boetes. Het betreft hier ernstige overtredingen, omdat consumenten erop moeten kunnen vertrouwen dat een vergunninghouder beschikt over beleidsbepalers die door de AFM zijn getoetst op betrouwbaarheid en geschiktheid. Het nadeel dat verzoekers in hun professionele loopbaan kunnen ondervinden van de publicatie van de boetebesluiten is mede in dit licht bezien geen onevenredig nadeel bij publicatie en vormt daarom geen bijzondere individuele situatie. Dat verzoeker niet meer werkzaam is in de financiële sector maakt dit niet anders.*

### 78. Rechtbank Den Haag 7 maart 2018 (Vestival), ECLI:NL:RBDHA:2018:2643

Domeinnaam, merkenrecht, merkinbreuk, social media account, Facebook, Twitter, Instagram, mogelijkheid tot naamswijziging, goodwill, overdracht van account, databankenrecht, volgers als databank

*Aangezien het merkinbreukverbod wordt toegewezen, valt daaronder ook het gebruik van de domeinnaam met daarin het bestanddeel VESTIVAL. De domeinnaam wordt immers gebruikt ter onderscheiding van waren of diensten (in dit geval het muziekfestival van Havensluis c.s.) en het onderscheidende bestanddeel van de domeinnaam vestival.eu komt overeen met het dominante bestanddeel van het gele merk. Havensluis c.s. heeft op dit punt ook geen verweer gevoerd. Onder het merkinbreukverbod valt ook het doorlinken vanaf die domeinnaam naar een andere domeinnaam zonder het inbreukmakende bestanddeel.*
*De gevorderde tenaamstelling van deze domeinnaam is eveneens toewijsbaar, aangezien eiser er (spoedeisend) belang bij heeft dat deze domeinnaam wordt gebruikt ten behoeve van het gele merk en niet is gesteld of geble-*

*ken welk belang Havensluis c.s. heeft bij het aanhouden van een inbreukmakende domeinnaam.*
*Met betrekking tot de social-media-accounts (Facebook, Twitter en Instagram) ligt dit anders. Voor zover deze accounts een inbreukmakende naam hebben en/of deze gebruikt worden voor het aanbieden of promoten van muziekfestivals, valt ook dat gebruik onder het op te leggen inbreukverbod. Aangezien voor deze accounts (anders dan voor een domeinnaam) de mogelijkheid tot naamswijziging bestaat – zoals reeds met het Facebook-account is gebeurd –, bestaat er voorshands geen grond voor overdracht van deze accounts. Zonder nadere toelichting – die eiser niet heeft gegeven – valt niet in te zien dat het gebruik van deze accounts na naamswijziging, en met inachtneming van het inbreukverbod, nog inbreukmakend is op de merkrechten van eiser.*
*Voorshands is voorts onvoldoende duidelijk dat eiser recht heeft op de door hem beoogde overdracht van de volgers van de betreffende accounts. De enkele omstandigheid dat er sprake is geweest van inbreuk op een merk betekent niet zonder meer dat de merkrechthebbende recht heeft op overdracht van de goodwill die de inbreukmaker heeft gegenereerd. Om te beoordelen aan wie die goodwill (in de vorm van volgers) toekomt is nader feitenonderzoek noodzakelijk waarvoor dit kort geding zich niet leent. Hierbij zullen vragen spelen als: (i) hoeveel van die goodwill moet worden toegeschreven aan het inbreukmakende merkgebruik, (ii) hoeveel van die goodwill moet worden toegeschreven aan de (goede) organisatie van het evenement (hoe ook geheten) en bijbehorende line-up van artiesten, (iii) hoeveel volgers waren er in 2016 toen Havensluis c.s. de organisatie van A overnam en (iv) hoeveel is er door welke partij in de goodwill geïnvesteerd. Voor zover eiser stelt dat de volgers kunnen worden aangemerkt als een databank faalt deze grondslag omdat niet voldoende aannemelijk is dat hij rechthebbende van die (beweerdelijke) databank is. Volgens art. 1 onder b en art. 2 Databankenwet is rechthebbende de producent van de databank, dat wil zeggen degene die het risico draagt van de voor de databank te maken investering. Havensluis c.s. heeft gesteld dat zij tijdens haar beheer het aantal Facebook-volgers door middel van aanzienlijke investeringen heeft doen toenemen van 30 tot 64.000, terwijl eiser niet aannemelijk heeft gemaakt dat hij op enige wijze in deze accounts of de volgers heeft geïnvesteerd.*

