Digitalisering en het Nederlands Burgerlijk Wetboek

Marten Voulon*

I Probleemstelling

Het recht is van nature conservatief. Rechtsregels worden na een langdurig proces, bestaande uit wetgeving of rechtspraak, vastgelegd. Na vastlegging zijn zij in beton gegoten totdat zij overbodig worden gemaakt door nieuwe rechtsregels. De beginselen die ten grondslag liggen aan rechtsregels zijn universeler en meer flexibel in toepassing. In de praktijk zijn echter rechtsregels nodig, beginselen bieden onvoldoende houvast. In het kader van de immer voortschrijdende digitalisering van het maatschappelijk verkeer rijzen vragen rondom de verhouding tussen rechtsbeginselen en rechtsregels. Zijn er nieuwe rechtsbeginselen nodig? Zijn de rechtsregels zodanig geformuleerd dat zij recht doen aan de achterliggende beginselen? Kunnen rechtsregels wellicht meer open worden geformuleerd? Dit met het oog op een langere bestendigheid van de in beton vervatte regels. Zijn meer open geformuleerde rechtsregels voor de praktijk voldoende bruikbaar?

Ik wil het bovenstaande in de eerste plaats behandelen aan de hand van het juridisch regime inzake de elektronische handtekening. Dit komt de lezer van dit preadvies wellicht niet voor als een onderwerp waar anno 2017 nog veel discussie over zou moeten plaatsvinden. In 2003 is toch al Nederlandse wetgeving over de elektronische handtekening van kracht geworden, gebaseerd op een richtlijn uit 1999? In de praktijk wordt echter nog weinig gebruik gemaakt van ruimte die de wet biedt. Papier en de handgeschreven handtekening spelen daarom een grotere rol dan men in dit tijdsgewricht zou mogen verwachten. Een reden daarvoor ligt in het juridische: het blijft lastig om langs elektronische weg aan vormvereisten te voldoen. Ik verwacht echter dat met ingang van 2017 de elektronische handtekening eindelijk meer gangbaar gaat worden in het civielrechtelijke maatschappelijk verkeer.¹ Mijn verwachting is gebaseerd op een andere reden waarom het gebruik van elektronische handtekeningen niet populair is: het ontbreken van een toegankelijke wijze waarop deelnemers aan het maatschappelijk verkeer zich online kunnen authenticeren. Met authenticeren doel ik op het betrouwbaar kunnen aantonen van een identiteit. Authenticatie in deze betekenis is een noodzakelijke voorwaarde waaraan voldaan moet zijn voordat elektronisch ondertekenen überhaupt tot de mogelijkheden gaat behoren. Het authenticatieprobleem lijkt intussen deels opgelost. Vergeleken met pak 'm beet vijftien jaar geleden is er nu

* Marten Voulon is bedrijfsjurist bij ABN AMRO Bank N.V., Fellow aan de Universiteit Leiden en lid van de klachten- en geschillencommissie eHerkenning.

1 In het bestuursrechtelijk verkeer ligt dit anders. Zo dient de elektronische belastingaangifte sinds 2008 elektronisch te worden ondertekend met DigiD.

sprake van een betere beschikbaarheid van authenticatiemiddelen. Ik doel dan onder meer op het bancaire iDIN-systeem.

De achterliggende beginselen die een rol spelen bij de elektronische handtekening, zijn de beginselen van betrouwbare elektronische communicatie. Dit zijn de beginselen van identificatie & authenticatie, integriteit, confidentialiteit en onweerlegbaarheid. Dit zijn belangrijke beginselen die ten grondslag liggen aan veel rechtsregels die betrekking hebben op digitaal maatschappelijk verkeer. Naar mijn mening dienen juristen, en eigenlijk alle deelnemers aan het maatschappelijk verkeer, zich bewust te zijn van deze beginselen.

De elektronische handtekening en de beginselen van betrouwbare elektronische communicatie komen aan de orde in paragraaf 2. Ik zal in die paragraaf de handtekening bespreken in de context van de onderhandse akte. Indien voor de onderhandse akte een handgeschreven handtekening wordt gebruikt, is er naar mijn mening sprake van wat ik de *goede trouw-benadering* noem. Indien gebruik wordt gemaakt van een elektronische handtekening is in plaats daarvan sprake van de zogenoemde *risicogebaseerde benadering*. Dat is een benadering die tot nu toe wezensvreemd is aan het privaatrecht. Deze nieuwe benadering is echter typerend voor de toepassing van de beginselen voor een betrouwbare elektronische communicatie.

In paragraaf 3 zal ik aandacht besteden aan digitale producten zoals computerprogrammatuur en databestanden. Dit zijn objecten die vanuit goederenrechtelijk oogpunt ongrijpbaar lijken. Vanuit jurisprudentie (ik denk aan de arresten inzake *UsedSoft* en *De Beeldbrigade*) en wetgeving (de regulering van digitale inhoud) lijkt het recht er echter meer vat op te krijgen.

Tot slot zal ik in paragraaf 4 aandacht besteden aan het autonome systeem. Het gaat dan om systemen zoals zelfhandelende software, zelfrijdende auto's en robots. Ik ben zo vrij dit onderwerp enkel aan te stippen. Het autonome systeem noopt zonder twijfelen tot juridische analyse en aanvullende rechtsregels. Echter, ik denk niet dat autonome systemen het privaatrecht op zo een fundamentele manier uitdagen als dat bij de elektronische handtekening en het digitale product het geval is.

2 De elektronische handtekening

Bij het bespreken van de handgeschreven en de elektronische handtekening ga ik onder meer uit van twee essentiële elementen van de handtekening. Deze elementen zijn kenmerkend voor zowel de handgeschreven handtekening als de elektronische handtekening. Het eerste element is de *animus signandi*: de ondertekenaar heeft de wil om zijn handtekening te plaatsen om daarmee zijn instemming met een verklaring uit te drukken.² Door de handtekening te plaatsen geeft hij uitdrukking aan die wil. Het tweede element houdt in dat een handtekening beoogt de ondertekenaar te individualiseren:³ die specifieke persoon heeft getekend. De elektronische handtekening kan dit individualiseringsaspect verder voeren tot

2 P. van Eecke, *Naar een juridische status voor de elektronische handtekening* (diss. Leuven), Leuven: Icri 2004, nr. 125.

3 Pitlo/Rutgers & Krans 2014, Bewijs, nr. 71.

volledige identificatie van de persoon: deze persoon met dit identificerend unieke kenmerk heeft getekend.

De wetgeving regelt in algemene zin de rechtsgevolgen van de elektronische handtekening. Het is echter lastig de handtekening los te zien van de specifieke situatie waarin een handtekening wordt toegepast. Daarom behandel ik de handtekening in het kader van een bepaalde context, te weten de *onderhandse akte*.

2.1 Het wettelijk kader

De relevante wetgeving voor de elektronische handtekening bestaat op dit moment uit de zogenaemde eIDAS-verordening⁴ en uit de wet die de verordening uitvoert.⁵ Voor het privaatrecht is het van belang op te merken dat de uitvoeringswet op 10 maart 2017 artikel 3:15a BW heeft gewijzigd.⁶

Het wettelijke kader bestaat uit twee regimes die nagenoeg volledig los van elkaar staan. Het eerste regime is het elektronische identificatieregime. Dit regime is met name relevant voor bestuursorganen. Het regime regelt stelsels voor *elektronische identificatie*. Zo'n stelsel is het geheel van afspraken en voorschriften waarbinnen authenticatiemiddelen worden uitgegeven. Als zo'n stelsel voldoet aan de voorschriften van de eIDAS-verordening en door een lidstaat wordt aangemeld bij de Europese Commissie, dan zal de Europese Commissie het stelsel op de lijst van erkende stelsels plaatsen. Openbare instanties in andere lidstaten dan de lidstaat waar het authenticatiemiddel is uitgegeven, zijn dan verplicht om dat middel te erkennen. Kort gezegd moet dit burgers binnen de EU in staat stellen met hun nationale authenticatiemiddel ook in te loggen bij openbare instanties in andere lidstaten.

Het tweede regime is het regime betreffende de vertrouwensdiensten. Een voorbeeld van een vertrouwensdienst is het leveren van een dienst waarmee elektronische handtekeningen kunnen worden geplaatst. Andere vertrouwensdiensten betreffen onder meer het elektronisch zegel, het elektronische tijdstempel en de elektronische aangetekende bezorging.

2.2 De handgeschreven handtekening en de onderhandse akte

Een van de beginselen van het contractenrecht is het consensualisme: overeenkomsten komen tot stand door de wilsovereenstemming van partijen alléén. Zij behoeven daartoe niet aan een bepaalde vorm te voldoen.⁷ Constitutieve vorm-

4 Verordening (EU) nr. 910/2014 van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, PbEU 2014, L 257. De term 'eIDAS' is een acroniem van 'electronic identification and assurance services'. In de uiteindelijke verordening is echter gekozen voor de term 'trust service' (vertrouwensdienst) in plaats van 'assurance service'. Zie verder H.W. Wefers Betsink & J. Theeven, 'Een Gemeenschapsregime voor elektronische identificatie', NtEr 2013/1-2, p. 1-6; T.F.E. Tjong Tjin Tai, 'De eIDAS-verordening en de elektronische handtekening uit het BW', WPNR 20 mei 2017, 7151; M.B. Voulon, 'Een Europese verordening voor identity management (IdM)', Computerrecht 2013/118.

5 Wetsvoorstel Uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten, Kamerstukken II 2015/16-2016/17, 34413, 1-8; Kamerstukken I 2016/17, 34413, A-B; Stb. 2017, 13.

6 Stb. 2017, 81.

7 Asser/Hartkamp & Sieburgh 6-III 2014/272.

vereisten zijn dan ook de uitzondering. Toch spelen de handtekening en papier in het maatschappelijk verkeer een grote rol. Een reden daarvoor is dat contractspartijen in de praktijk een onderhandse akte willen bewerkstellingen. Voor de onderhandse akte spelen twee vormvereisten een rol.⁸ De onderhandse akte moet immers van een handtekening worden voorzien (handgeschreven dan wel elektronisch). Voorts is een onderhandse akte een geschrift, of op andere wijze opge maakt als aan een aantal alternatieve vereisten is voldaan.⁹ De meerwaarde van een onderhandse akte is dat zij een eventuele latere juridische procedure dwingend bewijs oplevert.¹⁰ Het gaat dan echter alleen om de zogenoemde materiële bewijskracht: is waar wat in de akte is verklaard? De onderhandse akte heeft geen uitwendige bewijskracht. Uitwendige bewijskracht zou inhouden dat de handtekening onder een onderhandse akte voor echt wordt gehouden totdat de beweerdelijke ondertekenaar bewijst dat zijn handtekening vervalst is. De beweerdelijke ondertekenaar kan echter volstaan enkel door ‘stellig te ontkennen’ dat hij de akte heeft ondertekend.¹¹ Degene die zich op de akte beroept, zal dan eerst moeten bewijzen dat de betreffende handtekening daadwerkelijk door de beweerdelijke ondertekenaar is gezet.¹² In gerechtelijke procedures wordt onder meer gebruikgemaakt van handschriftdeskundigen om aan te geven met welke mate van waarschijnlijkheid een handtekening daadwerkelijk door de beweerdelijke ondertekenaar is geplaatst.¹³

Het ontbreken van de uitwendige bewijskracht van een onderhandse akte kan een rechtzoekende in grote bewijsproblemen brengen. Het verbaast dan ook niet dat de rechter soms een mate van onderbouwing verwacht in plaats van enkel een stellige ontkenning.¹⁴ Voorts kan men zich afvragen welke pagina's van een akte de daadwerkelijke onderhandse akte vormen. Vaak is er immers sprake van meerdere pagina's waarbij enkel een handtekeningenblad de handtekeningen van partijen bevat. Hoe is vast te stellen dat de ondertekening betrekking heeft op alle pagina's? Het Hof Den Haag oordeelde in dit verband over een document bestaande uit twee pagina's waarbij de tweede pagina van twee handtekeningen was voorzien. Het Hof Den Haag stelde in dit verband dat een akte een ‘ondertekend geschrift’ is. Uit het woord ‘ondertekend’ en uit de memorie van toelichting bleek volgens het hof dan ook dat de akte hetgeen is dat *boven* de handtekening staat. De eerste pagina van het document, dat niet van handtekeningen was voorzien, gold daarom niet als (onderdeel van) de akte. Volgens het hof zou dit anders kunnen zijn, indien is vast te stellen dat de eerste en de tweede pagina bij elkaar horen. De tweede pagina bevatte overigens de zinsnede ‘de overeenkomst bestaat uit twee bladzijden’. Deze zinsnede was echter onder de handtekeningen geplaatst en behoorde daarom volgende het Hof evenmin tot de akte.¹⁵ We zullen hierna zien dat dit probleem door de elektronische handtekening wordt ondervangen doordat over de tekst van de te tekenen verklaring een hashwaarde wordt berekend.

8 Art. 156 lid 1 Rv.

9 Art. 156a Rv.

10 Art. 157 lid 2 Rv.

11 Art. 159 lid 2 Rv.

12 Zie ook HR 28 februari 1997, ECLI:NL:HR:1997:ZC2297, NJ 1997, 330.

13 Zie bijvoorbeeld Hof 's-Hertogenbosch 18 juni 2016, ECLI:NL:GHSHE:2013:CA4038.

14 Zie bijvoorbeeld Rb. Overijssel 8 mei 2013, ECLI:NL:RBOVE:2013:CA2970.

15 Hof Den Haag 21 februari 2017, ECLI:NL:GHDHA:2017:382.

In de praktijk wordt een en ander ondervangen door elke pagina van een document te paraferen. Naar Nederlandse recht werd er van oudsher van uitgegaan dat een paraaf niet als handtekening kan gelden.¹⁶ In 2012 overwoog de Hoge Raad echter: ‘Een geparafeerd geschrift kan gelden als een ondertekend geschrift in de zin van art. 156 lid 1 Rv indien de paraaf de desbetreffende persoon in voldoende mate individualiseert.’¹⁷ Hiermee is het onderscheid tussen een paraaf en een handtekening komen te vervallen: als de paraaf de betreffende persoon in voldoende mate individualiseert, kan het als een handtekening gelden.¹⁸

De hierboven kort aangestipte regeling van de onderhandse akte is niet perfect. De ondertekenaar van een onderhandse akte kan de boel bedonderen. Hij kan valselijk stellig ontkennen de akte te hebben ondertekend. De achterliggende gedachte bij de wettelijke regeling is de verwachting dat het echter vaker zal voorkomen dat een handtekening wordt vervalst, dan dat onterecht wordt ontkend dat een akte is ondertekend. Er wordt voorts van uitgegaan dat de deelnemers aan het maatschappelijk verkeer consciëntieus zullen handelen en daarom niet in strijd met de waarheid zullen ontkennen te hebben ondertekend.¹⁹ In meer algemene zin is opgemerkt dat niet alles a priori als verdacht hoeft te worden beschouwd.²⁰ De regeling van de onderhandse akte lijkt hiermee deels gebaseerd op de achterliggende gedachte dat betrokkenen bij een geschil consciëntieus zullen handelen. Zij zullen niet willens en wetens onterecht ontkennen een document te hebben getekend. Mogelijk is dit positieve mensbeeld gebaseerd op de feitelijke context waarbinnen een onderhandse akte wordt geproduceerd. Om tot een papieren, ‘analoge’ onderhandse akte te komen, moeten partijen soms fysiek afspreken. Zij zien elkaar in de ogen. Zij komen voorafgaand aan ondertekening de inhoud van de akte overeen.²¹ Mogelijk leidt deze fysieke context, waarbij beloftes zijn uitgesproken en verwachtingen zijn gewekt, tot de situatie dat de ondertekenaar het onprettig vindt om in een juridische procedure willens en wetens onwaarheden te verkondigen.

