

# De stellige ontkenning van een elektronische ondertekening

Is art. 159 lid 2 Rv toe aan modernisering?

*R o b v a n E s c h \**

## 1 Inleiding

In de huidige informatiemaatschappij wordt gebruik gemaakt van een elektronische handtekening voor het ondertekenen van een elektronische verklaring. Denk aan internetbankieren of bankieren door middel van een app op een mobiele telefoon. Het komt in de praktijk regelmatig voor dat iemand expliciet of impliciet ontkent dat hij de middelen heeft gebruikt om de elektronische handtekening aan te maken waarmee een elektronische verklaring is ondertekend, bijvoorbeeld door te stellen dat deze middelen zijn gestolen. De elektronische handtekening en de mogelijkheid om die op afstand anoniem te stellen brengen mee dat het bij ontkenning van ondertekening praktisch niet doenlijk zal zijn te bewijzen wie de middelen heeft gebruikt om de elektronische handtekening aan te maken. Wel zal in de regel bij een voldoende betrouwbare methode voor elektronische ondertekening met voldoende mate van zekerheid te bewijzen zijn welke middelen zijn gebruikt om de elektronische verklaring te ondertekenen.

Art. 159 lid 2 Rv bevat een bepaling die ziet op de bewijsrechtelijke gevolgen van een stellige ontkenning van een ondertekening. Deze bepaling stamt uit een tijd dat elektronische ondertekening een onbekend fenomeen was. Dat roept de vraag op hoe deze bepaling dient te worden toegepast als er sprake is van een stellige ontkenning van een elektronische ondertekening.

## 2 De functies van ondertekenen

Ondertekenen heeft twee hoofdfuncties. De eerste hoofdfunctie betreft de identificatie: door het ondertekenen legt de ondertekenaar zijn identiteit vast, waardoor het mogelijk wordt voor anderen om bij ondertekening en achteraf zijn identiteit aan de hand van de handtekening te verifiëren. De tweede hoofdfunctie betreft de wilsuiting: door het ondertekenen van een verklaring uit de ondertekenaar zijn wil ten aanzien van de verklaring waaraan de handtekening is verbonden. Hij eigent zich als het ware deze verklaring toe door haar te ondertekenen.

Het is overigens ook mogelijk dat iemand een handtekening plaatst zonder dat dit dient ter ondertekening van een verklaring. Dan kan de vraag rijzen welke betekenis aan een dergelijke ondertekening dient te worden toegekend. Wat betekent bijvoorbeeld de blote handtekening van een leverancier op een factuur? Is dit een verklaring dat de factuur is betaald door de schuldenaar of dient daar een andere betekenis aan te worden toegekend? Dat is een kwestie van uitleg door de feitelijke rechter.

Ondertekenen kan naast deze twee hoofdfuncties nog nevenfuncties hebben, zoals het creëren van een moment van bezinning bij de ondertekenaar. Het mondelinge 'ja'-woord is sneller gegeven en het klikken op een 'akkoord'-knop is sneller gedaan dan het zetten van een (elektronische) handtekening.<sup>1</sup> Door het stellen van het vormvereiste van een handtekening wordt de kans verkleind dat een ondertekenaar zich als gevolg van overijling bindt.

## 3 Juridische kwalificatie van ondertekening

Ondertekenen is een rechtsfeit. Ondertekenen kan onder omstandigheden een rechtshandeling als bedoeld in art. 3:33 BW zijn als er sprake is van een op een rechtsgevolg gerichte wil, die zich door een verklaring (de ondertekening) heeft geopenbaard.

Van een bloot rechtsfeit kan bijvoorbeeld sprake zijn als de ondertekening vereist is om ergens toegang toe te krijgen, bijvoorbeeld om toegang te krijgen tot een app op een mobiele telefoon of om toegang te krijgen tot de persoonlijke berichteninbox van de ondertekenaar op de website van een leverancier van zaken of diensten. Is in dat geval de ondertekening alleen bedoeld om de identiteit te verifiëren, dan behoeft er bij de ondertekenaar wat betreft het ondertekenen geen op een rechtsgevolg gerichte wil aanwezig te zijn. Dit betekent overigens niet dat de ondertekening in dat geval rechtens geen enkele betekenis heeft. Het kan bijvoorbeeld een omstandigheid zijn die een rechter meeweegt bij het beantwoorden van de vraag of de handelingen die in relatie tot de ondertekenaar na het krijgen van toegang zijn verricht, door hem zijn verricht

\* Mr. dr. R.E. van Esch is legal counsel bij Banning te Den Bosch.