## 79. Gerechtshof 's-Hertogenbosch 7 maart 2018 (illegaal vuurwerk uit Polen), ECLI:NL:GHSHE:2018:919

Strafrecht, handel via internet in illegaal vuurwerk, art. 174 Sr, art. 1.2.2 Vuurwerkbesluit
*Verdachte heeft gedurende enkele maanden, voor een deel alleen, voor een deel samen met medeverdachte via internet illegaal vuurwerk verkocht aan klanten in Nederland.*

*Omdat dit vuurwerk in Nederland verboden is, bestelde verdachte het vuurwerk in Polen en liet hij het vervolgens vanuit Polen door verschillende pakketdiensten bij de klanten in Nederland afleveren. Op de verpakkingen stond niet vermeld wat de inhoud was, zodat de bezorgers aan grote gevaren werden blootgesteld zonder dat zij daarvan op de hoogte waren.*
*Verdachte heeft onwetende derden aan gevaar blootgesteld, uitsluitend met het doel om zelf winst te behalen.*
*Ook de ontvangers van het vuurwerk zijn door verdachte niet op de hoogte gesteld van de gevaren, nu die gevaren niet op de website van verdachte waren vermeld en er bij het vuurwerk geen Nederlandse gebruiksaanwijzingen geleverd werden.*
*Bovendien konden zij, dan wel hun huisgenoten, niet weten wat zij in ontvangst namen, nu op de verpakking niet dan wel niet op de juiste wijze was aangegeven wat er zich in de verpakking bevond.*
*Aldus heeft verdachte door zijn handelen onverantwoorde risico's genomen en de gezondheid en veiligheid van mensen ernstig in gevaar gebracht.*
*Volgt veroordeling tot 720 dagen gevangenisstraf, waarvan 484 dagen voorwaardelijk.*

## 80. Rechtbank Gelderland 9 maart 2018 (gratis afslankpillen), ECLI:NL:RBGEL:2018:1149

E-commerce, consumentenrecht, oneerlijke handelspraktijk, bewijs, bestelformulier

*Vraag is of er een overeenkomst tot stand is gekomen.*
*Nog los van het feit dat de kantonrechter, gelet op de overige verweren van gedaagde, het vermoeden heeft gekregen dat de handelswijze van – de rechtsvoorganger van – Direct Pay mogelijk niet in overeenstemming is met de, ter bescherming van de consument, in de Europese 'Richtlijn oneerlijke handelspraktijken' (Richtlijn 2005/29/EG) alsmede de 'Richtlijn oneerlijke bedingen' (Richtlijn 93/13 EEG), opgenomen bepalingen, is naar het oordeel van de kantonrechter niet komen vast te staan dat tussen – de rechtsvoorganger van – Direct Pay en gedaagde een koopovereenkomst tot stand is gekomen.*
*Op Direct Pay rust de plicht om voldoende concrete feiten en omstandigheden te stellen ter staving van haar vordering en om bij gemotiveerde betwisting die stelling nader te onderbouwen, waarna op haar in beginsel de last rust de door haar aangedragen feiten en omstandigheden te bewijzen.*
*De kantonrechter is met gedaagde van oordeel dat uit de door Direct Pay overgelegde print screens niet kan worden afgeleid dat een koopovereenkomst tot stand is gekomen. Op het bestelformulier staan weliswaar de persoonsgegevens van gedaagde vermeld, maar op dit bestelformulier – waaruit niet volgt ten behoeve van welke onderneming dit formulier is ingevuld – staat geen prijs vermeld. Op het ander bestelformulier staan weliswaar de naam van de website Forskolin Naturals en een prijs van € 99,90 vermeld, maar op dit formulier zijn geen gegevens ingevuld. Niet blijkt dus dat gedaagde dit formulier heeft gezien en ingevuld.*

## 81. Rechtbank Gelderland 13 maart 2018 (verkrachtingsvideo's), ECLI:NL:RBGEL:2018:1112

Bestuursrecht, filmpje op internet, Commissariaat voor de Media, lex certa, bescherming van minderjarigen, art. 4.6 Mediawet 2008