De op een positief mensbeeld gestoelde achterliggende gedachte van de onderhandse akte duid ik aan als de *goede trouw-benadering*. De goede trouw-benadering staat in schril contrast met de achterliggende gedachte waar de wetgever van uit is gegaan bij het regelen van de elektronische handtekening. Bij de elektronische handtekening is sprake van wat ik hierna aanduid als de *risicogebaseerde benadering*.

2.3 De risicogebaseerde benadering

De risicogebaseerde benadering houdt in dat het recht (althans, een wettelijk voorschrift) een normadressaat instrueert bij de uitvoering van een voornemen eerst mogelijke risico's te inventariseren en vervolgens de risico's te mitigeren

¹⁶ HR 17 december 1885, W. 5251 en HR 6 mei 1910, W. 9025.

¹⁷ HR 5 oktober 2012, ECLI:NL:HR:2012:BV6698, r.o. 3-4.

¹⁸ Zie voorts P.C. van Es, ‘Paraaf als ondertekening’, JBN 2013/12, p. 3-5.

¹⁹ Pitlo/Rutgers & Krans 2014, Bewijs, nr. 75.

²⁰ Asser Procesrecht/Asser 3 2013/248.

²¹ Dit geldt natuurlijk in mindere mate voor gestandaardiseerde overeenkomsten die aan consumenten ter ondertekening worden aangeboden.

door het treffen van mitigerende maatregelen. Risico's worden ingeschat door middel van het adagium 'risico is kans maal impact' (hoe groot is de kans dat het risico zich voordoet en wat is dan de omvang van het risico?). Een voorbeeld hiervan biedt het gegevensbeschermingsrecht. Binnen dat rechtsgebied is de verantwoordelijke²² verplicht om aan de hand van een risicogebaseerde benadering beveiligingsmaatregelen te nemen ten aanzien van de verwerking van persoonsgegevens. De verantwoordelijke moet 'passende technische en organisatorische maatregelen' nemen. Die moeten dan een 'passend beveiligingsniveau' garanderen, 'gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen'.²³ De Autoriteit Persoonsgegevens heeft in 2013 ten aanzien van deze norm de richtsnoeren 'Beveiliging van persoonsgegevens' vastgesteld waarin de risicogebaseerde benadering verder wordt uitgewerkt. De richtsnoeren schrijven onder meer een 'plan-do-check-act'-cyclus voor. Ook wordt er een onderscheid gemaakt tussen preventieve, detectieve, repressieve, correctieve en herstellende maatregelen. Kortom: dit is een benadering die op het eerste gezicht niet eigen is aan het privaatrecht.²⁴ In paragraaf 2.9 wordt ingegaan op de rol van de risicogebaseerde benadering bij de elektronische handtekening.

2.4 Achterliggende technologie van de elektronische handtekening

Om met voldoende diepgang in te kunnen gaan op de wettelijke regeling van de elektronische handtekening, zal ik eerst uiteen moeten zetten welke beginselen van belang zijn om te kunnen spreken van een betrouwbare elektronische communicatie. Vervolgens zal ik de achterliggende technologie uiteen moeten zetten. Deze uiteenzetting is noodzakelijk omdat, hoewel de wetgeving claimt 'technologieneutraal' te zijn, er een specifieke technologie in het spel is. Het is van belang dat de lezer aan het eind van deze paragraaf begrijpt dat een technische elektronische handtekening bestaat uit een hashwaarde van de te ondertekenen verklaring en dat die hashwaarde is versleuteld met de private sleutel van de ondertekenaar.

Beginnelsen van betrouwbare elektronische communicatie

Om te kunnen spreken van betrouwbare elektronische communicatie, dient er in meer of mindere mate te zijn voldaan aan de volgende beginselen. Kennis van deze beginselen is noodzakelijk voor een goed begrip van de hierna te behandelen technologieën betreffende cryptografie, hashing en de elektronische handtekening. Die technologieën geven namelijk invulling aan de beginselen. Franken

22 De verantwoordelijke is de belangrijkste normadressaat van de Wet bescherming persoonsgegevens (Wbp) en de Algemene verordening gegevensbescherming (Avg). De verantwoordelijke is degene die het doel en de middelen van een verwerking van persoonsgegevens vaststelt, art. 1 sub d Wbp; art. 4 lid 7 Avg.

23 Art. 13 Wbp.

24 Een ander voorbeeld van de risicogebaseerde benadering wordt geleverd door de Richtlijn inzake netwerk- en informatiebeveiliging (Richtlijn (EU) 2016/1148, PbEU 2016, L 194). Zie art. 14 lid 1: 'De lidstaten zorgen ervoor dat aanbieders van essentiële diensten passende en evenredige technische en organisatorische maatregelen nemen om de risico's voor de beveiliging van netwerk- en informatiesystemen die zij bij hun activiteiten gebruiken, te beheersen. Deze maatregelen zorgen, gezien de stand van de techniek, voor een niveau van beveiliging van netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen.'

spreekt in bestuursrechtelijk verband (overigens in een iets andere samenstelling van de beginselen) van de ‘beginselen van behoorlijk ICT-gebruik’:²⁵

1. identificatie en authenticatie;
2. integriteit;
3. confidentialiteit; en
4. onweerlegbaarheid (ook wel: *non-repudiation* of onloochenbaarheid).

Identificatie en authenticatie houden nauw verband met elkaar. Identificatie is het claimen van een identiteit, authenticatie is het betrouwbaar verifiëren van de geclaimde identiteit. Dit kan worden vergeleken met het gebruik van een gebruikersnaam en een wachtwoord. Door de gebruikersnaam in te typen wordt een identiteit geclaimd. Met de invoer van het geheime wachtwoord wordt geverifieerd dat de persoon die de identiteit claimt, daadwerkelijk die identiteit heeft. In dit verband wordt ook gesproken van authenticatiemiddelen. Dat zijn middelen waarmee voldaan kan worden aan de beginselen van identificatie en authenticatie. Voorbeelden van authenticatiemiddelen zijn de combinatie gebruikersnaam/wachtwoord (denk aan het Nederlandse DigiD) of een bankpas met de bijbehorende pincode of andere middelen die een bank aan haar cliënten verstrekt waarmee zij kunnen worden geauthentiseerd bij online communicatie. De eIDAS-verordening noemt authenticatiemiddelen ‘elektronische identificatiemiddelen’.²⁶ In de praktijk wordt ook wel gesproken van ‘herkenningsmiddelen’.

Integriteit houdt in dat een bericht of verklaring niet is aangetast door manipulatie (door kwaadwillende derden dan wel door technische verstoringen). Confidentialiteit houdt in dat de inhoud van een elektronische verklaring geheim wordt gehouden. Zij mag niet leesbaar zijn voor anderen dan de opsteller en de bedoelde ontvanger van de verklaring. Onweerlegbaarheid houdt in dat niet onterecht kan worden ontkend dat een elektronische verklaring door een bepaalde persoon is opgesteld, verzonden of ontvangen.

Authenticatie & authenticatie

Zoals hierboven vermeld betreft het beginsel van authenticatie het betrouwbaar verifiëren van een gestelde identiteit. De term *authenticatie* heeft echter nog een betekenis, namelijk het instemmen met een verklaring. De tweede Europese richtlijn betreffende betalingsdiensten²⁷ (ook wel aangeduid als PSD2, *payment services directive* 2), spreekt bijvoorbeeld van de authenticatie van een transactie.²⁸

25 H. Franken, *Beschikken en automatiseren* (Preadviezen voor de Vereniging voor Administratief Recht), Alphen aan den Rijn: Vuga 1993, nr. 26; M. van Stekelenburg, *De betere byte in de strijd om het gelijk* (diss. Amsterdam VU), Delft: Eburon 2009, p. 25 t/m 37; M.B. Voulon, *Automatisch contracteren* (diss. Leiden), Leiden: Leiden University Press 2010, p. 250-252. Zie overigens ook Asser *Procesrecht/Asser* 3 2013/247 waar Asser in het bewijsrecht de beginselen authenticiteit en integriteit hanteert. Asser legt authenticiteit uit als het vaststaan van de herkomst van een bewijsmiddel of van informatie. Integriteit houdt in dat het bewijsmiddel als zodanig, en de inhoud ervan, onaangetaast zijn door onbevoegde manipulatie.

26 Art. 3 lid 2 Verordening (EU) nr. 910/2014 van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, PbEU 2014, L 257.

27 Richtlijn (EU) 2015/2366 betreffende betalingsdiensten, PbEU 2015, L 337.

28 Zie overweging 95 laatste volzin.

Diezelfde richtlijn definieert authenticatie als ‘een procedure waarmee een betalingsdienstaanbieder de identiteit van een betalingsdienstgebruiker dan wel de validiteit van het gebruik van een specifiek betaalinstrument kan verifiëren’.²⁹ In deze definitie zijn beide betekenissen van authenticatie terug te vinden: het verifiëren van de identiteit van een persoon en (de verificatie van) het instemmen van een betalingsdienstgebruiker met een betalingstransactie (blijkende uit het valide gebruik van een betaalinstrument).

Overigens komt men ook wel het begrip *authenticatie* tegen.³⁰ Authenticatie en authenticatie zijn wat mij betreft synoniemen. Ik vermoed dat in EU-wetgeving de Engelse term ‘authentication’ in de Nederlandse vertaling soms wordt aangeduid met het gallicisme ‘authenticatie’ en soms met het anglicisme ‘authentication’. Omdat de term authenticatie de hierboven genoemde twee betekenissen heeft, en wellicht nog meer betekenissen, kan gebruik van de term tot verwarring leiden.

Cryptografie, hashing en de elektronische handtekening

De beginselen van identificatie & authenticatie, integriteit, confidentialiteit en onweerlegbaarheid kunnen praktisch worden uitgewerkt met onder meer cryptografie, hashing en de elektronische handtekening.

Cryptografie dient er in eerste instantie toe om informatie geheim te houden voor derden door middel van geheimschrift. Er wordt met een wiskundig algoritme informatie omgezet naar geheimschrift. De oorspronkelijke, voor eenieder leesbare, informatie noemen we *plaintext*. Als de informatie is omgezet naar geheimschrift spreken we van *ciphertext*. Het omzetten van de *plaintext* naar de *ciphertext* is versleutelen (encryptie). Het terugdraaien van de versleuteling, waardoor de *ciphertext* weer in *plaintext* verandert, is ontsleutelen (decryptie). Om *plaintext* te transformeren naar *ciphertext* wordt het betreffende wiskundige algoritme gevoerd met de *plaintext* en een sleutel. Het algoritme produceert vervolgens de *ciphertext*. Een sleutel is een bepaalde waarde, een getal.

Een *plaintext*-bericht kan er bijvoorbeeld als het volgende e-mailbericht uitzien.

Geachte mevrouw De Kort,

Graag gaan wij akkoord met uw offerte d.d. 2 augustus 2017.

Met vriendelijke groet,
Vincent Hoogenes
Hoogenes B.V.

²⁹ Art. 4 lid 29.

³⁰ Zie Richtlijn 2007/64/EG betreffende betalingsdiensten (PbEU 2007, L 319), de inmiddels ingetrokken Richtlijn 1999/93/EG betreffende elektronische handtekeningen (PbEU 2000, L 13) en art. 3:15a BW van voor de wetswijziging per 10 maart 2017 (gewijzigd door Stb. 2017, 13).

De versleutelde variant van dit bericht, de *ciphertext*, zou er als volgt uit kunnen zien.

3081	8902	8181	00C2	6868	0EFF	1B1E	6C2F	0D64	4234
8A0C	AC5E	B1E1	6377	2BB0	4689	6004	3FF4	0BF2	83AA
237F	25AF	F545	DD27	478B	D995	D068	F6E3	C890	7524
C871	FB53	15F2	ECC9	819D	3635	4071	6377	2BB0	4689

Er wordt onderscheid gemaakt tussen symmetrische cryptografie en asymmetrische cryptografie.

Symmetrische cryptografie

Symmetrische cryptografie houdt in dat informatie wordt versleuteld en ontsleuteld met één en dezelfde sleutel. Stel, men zou een pdf-bestand willen versleutelen en ontsleutelen, dan zou dit als volgt kunnen worden weergegeven.

Figuur 1 Symmetrische encryptie

Een verzender en een ontvanger kunnen op een betrouwbare wijze informatie uitwisselen door middel van asymmetrische encryptie. Er wordt namelijk voldaan aan het beginsel van confidentialiteit omdat de informatie niet leesbaar is voor derden. De integriteit wordt in zeker zin geborgd omdat indien de *ciphertext* zou zijn gemanipuleerd, deze niet meer ontsleuteld kan worden naar een zinvolle *plaintekst*. Er kan sprake zijn van identificatie en authenticatie omdat enkel de verzender en de ontvanger over de sleutel beschikken. Al met al wordt hiermee de onweerlegbaarheid tot op zekere hoogte bevorderd: de verzender kan niet (althans niet op geloofwaardige wijze) jegens de ontvanger ontkennen de versleutelde informatie te hebben opgesteld en aan de ontvanger te hebben toegezonden omdat enkel de verzender en de ontvanger over de sleutel beschikken. Mits er correct wordt omgegaan met de sleutel (dat wil zeggen dat hij niet in verkeerde handen is gevallen), wordt voldaan aan de beginselen van een betrouwbare elektronische communicatie. Er is sprake van identificatie en authenticatie omdat alleen de verzender en de ontvanger over de sleutel beschikken. Er is sprake van confidentialiteit omdat het bericht is versleuteld tot *ciphertext* en alleen kan worden ontsleuteld door degenen die over de sleutel beschikken. Er is sprake van integriteit omdat indien het versleutelde bericht tijdens transport zou worden aangepast, de ontvanger het bericht niet correct kan ontsleutelen, waarmee duidelijk wordt dat het bericht na versleuteling is gewijzigd. Per saldo kan een

verzender hiermee niet onterecht ontkennen een bericht te hebben versleuteld en verzonden aan de ontvanger, waarmee deels voldaan is aan het beginsel van onweerlegbaarheid.

Asymmetrische cryptografie

Er kleeft een groot nadeel aan het gebruik van symmetrische cryptografie. Het veronderstelt dat de sleutel op een veilige manier tussen verzender en ontvanger wordt uitgewisseld en na uitwisseling niet is gecompromitteerd (dat wil zeggen, ter beschikking van onbevoegde derden is gekomen). Dit maakt symmetrische cryptografie (althans, voor zover geen aanvullende maatregelen worden genomen) voor veel situaties minder aantrekkelijk voor elektronische communicatie via het internet. De verzender en ontvanger zullen immers voorafgaand aan het gebruik van symmetrische cryptografie langs een veilig kanaal de private sleutel moeten uitwisselen.

Aan de zogenoemde *asymmetrische cryptografie* kleeft dit probleem niet. Bij asymmetrische cryptografie of *public key cryptografie* wordt gebruikgemaakt van twee sleutels: een private sleutel en een publieke sleutel.³¹ De private sleutel moet geheim worden gehouden en alleen door degene op wie de sleutel betrekking heeft, kunnen worden gebruikt. Deze persoon moet de uitsluitende controle hebben over de private sleutel.³² De private sleutel kan bijvoorbeeld op een smartcard worden bewaard die de betreffende persoon onder zich dient te houden. Toegang tot de private sleutel is dan doorgaans beschermd met een pincode. De private sleutel kan ook 'ergens in de cloud' worden bewaard. In dat geval bevindt de private sleutel zich op een speciale server (een 'HSM', *hardware security module*). De toegang tot de private sleutel moet dan op zodanige wijze zijn afgeschermd dat alleen degene op wie het sleutelpaar betrekking heeft, gebruik kan maken van de private sleutel.