1. Ik verwijs naar de afscheidsrede van A.A. van Velten, met de veelzeggende titel *Klik zei de muis en weg was het huis*, Deventer: Kluwer 2009.

of aan hem kunnen worden toegerekend. Denk aan het geval dat het wachtwoord van de ondertekenaar voor toegang tot een website is gewijzigd en de ondertekenaar ontkent dit zelf te hebben gedaan. Als vaststaat dat deze handeling is verricht nadat iemand die de beschikking had over het oude wachtwoord van de ondertekenaar toegang tot de berichteninbox is verleend en voordat hij weer is uitgelogd, zou de rechter op basis van de omstandigheden tot de overtuiging kunnen komen dat de ondertekenaar het wachtwoord heeft gewijzigd, althans dat aan hem is toe te rekenen dat het wachtwoord is gewijzigd.

Met het ondertekenen kan ook de wil van de ondertekenaar om bepaalde rechtsgevolgen teweeg te brengen, worden geuit, bijvoorbeeld de wil om een aanbod te aanvaarden en daarmee een overeenkomst tot stand te brengen. Het zal afhangen van de omstandigheden van het geval of een ondertekening kan worden gekwalificeerd als een rechtshandeling.

Bij de rechtsgevolgen verbonden aan het ondertekenen van een verklaring denk ik ook aan bewijsrechtelijke rechtsgevolgen, neergelegd in Rv. Een bewijsrechtelijk rechtsgevolg is dat de waarheid van de ondertekende verklaring wordt aangenomen, totdat de ondertekenaar stelt en zo nodig bewijst dat de ondertekende verklaring niet waar is.

Kwalificatie van ondertekenen als het verrichten van een rechtshandeling brengt bijvoorbeeld mee dat als de ondertekenaar ontkent bepaalde rechtsgevolgen gewild te hebben, de rechter op basis van art. 3:35 BW zal moeten beslissen of aan het ontbreken van deze wil het gevolg moet worden verbonden dat de wederpartij de rechtsgevolgen niet kan invoeren jegens de ondertekenaar. Ook kan er dan bijvoorbeeld sprake zijn van een wilsgebrek, dat de rechtshandeling vernietigbaar maakt. Denk aan het geval dat iemand met een pistool op zijn hoofd is gedwongen om te ondertekenen.

#### 4 De elektronische handtekening<sup>2</sup>

De elektronische handtekening is een elektronisch bestand. De term 'elektronische handtekening' is een containerbegrip en heeft betrekking op een variëteit aan (combinaties van) middelen en methoden die worden gebruikt voor het genereren van een elektronische handtekening. Zij hebben gemeen dat daarmee een of beide hoofdfuncties van ondertekenen kunnen worden vervuld.

Voor het vervullen van de hoofdfunctie van identificatie kan bijvoorbeeld gebruik worden gemaakt van vinger- of gelaatskenmerken van de ondertekenaar. De kenmerken

worden met behulp van een apparaat uitgelezen en vergeleken met vooraf opgeslagen gegevens over deze kenmerken (de *template*). Via deze methode kan worden geverifieerd of iemand is die hij zegt te zijn. Deze vorm van elektronisch ondertekenen volstaat bijvoorbeeld om toegang te geven tot een bestand of een applicatie op een mobiele telefoon. Ik gebruik regelmatig de internetbankiersapp van een Nederlandse bank op mijn mobiele telefoon. Door middel van deze app krijg ik toegang tot bijvoorbeeld gegevens over mijn betaalrekening nadat ik door middel van mijn vingerafdruk de mogelijkheid heb geboden om de kenmerken van mijn vingerafdruk te vergelijken met een template daarvan in een beveiligd compartiment van de chip van mijn mobiele telefoon en deze verificatie een positief resultaat heeft opgeleverd.