*Beroep tegen boete opgelegd door commissariaat voor de media wegens overtreding van art. 4.6 lid 2 Mediawet 2008.*
*Op de websites van eiseres zijn twee video's aangetroffen, genaamd 'Tiener door vier mannen verkracht' en 'Vastgebonden en gruwelijk verkracht'. De twee video's werden zonder enige (technische) maatregel voor leeftijdsverificatie beschikbaar gesteld en speelden direct af bij het openen van de pagina. Volgens verweerder kunnen de twee video's de lichamelijke, geestelijke of zedelijke ontwikkeling van personen jonger dan zestien jaar ernstige schade toebrengen.*
*In de samenwerkingsovereenkomsten met haar leveranciers heeft de rechtbank geen verplichting voor eiseres aangetroffen om alle door de leveranciers aangeboden materiaal op haar websites te plaatsen. Dat betekent dat eiseres vooraf ruimte heeft om het materiaal te selecteren. Zij kan ook besluiten om de video's niet te plaatsen. Gebleken is dat eiseres de video's zelf vooraf bekijkt om ze te kunnen rubriceren en tags te plaatsen. Verweerder heeft zich dan ook terecht op het standpunt gesteld dat eiseres effectieve controle kon uitoefenen over de keuze van het media-aanbod op haar websites. Eiseres draagt dus wel redactionele verantwoordelijkheid.*
*Het lex certa-beginsel verlangt van de wetgever dat hij zo duidelijk mogelijk de verboden gedragingen omschrijft. Dat komt de rechtszekerheid ten goede. Aan een zekere vaagheid in die omschrijving valt echter meestal niet te ontkomen. Dat is inherent aan vrijwel alle moderne wetgeving. Een zekere vaagheid is hier ook aan de orde. Het betreft de omschrijving in art. 4.6 lid 2 Mediawet 2008: 'het ernstige schade zou kunnen toebrengen' en 'de lichamelijke, geestelijke of zedelijke ontwikkeling van personen jonger dan zestien jaar'. Bij de toepassing van zo'n vage norm zal sprake zijn van een grijs gebied. In dat gebied is niet duidelijk of er nu wel of niet sprake is van een overtreding. Dat betekent op zichzelf nog niet dat een dergelijke wettelijke norm in strijd is met het lex certa-beginsel en daarom buiten toepassing moet blijven. Het betekent ook niet dat een dergelijke norm niet eerder mag worden toegepast dan nadat verweerder deze norm heeft verduidelijkt, bijvoorbeeld door zijn interpretatie te geven of door voorbeelden te geven van wat er wel onder valt en wat niet. Het is uiteindelijk de rechter die de vage norm uitlegt en beslist of een bepaald gedrag al dan niet onder de norm valt. Eiseres heeft twee video's aangeboden op haar website, waarin acteurs op realistische wijze een verkrachting spelen, en waartoe iedereen (ook jongeren) direct toegang konden krijgen. Dit is een gedraging die duidelijk valt onder de norm van art. 4.6 lid 2 Mediawet 2008. Wat eiseres heeft gedaan valt niet in een grijs gebied. De norm van artikel 4.6 lid 2 Mediawet 2008 is voldoende duidelijk en is daarom niet in strijd met het lex certa-beginsel. Verweerder heeft dan ook terecht eiseres een boete kunnen opleggen.*

## 82. Hoge Raad 13 maart 2018 (smaadschrift via Facebook), ECLI:NL:HR:2018:331

Strafrecht, Facebook, smaadschrift, hyperlink, verspreiding, pedojagen, bepaald feit, art. 261 Sr