De publieke sleutel moet juist openbaar worden gemaakt. Zij is beschikbaar voor eenieder die met de houder van de private sleutel betrouwbaar wil communiceren. Een belangrijk middel om de publieke sleutel voor eenieder beschikbaar te stellen, is het zogenoemde *certificaat*. Een certificaat is een computerbestand dat onder meer de publieke sleutel bevat en melding maakt van de identiteit van degene aan wie de corresponderende private sleutel is toegekend. Het certificaat zelf is op zijn beurt weer elektronisch ondertekend (dus voorzien van een versleutelde hashwaarde) door de uitgever ervan, om te voorkomen dat het certificaat manipuleerbaar is. De toepassing van asymmetrische encryptie ten aanzien van een pdf-bestand kan als volgt worden weergegeven.

³¹ De eIDAS-verordening noemt de private en de publieke sleutel die worden gebruikt voor elektronische handtekeningen respectievelijk 'gegevens voor het aanmaken van elektronische handtekeningen' en 'gegevens die worden gebruikt om een elektronische handtekening te valideren', art. 3 sub 13 en sub 40.

³² Vgl. het vereiste in art. 26 van de eIDAS-verordening inhoudende dat een zogenoemde geavanceerde elektronische handtekening tot stand komt met gegevens die de ondertekenaar 'onder zijn uitsluitende controle kan gebruiken.'

Figuur 2 Asymmetrische encryptie, versleuteling met private sleutel

In dit voorbeeld wordt gebruikgemaakt van het sleutelpaar (de met elkaar corresponderende private en publieke sleutel) van de verzender. Er wordt versleuteld met diens private sleutel en ontsleuteld met diens publieke sleutel. Hierdoor wordt invulling gegeven aan het beginsel van identificatie en authenticatie. Enkel de houder van de geheime private sleutel kan immers met die sleutel het bestand versleutelen. Voorts wordt invulling gegeven aan het beginsel van integriteit. Mocht het versleutelde bestand worden gemanipuleerd of verminkt, dan zal dat bij ontsleuteling blijken. Ook de onweerlegbaarheid is geborgd, althans, de verzender zal geen geloofwaardige indruk maken als hij ontkent het bestand te hebben versleuteld. Enkel de verzender beschikt immers over de private sleutel. Het is van belang dat de lezer zich realiseert dat aan het beginsel van confidentialiteit niet wordt voldaan. De publieke sleutel is immers voor eenieder toegankelijk. Eenieder kan dus het bestand ontsleutelen en kennisnemen van de inhoud ervan.

Het is uiteraard ook te versleutelen met het sleutelpaar van de ontvanger. In dat geval wordt versleuteld met de publieke sleutel van de ontvanger en ontsleuteld met diens private sleutel. Dat kan als volgt worden weergegeven.

Figuur 3 Asymmetrische encryptie, versleuteling met publieke sleutel

Een belangrijk verschil met de vorige situatie is dat de confidentialiteit nu wel is geborgd. Immers, enkel de ontvanger kan beschikken over de private sleutel en dus het bestand ontsleutelen. Voorts is ook de integriteit geborgd. Manipulatie van het bestand zal namelijk blijken bij ontsleuteling. De identificatie & authenticatie van de verzender is *niet* geborgd. Er is immers versleuteld met de publieke

sleutel, en die is voor eenieder beschikbaar en te gebruiken. Daardoor is er ook geen sprake van onweerlegbaarheid.

Dubbele versleuteling en ontsleuteling om aan alle beginselen te voldoen

De vraag is nu natuurlijk hoe er met asymmetrische encryptie aan alle vereisten van betrouwbare communicatie kan worden voldaan. Dat kan geschieden door een bestand tweemaal te versleutelen en vervolgens tweemaal te ontsleutelen. De eerste versleuteling zou dan bijvoorbeeld dienen te geschieden door toepassing van de private sleutel van de verzender. Vervolgens wordt het versleutelde bestand nogmaals versleuteld met toepassing van de publieke sleutel van de ontvanger. Na verzending en ontvangst van het bestand kan het worden ontsleuteld. Dan kan dan geschieden door toepassing van eerst de private sleutel van de ontvanger, en vervolgens door de tweede ontsleuteling uit te voeren met toepassing van de publieke sleutel van de verzender.

Hashalgoritmes

Een van de meest basale bouwstenen voor betrouwbare elektronische communicatie bestaat uit het gebruik van hashalgoritmes. Begrip van hashalgoritmes is voorts van belang voor een goed begrip van de elektronische handtekening en van blockchain technologie. Een hashalgoritme heeft onder meer de volgende kenmerken. In de eerste plaats kan hetgeen in het algoritme kan worden ingevoerd, de *input*, bestaan uit een verzameling tekens (letters, cijfers, symbolen) waarvan het niet van belang is hoe groot die verzameling is. De invoer kan aldus bestaan uit een kleine verzameling tekens zoals een wachtwoord, of een grote verzameling tekens, zoals een pdf-bestand van enkele honderden pagina's. In de tweede plaats bestaat de uitvoer van het algoritme, de *output*, uit een verzameling tekens met een vaste lengte. Het veelgebruikte standaard hashalgoritme SHA-1 (*Secure Hash Algorithm 1*) resulteert bijvoorbeeld in een uitvoer, een *hash value*, van 160 bits (20 bytes), vaak weergegeven als een hexadecimaal getal van 40 tekens. Het derde kenmerk is dat de toepassing van het algoritme onomkeerbaar is. De oorspronkelijke tekens kunnen niet worden herleid uit de hashwaarde. In de vierde plaats mag een hashalgoritme er niet voor zorgen dat verschillende *input* leidt tot identieke *output*. Als dat wel het geval is dan wordt er gesproken van een *collision*, een 'botsing'. Hashalgoritmes dienen *collision resistant* te zijn. Tot slot dient dezelfde *input* bij elke berekening opnieuw te leiden tot dezelfde *output*.

Figuur 4 Toepassing van een hashalgoritme, resulterend in een hashwaarde

In het kader van betrouwbare elektronische communicatie worden hashalgoritmes onder meer gebruikt bij het opslaan van wachtwoorden. Als een online dienst (bijvoorbeeld een website of mobiele app) vereist dat de gebruiker met een wacht-

woord inlogt, dan wordt niet het wachtwoord van de gebruiker opgeslagen maar een hashwaarde daarvan. Bij het inloggen wordt nagegaan of de hashwaarde van het ingetypte wachtwoord overeenstemt met de hashwaarde van het wachtwoord zoals die oorspronkelijk is opgeslagen bij het aanmaken van het wachtwoord. Het gebruik van een hashalgoritme voorkomt zo dat er een gevoelige lijst van wachtwoorden hoeft te worden opgeslagen.³³

Hashalgoritmes spelen een belangrijke rol ten aanzien van het beginsel van integriteit. Door de hashwaarde van een bericht of document die is berekend voordat het bericht of document via elektronische communicatie is getransporteerd, te vergelijken met de hashwaarde die na transport is berekend, kan worden nagegaan of het bericht of document is gewijzigd.

Elektronische ondertekening is een combinatie van hashing en versleuteling

Door asymmetrische encryptie en hashalgoritmes te combineren kunnen betrouwbare elektronische handtekeningen worden geplaatst. Hierboven is besproken hoe het gebruik van asymmetrische encryptie kan voorzien in de beginselen van betrouwbare communicatie tussen een verzender en ontvanger. Dit brengt echter met zich mee dat het hele bericht wordt versleuteld. Het is in de meeste situaties echter niet nodig om het gehele bericht te versleutelen. Het kan zelfs onpraktisch zijn om de ontvanger eerst een bericht te laten ontsleutelen voordat hij er kennis van kan nemen. Door een bericht zoals hierna omschreven elektronisch te ondertekenen, hoeft niet het hele bericht te worden versleuteld. Als eerste wordt er een hashwaarde van de te ondertekenen tekst berekend. De hashwaarde kan bijvoorbeeld betrekking hebben op een verklaring in een e-mailbericht of op de tekst in een pdf-bestand. Volgens wordt de hashwaarde versleuteld door toepassing van de private sleutel door de ondertekenaar. Ten aanzien van het ondertekenen van een pdf-bestand kan dit als volgt worden weergegeven.

Figuur 5 Elektronische ondertekening

³³ Dit betekent overigens niet dat er kan worden volstaan met het onbeveiligd opslaan van de hashwaardes aangezien er methoden zijn om het juiste wachtwoord bij een hashwaarde te zoeken. Dit geschiedt aan de hand van lange lijsten met veel voorkomende wachtwoorden. De hashwaardes van die wachtwoorden kunnen worden vergeleken met onrechtmatig buitgemaakte hashwaardes om zo het bij een inlognaam behorende wachtwoord te achterhalen. Zie bijvoorbeeld <http://www.passwordrandom.com/most-popular-passwords> voor een lijst van de 1000 meest voorkomende wachtwoorden.

In een e-mailbericht zou een zodanige elektronische handtekening (dat wil zeggen een versleutelde hashwaarde) er als volgt uit kunnen zien. In de praktijk zal dit op een visueel prettiger wijze aan de ontvanger worden gepresenteerd, bijvoorbeeld met een icoontje van een zegel. Het is niet nodig de ontvanger de daadwerkelijke handtekening zelf te tonen.

Geachte mevrouw De Kort,

Graag gaan wij akkoord met uw offerte d.d. 2 augustus 2017.

Met vriendelijke groet,
Vincent Hoogenes
Hoogenes B.V.

```
-----Start signature block---  
3081 8902 8181 00C2 6868 0EFF  
1B1E 6C2F 2BB0 4689 25AF F545  
DD27 478B D995 4689 6004 3FF4  
-----End signature block-----
```

Met deze vorm van elektronische ondertekening kan de identificatie & authenticatie van de ondertekenaar worden geborgd. Dan dient voorafgaand aan de verstrekking van de private sleutel aan de ondertekenaar, de ondertekenaar afdoende zijn geïdentificeerd. Voorts dient de private sleutel op een veilige manier aan de ondertekenaar zijn uitgereikt. Bovendien is de integriteit geborgd. Wanneer de ontvanger de handtekening valideert, zal blijken of de ondertekende verklaring is gemanipuleerd. Er is ook sprake van onweerlegbaarheid. De ondertekenaar kan niet terecht ontkennen die specifieke verklaring te hebben ondertekend.

Een elektronische handtekening gebaseerd op asymmetrische encryptie, waarbij de hashwaarde wordt versleuteld, wordt door sommigen ook wel aan geduid als een *digitale handtekening*.³⁴

Een belangrijke toepassing van een systeem van elektronische ondertekening met asymmetrische encryptie is dat dit systeem de handtekening kan valideren. De IT-toepassing waarmee het systeem is geïmplementeerd zal kunnen aangeven of de handtekening geldig is. Dat wil in die context bijvoorbeeld zeggen dat de private sleutel correct is toegekend aan de gebruiker en niet is gecompromitteerd en dat de integriteit is geborgd.³⁵

34 J. Dumortier & P. Van Eecke, 'De Europese ontwerprichtlijn over de digitale handtekening: waarom is het misgelopen?', *Computerrecht* 1999/1, p. 3 e.v.; P. van Eecke, *Naar een juridische status voor de elektronische handtekening* (diss. Leuven), Leuven: Icri 2004, nr. 350; M.H.M. Schellekens, *Electronic signatures. Authentication technology from a legal perspective* (IT&Law nr. 5), Den Haag: T.M.C. Asser Press 2004, p. 27.

35 De eIDAS-verordening definieert 'validering' als 'proces waarmee wordt nagegaan of en bevestigd dat een elektronische handtekening (...) geldig is', art. 3 sub 41.

2.5 De noodzaak van een authenticatiesysteem

Het kunnen authenticeren van een persoon (dat wil zeggen, het betrouwbaar verifiëren van de geclaimde identiteit van die persoon) is een noodzakelijke voorwaarde waaraan voldaan moet zijn voordat die persoon een betrouwbare elektronische handtekening kan plaatsen. Een handtekening moet immers aan een persoon te relateren zijn. Een afdoende identificatie & authenticatie is dus een noodzakelijke voorwaarde voor elektronisch ondertekenen. Het opzetten van een authenticatiesysteem heeft echter nogal wat voeten in aarde. Gebruikers moeten worden geïdentificeerd, aan elke gebruiker moet op betrouwbare wijze een authenticatiemiddel worden uitgereikt, dienstverleners waarbij de gebruiker zich kan authenticeren (kan inloggen) moeten worden aangesloten, authenticatiehandelingen moeten worden geverifieerd, authenticatiemiddelen moeten op den duur weer worden ingetrokken, enzovoort.

Voor het elektronisch communiceren met de overheid heeft de overheid voor een groot deel deze taak op zich genomen. Zo is DigiD het door de overheid aangeboden authenticatiesysteem dat burgers kunnen gebruiken bij het elektronisch communiceren met bestuursorganen en semipublieke instellingen. Het gebruik van DigiD is beperkt tot de (semi)publieke sector omdat de organisatie waarbij de burger inlogt met zijn DigiD, door het inloggen de beschikking krijgt over het burgerservicenummer (BSN) van die burger. Het BSN mag alleen worden verwerkt door die organisaties die het BSN nodig hebben voor het uitvoeren van een publieke taak, of door organisaties die op grond van een wettelijke grondslag daartoe bevoegd zijn.³⁶

Bedrijven kunnen voor de elektronische communicatie met de overheid gebruikmaken van *eHerkenning*.³⁷ Anders dan DigiD is *eHerkenning* geen centrale voorziening die wordt aangeboden door de overheid maar een afsprakenstelsel waarbinnen door particuliere partijen authenticatiediensten worden verleend. Een bedrijf dient aldus één (of meer) authenticatiemiddel(en) aan te schaffen bij een dienstverlener die is toegelaten tot het stelsel. Met dat authenticatiemiddel kan het bedrijf zich vervolgens authenticeren in de elektronische communicatie met de overheid.³⁸

Het bestaansrecht van DigiD en *eHerkenning* is het verzorgen van identificatie & authenticatie, en mogelijk ook het elektronisch ondertekenen, ter ondersteuning van de elektronische communicatie met de overheid. Deze twee authenticatiesystemen zijn daarom (privaatrechtelijk) minder relevant voor de elektronische handtekening die tot een onderhandse elektronische akte leidt. Sinds eind 2016 is er echter sprake van een authenticatiesysteem dat voor velen beschikbaar is en dat ook in een puur privaatrechtelijke context kan worden toegepast. Dit is het zogenoemde iDIN.³⁹ iDIN is een initiatief van de Nederlandse banken. Het houdt in dat

36 Zie ten aanzien van het BSN: M.B. Voulon, 'Basisregistraties', in: M.M. Groothuis (red.), *Bestuursrecht en ICT*, Den Haag: Sdu Uitgevers 2012, p. 84-88.

37 Zie <https://www.eherkenning.nl>.

38 Het afsprakenstelsel *eHerkenning* is online raadpleegbaar: <https://www.eherkenning.nl/over-eherkenning/afsprakenstelsel/>. Naast DigiD en *eHerkenning* spreekt de overheid ook van *Idensys*, <https://www.idensys.nl>. Als ik het goed begrijp is dat een overkoepelend afsprakenstelsel dat zowel DigiD als *eHerkenning* zou kunnen omvatten.