De hoofdfunctie van wilsuiting kan worden vervuld doordat de elektronische handtekening op enigerlei wijze wordt verbonden met de verklaring. De verbondenheid van een elektronische handtekening met een verklaring kan op verschillende wijzen worden gecreëerd. Plak ik een digitale scan van mijn schriftelijke handtekening in een elektronisch document, dan is er verbondenheid doordat de elektronische verklaring en de elektronische handtekening deel uitmaken van hetzelfde elektronische bestand, net als de verbondenheid tussen de schriftelijke handtekening en de schriftelijke verklaring wordt gecreëerd doordat beide staan op hetzelfde papier. Er kan ook sprake zijn van een logische verbondenheid, bijvoorbeeld doordat de methode van het aanmaken van de elektronische handtekening zodanig is ingericht dat de elektronische handtekening onder meer op basis van de gegevens van de verklaring wordt aangemaakt. Zo'n logische verbondenheid tussen de elektronische handtekening en de verklaring wordt bijvoorbeeld gecreëerd als een elektronische betaelopdracht met behulp van een random reader of een scanner en de betaalpas in combinatie met de pincode<sup>3</sup> wordt ondertekend.

De betrouwbaarheid van een methode voor elektronisch ondertekenen hangt van een groot aantal factoren af, waaronder de inrichting en de beveiliging van de middelen en de methode die worden gebruikt om de elektronische handtekening aan te maken en te verbinden aan de verklaring, het proces van uitgifte van de middelen voor het aanmaken van elektronische handtekeningen en de wijze waarop bestanden met verificatiegegevens (zoals templates) zijn beschermd tegen

2. Ik verwijs voor juridische literatuur over de elektronische handtekening naar M.H.M. Schellekens, *Electronic signatures. Authentication technology from a legal perspective*, Den Haag: T.M.C. Asser Press 2004; A.R. Lodder, J. Dumortier & S.H. Bol, *Het recht rond elektronische handtekeningen*, Deventer: Kluwer 2005; R.E. van Esch, *Juridische aspecten van elektronische handel*, Deventer: Kluwer 2007, p. 123-142; J.J. Linnemann, 'Uitvoering van de verordening elektronische identificatie en vertrouwensdiensten', *IR* 2015, afl. 5/6, p. 176-181; T.F.E. Tjong Tjin Tai, 'De eIDAS-verordening en de elektronische handtekening uit het BW', *WPNR* 2017/7151; T.J. de Graaf, 'De lappendeken van de gelijkstelling van elektronisch met schriftelijk in het licht van vormvereisten en bewijskracht', *MvV* 2018, afl. 7/8, p. 245-246.

3. In dat geval zijn de middelen voor het vaststellen van de elektronische handtekening de random reader/scanner en de betaalpas met pincode. De methode is als volgt ingericht. Nadat de gegevens van de betaelopdracht zijn ingevuld, klikt de betaler op een knop die wordt aangeduid met de term 'ondertekenen' of met een andere term met dezelfde strekking. De applicatie van de betaaldienstverlener berekent op basis van deze gegevens een daaraan gerelateerde (kleur)code (ook wel de *challenge* genoemd). De betaler vult de challenge in op zijn random reader of scant met zijn scanner de kleurcode. De random reader of de scanner berekent vervolgens op basis van een bepaald algoritme een code. Deze code is de elektronische handtekening, die logisch is verbonden met de elektronische verklaring (betaelopdracht) doordat de challenge uniek is voor de betreffende verklaring, in die zin dat iedere wijziging van de verklaring leidt tot een andere challenge en daarmee tot een andere elektronische handtekening.

ongeautoriseerde toegang en wijziging.<sup>4</sup> In deze tijd wordt ter bevordering van de betrouwbaarheid van een methode voor elektronisch ondertekenen wat betreft de identificatiefunctie een combinatie van twee van de drie factoren (1) wat je weet (zoals pincode), (2) wat je bent (bijvoorbeeld vinger- of gelaatskenmerken) en (3) wat je hebt (bijvoorbeeld een chipkaart, een mobiele telefoon of een paspoort/rijbewijs) geadviseerd of voorgeschreven.<sup>5</sup> Dit wordt de tweefactorenauthenticatie genoemd.

Met de opkomst van de elektronische handel werden middelen en methoden ontwikkeld als elektronisch functioneel equivalent van de schriftelijke handtekening. Tot deze middelen en methoden behoorde de elektronische gekwalificeerde handtekening. Omdat de Europese regelgeving en daardoor de Nederlandse regelgeving (in art. 3:15a BW) gewag maken van de elektronische gekwalificeerde handtekening, leg ik hierna uit op welke wijze zij wordt aangemaakt.