*Uit de bewijsmiddelen blijkt dat de inhoud van het bericht op de website www.stopkinderseks.com van de verdachte afkomstig is. Voorts blijkt uit de bewijsmiddelen dat de verdachte een hyperlink naar voormeld bericht op haar Facebookpagina heeft gedeeld en dat zij daarbij anderen heeft verzocht het bericht verder te delen. Gelet hierop en in aanmerking genomen dat het Hof tevens heeft vastgesteld dat door het delen van die hyperlink op haar Facebookpagina het bericht waar die hyperlink naartoe leidde voor iedere willekeurige bezoeker van de Facebookpagina van de verdachte zichtbaar was en dat het bericht vervolgens ook daadwerkelijk door derden verder is gedeeld, geeft het oordeel van het Hof dat de verdachte zich schuldig heeft gemaakt aan 'verspreiding van een geschrift en/of afbeelding' niet blijk van een onjuiste rechtsopvatting en is het toereikend gemotiveerd.*
*Er is sprake van telastlegging van een 'bepaald feit' als bedoeld in art. 261 Sr, indien het feit op een zodanige wijze door de verdachte is tenlastegelegd dat het een duidelijk te onderkennen concrete gedraging aanwijst. Daarvan is bijvoorbeeld geen sprake indien het 'feit' niet het gedrag van de betrokkene betreft maar een eigenschap die hem wordt toegedicht en evenmin, zo het wel gaat om diens gedrag, indien dat gedrag slechts in algemene termen wordt geduid en derhalve niet wordt toegespitst op een voldoende geconcretiseerde gedraging. (Vgl. HR 29 september 2009, ECLI:NL:HR:2009: BI1171, NJ 2009/541.)*
*Het oordeel van het Hof dat het in de bewezenverklaring bedoelde bericht, dat is gekoppeld aan de website www.stopkinderseks.com, – onder meer bestaande uit de woorden: 'Postcode IJmuiden let op je kinderen. In of rond de a-straat woont een man die niet van kleine kinderen af kan blijven. De politie is sinds augustus 2013 op de hoogte maar doet er niets aan' en een foto van de aangever, waarbij deze een zwarte balk over zijn ogen heeft – de telastlegging van een 'bepaald feit' als bedoeld in art. 261 lid 1 Sr oplevert, geeft niet blijk van een onjuiste rechtsopvatting. Dat oordeel is ook niet onbegrijpelijk, mede in aanmerking genomen dat het bericht niet slechts vermeldt het 'niet van kleine kinderen af kunnen blijven' maar ook dat de politie daarvan sinds augustus 2013 op de hoogte is, alsmede in aanmerking genomen dat uit de overige door het Hof vastgestelde feiten blijkt dat de verdachte ook ter kennis van het publiek heeft gebracht dat de aangever haar kind heeft misbruikt.*

## 83. Rechtbank Limburg 20 maart 2018 (failliet), ECLI:NL:RBLIM:2018:2751

Gegevensbeschermingsrecht, Google, recht om te worden vergeten, vergeetrecht, right to be forgotten, Costeja-arrest, maatschappelijk debet, faillissement, belangenafweging, art. 17 AVG, art. 36 Wbp, art. 40 Wbp

*Verzoek om zoekresultaten uit pagerank van Google te verwijderen.*
*Met Google is de rechtbank van oordeel dat de informatie die in de URL's staat opgenomen niet irrelevant is. De informatie is namelijk om meerdere redenen nog steeds actueel en relevant. Allereerst zijn de betreffende faillissementen nog niet afgewikkeld en loopt er bij het gerechtshof te 's-Hertogenbosch nog een procedure tegen verzoeker inzake bestuurdersaansprakelijkheid. Hier komt bij dat berichten over faillissementen waarbij fraude of wanbeleid mogelijk een rol hebben gespeeld onderwerp zijn van een maatschappelijk debat. Het publiek heeft er derhalve belang bij om (journalistieke) berichtgeving, uit verschillende bronnen en niet enkel en alleen via insolventies.rechtspraak.nl – een bij het brede publiek niet bekende en ook niet gemakkelijk te raadplegen bron (immers alleen als de naam van de vennootschap wordt ingetypt) – hieromtrent te kunnen vinden. Dat de (inhoudelijke) informatie in de URL's onjuist is heeft verzoeker, bij gemotiveerde betwisting van Google, niet kunnen aantonen.*

## 84. Rechtbank Den Haag 28 maart 2018 (Tom Kabinet prejudiciële vragen), ECLI:NL:RBDHA: 2018:3455

Auteursrecht, e-books, tweedehands e-books, distributie, distributierecht, uitputting, downloaden, rechtmatig verkregen exemplaar, art. 2 Arl, Art 4 Arl., art 5 Arl