39 Zie <https://www.idin.nl>.

een klant van een bank de authenticatiemiddelen die de bank aan de klant heeft verstrekt, ook kan gebruiken om zich bij andere partijen dan die bank te authenticeren. De introductie van iDIN heeft naar mijn mening de juridische discussie over de rol van de elektronische handtekening doen herleven. Voorafgaand aan iDIN ontbrak een algemeen toepasbaar authenticatiesysteem op basis waarvan deelnemers aan het maatschappelijk verkeer zich jegens elkaar kunnen authenticeren. Daarnaast kan op basis van een iDIN-authenticatie een elektronische handtekening worden geplaatst. Overigens is dat vooralsnog geen onderdeel van het iDIN-systeem zelf. Er zullen aanvullende maatregelen moeten worden getroffen om op basis van een iDIN-authenticatie een elektronische handtekening te genereren.⁴⁰

2.6 De wettelijke definities van de elektronische handtekening

De wet kent drie soorten elektronische handtekening. Met een toenemende mate van betrouwbaarheid zijn dat de *elektronische handtekening*, de *geavanceerde elektronische handtekening* en de *gekwalficeerde elektronische handtekening*. Ten aanzien van de handgeschreven handtekening maakt de wet geen onderscheid naar de mate van betrouwbaarheid. Voor de elektronische handtekening is dat wel het geval. Dat komt doordat de wetgever een risicogebaseerde benadering hanteert.

Ik bespreek hieronder de drie soorten elektronische handtekening. Deze bouwen op elkaar voort. De elektronische handtekening maakt onderdeel uit van de definities van de andere twee soorten elektronische handtekening. De geavanceerde elektronische handtekening maakt onderdeel uit van de definitie van de gekwalificeerde elektronische handtekening.

De elektronische handtekening

De elektronische handtekening bestaat uit (1) gegevens in elektronische vorm, (2) die gehecht zijn aan of logisch verbonden zijn met (3) andere gegevens in elektronische vorm en die (4) door de ondertekenaar worden gebruikt om te ondertekenen.⁴¹ Bij eerste lezing zal deze omschrijving een cryptische indruk maken. Het is van belang de twee eerdergenoemde essentiële elementen van de handtekening in het achterhoofd te houden: het uitdrukking geven aan een *animus signandi* en het individualiseren van de ondertekenaar. Vanuit die elementen bezien is het duidelijk dat de gegevens genoemd onder (3) de gegevens betreffen die uitdrukking geven aan de verklaring die de ondertekenaar wenst te ondertekenen; dit is de te tekenen verklaring. De gegevens genoemd onder (1) zijn de gegevens waaruit de handtekening zelf bestaat. De verbinding genoemd onder (2) is de associatie tussen de handtekening en de verklaring. De handtekening dient immers betrekking te hebben op een specifieke verklaring. De betekenis van het vereiste onder (4) is op het eerste gezicht niet duidelijk. Het lijkt een cirkelredenering te introduceren. Een voorgaande versie van de wettelijke definitie luidde overigens anders. In plaats van ‘die door de ondertekenaar worden gebruikt om

⁴⁰ Een voorbeeld van een dienstverlener die dit soort diensten levert, is Evidos: <https://www.evidos.nl>.

⁴¹ Art. 3 lid 10 eIDAS-verordening.

te ondertekenen', werd er gesproken van 'die worden gebruikt als middel voor authenticatie'.⁴² De term 'authenticatie' introduceerde onduidelijkheid (zie de discussie over de term authenticatie in paragraaf 2.4). In de literatuur werd dit geïnterpreteerd als het verifiëren van een identiteit.⁴³ Het zou echter ook kunnen worden geïnterpreteerd als het instemmen met een verklaring, oftewel het uiten van een *animus signandi*. Door 'middel voor authenticatie' te vervangen door 'gebruikt om te ondertekenen' is de onduidelijkheid niet weggenomen. Beide interpretaties zijn nog steeds verdedigbaar.

De geavanceerde elektronische handtekening

Dan de geavanceerde elektronische handtekening. Dit is de elektronische handtekening die voldoet aan vier aanvullende eisen: (a) zij is op unieke wijze aan de ondertekenaar verbonden; (b) zij maakt het mogelijk de ondertekenaar te identificeren; (c) zij komt tot stand met 'gegevens voor het aanmaken van elektronische handtekeningen die de ondertekenaar, met een hoog vertrouwensniveau onder zijn uitsluitende controle kan houden'; en (d) zij is op zodanige wijze aan de ondertekende gegevens verbonden dat elke wijziging achteraf van de gegevens kan worden opgespoord.⁴⁴ Met name sub c introduceert hier enige onduidelijkheid. Wat kan er precies worden verstaan onder deze 'gegevens voor het aanmaken van een elektronische handtekening'? De eIDAS-verordening definieert deze gegevens als 'unieke gegevens die door de ondertekenaar worden gebruikt om een elektronische handtekening aan te maken'.⁴⁵ Dat verduidelijkt niet veel, behalve dan dat de gegevens kennelijke *uniek* moeten zijn. De richtlijn inzake elektronische handtekeningen, de voorganger van de eIDAS-verordening, noemde op dit punt twee voorbeelden, namelijk 'codes of cryptografische privésleutels'.⁴⁶ Een private sleutel zal dus naar alle waarschijnlijkheid in elk geval kunnen worden aangemerkt als een 'gegeven voor het aanmaken van een elektronische handtekening'. De onduidelijkheid die het vereiste echter introduceert, betreft de vraag welke andere gegevens dan een private sleutel in aanmerking komen om als 'gegevens voor het aanmaken van elektronische handtekeningen' te kwalificeren. Als dit iets anders zou zijn dan een private sleutel, dan is het technische betrouwbaarheidsniveau wellicht lager dan waarvan bij toepassing van asymmetrische encryptie sprake van zou kunnen zijn. De wetgever lijkt van mening te zijn dat een geavanceerde elektronische handtekening niet per se op asymmetrische encryptie hoeft te zijn

⁴² Art. 2 lid 1 Richtlijn 1999/93/EG betreffende een gemeenschappelijk kader voor elektronische handtekeningen, PbEU 2000, L 13.

⁴³ A.R. Lodder, J. Dumortier & S.H. Bol, *Het recht rond elektronische handtekeningen*, Deventer: Kluwer 2005, p. 24 & 51.

⁴⁴ Art. 26 eIDAS-verordening.

⁴⁵ Art. 3 lid 13 eIDAS-verordening.

⁴⁶ In de richtlijn luidde het vereiste onder (c) als volgt: 'zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden', art. 2 lid 2 sub c Richtlijn 1999/93/EG. Volgens art. 2 lid 5 van de richtlijn werd dit middel dan weer gebruikt om 'gegevens voor het aanmaken van elektronische handtekeningen te implementeren'. Deze gegevens werden vervolgens gedefinieerd als 'unieke gegevens, zoals codes of cryptografische privé-sleutels, die door de ondertekenaar worden gebruikt om een elektronische handtekening aan te maken', aldus art. 2 lid 4 van de richtlijn.

gebaseerd.⁴⁷ De grote vraag is dan wat voor gegevens, anders dan een private sleutel, deze rol zouden kunnen vervullen. Bovendien, als wordt aangenomen dat er geen asymmetrische encryptie hoeft te worden ingezet om tot een geavanceerde handtekening te komen, dan verwatert het begrip geavanceerde elektronische handtekening, het begrip wordt te ruim.

De gekwalificeerde elektronische handtekening

Vanuit technisch oogpunt is de gekwalificeerde elektronische handtekening gebaseerd op asymmetrische encryptie. Er is sprake van een hashwaarde van de ondertekende verklaring en die hashwaarde is versleuteld met de private sleutel van de ondertekenaar. De wettelijke definitie omschrijft de gekwalificeerde elektronische handtekening als een geavanceerde elektronische handtekening die is aangemaakt met een *gekwaliificeerd middel* en die is gebaseerd op een *gekwaliificeerd certificaat*.⁴⁸

Een *middel* wordt enigszins cryptisch gedefinieerd als geconfigureerde hardware of software die wordt gebruikt om een elektronische handtekening aan te maken.⁴⁹ Een *gekwaliificeerd middel* dient aan een aantal specifieke eisen te voldoen.⁵⁰ Meer praktisch omschreven is het middel dat element waarmee de ondertekenaar zijn private sleutel kan toepassen om een elektronische handtekening te genereren. De functie van het middel is dus onder meer dat alleen de ondertekenaar toegang heeft tot de private sleutel en dat de sleutel op een veilige manier wordt toegepast. Een klassieke wijze van omgang met de private sleutel is dat deze zich op een chipcard bevindt. De ondertekenaar kan de private sleutel toepassen door de chipcard in een kaartlezer te plaatsen en een pincode in te toetsen. Het geheel van de kaart, de kaartlezer en de software is dan het ‘middel voor het aanmaken van elektronische handtekeningen’. Een private sleutel zou zich ook in ‘de cloud’ kunnen bevinden.⁵¹ De sleutel bevindt zich dan in een server die met het internet is verbonden en is voor de ondertekenaar te gebruiken om handtekeningen te plaatsen. Dit systeem moet er dan uiteraard voor zorgdragen dat de sleutel goed is beveiligd zodat alleen de ondertekenaar de sleutel kan gebruiken. Dat betekent dat niet alleen de server zelf (er wordt in dit verband gesproken van de reeds eerder benoemde HSM, *hardware security module*) maar ook de toegang van de ondertekenaar tot de sleutel via het openbare internet, afdoende is beveiligd. De ondertekenaar zal dus onder meer over een geschikt authenticatiemiddel moeten beschikken.

Dan het gekwalificeerde certificaat. Zoals hierboven reeds aangegeven is een certificaat het middel waarmee publieke sleutels aan eenieder beschikbaar worden gesteld. Het certificaat geeft aan, aan welke persoon de met de publieke sleutel corresponderende private sleutel is uitgereikt. Volgens de wettelijke definitie is een certificaat ‘een elektronische attestering die valideringsgegevens voor

47 Kamerstukken II 2015/16, 34413, 6, p. 14: ‘Voor een geavanceerde handtekening kan de techniek van digitale certificaten worden gebruikt, maar dit hoeft niet.’

48 Art. 3 lid 2 eIDAS-verordening.

49 Art. 3 lid 22 eIDAS-verordening.

50 Art. 3 lid 23 en bijlage II eIDAS-verordening.

51 Overweging 52 van de eIDAS-verordening noemt expliciet het ‘aanmaken van elektronische handtekeningen op afstand’.

elektronische handtekeningen aan een natuurlijk persoon koppelt en ten minste de naam of het pseudoniem van die persoon bevestigt'.⁵² Ook deze definitie lijkt meer te verhullen dan duidelijk te maken vanwege de cryptisch omschrijving van de publieke sleutel. De publieke sleutel wordt in deze definitie omschreven als 'valideringsgegevens'. Valideringsgegevens worden vervolgens gedefinieerd als 'gegevens die worden gebruikt om een elektronische handtekening te valideren'.⁵³ 'Valideren' is het 'proces waarmee wordt nagegaan of en bevestigd dat een elektronische handtekening geldig is'.⁵⁴ De omslachtige, cryptische wijze van definiëren laat zich wellicht verklaren uit het feit dat de wetgeving aan de ene kant technologie-neutraal wenst te zijn⁵⁵ en aan de andere kant specifiek de op asymmetrische encryptie gebaseerde elektronische handtekening op het oog heeft. Wil er vervolgens sprake zijn van een *gekwalificeerd* certificaat, dan moet er aan een aantal vereisten zijn voldaan. Een gekwalificeerd certificaat moet bepaalde gegevens bevatten.⁵⁶ Een gekwalificeerd certificaat mag alleen worden uitgegeven door de gekwalificeerde vertrouwensdienstverlener. Die gekwalificeerde vertrouwensdienstverlener moet de beoogde ondertekenaar op een betrouwbare manier identificeren (door fysieke aanwezigheid (!) of op een andere wijze met een gelijkwaardige mate van betrouwbaarheid) voordat hij het certificaat mag afgeven.⁵⁷ Hij moet zich minstens één keer per twee jaar onderwerpen aan een audit.⁵⁸ Verder moet de gekwalificeerde vertrouwensdienstverlener voldoende deskundig en betrouwbaar personeel in dienst te hebben, over voldoende financiële middelen beschikken of een afdoende verzekering hebben, voldoende beveiligde systemen en producten gebruiken, enzovoort.⁵⁹

Overigens blinkt de formulering dat de gekwalificeerde elektronische handtekening is 'gebaseerd op een gekwalificeerd certificaat' niet uit door duidelijkheid. Het is juister om te stellen dat de handtekening wordt aangemaakt met de private sleutel die correspondeert met de publieke sleutel die in het certificaat is opgenomen. De handtekening wordt immers aangemaakt met de private sleutel, niet met de publieke sleutel of anderszins met het certificaat.

De gekwalificeerde elektronische handtekening is een hoofdcomponent van de risicogebaseerde benadering waarvan de wetgever ten aanzien van de elektronische handtekening is uitgegaan. De wetgever heeft getracht de meeste risico's te minimaliseren door middel van uitgebreide wettelijke voorschriften. Het risico dat een private sleutel niet aan de juiste persoon wordt gekoppeld bij toewijzing, wordt ondervangen door de verplichting de persoon met een hoge mate van zekerheid te identificeren. Het risico dat de private sleutel kan worden gecompromitteerd door hackers wordt gemitigeerd door voorschriften ten aanzien van het gekwalificeerde middel. Het risico dat personeel van de gekwalificeerde vertrouwensdienstverlener kan worden beïnvloed door kwaadwillenden wordt

52 Art. 3 lid 14 eIDAS-verordening.

53 Art. 3 lid 40 eIDAS-verordening.

54 Art. 3 lid 41 eIDAS-verordening.

55 Overweging 27 eIDAS-verordening.

56 Bijlage I eIDAS-verordening.

57 Art. 24 lid 1 eIDAS-verordening.

58 Art. 20 eIDAS-verordening.

59 Art. 24 lid 2 eIDAS-verordening.

gemitigeerd door te eisen dat het personeel betrouwbaar en deskundig moet zijn, enzovoort.

2.7 Betrouwbaarheidsniveaus

De risicogebaseerde benadering schrijft voor dat er mitigerende maatregelen moeten worden genomen die passend zijn ten aanzien van eventueel vastgestelde risico's. Omdat sommige online transacties lage risico's kennen, en andere hogere risico's, dienen de mitigerende maatregelen ook in verschillende betrouwbaarheidsniveaus te worden onderscheiden. Vanuit juridisch oogpunt is de eIDAS-verordening hier leidend. Zoals hierboven aangegeven gaat de verordening uit van twee regimes, één betreffende elektronische identificatie en één betreffende vertrouwensdiensten. Ten aanzien van elektronische identificatie zijn er drie betrouwbaarheidsniveaus ('Levels of Assurance, LoA's'): laag, substantieel en hoog.⁶⁰ De Europese Commissie heeft deze drie niveaus in een uitvoeringsverordening nader uitgewerkt.⁶¹ Kenmerkend voor de wijze waarop de vereisten voor de drie niveaus worden gestipuleerd is de fasering van de bedrijfsprocessen van een stelsel voor elektronische identificatie. De eerste fase is de inschrijvingsfase. De gebruiker van een authenticatiemiddel vraagt een authenticatiemiddel aan en moet worden geïdentificeerd. Voor een laag betrouwbaarheidsniveau is het niet nodig uitgebreid de identiteit van de aanvrager te onderzoeken. Voor een hoog betrouwbaarheidsniveau is het wellicht nodig de aanvrager in persoon te identificeren en diens identificatiemiddel te controleren. De tweede fase is de uitgiftefase. Dit betreft de verstrekking van het authenticatiemiddel aan de gebruikers. Op een laag niveau kan mogelijk worden volstaan met een verzending per post van het middel aan de gebruiker. Op een hoger niveau kan verstrekking in persoon noodzakelijk zijn. De derde fase betreft het gebruik van het middel. Aan welke technische beveiligingsmaatregelen dienen het middel en het authenticatieproces te voldoen? De vierde fase betreft het intrekken van het middel. Als een authenticatiemiddel is gecompromitteerd, dient het middel snel te kunnen worden geblokkeerd. Naast de chronologische fasering kunnen vanuit het oogpunt van de betrouwbaarheidsniveaus ook eisen worden gesteld aan de organisatie die het middel uitgeeft, beheert en het authenticatieproces ondersteunt.