De ondertekenaar berekent met behulp van een computerprogramma op basis van een algoritme de hashwaarde<sup>6</sup> van zijn elektronische verklaring. Vervolgens wordt de hashwaarde versleuteld met de geheime privésleutel van de ondertekenaar. De versleutelde hashwaarde is de elektronische handtekening. In dat geval kan tweefactorenauthenticatie bijvoorbeeld worden gerealiseerd doordat de geheime privésleutel is opgeslagen in een beveiligd compartiment van een chip op een chipkaart (wat je hebt) die wordt gebruikt bij het elektronisch ondertekenen, en dit compartiment van de chip alleen kan worden ontsloten met behulp van een chipkaartlezer en een pincode (wat je weet) of een vingerafdruk (wat je bent). Nadat hij de hashwaarde heeft versleuteld, stuurt de ondertekenaar de elektronische verklaring met de elektronische handtekening (versleutelde hashwaarde) naar de geadresseerde. De geadresseerde ontcijfert met behulp van een computerprogramma de elektronische handtekening met de publieke sleu-

tel van de ondertekenaar, die hoort bij diens geheime privésleutel. Daarmee verkrijgt hij de oorspronkelijke hashwaarde van de elektronische verklaring, zoals die is berekend door de ondertekenaar. De geadresseerde berekent zelf de hashwaarde van de ontvangen elektronische verklaring aan de hand van hetzelfde algoritme dat is gebruikt door de ondertekenaar voor het berekenen van de hashwaarde. Hij vergelijkt de door hemzelf berekende hashwaarde van de ontvangen verklaring met de ontcijferde hashwaarde van de elektronische handtekening van de ondertekenaar. Als deze hashwaarden hetzelfde zijn, kan hij van twee dingen uitgaan: (1) de verklaring is ondertekend door iemand die de beschikking had over de geheime privésleutel van de afzender, en (2) de verklaring is na het berekenen van de hashwaarde door de ondertekenaar niet meer van inhoud veranderd.<sup>7</sup> De geadresseerde kan verifiëren of de publieke sleutel waarmee hij de elektronische gekwalificeerde handtekening van de ondertekenaar ontcijfert, hoort bij de ondertekenaar en de door de ondertekenaar gebruikte geheime privésleutel, door middel van de elektronische verklaring van een betrouwbare partij, zoals een notaris, waarin zij bevestigt dat dit het geval is. Deze verklaring is vastgelegd in een elektronisch certificaat, dat op zijn beurt weer elektronisch is ondertekend door de uitgever (in het voorbeeld: de notaris). Van een gekwalificeerde elektronische handtekening is sprake als (1) de handtekening is aangemaakt volgens de hiervoor beschreven methode en (2) de middelen voor het aanmaken van deze handtekening, de uitgever van het certificaat met de publieke sleutel en dit certificaat zelf aan bepaalde betrouwbaarheidseisen voldoen.

## 5 Ontwikkelingen in regelgeving wat betreft elektronische handtekeningen

Om te voorkomen dat de ontwikkeling van de grensoverschrijdende elektronische handel binnen de EG werd belemmerd door verschillen in de lidstaten wat betreft de juridische regulering en erkenning van de elektronische handtekening, hebben het Europees Parlement en de Raad in 1999 de Richtlijn elektronische handtekeningen vastgesteld.<sup>8</sup> Een belangrijk deel van deze richtlijn bestond uit regels die tot doel hadden de regulering van het verlenen van vertrouwensdiensten, zoals het uitgeven van elektronische certificaten voor elektronische gekwalificeerde handtekeningen, te harmoniseren. Deze regels zijn in de Nederlandse wetgeving door een wijziging van de Telecommunicatiewet geïmplementeerd. Omdat deze regels niet direct van belang zijn voor het onderwerp van dit artikel, ga ik daarop in dit artikel niet verder in. Voor dit artikel is met name van belang art. 5 Richtlijn elektronische handtekeningen. Kort gezegd legde dit artikel aan de lidstaten de verplichting op om ervoor te zorgen dat (1) een elektronische gekwalificeerde handtekening die voldoet aan de

4. Ik verwijs voor een verhandeling over de gezichtspunten die van belang zijn voor de beoordeling van de betrouwbaarheid van een elektronische handtekening, naar R.E. van Esch, 'Gezichtsponen voor de beoordeling van de betrouwbaarheid van een methode voor elektronische ondertekening', *FR* 2018, afl. 8/9, p. 397-405.

5. Voor een voorbeeld van een voorschrift ter zake verwijs ik naar art. 26h lid 4 Besluit prudentiële regels Wft, dat betrekking heeft op sterke cliënt-authenticatie in het betalingsverkeer. Zie ook de opinie van de European Banking Authority hierover van 21 juni 2019 (EBA-Op-2019-06), waarin zij op ieder van deze factoren nader ingaat.