*Prejudiciële vragen die voorgelegd worden aan het HvJ EU:*
*1. Dient artikel 4 lid 1 van de Auteursrechtrichtlijn aldus te worden uitgelegd dat onder 'elke vorm van distributie onder het publiek van het origineel van hun werken of kopieën daarvan door verkoop of anderszins' als daar bedoeld mede is te verstaan het op afstand door middel van downloaden voor gebruik voor onbeperkte tijd ter beschikking stellen van e-books (zijnde digitale kopieën van auteursrechtelijk beschermde boeken) tegen een prijs waarmee de houder van het auteursrecht een vergoeding verkrijgt die overeenstemt met de economische waarde van de kopie van het hem toebehorende werk?*
*2. Indien vraag 1 bevestigend moet worden beantwoord, is het distributierecht met betrekking tot het origineel of kopieën van een werk als bedoeld in artikel 4 lid 2 van de Auteursrechtrichtlijn in de Unie uitgeput, wanneer de eerste verkoop of andere overdracht van dat materiaal, waaronder hier is te verstaan het op afstand door middel van downloaden voor gebruik voor onbeperkte tijd ter beschikking stellen van e-books (zijnde digitale kopieën van auteursrechtelijk beschermde boeken) tegen een prijs waarmee de houder van het auteursrecht een vergoeding verkrijgt die overeenstemt met de economische waarde van de kopie van het hem toebehorende werk, in de Unie geschiedt door de rechthebbende of met diens toestemming?*
*3. Dient artikel 2 van de Auteursrechtrichtlijn aldus te worden uitgelegd, dat een overdracht tussen opvolgende verkrijgers van het rechtmatig verkregen exemplaar waarvan het distributierecht is uitgeput, een toestemming voor de daar bedoelde reproductiehandelingen inhoudt, voor zover die reproductiehandelingen noodzakelijk zijn voor een rechtmatig gebruik van dat exemplaar en, zo ja, welke voorwaarden gelden daarbij?*
*4. Dient artikel 5 van de Auteursrechtrichtlijn aldus te worden uitgelegd dat de auteursrechthebbende zich niet meer kan verzetten tegen de voor een overdracht tussen opvolgende verkrijgers noodzakelijke reproductiehandelingen van het rechtmatig verkregen exemplaar ter zake waarvan het distributierecht is uitgeput en, zo ja, welke voorwaarden gelden daarbij?*

# Wet- en regelgeving

*Onder redactie van mr. H.W. Roerdink*

## Nationaal

### Uitvoeringswet AVG

De Eerste Kamercommissie voor Justitie en Veiligheid (J&V) heeft op 18 april 2018 de memorie van antwoord ontvangen bij het wetvoorstel Regels ter uitvoering van 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) (Uitvoeringswet Algemene verordening gegevensbescherming) en de Memorie van Toelichting.

Het wetsvoorstel regelt de oprichting en inrichting van de Autoriteit persoonsgegevens en de taken en bevoegdheden van de Autoriteit persoonsgegevens. Daarnaast bevat het wetsvoorstel bepalingen ter uitvoering van de AVG op het gebied van bijzondere persoonsgegevens, persoonsgegevens van strafrechtelijke aard, rechtsbescherming, de functionaris voor gegevensbescherming en enige uitzonderingen en beperkingen van regels uit de AVG. Met het wetsvoorstel wordt tevens de Wet bescherming persoonsgegevens ingetrokken.

Bron: https://www.eerstekamer.nl/wetsvoorstel/34851_uitvoeringswet_algemene

### Wet bescherming bedrijfsgeheimen aangenomen door de Tweede Kamer

Op 17 april 2018 is het wetsvoorstel bescherming bedrijfsgeheimen aangenomen door de Tweede Kamer. Dit wetsvoorstel geeft regels ter uitvoering van Richtlijn 2016/943/EU van het Europees Parlement en de Raad van 8 juni 2016 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan (*PbEU* 2016, L157). De richtlijn beoogt de harmonisatie in de lidstaten van de Europese Unie (hierna: EU) van de regels inzake bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (hierna: bedrijfsgeheimen) en geeft aan wat onder een bedrijfsgeheim wordt verstaan, tegen welke vormen van inbreuk daarop (onrechtmatig verkrijgen, gebruiken of openbaar maken) kan worden opgetreden en welke maatregelen, procedures en rechtsmiddelen daarvoor kunnen worden ingezet. Het grootste deel van de richtlijn wordt geïmplementeerd in een nieuwe wet, de Wet bescherming bedrijfsgeheimen.

De procesrechtelijke aspecten worden afzonderlijk geregeld in Rv (art. 1019ia – 1019id).