Ten aanzien van de elektronische handtekening kunnen ook drie niveaus van betrouwbaarheid worden onderscheiden, die bestaan immers uit de elektronische handtekening, de geavanceerde elektronische handtekening en de gekwalificeerde elektronische handtekening.⁶² Er kan een tussenniveau worden geïdentificeerd, te weten de geavanceerde elektronische handtekening die is gebaseerd op een gekwalificeerd certificaat (maar zonder dat er gebruik wordt gemaakt van een gekwalificeerd middel).

⁶⁰ Art. 8 eIDAS-verordening.

⁶¹ Uitvoeringsverordening (EU) 2015/1502 inzake betrouwbaarheidsniveaus voor elektronische handtekeningen, PbEU 2015, L 235.

⁶² De vereisten voor de betrouwbaarheidsniveaus zijn vervat in de eIDAS-verordening zelf, in een uitvoeringsbesluit (uitvoeringsbesluit 2015/1506, PbEU 2015, L 235) en in diverse technische standaarden, onder meer zoals vastgesteld in technische normen van de European Telecommunications Standards Institute, ETSI, en in die van de European Committee for Standardization, CEN.

Net zoals bij de betrouwbaarheidsniveaus ten aanzien van authenticatiemiddelen hebben de diverse betrouwbaarheidsniveaus betrekking op de fasering van de bedrijfsprocessen (inschrijvingsfase, uitgiftedfase, gebruiksfase, intrekkingdase) en op de organisatie die het ondertekenmiddel uitdeeft en verder de ondertekendienst verleent.

Het valt op dat de vereisten ten aanzien van de betrouwbaarheidsniveaus voor elektronische handtekeningen volledig losstaan van de vereisten ten aanzien van de betrouwbaarheidsniveaus voor authenticatiemiddelen. Authenticatie en ondertekenen is weliswaar niet hetzelfde, toch zou het uit het oogpunt van consistentie en begripelijkheid beter zijn als er één regime zou zijn dat de betrouwbaarheidsniveaus van zowel authenticatie als de elektronische handtekening (en de vertrouwensdiensten in het algemeen) zou behandelen.

2.8 De gelijkstelling van de elektronische handtekening met de handgeschreven handtekening volgens eIDAS

Na bespreking van de drie soorten van de elektronische handtekening is de grote vraag natuurlijk: wat is de toegevoegde waarde ervan? De hoofdregel ten aanzien hiervan wordt gesteld door de eIDAS-verordening: een gekwalificeerde elektronische handtekening heeft hetzelfde rechtsgevolg als een handgeschreven handtekening.⁶³

2.9 De risicogebaseerde benadering van de Nederlandse wetgever

Het Nederlandse BW vult de eIDAS-gelijkstellingsregel aan.⁶⁴ Hierboven hebben we gezien dat deze gelijkstellingsregel van de eIDAS inhoudt dat de gekwalificeerde elektronische handtekening hetzelfde rechtsgevolg heeft als de handgeschreven handtekening. Artikel 3:15a BW voegt daaraan toe dat de ‘gewone’ elektronische handtekening en de geavanceerde elektronische handtekening

‘dezelfde rechtsgevolgen [hebben] als een handgeschreven handtekening, indien voor deze beide elektronische handtekeningen de methode voor ondertekening die gebruikt is voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische handtekening is gebruikt en op alle overige omstandigheden van het geval.’

Een handtekening van een lager niveau dan de gekwalificeerde handtekening heeft dus dezelfde rechtsgevolgen als een handgeschreven handtekening mits zij voldoende betrouwbaar is, gelet op het doel waarvoor zij wordt gebruikt en gelet op alle overige omstandigheden van het geval.

⁶³ Art. 25 lid 2 eIDAS-verordening. Overigens laat ik een bespreking van de zogenoemde ‘non-discriminatie benadering’ hier achterwege. Deze benadering houdt in dat een wettelijke regel stelt dat bijvoorbeeld een handtekening of document geen rechtsgevolg mag worden ontzegd enkel op grond van het feit dat het een elektronische handtekening of elektronisch document betreft, zie art. 25 lid 1 eIDAS-verordening.

⁶⁴ Zie ook overweging 49 van de eIDAS-verordening: ‘Het nationaal recht moet echter bepalen welk rechtsgevolg elektronische handtekeningen hebben, met uitzondering van de in deze verordening vastgestelde voorschriften dat een gekwalificeerde elektronische handtekening hetzelfde rechtsgevolg dient te hebben als een handgeschreven handtekening.’

De vraag is nu hoe deze betrouwbaarheidstoets moet worden ingevuld. Volgens de parlementaire geschiedenis zal een elektronische handtekening met meer waarborgen moeten worden omkleed, 'naarmate het belang van de rechtshandeling toeneemt.' De parlementaire geschiedenis vervolgt:

'Bij de beoordeling van het belang van de rechtshandeling zullen partijen naar verwachting onder meer rekening houden met de hoogte van de economische waarde die met de rechtshandeling is gemoeid. Zo zal bij de koop van een boek of een cd langs elektronische weg doorgaans met het gebruik van een gewone elektronische handtekening kunnen worden volstaan. Bij grotere transacties als het kopen van een huis of een auto langs elektronische weg zal eerder gebruik worden gemaakt van een elektronische handtekening die met de meeste waarborgen is omgeven. Het belang van de transactie wordt in dit verband echter niet uitsluitend in economische termen bepaald. Zo zal het gebruik van een geavanceerde elektronische handtekening ook voor de hand liggen indien de aard van de transactie vereist dat zoveel mogelijk beveiligingsmaatregelen worden getroffen om de integriteit van het bericht te waarborgen, zoals in het geval van langs elektronische weg gegeven juridische of medische adviezen.'⁶⁵

De wetgever heeft blijkens deze overweging voor een risicogebaseerde benadering gekozen: bepalend voor het niveau van de handtekening is het belang van de rechtshandeling. De economische waarde van de rechtshandeling en de (waarborging van de) integriteit van de uit te wisselen gegevens kunnen mede het belang van de rechtshandeling bepalen. Mogelijk heeft de wetgever het risico van frauduleuze internetaankopen, en het risico van gecompromitteerde integriteit van juridische en medische adviezen in gedachten gehad. Conform de risicogebaseerde benadering kunnen na identificatie van relevante risico's, deze risico's worden gemitigeerd door de inzet van een afdoende elektronische handtekening. Vanuit een oogpunt van risicobeheersing is dit een voor de hand liggende redenering. Er wordt echter wel afgedwaald van de oorspronkelijk rol van de handgeschreven handtekening. Ons burgerlijk recht gaat nog steeds uit van consensualisme. Voor het doen van aankopen is in beginsel geen handtekening vereist. Ook voor het geven van juridische of medisch adviezen fungeert de handgeschreven handtekening momenteel niet als integriteitsmechanisme.

Het bovenstaande brengt ons tot een aanverwante vraag: wat betekent de algemene gelijkstelling met de handgeschreven handtekening überhaupt? Ten aanzien van de handgeschreven handtekening ben ik er in deze bijdrage van uitgegaan dat de handgeschreven handtekening met name van belang is voor het realiseren van een onderhandse akte. In veel gevallen dient de handtekening in die context te worden gezien. In de parlementaire geschiedenis merkt de wetgever het volgende op ten aanzien van de vraag op welke rechtsgevolgen van de handtekening de gelijkstellingsregel doelt:

⁶⁵ Kamerstukken II 2001/02, 27743, 6, p. 2.

‘Zoals uit artikel 3:15a BW blijkt, heeft een elektronische handtekening onder voorwaarden dezelfde rechtsgevolgen als een handgeschreven handtekening. Het gaat hier om een gelijkstelling die uit de aard der zaak alleen daar consequenties heeft waar het al of niet gezet zijn van een handtekening tot verschillende rechtsgevolgen leidt. Indien een handtekening vereist is om een bepaald rechtsgevolg te bewerkstelligen (bijvoorbeeld het sluiten van een koopovereenkomst, het sluiten van een huurovereenkomst of ondertekening van een bepaalde wilsverklaring) kan hieraan zowel door een handgeschreven als een elektronische handtekening worden voldaan. Het gewenste rechtsgevolg blijft derhalve gelijk, of nu is ondertekend met de hand of langs elektronische weg, mits aan het criterium van 3:15a lid 1 BW is voldaan.’⁶⁶

De wetgever draait hier om de hete brij heen. Voor het aangaan van een overeenkomst is in beginsel geen handtekening vereist.⁶⁷ Een wilsverklaring kan uiteraard kracht worden bijgezet door een handtekening er onderdeel van uit te laten maken. De toegevoegde waarde van de handtekening is echter eerder te vinden in het realiseren van een onderhandse akte of om aan een (ander) specifiek vormvereiste te voldoen. In de praktijk zijn regelmatig contractuele clausules aan te treffen die stellen dat door gebruik te maken van een bepaalde wijze van elektronische ondertekenen, de daarmee geplaatste handtekening ‘dezelfde rechtsgevolgen heeft als een handgeschreven handtekening’.⁶⁸ Welke rechtsgevolgen dat zijn, blijft onbesproken.

2.10 Tussenconclusie: de risicobaseerde benadering en de elektronische handtekening

Aan de elektronische handtekening, in de context van de onderhandse akte, ligt naar mijn mening een andere achterliggende benadering ten grondslag dan waarvan bij de handgeschreven handtekening sprake is. Bij de handgeschreven handtekening wordt uitgegaan van de goede trouw-benadering. Er wordt aangenomen dat deelnemers aan het maatschappelijk verkeer consciëntieus zullen handelen. Niet alles is a priori verdacht. Voorts kan de beweerdelijk ondertekenaar stellig ontkennen te hebben getekend. In dat geval zal degene die zich op de rechtsgevolgen van de akte beroept, aannemelijk moeten maken dat de handtekening wel degelijk authentiek is.

Bij de risicobaseerde benadering wordt uitgegaan van wantrouwen. Risico's dienen te worden geanalyseerd en gemitigeerd. Wet- en regelgeving schrijven uitputtend voor welke maatregelen dienen te worden genomen bij welke betrouwbaarheidsniveaus van authenticatiemiddelen en ondertekenmiddelen. Op de hoogste betrouwbaarheidsniveaus worden ondertekenaars vooraf betrouwbaar

66 Kamerstukken I 2002/03, 27743, 35, p. 10.

67 Ik heb dit besproken in mijn proefschrift, Voulon 2010, p. 270. Van Es heeft hier in 2002 reeds op gewezen, P.C. van Es, ‘Nadere opmerkingen over de Wet elektronische handtekeningen’, WPNR 2002, 6515, p. 857-858.

68 Zie bijvoorbeeld C. Drion, *Internet en e-commerce* (Boom modellen en commentaar), Den Haag: Boom Juridische uitgevers 2003, het modelcontract ‘Voorwaarden voor het gebruik van digitale handtekening en timestamping’, art. 4 ‘Rechtsgevolgen’: ‘De door Partijen in overeenstemming met deze Overeenkomst gebruikte Digitale handtekening zal tussen Partijen dezelfde rechtsgevolgen hebben als een geschreven handtekening.’

geïdentificeerd. Ondertekenmiddelen worden welhaast persoonlijk de ondertekenaar in handen gedrukt om te voorkomen dat zij in verkeerde handen vallen. Betrouwbaarheid van ondertekenmiddelen en betrokken vertrouwensdienstverleners worden geborgd met technische normen en *audits*.

In het licht van de tegenstelling tussen de twee benaderingen heb ik ten aanzien van de elektronische situatie grote moeite met het voorschrift dat een beweerdelijke ondertekenaar door enkel stellig te ontkennen zijn handtekening ter discussie kan stellen. In geval van een elektronische handtekening, met alle daartoe behorende betrouwbaarheidsmaatregelen, mag van die persoon worden verlangd aannemelijk te maken waarom de handtekening niet zijn handtekening betreft. Is zijn authenticatiemiddel en/of zijn ondertekenmiddel gecompromitteerd? Is hij gedwongen? Is hij het slachtoffer van een *hack* of van identiteitsdiefstal? In het licht van de vele beveiligingsmaatregelen legt de huidige mogelijkheid van de stellige ontkenning een onredelijke bewijslast bij degene die zich op de rechtsgevolgen van de onderhandse akte wenst te beroepen.

Er is overigens nog een wettelijk voorschrift waarvoor in de elektronische situatie geen plaats is. Dit betreft de regel dat de kracht van het schriftelijke bewijs in de oorspronkelijke akte is gelegen.⁶⁹ Ik heb dit in deze paragraaf niet besproken, maar het begrip origineel heeft in de digitale omgeving geen waarde. Het heeft geen zin te onderscheiden naar originele en gekopieerde elektronische akten, inclusief handtekeningen. Het enkel transporteren via een netwerk van een elektronische ondertekende akte behelst al meerdere kopieën. Dat tast de elektronische handtekening echter niet aan.

De risicogebaseerde benadering is tot slot moeilijk te rijmen met het privaatrechtelijke beginsel van gelijkwaardigheid van partijen. Het nemen van mitigerende maatregelen, en überhaupt het bieden van authenticatie- en ondertekendiensten, vergt grote investeringen en inspanningen. In de praktijk zal dit bijvoorbeeld alleen door een grotere onderneming aan haar klanten kunnen worden aangeboden.

3 Het digitale product

De immer voortschrijdende digitalisering van het maatschappelijk verkeer heeft geleid tot de vraag hoe digitale producten juridisch moeten worden geduid. De term ‘digitale producten’ gebruik ik gemakshalve voor die digitale objecten die goederenrechtelijk ongrijpbaar lijken: computerprogrammatuur, databestanden, *cryptocurrencies*, *virtual reality*-objecten. De goederenrechtelijke ongrijpbaarheid blijkt uit juridische vragen zoals: wat koop je als je software koopt? Gelden wettelijke bepalingen inzake conforme levering (‘garantie’) ook voor een mobiele app? Als ik een computergame hebt gekocht, kan ik die doorverkopen? Zo ja, hoe kan ik de game dan overdragen? Kan er beslag worden gelegd op een *bitcoins*, of op een *big data*-databestand? Hoe moet een databestand worden overgedragen? Kan ik een zwaard in een computergame stelen?

⁶⁹ Art. 160 lid 1 Rv.

Ik ben niet in staat op elk van deze vragen uitputtend in te gaan. Daarnaast zijn er recent publicaties verschenen die reeds diepgaand op de goederenrechtelijke kwalificatie van digitale producten ingaan.⁷⁰ Ik ben daarom zo vrij mij te beperken tot wat volgens mij de essentiële punten van discussie zijn.

Typerend aan het vraagstuk van digitale producten is dat andere rechtsgebieden een rol spelen. Het kan gaan om het gegevensbeschermingsrecht, het auteursrecht of wellicht het databankenrecht. De vraag die dan rijst, is wat de toegevoegde waarde is van het privaatrecht. Het antwoord daarop zit hem in de vragen die hierboven zijn geformuleerd. Het privaatrecht dient die vragen, bijvoorbeeld inzake beslag (inclusief faillissement) en doorverkoop te beantwoorden. Ook kan worden gewezen op de vraag of digitale producten voor verpanding vatbaar zijn.⁷¹

Om de ontwikkelingen van de laatste tijd niet aan de lezer te onthouden, is het van belang de uitspraak van het Europees Hof van Justitie inzake *UsedSoft*⁷² en de uitspraken van onze Hoge Raad inzake *De Beeldbrigade*⁷³ te bespreken. Voorts dient het voorstel voor een Europese richtlijn inzake digitale inhoud⁷⁴ te worden genoemd.