6. De hashwaarde van een elektronische verklaring is een code die met behulp van een compressiealgoritme wordt berekend over de tekens van de elektronische verklaring. Ervan uitgaande dat ieder teken in een elektronische verklaring bestaat uit een unieke combinatie van nullen en enen, zou een eenvoudig algoritme voor het berekenen van de hashwaarde van een elektronische verklaring als volgt kunnen luiden: *Tel alle enen van de tekens van de elektronische verklaring bij elkaar op. Tel de cijfers van het getal dat daarvan de resultante is bij elkaar op. Indien dit leidt tot 10 of een hoger getal, herhaal dan de laatste instructie totdat de resultante een getal kleiner dan 10 is.* Als bijv. bij toepassing van dit algoritme blijkt dat de tekens van de elektronische verklaring tezamen 356 enen bevatten, zou de hashwaarde van de betreffende verklaring 5 zijn ( $3 + 5 + 6 = 14$ ;  $1 + 4 = 5$ ). Uiteraard zijn de algoritmen die in de praktijk worden gebruikt voor het aanmaken van elektronische handtekeningen vele malen complexer dan het algoritme in dit voorbeeld.

7. Dit uitgangspunt is gebaseerd op het feit dat iedere wijziging in de verklaring leidt tot een andere hashwaarde behorende bij de ondertekende verklaring.

8. Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen, *PbEG* 2000, L 13/12.

wettelijke vereisten daaromtrent, dezelfde rechtsgevolgen heeft als een schriftelijke handtekening, en (2) aan andere elektronische handtekeningen geen rechtsgeldigheid wordt ontzegd om de enkele reden dat ze elektronisch zijn. Nederland heeft als lidstaat aan deze verplichting uit de Richtlijn elektronische handtekeningen voldaan door in Boek 3 BW art. 15a op te nemen.<sup>9</sup> Dit artikel bepaalde onder meer dat een elektronische handtekening dezelfde rechtsgevolgen heeft als een handgeschreven handtekening indien de methode die daarbij gebruikt is voor authenticatie voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval.

De Richtlijn elektronische handtekeningen is in 2014 met de inwerkingtreding van de eIDAS-verordening<sup>10</sup> ingetrokken. Voor het onderwerp van dit artikel is met name van belang art. 25 eIDAS-verordening, dat inhoudelijk overeenkomt met art. 5 van de ingetrokken Richtlijn elektronische handtekeningen. Desalniettemin heeft de uitvoering van de eIDAS-verordening geleid tot een aanpassing van art. 3:15a BW.<sup>11</sup> Deze aanpassing heeft naar mijn oordeel alleen tot een vereenvoudiging en modernisering van de tekst van dit artikel geleid en niet tot een inhoudelijke wijziging.

Wil een elektronische handtekening dezelfde rechtsgevolgen hebben als een handgeschreven handtekening, dan moet volgens art. 3:15a BW de methode voor ondertekening die is gebruikt voldoende betrouwbaar zijn, gelet op het doel waarvoor de elektronische handtekening is gebruikt en op alle overige omstandigheden van het geval. Welke methode voor ondertekening voldoende betrouwbaar is, hangt af van de omstandigheden van het geval, met dien verstande dat een elektronische gekwalificeerde handtekening onder alle omstandigheden voldoende betrouwbaar is.

Vereist het doel van een verklaring dat een persoon zelf ondertekent, dan brengt art. 3:15a BW mee dat het plaatsen van een ingescande handtekening onder een elektronische verklaring door een ander dan de ondertekenaar een niet voldoende betrouwbare methode voor ondertekening is.<sup>12</sup>

## 6 Ontwikkelingen in regelgeving wat betreft de onderhandse akte

De onderhandse akte is thans geregeld in de tweede paragraaf van de negende afdeling van Rv. De negende afdeling gaat over bewijs. De tweede paragraaf van deze afdeling gaat over akten en vonnissen. Het gevolg van de stellige ontkenning van de

ondertekening van een onderhandse akte is geregeld in art. 159 lid 2 Rv. De tekst van deze bepaling komt letterlijk overeen met de tekst van het tweede lid van art. 186 Rv (oud), dat met de inwerkingtreding van de nieuwe regeling van het bewijsrecht in burgerlijke zaken in 1988 van kracht werd. Het wetsvoorstel voor deze nieuwe regeling werd in 1969 bij de Tweede Kamer ingediend.<sup>13</sup> Het heeft derhalve lang geduurd voordat dit voorstel het bracht tot wet. Ik acht het zeer onwaarschijnlijk, zo niet uitgesloten, dat bij de formulering van de bepaling die thans is neergelegd in art. 159 lid 2 Rv is voorzien dat er zich in de toekomst elektronisch verkeer tussen rechtssubjecten zou ontwikkelen zoals thans het geval is, waarin behoefte zou bestaan aan een elektronische handtekening.