Bron: https://www.eerstekamer.nl/wetsvoorstel/34821_wet_bescherming

## EU

### Voorstel Europese Commissie 'new deal' voor consumenten

Op 11 april 2018 heeft de Europese Commissie een 'new deal' voor consumenten voorgesteld. Het voorstel bestaat uit twee voorstellen voor richtlijnen: (1) een voorstel tot wijziging van de Richtlijn over oneerlijke bedingen in consumentenovereenkomsten, de Richtlijn ter bescherming van de consument inzake prijsaanduidingen, de Richtlijn over oneerlijke handelspraktijken en de Richtlijn over consumentenrechten. Dit voorstel moet de regels voor consumentenbescherming in de EU moderniseren en de handhaving verbeteren, met name in het licht van de digitale ontwikkelingen en (2) een voorstel betreffende representatieve vorderingen ter bescherming van de collectieve belangen van consumenten en tot intrekking van Richtlijn 2009/22/EG. Dit voorstel moet het de consument makkelijker maken om verhaal te halen in situaties van massaschade, waarbij velen het slachtoffer zijn van dezelfde schending van hun rechten.

Bron: http://europa.eu/rapid/press-release_IP-18-3041_nl.htm

# Signaleringen

*Onder redactie van mr. P.G. van der Putt*

### 10.000 datalekken gemeld in 2017

In 2017 zijn 10.000 datalekken gemeld bij de Autoriteit persoonsgegevens. Het aantal meldingen is daarmee met ruim 70% toegenomen ten opzichte van 2016. De meeste datalekken werden gemeld door organisaties uit de sectoren zorg en welzijn, openbaar bestuur en financiële dienstverlening. Voorzitter Aleid Wolfsen: *'We zien een flinke toename van het aantal gemelde datalekken. Het lijkt er enerzijds op dat de bekendheid van de meldplicht toeneemt. Anderzijds baart het ons zorgen dat de beveiliging nog vaak niet op orde is.'* Bij bijna de helft van de datalekken (47%) die in 2017 zijn gemeld, gaat het om persoonsgegevens die aan een verkeerde ontvanger zijn gestuurd. Meldingen van kwijtgeraakte persoonsgegevens door bijvoorbeeld een verloren of gestolen laptop, usb-stick of tas met dossiers vormen 15% van het totale aantal gemelde datalekken.
Bron: https://autoriteitpersoonsgegevens.nl/nl/nieuws/10000-datalekken-gemeld-2017

### WiFi4EU: gratis Wifi in openbare ruimten

De Europese Commissie heeft het WiFi4EU-webportaal geopend. Gemeenten uit heel Europa kunnen zich nu inschrijven om in aanmerking komen voor EU-financiering om gratis Wifi te installeren. De Wifi is bedoeld voor openbare ruimten, zoals bibliotheken, musea, parken en pleinen. Volgens voorzitter Jean-Claude Juncker is het doel van het initiatief WiFi4EU *'om elk Europees dorp en iedere stad tegen 2020 te voorzien van vrije, draadloze internettoegang in de omgeving van de voornaamste centra van het openbare leven'*. Er wordt tot 2020 een bedrag van 120 miljoen euro uit de EU-begroting uitgetrokken ten behoeve van de financiering van apparatuur voor gratis wifi in tot 8 000 gemeenten in alle lidstaten, Noorwegen en IJsland.
Bron: http://europa.eu/rapid/press-release_IP-18-2065_nl.htm

### NPO ontmantelt tracking wall

De NPO maakt een einde aan de tracking wall in haar app. Voortaan kan je dus programma's van de publieke omroep kijken zonder dat je kijkgedrag wordt gedeeld met adverteerders en andere partijen. Bij installatie van de app wordt de gebruiker de keuze gegeven om al dan niet akkoord te gaan met het volgen van kijkgedrag (opt-in). Overigens blijft de app in alle gevallen advertenties tonen. De NPO ligt al geruime tijd onder vuur met betrekking tot het gebruik van cookies. Criticasters betogen dat de NPO, gefinancierd met gemeenschapsgeld en bedoeld om het algemeen belang te dienen, gebruik van haar website of app niet afhankelijk zou mogen stellen van het accepteren van cookies.
Bron: https://www.bof.nl/2018/03/06/npo-ontmantelt-tracking-wall/