3.1 Het executoriale deurwaardersbeslag op een kandidatenbestand

De onderhavige problematiek wordt geïllustreerd door een recente uitspraak van de voorzieningenrechter Amsterdam inzake een executoriaal deurswaardersbeslag op een databestand. Het gaat in deze uitspraak⁷⁵ om een ‘Head Hunters bureau met een “executive search” karakter’, met de naam ‘Woman Capital’. Woman Capital richtte zich met name op ‘topvrouwen’ (mogelijk betreft dit vrouwen in bestuurlijke functies). Het bedrijf beschikte over een databestand met ongeveer 10.000 kandidaten. Het databestand bevatte onder meer de volgende informatie over de kandidaten: naam, adres, telefoonnummer, huidige functie, eerdere functies, specialisaties, expertises, cv’s, inkomensgegevens, en een aantal categorieën zoals: interessant/niet interessant, topvrouw, High Potential, ondernemer en concurrentie. Woman Capital was bij een eerder vonnis veroordeeld om aan een schuldeiser ruim € 50.000 te betalen. Vervolgens legde een deurwaarder een executoriaal beslag op ‘voor overdracht vatbare data’. De deurwaarder was voornemens het betreffende databestand openbaar te verkopen. Er waren reeds onderhandse biedingen ontvangen met een waarde tussen € 10.000 en € 30.000. De deurwaarder had echter zo’n 40 bezwaren ontvangen van personen die in het relatiebestand waren opgenomen. Volgens de deurwaarder waren

70 Ik wijs hier slechts op J.H.M. van Erp & W. Loof, ‘Eigendom in het algemeen; eigendom van digitale inhoud (titel 1)’, in: L.C.A. Verstappen (red.), *Boek 5 BW van de toekomst. Over vernieuwingen in het zakenrecht* (KNB Preadviezen 2016), Den Haag: Sdu Uitgevers 2016, p. 23-63; E.D.C. Neppelenbroek, *Softwarebetrekkingen. De auteur, de verkrijger en hun vermogensrechtelijke positie jegens derden* (diss. Groningen), Den Haag: Boom Juridische uitgevers 2013; T.F.E. Tjong Tjing Tai, *Privaatrecht voor de homo digitalis: eigendom, gebruik en handhaving* (Handelingen NJV), Deventer: Wolters Kluwer 2016.

71 T.F.E. Tjong Tjin Tai, ‘Data in het vermogensrecht’, WPNR 28 november 2015, 7085.

72 HvJ 3 juli 2012, C-128/11, ECLI:EU:C:2012:407.

73 HR 27 april 2012, NJ 2012, 293 (Hulskamp/De Beeldbrigade) en 294 (Hulskamp/Bell).

74 Voorstel voor een richtlijn betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud, 9 december 2015, COM(2015)634 final.

75 Rb. Amsterdam 22 oktober 2015, ECLI:NL:RBAMS:2015:7501.

de bezwaren van dien aard dat het onverminderd voorzetten van de executie onjuist zou zijn. Daarom legde hij aan de voorzieningenrechter de vraag voor of hij de executieverkoop van het databestand al dan niet kon voortzetten. De voorzieningenrechter oordeelde dat het de deurwaarder was toegestaan de executie van het databestand voort te zetten. De hoofdoverwegingen van de voorzieningenrechter luiden als volgt:

‘4.3 Woman Capital heeft het databestand gemaakt met als doel een goede match te vinden tussen werkgevers en werknemers. De personen die zich bij Woman Capital hebben aangemeld, hebben zich vrijwillig in het databestand laten opnemen. Volgens Woman Capital dient het databestand thans te worden vernietigd in verband met de privacy van de daarin opgenomen personen en om misbruik van vertrouwelijke gegevens te voorkomen. De deurwaarder heeft echter naar aanleiding van de bezwaren in de veilingvoorwaarden opgenomen dat alleen organisaties die aantoonbaar in dezelfde branche als Woman Capital opereren (arbeidsbemiddeling tussen werkgevers en werknemers) een bod mogen uitbrengen tijdens de executieverkoop op het databestand. Hieruit vloeit voort dat degenen die mogen bieden op het databestand gebonden zullen zijn aan dezelfde regelgeving met betrekking tot persoonsgegevens en privacy als Woman Capital en dezelfde discretie in acht dienen te nemen. Voldoende aannemelijk is dan ook dat de koper van het databestand dit voor hetzelfde doel als Woman Capital zal gebruiken. Hiermee zijn de gegevens van de personen die zijn opgenomen in het databestand en hun privacy vooralsnog voldoende gewaarborgd.

4.4 Op dit moment is de toegang tot het databestand geblokkeerd en kunnen er geen gegevens worden verwijderd. Indien er personen zijn die niet langer in het databestand opgenomen willen zijn wanneer de eigendom van het databestand wordt overgedragen, kunnen zij aan de koper van het databestand een verzoek doen om daaruit te worden verwijderd. De koper zal hierbij uiteindelijk ook gebaat zijn, omdat er dan een databestand zal overblijven met gegevens van personen die daadwerkelijk willen worden benaderd.’

Volgens Van den Heuvel is de benadering van de voorzieningenrechter een ‘juiste en praktische toepassing’.⁷⁶ Ik ben het echter met Konings eens dat het goederenrechtelijke executoriale beslag – althans zoals hier toegepast door de voorzieningenrechter – wringt met het gegevensbeschermingsrecht.⁷⁷ De voorzieningenrechter voert een zeer marginale gegevensbeschermingsrechtelijke toets uit. Het gegevensbeschermingsrecht schrijft onder meer voor dat de verantwoordelijke alleen persoonsgegevens mag verwerken in overeenstemming met de doeleinden die hij daarvoor heeft vastgesteld. Een verdere verwerking (in casu de verstrekking en verwerking door een nieuwe verkrijger) mag niet onverenigbaar zijn met die doeleinden.⁷⁸ De rechter lijkt vrij eenvoudig aan te nemen dat het doeleinde van de verwerking bestaat uit ‘een goede match te vinden tussen werkgevers en werknemers’. Vervolgens neemt hij aan dat ‘de koper van het databestand dit voor hetzelfde doel als Woman Capital zal gebruiken’. Dat hoeft niet onjuist te zijn. De gegevensbeschermingsrechtelijke toets is echter geen objectieve toets.

⁷⁶ N.W.M. van den Heuvel, ‘Beslag op data’, WPNR 4 juni 2016, 7110.

⁷⁷ Zie zijn annotatie in JBP 2015/129.

⁷⁸ Art. 7, 9 Wbp; art. 5 lid 1 sub b Avg.

Het gaat er daarentegen om welk doeleinde deze verantwoordelijke daadwerkelijk heeft vastgesteld. De voorzieningenrechter houdt wel een slag om de arm door te stellen dat de verkrijger gebonden is aan de gegevensbeschermingsrechtelijke voorschriften. Een en ander kan er echter toe leiden dat de verkrijger (de nieuwe verantwoordelijke) met een gegevensbeschermingsrechtelijke verrassing wordt gepresenteerd. Wellicht heeft de eerste verantwoordelijke immers bepaalde beperkingen ten aanzien van het verwerkingsdoeleinde vastgesteld waar de verkrijger pas later van op de hoogte geraakt. Kortom: het gegevensbeschermingsrecht dient expliciet betrokken te worden rondom vragen inzake beslag (en overdracht) van databestanden waarmee persoonsgegevens gemoeid zijn.

Naast de relevantie van het gegevensbeschermingsrecht illustreert de uitspraak van de voorzieningenrechter Amsterdam een anders aspect, te weten het object van het beslag. De deurwaarder en de rechter spreken van beslag op een databestand. Van den Heuvel en Konings lijken aan te nemen dat er sprake is van een beslag op een databankenrecht in de zin van de Databankenwet.⁷⁹ Dit databankenrecht houdt in dat de producent van een databank het uitsluitend recht heeft om toestemming te verlenen voor het opvragen en hergebruiken van de inhoud van de databank.⁸⁰ Wibier wijst er echter terecht op dat het databankenrecht niet moet worden vereenzelvigd met de databank.⁸¹

3.2 Big data

De problematiek inzake digitale producten kan met name relevant worden ten aanzien van *big data*.⁸²

Target en de zwangere klant

De lezer heeft wellicht reeds meerdere malen introducties over *big data* gelezen. Voor de volledigheid en voor een goed begrip van *big data* vind ik het van belang toch de kernelementen ervan te benoemen. Een inmiddels klassiek voorbeeld van het gebruik van *big data* betreft de Amerikaanse supermarkt Target. Het verhaal gaat dat een vader geërgerd aan Target liet weten niet op prijs te stellen dat zijn tienerdochter reclame ontving waarin producten voor zwangere vrouwen werden aangeprezen. Toen de manager van de plaatselijke Target-vestiging contact opnam met de vader, bood de vader zijn excuses aan. De dochter bleek inderdaad zwanger.⁸³

Aan de hand van het Target-voorbeeld kunnen twee elementen rondom *big data* worden geïllustreerd, te weten *datafication* en de verschuiving van causaliteit naar correlatie. *Datafication* houdt in dat steeds meer gedrag in het maatschappelijk verkeer data genereert. Ten aanzien van het Target-voorbeeld kan worden gewe-

79 N.W.M. van den Heuvel, 'Beslag op data', WPNR 4 juni 2016, 7110; annotatie bij JBP 2015/129.

80 Art. 2 lid 1 Databankenwet.

81 R.M. Wibier, 'Big data en goederenrecht', WPNR 4 juni 2016, 7110.

82 Zie voorts R.M. Wibier, 'Big data en goederenrecht', WPNR 4 juni 2016, 7110.

83 De bespreking van *big data* in deze paragraaf is ontleend aan V. Mayer-Schönberger & K. Cukier, *Big data. A revolution that will transform how we live, work and think*, London: John Murray 2013. Het Target-voorbeeld is te vinden op p. 58.

zen op het gebruik van klantenkaarten (zoals de Albert Heijn bonuskaart). Bedrijven spreken van *loyalty*-programma's. Door klanten gebruik te laten maken van een klantenkaart, is de supermarkt in staat een databank op te bouwen van alle aankopen die de betreffende klanten doen. Target bood daarnaast de mogelijkheid voor zwangere vrouwen om een cadeaulijst bij te houden. Hierdoor beschikte Target niet alleen over het koopgedrag van haar klanten (die gebruikmaakten van de klantenkaart) maar wist Target ook met zekerheid welke klanten binnen die groep op een bepaald moment zwanger waren. In dit voorbeeld is de reikwijdte van het *datafication*-aspect nog beperkt. In andere situaties is het aspect indringender. Smartphones, smart watches en *wearables* houden 24 uur per dag bij waar de gebruikers zich bevinden. Auto's houden locaties en rijgedrag bij. Facebook en twitter registreren het surfgedrag van hun gebruikers. Google kent alle zoektermen die je ooit hebt ingevoerd.

Terug naar Target. Na het verzamelen van de data ging Target op zoek naar koopgedrag waarmee de zwangere klant is te onderscheiden. Uit de data bleek dat zwangere klanten in de derde maand van hun zwangerschap met name veel ongeparfumeerde *body lotion* kochten. Enkele weken later bleken zij voedings-supplementen zoals magnesium, calcium en zink te kopen. Uiteindelijk bleken er twee dozijn producten te zijn aan de hand waarvan een 'zwangerschapsvoorspelling' kon worden gedaan en kon voorts een betrouwbare voorspelling worden gedaan ten aanzien van de uitgerekende datum. Dit is de correlatie. Target weet zonder twijfel dat deze correlatie er is. Het *waarom*, de causaliteit, ontbreekt echter. Mogelijk kan de causaliteit achteraf wel worden beredeneerd. Voor Target is dat op dat moment echter niet meer relevant.

Betalingstransacties – toegang tot de betaalrekening volgens de nieuwe Richtlijn betaaldiensten

In de toekomst zouden betaaldata een belangrijke bron voor *big data*-analyses kunnen zijn. Met betaaldata doel ik op de gegevens betreffende betaalgedrag. Elke betaling met een bankpas in een winkel, elke overboeking en elke internetbetaling wordt geregistreerd bij de bank (of bij een andere betaaldienstverlener). Zeker in combinatie met andere data, zoals locatiegegevens of gegevens betreffende surfgedrag, kunnen er ongetwijfeld exploiteerbare correlaties uit deze data worden afgeleid die we nu nog niet kunnen verzinnen. Tot nu toe is er echter sprake van maatschappelijke weerstand zodra een partij plannen ontvouwt om betaaldata te exploiteren.⁸⁴

De discussie omtrent het gebruik van betaaldata komt in een ander daglicht te staan vanwege nieuwe wetgeving inzake betalingstransacties. De betalingstransactie is op dit moment (civielrechtelijk) geregeld in titel 7b van Boek 7 BW.⁸⁵ Het betreft hier de implementatie van de Europese Richtlijn inzake betalingsdiensten

84 Zie bijvoorbeeld NRC, 'Equens ziet voorlopig af van doorverkopen pingegevens klanten', 23 mei 2013, <https://www.nrc.nl/nieuws/2013/05/24/equens-ziet-voorlopig-af-van-doorverkopen-gegevens-pintransacties-a1434505>; en Algemeen Dagblad, 'AFM waarschuwt ING om plannen betaalgegevens', 14 maart 2014, <http://www.ad.nl/economie/afm-waarschuwt-ing-om-plannen-gebruik-betalgegevens-aer3f4fc/>.

85 Zie Kamerstukken II 2008/09, 31892, I-12; Kamerstukken I 2008/09-2009/10, 31892, A-D; Stb. 2009, 436.

uit 2002.⁸⁶ Deze richtlijn zal worden ingetrokken. De herziene Richtlijn betalingsdiensten (de *payment services directive 2*, PSD2) zal ervoor in de plaats treden.⁸⁷ PSD2 schrijft expliciet voor dat banken betaalgegevens moeten delen. Juridisch is dit als volgt geformuleerd. De zogenoemde rekeninghoudende betalingsdienst-aanbieder (dat wil zeggen, de betaaldienstverlener bij wie een betaler zijn betaalrekening aanhoudt), moet de betalingsdienstgebruiker in staat stellen via andere betalingsdienstaanbieders zijn betaalrekening te gebruiken. Een van de wijzen waarop dat dient te geschieden, is via de zogenoemde rekeninginformatiedienst-aanbieder. Als de betalingsdienstgebruiker via het internet gebruik kan maken van zijn betaalrekening (de klant van de bank kan online bankieren), dan moet hij ook in staat worden gesteld via een rekeninginformatiedienstverlener de rekeninginformatie die zich bij de rekeninghoudende betalingsdienstverlener bevindt, te ontsluiten.⁸⁸ PSD2 moet per 13 januari 2018 in het nationale recht zijn geïmplementeerd.⁸⁹ De (nabije) toekomst zal moeten uitwijzen hoe er met betaaldata zal worden omgegaan.