In dit verband is het vermelden waard dat de wetgever destijds heeft overwogen of een voorschrift gewenst was *betreffende de rechtskracht* van de op werktuigelijke wijze onder een onderhandse akte gestelde handtekening, zoals een handtekeningstempel. Omdat uit onderzoek bleek dat het gebruik van een facsimile in de praktijk geen moeilijkheden meebracht, kwam de wetgever tot de conclusie dat aan een wettelijke bepaling over dit onderwerp geen behoefte bestond.<sup>14</sup>

Een ontwikkeling in de Nederlandse regelgeving die van belang is voor het onderwerp van dit artikel betreft de Wet elektronisch verkeer.<sup>15</sup> Een belangrijk onderdeel van deze wet betrof de invoeging van art. 156a Rv. Dit artikel brengt mee dat een onderhandse akte ook elektronisch kan worden opge maakt, mits degene ten behoeve van wie de akte bewijs oplevert, in staat wordt gesteld om de inhoud van de akte op te slaan op een duurzame drager. Hoewel art. 156a Rv met geen woord rept over een elektronische handtekening, blijkt uit de wetsgeschiedenis dat een elektronisch bestand alleen kan kwalificeren als een onderhandse akte als het een elektronische verklaring bevat die is ondertekend met een voldoende betrouwbare elektronische handtekening<sup>16</sup> als bedoeld in art. 3:15a BW.<sup>17</sup>

## 7 De stellige ontkenning van de ondertekening in het algemeen

Stellige ontkenning van de ondertekening kan inhouden (1) dat degene tegen wie het stuk als onderhandse akte wordt ingeroepen (hierna: de vermeende ondertekenaar), ontkent dat het zijn handtekening is, of (2) dat de vermeende ondertekenaar erkent dat het zijn handtekening is, maar ontkent dat hij of een daartoe bevoegde die handtekening heeft gezet. Bij

9. Wet elektronische handtekening, *Stb.* 2003, 199.

10. Verordening (EU) 910/2014 van het Europees Parlement en de Raad 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 257/73.

11. Wet uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten, *Stb.* 2017, 13.

12. Aldus HR 14 juni 2019, ECLI:NL:HR:2019:957. In dit arrest oordeelde de Hoge Raad over de betrouwbaarheidseisen die dienen te worden gesteld aan de methode voor elektronische ondertekening van een geneeskundige verklaring door de geneesheer-directeur van een instelling.

13. Zie *Kamerstukken II* 1969/70, 10377, 1. In dat wetsvoorstel werd het gevolg van de stellige ontkenning van een handtekening geregeld in art. 185 Rv.

14. Zie *Kamerstukken II* 1969/70, 10377, 3, p. 14, eerste en tweede kolom.

15. Wet van 20 februari 2010 tot wijziging van enige bepalingen van het Wetboek van Burgerlijke Rechtsvordering en het Burgerlijk Wetboek teneinde naast het in deze bepalingen gestelde vereiste van schriftelijkheid ook ruimte te bieden aan de ontwikkelingen op het gebied van het elektronisch verkeer, *Stb.* 2010, 222.

16. Voor een antwoord op de vraag welke methode voor ondertekening voldoende betrouwbaar is, verwijs ik naar par. 4 van dit artikel.

17. *Kamerstukken II* 2007/08, 31358, 3, p. 3.

de tweede categorie van stellige ontkenningen kan worden gedacht aan handtekeningen die op werktuigelijke wijze onder een onderhandse akte zijn gesteld.<sup>18</sup> Denk aan het geval dat van de schriftelijke handtekening van een persoon een stempel is gemaakt. Is met behulp van deze stempel een handtekening geplaatst onder een verklaring, dan houdt de stellige ontkenning van de ondertekening niet in dat de handtekening niet de handtekening van de vermeende ondertekenaar is, als wel dat zij niet door de vermeende ondertekenaar of iemand die daartoe bevoegd was met behulp van de stempel is gezet. Hetzelfde geldt als voor het ondertekenen van een (elektronische) verklaring gebruik is gemaakt van een digitale scan van een schriftelijke handtekening.