### Militaire Cyberkracht

Nederland scoort een 0,676 op de landenlijst waarmee inzichtelijk wordt gemaakt hoe goed een land beschermd is tegen cyberaanvallen. Nederland staat daarmee op de 18e plaats. Het beste beschermd zou de VS zijn, met een score van 0,824. Tijdens het World Economic Forum in Davos dit jaar was cyber security één van de leidende thema's. Onder het adagium *'if you can't measure it, you can't manage it'* werd gediscussieerd over de vraag hoe je militaire cyberkracht inzichtelijk kunt maken. Een vraag die ook aan de orde kwam was wanneer een cyberaanval gelijk gesteld moet worden met een oorlogshandeling.
Bron: https://www.weforum.org/agenda/2018/03/why-we-need-to-measure-military-cyber-power

### Anti-DDoS radar

Bij een DDoS-aanval worden websites bestookt met oneigenlijke informatieverzoeken, waardoor de werking van de website wordt verstoord of deze zelfs helemaal vastloopt. Bij een recente DDos-aanval op Nederlandse banken ging het om aanvallen met 40 gigabit per seconde. DDos-aanvallen worden echter steeds groter en complexer. Het gaat al over aanvallen met één terabit per seconde. De maatschappij dient zich daartegen te wapenen. Onderzoekers van de Universiteit Twente, SIDN en SURF pleiten daarom voor een 'DDoS-radar'. Een DDoS-radar, zoals de auteurs van de oproep hun remedie noemen, identificeert DDoS 'fingerprints', herkent patronen en stelt aanbieders in staat om maatregelen te nemen. De input van de radar kan ook worden gebruikt om websites die onder vuur liggen los te koppelen van de rest van de infrastructuur.
Bron: https://www.sidnlabs.nl/a/nieuws/een-proactieve-en-collectieve-ddos-bestrijdingsstrategie-voor-de-nederlandse-vitale-infrastructuur

### Subsidie voor onderzoek big data in de gezondheidszorg

Aan Erasmus School of Health Policy & Management (ESHPM) is een Europese subsidie toegekend van één miljoen euro voor het onderzoek naar de brede toepassing van big data in de gezondheidszorg. Dr. Anne Marie Weggelaar, samen met prof. dr. Antoinette de Bont coördinator van het project: *'Big data technologieën kunnen de zorg betaalbaar houden. Door de koppeling van data van ziekenhuizen, verzekeraars en technische bedrijven, kunnen we beter voorspellen wie welke zorg nodig heeft. De uitdaging waarvoor we staan, is om succesvolle big data projecten*

*op groter schaal uit te voeren.'* Privacy en veiligheid krijgen bijzondere aandacht. Tijdens het onderzoek zal de toepasselijke wetgeving in kaart worden gebracht.
Bron: https://www.eur.nl/eshpm/nieuws/een-miljoen-voor-big-data-project-eur

### Verbod op VPN verbindingen in China

De Chinese overheid houdt streng toezicht op het internet. Als reden wordt onder meer gegeven de noodzaak om China te beschermen tegen bedreigingen, zoals hacking en terrorisme. In dit kader wordt wel gesproken van *'China's Great Firewall'*. Met moderne VPN-technieken kon deze Chinese muur worden omzeild. Reden voor de Chinese overheid om VPN in de ban te doen. Voortaan mogen alleen door de overheid goedgekeurde VPN-oplossingen worden gebruikt. Er is weinig transparantie over hoe deze nieuwe regelgeving wordt toegepast. Dar roept vragen op bij bedrijven die gebruik maken van VPN.
Bron: https://www.reuters.com/article/us-china-vpns/businesses-consumers-uncertain-ahead-of-china-vpn-ban-idUSKBN1H612F

### Appfraude naar 700 tot 800 miljoen dollar

De fraude met apps is in 2018 met 30% gestegen ten opzichte van 2017. Mobiel tracking- en marketingbureau AppsFlyer concludeert dat op basis van haar onderzoek. De fraude betreft met name het genereren van oneigenlijke 'clicks'. Online wordt veel gewerkt met zogenaamde affiliate programs. Dit zijn samenwerkingen waarbij partijen naar elkaar doorverwijzen en afrekenen op basis van verwijzingen. Frauduleuze apps genereren oneigenlijke clicks die recht geven op een bepaalde omzet. Met dit misbruik is een bedrag van ca. 700 tot 800 miljoen per jaar gemoeid.
Bron: https://venturebeat.com/2018/04/02/appsflyer-mobile-app-fraud-hit-800-million-in-q1-up-30/