3.3 Software

Software is bij uitstek een digitaal product dat goederenrechtelijk ongrijpbaar is gebleken. Eerst de basics. Begin jaren tachtig van de vorige eeuw speelde de vraag hoe software juridisch moest worden geduid. Vandenberghe pleitte voor een *sui generis* regime. Software zou niet thuishoren in het auteursrecht.⁹⁰ De heersende leer hield echter in dat het auteursrecht wel degelijk de natuurlijk plek zou zijn om software te regelen.⁹¹ In 1991 werd de heersende leer kracht bijgezet door de Europese Softwarerichtlijn.⁹² De richtlijn stelde buiten twijfel dat software, computerprogrammatuur, in het domein van het auteursrecht viel. Vijfentwintig jaar later verschijnt een redactioneel commentaar van Hugenholtz met de veelzeggende titel 'Guy Vandenberghe had gelijk'. Hugenholtz is in deze bijdrage gecharmeerd van een *sui generis*-benadering. Hij wijst met name op de tegenwoordig ruime reikwijdte van het auteursrechtelijke werkbegrip (het 'domeinprobleem') waarmee het auteursrecht 'ver buiten zijn oevers is getreden'.⁹³ Deze historische context zet de toon om terug te gaan tot de basisbegrippen van het auteursrecht. De kern van het subjectieve auteursrecht is dat alleen de maker het recht heeft zijn werk openbaar te maken en te verveelvoudigen, behoudens wettelijke beperkingen.⁹⁴ De kwalificatie van computerprogrammatuur als auteursrechtelijk werk gaat uit van een auteursrechtelijk-dogmatische vooronderstelling dat het gebruik van programmatuur een auteursrechtelijk relevante verveelvoudiging met

86 Richtlijn 2007/64/EG betreffende betalingsdiensten, PbEU 2007, L 319.

87 Richtlijn (EU) 2015/2366 betreffende betalingsdiensten, PbEU 2015, L 337.

88 Art. 67 Richtlijn (EU) 2015/2366.

89 Art. 115 Richtlijn (EU) 2015/2366.

90 G. Vandenberghe, *Bescherming van software*, Antwerpen: Kluwer 1984.

91 Als vertolker van die heersende leer wijs ik op het later gepubliceerde proefschrift van Thole: E.P.M. Thole, *Software. Een 'novum' in het vermogensrecht* (diss. Utrecht), Deventer: Kluwer 1991.

92 Richtlijn 91/250/EEG betreffende de rechtsbescherming van computerprogramma's, PbEG 1991, L 122, later hernieuwd gepubliceerd als Richtlijn 2009/24/EG, PbEU 2009, L 111.

93 B. Hugenholtz, 'Guy Vandenberghe had gelijk', *Computerrecht* 2009/91, p. 107.

94 Art. 1 Auteurswet.

zich meebrengt.⁹⁵ Door programmatuur te gebruiken worden er immers kopieën gemaakt van (delen van) de programmatuur, op datadragers, in het werkgeheugen en in het videogeheugen van computersystemen. Dit heeft tot gevolg dat voor het gebruik van computerprogrammatuur de toestemming (een licentie) van de maker vereist is. Rond 1990 leek dit wellicht een voor de hand liggende keuze. Auteursrechtelijk gezien werd hiermee echter een grens verlegd: voor het gebruik van het auteursrechtelijk werk is nu toestemming nodig. Voor een meer traditioneel auteursrechtelijk werk, zoals een boek of een schilderij, is dat natuurlijk niet te geval.⁹⁶

Wellicht door de auteursrechtelijke benadering is software ontglipt aan het goederenrecht. Dit heeft geleid tot principiële vragen als: kan ik software doorverkopen? Kan ik beslag leggen op software? Hierboven bij de casus inzake *Woman Capital* hebben we gezien dat het van belang is duidelijk voor ogen te houden wat het object van bijvoorbeeld beslag zou moeten zijn. Een beslag op een vermogensrecht inzake een databankenrecht op een databank of op het auteursrecht op een computerprogramma, houdt geen beslag op het bestandbestand respectievelijk de software zelf in.

UsedSoft

De uitspraak van het Europees Hof van Justitie inzake *UsedSoft*⁹⁷ betreft de auteursrechtelijke uitputting. *UsedSoft* is een bedrijf wiens dienstverlening bestaat uit de doorverkoop van reeds door anderen aangeschafte computerprogramma's, 'tweedehands software'. In een juridische procedure tegen softwareproducent Oracle speelde de vraag of *UsedSoft* zich kon beroepen op uitputting. Zoals hierboven aangegeven, houdt het subjectieve auteursrecht onder meer in dat de maker het exclusieve recht van openbaarmaking heeft. Dit geldt echter alleen voor de eerste openbaarmaking van een exemplaar: als een boek eenmaal op de markt is gebracht, mag de verkrijger het boek naar believen verder verkopen. Het openbaarmakingsrecht is 'uitgeput'. De *Softwarerichtlijn* heeft dit ook voor computerprogrammatuur willen bepalen: 'De eerste verkoop (...) van een kopie van een programma door de rechthebbende of met diens toestemming leidt tot verval van het recht om controle uit te oefenen op de distributie van die kopie (...)', aldus – verkort – de *Softwarerichtlijn*.⁹⁸ Wil er sprake zijn van uitputting, dan moet er dus eerst sprake zijn van een 'eerste verkoop'. 'Koop' ziet naar Nederlands recht natuurlijk op een zaak, een voor menselijke beheersing vatbaar stoffelijk object. Het Hof geeft aan dat 'verkoop' hier moet worden gezien als een autonoom Europeesrechtelijk begrip.⁹⁹ Het Hof definieert 'verkoop' vervolgens als 'een overeenkomst waarbij een persoon tegen betaling van een prijs zijn eigendomsrech-

95 Zie E.P.M. Thole, *Software. Een 'novum' in het vermogensrecht* (diss. Utrecht), Deventer: Kluwer 1991.

96 De *Softwarerichtlijn* gaat overigens niet letterlijk uit van openbaarmaken en vervelvoudigen, maar – kort gezegd – van 'de permanente of tijdelijke reproductie', 'het vertalen, bewerken, arrangeren of anderszins veranderen van een programma, en de reproductie van het resultaat daarvan' en van 'elke vorm van distributie (...) onder het publiek', art. 4 lid 1 *Richtlijn* 2009/24/EG.

97 HvJ 3 juli 2012, C-128/11, ECLI:EU:C:2012:407. Ik bespreek hier niet het volledige arrest maar enkel de overwegingen die relevant zijn voor een goederenrechtelijke vergelijking.

98 Art. 4 lid 2.

99 R.o. 40.

ten op een hem toebehorende lichamelijke of onlichamelijke zaak aan een ander overdraagt'. Hieruit volgt volgens het Hof dat een handelstransactie die conform de Softwarerichtlijn tot uitputting leidt, impliceert dat het eigendomsrecht op de kopie van het computerprogramma is overgedragen.¹⁰⁰ De tegenwerping van Oracle dat kopieën van de programmatuur gratis ter beschikking worden gesteld (maar alleen mogen worden gebruikt op grond van een licentie) wordt door het Hof weerlegd. Volgens het Hof vormen het downloaden van een kopie en het sluiten van de daarop betrekking hebbende licentieovereenkomst een ondeelbaar geheel.¹⁰¹ Het Hof laat voorts meewegen dat een klant van Oracle die een kopie van de software downloadt en een licentieovereenkomst voor het gebruik van die kopie aangaat, tegen betaling van een prijs een in de tijd onbeperkt gebruiksrecht voor die kopie verkrijgt.¹⁰² Met de bovenstaande overwegingen komt het Hof tot de conclusie dat de eigendom van de kopie van het betreffende computerprogramma wordt overgedragen.¹⁰³

Kopie-begrip ten aanzien van software is onhoudbaar

Het is te prijzen dat het Hof in *UsedSoft* in zekere zin praktisch te werk gaat. Zo spreekt Van Camp van een 'economisch-functionele benadering (...) die ertoe leidt dat de moeizame technisch-juridische debatten aangaande de "verkoop" van software, die reeds decennia meegaan, vrij eenvoudig opzij worden gezet'.¹⁰⁴ Waar ik echter grote moeite mee heb, is de rol van de kopie. De Softwarerichtlijn, en dus ook het Hof, kennen een centrale rol toe aan de kopie van de computerprogrammatuur. De licentie in de *UsedSoft*-casus heeft betrekking op een specifieke kopie. Verder moet kennelijk het downloaden van een specifieke kopie en het aangaan van een daarop betrekking hebbend gebruiksrecht als één geheel worden gezien. Het valt naar mijn mening niet te verklaren hoe het kopiebegrip uit de Software-richtlijn in de digitale wereld moet worden geduid. Zodra een bestand, en dus ook software, wordt gedownload, is er sprake van een nieuwe kopie. Het transporteren van een elektronisch bestand houdt immers in dat het naar een nieuwe locatie wordt gekopieerd, en dat het bestand op de oorspronkelijke locatie wordt gewist (althans, aldaar niet zonder meer beschikbaar is). Een onderneming als rechtmatige verkrijger zal meerdere kopieën van programmatuur moeten maken om het correct in zijn IT-landschap te implementeren.¹⁰⁵ Sterker nog, zoals hierboven aangegeven gaat de auteursrechtelijke dogmatiek ervan uit dat het gebruik van software reeds nieuwe kopieën met zich meebrengt. Zolang echter in het soft-

¹⁰⁰ R.o. 42.

¹⁰¹ R.o. 43-44.

¹⁰² R.o. 45.

¹⁰³ R.o. 46.

¹⁰⁴ S. Van Camp, 'Het doorverkopen van gedownloade software en communautaire uitputting: het *UsedSoft*-arrest van het Hof van Justitie', *Computerrecht* 2012/183.

¹⁰⁵ Zo was tussenkomst van de Rechtbank Amsterdam nodig om te bepalen dat het Delta Lloyd was toegestaan kopieën van software op een testserver en acceptatieserver te plaatsen, Rb. Amsterdam 29 oktober 2014, ECLI:NL:RBAMS:2014:7005, m.n. Krikke (*Computerrecht* 2015/46, p. 73-80). Overigens zijn test en acceptatie enkel de T en de A van het acroniem OTAP, dat staat voor ontwikkeling, testen, acceptatie en productie. In veel gevallen zal ten minste voor elk van deze fasen een kopie (althans een geïnstalleerd en functionerend exemplaar) van de gebruikte computerprogrammatuur nodig zijn.

warerecht de kopie centraal staat, is het lastig een consistent systeem te construeren. Een latere uitspraak waarin het Hof prejudiciële vragen van de strafrechter te Riga beantwoordt, komt mij daarom willekeurig voor. In dat arrest betrof het, anders dan in de *UsedSoft*-casus, geen software die werd gedownload, maar de verstrekking van een fysieke drager met daarop de software. De ‘eerste verkoop’ betrof aldus de verstrekking van een fysiek exemplaar met een onbeperkte gebruikslicentie. Het Hof oordeelde dat indien de fysieke drager van de oorspronkelijk geleverde kopie beschadigd raakt, wordt vernietigd of verloren gaat, dat dan de eerste verkrijger niet een reservekopie van de software aan de nieuwe verkrijger mag verschaffen (althans niet zonder toestemming van de auteursrechthebbende).¹⁰⁶ Er wordt hier naar mijn mening te strikt vastgehouden aan het ‘analoge’ idee van een fysiek auteursrechtelijk werk. Dit leidt tot een onverdedigbaar onderscheid tussen software die bij eerste verkrijging wordt gedownload en software die op een fysieke drager wordt verkregen.

De Beeldbrigade

In de *Beeldbrigade*-arresten¹⁰⁷ van de Hoge Raad gaat het om het computerprogramma ImageSan. De auteursrechthebbende ten aanzien van ImageSan is Bell. De Beeldbrigade is de gebruiker van de software. De Beeldbrigade, een producent van televisieprogramma’s, heeft de software aangeschaft via reseller Hulskamp. De Beeldbrigade heeft problemen met de software en leidt daardoor schade. Zo moet er onder meer een vervangend computerprogramma worden geïnstalleerd. De Beeldbrigade stelt Hulskamp aansprakelijk. Opmerkelijk genoeg beroepen Hulskamp (de verkoper) en Bell (de auteursrechthebbende) zich vervolgens op de toepasselijkheid van het kooprecht. Een rechtsvordering die is gebaseerd op de stelling dat er sprake is van non-conformiteit verjaart immers na verloop van twee jaar.¹⁰⁸ De rechtsvraag die aldus voorligt, is of het kooprecht hier van toepassing is. De Hoge Raad stelt allereerst dat de goederenrechtelijke aard van software, en de kwalificatie van (de titel verkrijging van) de gebruiksrechten die bij de aanschaf van de software wordt verkregen, niet aan de orde zijn.¹⁰⁹ De Hoge Raad komt tot de conclusie dat de kooptitel van toepassing is op de overeenkomst op grond waarvan standaardprogrammatuur wordt aangeschaft voor een niet in tijdsduur beperkt gebruik, tegen betaling van een bepaald bedrag, ongeacht of er sprake is van een aanschaf op een gegevensdrager of via een download. De Hoge Raad baseert deze conclusie op het wettelijke voorschrift dat een koop ook op een vermogensrecht betrekking kan hebben.¹¹⁰ ‘Het is opvallend hoe zeer de Hoge Raad wenst te vermijden in dogmatisch lastig goederenrechtelijk of auteursrechtelijk vaarwater te komen’, aldus Neppelenbroek.¹¹¹ Dat zou wellicht zijn te verklaren uit het naar mijn mening onwerkbaar begrip ‘kopie’ waar de Softwarerichtlijn van uitgaat. De termen ‘kopie’ of ‘exemplaar’ komen overigens

¹⁰⁶ HvJ EU 12 oktober 2016, gevoegde zaken C-14/15 en C-116/15, ECLI:EU:C:2016:715.

¹⁰⁷ HR 27 april 2012, NJ 2012, 293 (*Hulskamp/De Beeldbrigade*) en 294 (*Hulskamp/Bell*).

¹⁰⁸ Art. 7:23 lid 2 BW.

¹⁰⁹ R.o. 3.4.

¹¹⁰ R.o. 3.5.

¹¹¹ E.D.C. Neppelenbroek, *Softwarebetrekkingen. De auteur, de verkrijger en hun vermogensrechtelijke positie jegens derden* (diss. Groningen), Den Haag: Boom Juridische uitgevers 2013, p. 177.

überhaupt niet voor in het arrest.¹¹² In *UsedSoft* vereenzelvigd het Hof de aanschaf van de licentie met de verkrijgen van een kopie, in *De Beeldbrigade* zwijgt de Hoge Raad over de kopie.

3.4 Digitale inhoud

Sinds 2015 regelt ons BW ook digitale inhoud. Hieronder wordt verstaan ‘gegevens die in digitale vorm geproduceerd en geleverd worden’.¹¹³ Ook moeten hieronder computerprogramma’s, toepassingen, spellen, muziek, video’s en teksten worden begrepen, ongeacht of de toegang tot deze gegevens wordt verkregen via downloaden of streaming, vanaf een materiële drager of langs een andere weg.¹¹⁴ De kooptitel is gedeeltelijk van toepassing op digitale inhoud. Sinds de Wet verduidelijking koopregels¹¹⁵ zijn de bepalingen inzake consumentenkoop groten-deels van toepassing ‘op de levering van digitale inhoud die niet op een materiële drager is geleverd, maar die wel is geïndividualiseerd en waarover feitelijke macht kan worden uitgeoefend, aan een natuurlijk persoon, die handelt voor doeleinden buiten zijn handels-, bedrijfs-, ambachts- of beroepsactiviteit’.¹¹⁶ Het gaat om downloaden, maar niet om streamen.¹¹⁷

Dankzij de Wet verduidelijking koopregels leidt het nu geen twijfel dat computerprogrammatuur bijvoorbeeld conform moet worden geleverd.¹¹⁸ Voorheen was dit onduidelijk. Er kon immers wel worden gewezen op de bepaling dat een koop ook op een vermogensrecht betrekking kan hebben.¹¹⁹ Dan rijst uiteraard de discussie of het gebruiksrecht, dan wel de programmatuur zelf als vermogensrecht zou moeten worden gezien. De nieuwe wetgeving heeft deze discussie eindelijk beslecht. De wet bevat echter geen voorschriften die een grondslag leveren voor een goederenrechtelijke kwalificatie van digitale inhoud.

In december 2016 publiceerde de Europese Commissie een voorstel voor een richtlijn inzake digitale inhoud.¹²⁰ Het richtlijnvoorstel schaaft ook diensten onder het begrip digitale inhoud: ‘diensten die de totstandkoming, verwerking of opslag van gegevens in digitale vorm mogelijk maken, wanneer deze gegevens door de consument worden verstrekt’ en ‘diensten die het delen van gegevens en alle andere interactie met gegevens in digitale vorm die door andere gebruikers van

¹¹² Het arrest betreffende de vrijwaring (NJ 2012, 294) bevat overigens wel tweemaal de term ‘exemplaar’.