Wanneer is er sprake van een stellige ontkenning? Daarvoor is voldoende dat de partij tegen wie een stuk als onderhandse akte wordt tegengeworpen, in duidelijke en ondubbelzinnige bewoording verklaart dat de handtekening onder de akte niet de hare is of niet door haar gezet is.<sup>19</sup> Stellingen als 'Dat is niet mijn handtekening' of 'Die handtekening heb ik niet gezet' lijken mij voldoende. Of een stelling als 'De handtekening lijkt niet op mijn handtekening' een stellige ontkenning inhoudt, is een kwestie van uitleg. Dat is een feitelijk oordeel, waarbij deze stelling moet worden uitgelegd in de context waarin zij is gegeven.

De ontkenner behoeft zijn ontkenning niet te onderbouwen,<sup>20</sup> maar mag dat wel.

### 8 De bewijslastverdeling bij stellige ontkenning van de ondertekening in het algemeen

Het gevolg van de stellige ontkenning van de ondertekening van een onderhandse akte is omschreven in art. 159 lid 2 Rv. Het stuk levert geen bewijs op totdat degene die zich op het stuk beroept als ware het een onderhandse akte (hierna: de inroeper), bewijst van wie de ondertekening afkomstig is.

De bewijslastverdeling bij stellige ontkenning van ondertekening is daardoor te verklaren dat bij de onderhandse akte – anders dan bij de authentieke akte – de waarborg ontbreekt dat zij is opgemaakt door een daartoe door de wet aangewezen persoon belast met het opmaken van zekere akten. Wordt de handtekening ontkend, dan moet eerst vast komen te staan dat de onderhandse akte echt is, voordat daaraan enige bewijskracht kan worden toegekend.<sup>21</sup>

Zoals gezegd ligt de bewijslast ten aanzien van de echtheid van de handtekening bij een stellige ontkenning van de ondertekening bij de inroeper.<sup>22</sup> De rechter kan daarvan niet afwijken, ook niet als hij van mening is dat de redelijkheid en bil-

lijkheid onder de gegeven omstandigheden een dergelijke omkering van bewijslast meebrengen.<sup>23</sup> Wel kan hij besluiten om de echtheid van de handtekening niet te laten onderzoeken als hij op grond van de vaststaande feiten ervan overtuigd is dat de handtekening onder het stuk niet de handtekening van de vermeende ondertekenaar is.<sup>24</sup>

### 9 De inhoud van de wettelijke bewijsopdracht in het algemeen

Bij stellige ontkenning van ondertekening dient de inroeper krachtens art. 159 lid 2 Rv, wil aan het ondertekende stuk enig bewijs ten aanzien van de waarheid van de ondertekende verklaring kunnen worden toegekend, te bewijzen van wie de ondertekening afkomstig is. Hoe moet deze bepaling worden uitgelegd? Welke betekenis moet worden toegekend aan het woord 'afkomstig' in deze bepaling? Een strikte uitleg van deze bepaling brengt mee dat de inroeper, om te bewijzen van wie de ondertekening afkomstig is, niet alleen moet bewijzen wiens handtekening op het stuk prijkt, maar ook wie die handtekening op het stuk heeft geplaatst. Een ruime uitleg van deze bepaling houdt in dat de inroeper daarvoor alleen hoeft te bewijzen wiens handtekening op het stuk prijkt. Het verschil in de strikte en de ruime uitleg komt onder meer naar voren als er sprake is van een werktuigelijke ondertekening, bijvoorbeeld met behulp van een handtekeningstempel. Bij een strikte uitleg zou de inroeper, om aan de wettelijke bewijsopdracht te voldoen, in het voorbeeld van de stempel niet alleen moeten bewijzen wiens handtekening op het stuk staat, maar ook wie de stempel heeft gebruikt om het stuk te ondertekenen. Bij een ruime uitleg zou de inroeper in het gegeven voorbeeld van de handtekeningstempel alleen hoeven te bewijzen wiens handtekeningstempel is gebruikt.

Voor het antwoord op de vraag hoe de bepaling van art. 159 lid 2 Rv dient te worden uitgelegd in het geval van een werktuigelijke ondertekening, zoals een elektronische ondertekening, heb ik de relevante wetsgeschiedenis, rechtspraak en literatuur geraadpleegd.