### ACM: advertentieprijzen tweedehands auto's moeten duidelijker

De meeste advertenties voor tweedehands auto's staan online op platforms als Autotrack, Autoscout24 of Marktplaats. De ACM heeft vastgesteld dat er vaak onduidelijkheid bestaat over de prijs die wordt genoemd in de advertentie en wat de consument precies voor die prijs krijgt. Uitgangspunt is dat de consument de auto voor de prijs uit de advertentie moet kunnen meenemen. Nu is het vaak niet duidelijk of de prijs alle verplichte kosten bevat. Ook de informatie over de garantie is vaak niet correct en volledig. De ACM eist dat de branche de advertenties uiterlijk half mei heeft aangepast. Een koper heeft altijd de wettelijke garantie bij de aankoop van een tweedehands auto. Dus een auto aanbieden 'zonder garantie' mag niet.
Bron: https://www.acm.nl/nl/publicaties/acm-advertentieprijzen-tweedehands-autos-moeten-duidelijker

Berghauser Pont ACADEMY

DEN HOLLANDER UITGEVERIJ

1-daagse cursus

# Financieel toezicht in vogelvlucht

6 PUNTEN PO ADVOCATUUR

NEDERLANDSE ORDE VAN ADVOCATEN

## De Wft in a day

- **De laatste jaren een niet aflatende stroom van nieuwe financieel toezichtregelgeving**
- **Financieel toezichtrecht enorm complex geworden**
- **Deze cursus brengt structuur aan in de wirwar van toezichtregelgeving**
- **Met deze 1-daagse cursus bent u bovendien weer up-to-date**
- **Zodat u financieel toezichtsaspecten tijdig kunt signaleren en in de juiste context kunt plaatsen**

**Aanleiding**
De Wet op het financieel toezicht (Wft) trad in 2007 in werking. Toen was deze wet al behoorlijk ingewikkeld. Sindsdien heeft de financieel toezichtwetgeving zo'n enorme ontwikkeling doorgemaakt dat de Wft een buitengewoon complexe wet is geworden die bovendien een breed scala aan instellingen en activiteiten reguleert. Deze cursus zorgt ervoor dat u alle ontwikkelingen in de juiste context kunt plaatsen en mogelijke toezichtissues binnen uw organisatie zodoende kunt herkennen.

**Inhoud en resultaat**
De cursus behandelt onder meer de volgende onderwerpen:
- inhoud en de structuur van de Wft, waarbij onder meer de rolverdeling AFM/DNB aan bod komt
- de belangrijkste soorten marktpartijen en activiteiten die door de Wft worden gereguleerd, zoals banken, beleggingsinstellingen (AIFMD), beleggingsondernemingen (incl. MiFID II) en betaaldienstverleners
- voorts worden enkele onderwerpen behandeld die alle financiële ondernemingen raken en die recent veel aandacht hebben gekregen, zoals de betrouwbaarheids- en geschiktheidstoetsing van personen, de bankierseed en de regels omtrent beloningen in de financiële sector

De cursus beoogt te bereiken dat de cursisten financieel toezichts-aspecten tijdig kunnen signaleren en in de juiste context kunnen plaatsen. De cursus is géén verdiepingscursus. Dat betekent dat de verschillende onderdelen goed, maar relatief kort worden behandeld. Een praktische benadering staat voorop. Er wordt gewerkt met hulpmiddelen zoals stroomschema's en casussen.

**Doelgroep**
De cursus is met name geschikt voor:
- juristen werkzaam bij financiële instellingen
- advocaten die zich net op het gebied van het financieel toezichtrecht begeven of overwegen dat te gaan doen
- andere geïnteresseerde juristen

**Docenten**
Deze cursus heeft twee docenten:
- Mr. Rosemarijn Labeur
- Mr. Pien Kerckhaert

Beiden werkzaam bij Finnius advocaten (www.finnius.nl)

**Datum, locatie en prijs**
Zie voor de actuele data:
www.berghauserpontacademy.nl
Amsterdam
€ 595

**Voor meer informatie, ga naar de website: www.berghauserpontacademy.nl**