¹¹³ Art. 6:230g lid 1 sub i BW, door de implementatie van Richtlijn 2011/83/EU inzake consumentenrechten, PbEU 2011, L 304.

¹¹⁴ Overweging 19 Richtlijn consumentenrechten.

¹¹⁵ Stb. 2015, 220.

¹¹⁶ Art. 7:5 lid 5 BW.

¹¹⁷ Kamerstukken II 2014/15, 34071, 3, p. 2-3. De memorie van toelichting verwijst overigens expliciet naar de arresten van de Hoge Raad inzake *De Beeldbrigade*. In de overwegingen van de Hoge Raad ziet de wetgever een aanleiding om de toepasselijkheid van de kooptitel op ‘streaming-overeenkomsten’ uit te sluiten.

¹¹⁸ Art. 7:17 lid 1 BW.

¹¹⁹ Art. 7:47 BW.

¹²⁰ Voorstel voor een richtlijn betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud, 9 december 2015, COM(2015)634 final.

de dienst worden verstrekt, mogelijk maken'.¹²¹ Ook het voorstel voor een richtlijn is qua reikwijdte beperkt tot de levering van digitale inhoud aan consumenten.¹²²

3.5 Tussenconclusie

Ten aanzien van digitale producten spelen het gegevensbeschermingsrecht, het auteursrecht en het databankenrecht al snel een rol. Naar mijn mening dient het gegevensbeschermingsrecht te worden betrokken rondom vragen inzake beslag en overdracht van databestanden waarmee persoonsgegevens gemoeid zijn. De uitspraak inzake *Womans Capital* is een voorbeeld waarin dat onvoldoende is gebeurd. Onvoldoende rekenschap van het gegevensbeschermingsrecht zal ertoe leiden dat verkrijgers van databestanden worden blij gemaakt met een dode mus. Aan hen zullen mogelijk databestanden ter beschikking worden gesteld waarvan zij op grond van het gegevensbeschermingsrecht geen, of mogelijk slechts onder strenge voorwaarden, gebruik kunnen maken. Dit zal ook gevolgen hebben voor de evaluatie van de financiële waarde van zulke bestanden, hetgeen van groot belang is voor een executoriaal beslag.

Het begrip 'kopie' zoals gehanteerd door de Softwarerichtlijn is naar mijn mening onwerkbaar. De kopie waarvan de (zelfs rechtmatige) verkrijger gebruikmaakt, zal technisch gezien nooit dezelfde kopie zijn als degene die is geleverd. Het idee dat het überhaupt mogelijk zou zijn in een digitale wereld een specifieke kopie te individualiseren is absurd.

4 Het autonome systeem

In deze paragraaf zal ik stil staan bij het autonome systeem. Zoals in de inleiding reeds aangekondigd doe ik dat zeer bondig. Er zijn talloze juridische vragen die rondom het autonome systeem beantwoording behoeven. Ik denk echter niet dat het privaatrecht ten aanzien van dit onderwerp met fundamentele problemen wordt geconfronteerd.

Onder autonoom systeem versta ik een door een mens gecreëerd hardware- of softwarematig systeem dat autonoom kan handelen. We geraken hier overigens al vrij snel in terminologisch drijfzand. *Autonoom handelen* kan worden aangemerkt als het handelen door het systeem zonder menselijke tussenkomst. Het is lastig om autonoom handelen te onderscheiden van automatisch handelen.¹²³ Bij autonoom handelen denken we echter snel aan handelingen die voorheen door mensen zouden worden verricht, of wellicht een grotere reikwijdte waarbinnen een systeem automatisch kan handelen.¹²⁴ Bij automatisch handelen denken we eerder aan het automatisch verrichten van simpele handelingen. Ook bij het element

¹²¹ Art. 2 lid 1 sub b & c richtlijnvoorstel.

¹²² Art. 3 lid 1 richtlijnvoorstel.

¹²³ Voulon 2010, p. 20.

¹²⁴ Zo onderscheidt de *Society of Automotive Engineers* vijf stadia van autonomie voor zelfrijdende auto's. Stadium 0 (omschreven als 'no automation') betreft de auto die volledig door de mens wordt bestuurd. In Stadium 5 rijdt de auto geheel zelfstandig. Er is dan geen menselijke tussenkomst nodig. Zie: SAE International, *Automated Driving*, 2014, https://www.sae.org/misc/pdfs/automated_driving.pdf.

‘door de mens gecreëerd’ kunnen kanttekeningen worden gezet. Een systeem kan immers ook door een ander systeem worden gecreëerd.

Voorbeelden van autonome systemen zijn automatische biedsystemen op internetveilingen, *algorithmic trading/automated trading* systemen waarmee wordt deelgenomen aan effectenhandel,¹²⁵ zelfrijdende auto’s, drones (voor zover zelfstandig handelend), (zelfhandelende) computerprogramma’s en (zelfhandelende) robots. Ook kan worden gewezen op het gebruik van zogenoemde *smart contracts*.¹²⁶

Het autonoom systeem confronteert het privaatrecht met twee hoofdvragen. De eerste vraag is of en hoe het handelen van een autonoom systeem tot contractuele gebondenheid kan leiden. De tweede vraag is of en hoe het handelen van een autonoom systeem tot aansprakelijkheid kan leiden.

4.1 Contractuele gebondenheid

Bij contracterende autonome systemen ga ik uit van de inzet van softwaresystemen bij het aangaan van overeenkomsten. Het uitgangspunt bij het bespreken van de contractuele gebondenheid is de wilsvertrouwensleer: primair de verklaarde wil is de grondslag voor de rechtshandeling. In de uitzonderingssituatie dat wil en verklaring van elkaar afwijken, is het bij de wederpartij gewekte gerechtvaardigde vertrouwen de grondslag voor de rechtshandeling.¹²⁷ Ten aanzien van handelingen die worden verricht door een autonoom systeem kan nu worden gesproken van het zogenoemde *wilsverklaringsprobleem*: hoe kan een verklaring afgelegd door het autonome systeem worden gekwalificeerd als wilsuiting van de gebruiker van dat systeem? Sinds jaar en dag¹²⁸ geschiedt dit door middel van de theorie van de geprogrammeerde wil en de theorie van de algemene wil. De theorie van de geprogrammeerde wil houdt in dat de gebruiker zijn wilsbesluit vastlegt in de instructies die hij het systeem meegeeft. Het systeem handelt vervolgens binnen de gegeven parameters. Voor meer complexe of meer autonome systemen levert dat echter een onvoldoende onderbouwing van de uitingen van het systeem. Er kan dan worden uitgegaan van de theorie van de algemene wil, op grond waarvan niet elke uiting van het autonome systeem hoeft te zijn terug te voeren op een specifiek voor die uiting gevormde wil van de gebruiker van het systeem. De voor de rechtshandeling vereiste wil is te vinden in de algemene wil die is gericht op de rechtsgevolgen van de verklaringen die door middel van het autonome systeem worden afgelegd. Die verklaringen zijn de resultaten van de omstandigheden en van de keuzes van de gebruiker. Deze algemene wil wordt kenbaar gemaakt door het in gebruik nemen en houden van het systeem.

De theorie van de algemene wil kent een beperking: zij gaat uit van het functioneren van het autonome systeem onder gelijkblijvende omstandigheden en overeenkomstig hetgeen de gebruiker daarvan redelijkerwijs mocht verwachten.¹²⁹ In

¹²⁵ T.F.E. Tjong Tjin Tai, ‘Aansprakelijkheid voor robots en algoritmes’, *NTHR* 2017/3, p. 123-124.

¹²⁶ Zie o.a. J.B. Schmaal & E.M. van Genuchten, ‘Smart contracts en de Haviltex-norm’, *Tvl* 2017/1, p. 12-17; E. Tjong Tjin Tai, ‘Smart contracts en het recht’, *NJB* 2017/3, p. 176-182.

¹²⁷ Art. 3:33, 3:35, 6:217 BW. Voulon 2010, p. 51.

¹²⁸ Althans, tenminste sinds het verschijnen van de dissertatie van Van Esch in 1999: R.E. van Esch, *Electronic Data Interchange (EDI) en het vermogensrecht* (diss. Nijmegen), Deventer: W.E.J. Tjeenk Willink 1999.

¹²⁹ Voulon 2010, p. 56-57.

die beperking kan hem nou juist de kneep zitten.¹³⁰ Naarmate er meer gebruik wordt gemaakt van autonome systemen, waardoor bijvoorbeeld zowel aan aanbod- als aan aanvaardingszijde autonome systemen worden ingezet, en de mate van autonomie van die systemen toeneemt, wordt de kans groter dat het systeem verklaringen aflegt die de gebruiker niet gewild heeft. Linnemann en Schmaal pleiten in dit verband terecht voor een ruime interpretatie van het vertrouwen-aspect van de wilsvertrouwensleer. Bij inzet van een autonoom systeem mag de gebruiker daarvan zich niet te snel verschuilen achter zijn systeem. Als de wederpartij geen reden heeft om te twijfelen of het handelen van het systeem wel overeenstemde met de wil van de gebruiker, is de gebruiker gebonden.¹³¹

Het is van belang te onderscheiden naar het onderliggende beginsel op grond waarvan een verklaring aan een persoon wordt toegerekend. Als een discrepantie tussen wil en verklaring is ontstaan doordat de gebruiker zijn autonoom systeem verkeerd heeft geïnstrueerd, dan kan de verklaring op basis van het gewekte vertrouwen toch aan de gebruiker worden toegerekend. Het onderliggende beginsel is dan dat van de *culpa in contrahendo*, er is sprake van een *verwijtbaarheid* van de gebruiker.¹³² Als de vertrouwensleer ruimer wordt geïnterpreteerd, zoals voorgesteld door Linnemann en Schmaal, dan kan er een verschuiving optreden van het verwijtbaarheidsbeginsel naar het risicobeginsel; de verklaring wordt toegerekend omdat de gebruiker het risico van een afwijking tussen wil en verklaring heeft te accepteren, niet omdat hem iets te verwijten valt. Ter vergelijking kan worden gewezen op de wettelijk regels dat degene die het middel kiest voor de overdracht van een verklaring, het risico draagt ten aanzien van het gebruik van dat middel.¹³³ Ik heb overigens moeite om mij een concrete casus voor te stellen waarin het handelen van het systeem inderdaad in een zo vergaande mate van de wil van de gebruiker verwijderd is geraakt dat deze verruiming van de vertrouwensleer noodzakelijk is.

Een praktisch aspect is dat het de gebruiker van een autonoom systeem is aan te raden ervoor zorg te dragen dat de handelingen van het systeem worden vastgelegd zodat achteraf kan worden gereproduceerd wat er precies is gebeurd.

4.2 Aansprakelijkheid

Ten aanzien van aansprakelijkheid en autonome systemen denkt men al snel aan hardwarematige, fysieke, autonome systemen zoals de zelfrijdende auto en de robot die in de industrie en de zorg wordt toegepast. Dit soort robots kan immers voor fysieke schade en letsel zorgen. Er kan echter ook worden gedacht aan softwarematige autonome systemen zoals de systemen waarvan gebruik wordt gemaakt bij *algorithmic trading* en *automated trading systems* bij effectenhandel.¹³⁴ Ten aanzien van de aansprakelijkheid voor schade die is veroorzaakt door deze autonome systemen ben ik zo vrij te verwijzen naar Van Wees en Tjong Tjin Tai. Van Wees heeft ten aanzien van de zelfrijdende auto erop gewezen dat in het verkeers-

¹³⁰ J.J. Linnemann & J.B. Schmaal, 'Intelligent contracteren', *Computerrecht* 2010, 175.

¹³¹ Idem.

¹³² Vgl. Asser/Hartkamp & Sieburgh 6-III 2014/145.

¹³³ Art. 37 lid 4 BW.

¹³⁴ Vgl. T.F.E. Tjong Tjin Tai, 'Aansprakelijkheid voor robots en algoritmes', *NTHR* 2017/3, p. 123-124.

recht op dit moment de bestuurder een centrale rol inneemt. Dat lijkt bij mogelijk toekomstige wetgeving inzake zelfrijdende auto's niet te veranderen. Zo is er een voorstel gedaan tot wijziging van het Verdrag van Wenen inzake het wegverkeer. Het wijzigingsvoorstel baseert zich op het uitgangspunt dat de bestuurder van het voertuig in staat moet zijn in te grijpen. Volledige autonomie lijkt hiermee niet toegestaan.¹³⁵ Daarnaast kan er in navolging van Tjong Tjin Tai op worden gewezen dat een actieve, toezichthoudende rol van de bestuurder een extra aandachtsverplichting oplevert. De toegevoegde waarde van een zelfrijdende auto is nu juist dat de verplichting tot aandacht door de auto uit handen wordt genomen.¹³⁶ Ten aanzien van schade veroorzaakt door autonome systemen in het algemeen, dus niet alleen ten aanzien van zelfrijdende auto's, voorziet Tjong Tjin Tai een verschuiving van schuldaansprakelijkheid naar risicoaansprakelijkheid. Hij stelt een alternatieve benadering voor op basis van het effectiviteitsbeginsel. Dit beginsel eist dat er adequate remedies zijn in geval van een aantasting van rechten die in Europese regels zijn erkend. De uitkomst zou zijn dat schade wordt gedragen door degene die de schade het beste had kunnen voorkomen.¹³⁷

5 Besluit

In dit preadvies is een aantal thema's rondom de wisselwerking tussen digitalisering en het Nederlands BW besproken. Ten aanzien van de handtekening, in de context van de onderhandse akte, heb ik gepoogd aan te tonen dat het recht bij de handgeschreven handtekening uitgaat van een fundamenteel andere benadering dan bij de elektronische handtekening. Bij de handgeschreven handtekening is sprake van de goede trouw-benadering (zie paragraaf 2.2), bij de elektronische handtekening van de risicogebaseerde benadering (zie paragraaf 2.3 e.v.). De goede trouw-benadering gaat uit van consciëntieus handelende deelnemers aan het maatschappelijk verkeer. Niet alles hoeft a priori als verdacht te worden beschouwd. De risicogebaseerde benadering gaat uit van wantrouwen. Risico's worden geïdentificeerd en systematisch gemitigeerd. In het licht van de beginselen van betrouwbare elektronische communicatie is er geen plaats meer voor de stellige ontkenning van de ondertekening van een akte. Als een beweerdelijke ondertekenaar aanvoert niet te hebben ondertekend, zal hij aannemelijk moeten maken waarom dat niet het geval is.

De elektronische akte en het digitale product, zoals computerprogrammatuur, hebben gemeen dat er geen sprake kan zijn van een origineel en daarvan afgeleide kopieën. In een digitale omgeving kan geen sprake zijn van originelen.

Mogelijk krijgt de uitspraak van de voorzieningenrechter te Amsterdam inzake *Woman Capital* navolging. Dat zou inhouden dat executoriaal beslag op databestanden, inclusief data die persoonsgegevens kunnen betreffen, vaker zal gaan voorkomen. In dat geval zou de rechter ook moeten toetsen aan het gegevensbeschermingsrecht.

¹³⁵ K.A.P.C. van Wees, 'Enkele juridische aspecten van de (deels) zelfrijdende auto', *Computerrecht* 2015/198.

¹³⁶ T.F.E. Tjong Tjin Tai, 'Aansprakelijkheid voor robots en algoritmes', *NTHR* 2017/3, p.129.

¹³⁷ T.F.E. Tjong Tjin Tai, 'Aansprakelijkheid voor robots en algoritmes', *NTHR* 2017/3, p.123-132.