Ik heb de indruk dat de wetgever bij de formulering van de bepaling van art. 159 lid 2 Rv met name heeft gedacht aan de handgeschreven handtekening en minder aan de handtekening die op werktuigelijke wijze is gesteld. Wellicht dat daardoor het hiervoor door mij gemaakte onderscheid niet op zijn netvlies stond bij de redactie van deze bepaling. Wat daar ook van zij, ik heb in de wetsgeschiedenis geen aanknopingspunten kunnen vinden voor de strikte noch voor de ruime uitleg van art. 159 lid 2 Rv.

De Hoge Raad heeft zich bij mijn weten nog niet uitgelaten over het antwoord op de hiervoor gestelde vraag. Ons hoogste rechtscollege legt deze bepaling aldus uit, dat de inroe-

18. *Kamerstukken II 1969/70*, 10377, 3, p. 14, tweede kolom.

19. Randnr. 3.4 en de literatuur vermeld in noot 5 van de conclusie van A-G Wissink bij HR 12 april 2019, ECLI:NL:PHR:2019:238; Hof Arnhem-Leeuwarden 12 maart 2019, ECLI:NL:GHARL:2019:2299, r.o. 5.5.

20. HR 28 februari 1997, ECLI:NL:HR:1997:ZC2297, r.o. 3.3; Hof Arnhem-Leeuwarden 12 maart 2019, ECLI:NL:GHARL:2019:2299, r.o. 5.5; HR 12 april 2019, ECLI:NL:HR:2019:572, r.o. 3.3.2.

21. *Kamerstukken II 1969/70*, 10377, 3, p. 13-14.

22. Zie bijv. Hof Den Haag 24 september 2019, ECLI:NL:GHDHA:2019:2460.

23. Aldus A-G Wissink in zijn conclusie bij HR 12 april 2019, ECLI:NL:PHR:2019:238, randnr. 3.5.2.

24. Hof Den Haag 4 juni 2019, ECLI:NL:GHDHA:2019:1279. In dat geval had de vermeende ondertekenaar afdoende aangetoond dat hij zich ten tijde van de ondertekening niet thuis in Nederland maar in Lissabon bevond. Bovendien leek de handtekening onder het ondertekende stuk niet op de handtekening van de vermeende ondertekenaar in zijn paspoort.

per bij stellige ontkenning van de ondertekening *de echtheid* van de handtekening moet bewijzen, wil aan het ondertekende stuk jegens de vermeende ondertekenaar de bewijskracht van een onderhandse akte kunnen worden toegekend.<sup>25</sup> Deze uitleg van de bepaling van art. 159 lid 2 Rv wordt ook in de lagere rechtspraak gehanteerd. Zie bijvoorbeeld Hof 's-Gravenhage 30 oktober 2012<sup>26</sup> en meer recent Hof Arnhem-Leeuwarden 12 maart 2019.<sup>27</sup> Deze rechtspraak geeft echter geen antwoord op de vraag of voor de toepassing van art. 159 lid 2 Rv bij een werktuigelijk gestelde handtekening voor het inroepen van de bewijsrechtelijke rechtsgevolgen verbonden aan een onderhandse akte volstaat dat wordt bewezen wiens middelen zijn gebruikt om de handtekening te stellen, of dat tevens moet worden bewezen wie die middelen heeft gebruikt. Het woord 'echtheid' roept naar mijn oordeel dezelfde vragen op als het woord 'afkomstig' uit art. 159 lid 2 Rv. Is een handtekening die werktuigelijk is gesteld echt als vaststaat dat de middelen van de vermeende ondertekenaar voor het genereren van de elektronische handtekening zijn gebruikt, of is zij alleen echt als bovendien vaststaat dat deze middelen zijn gebruikt door de vermeende ondertekenaar of door iemand die daartoe bevoegd was?

Ook de literatuur geeft geen aanknopingspunten voor het antwoord op de hiervoor gestelde vraag. Naar mijn oordeel wordt in de literatuur dezelfde uitleg gegeven aan de bepaling van art. 159 lid 2 Rv als die de Hoge Raad daaraan geeft, namelijk dat de inroeper bij een stellige ontkenning van de ondertekening door de vermeende ondertekenaar de echtheid van de handtekening moet bewijzen.<sup>28</sup> De opvattingen in de literatuur roepen dezelfde vraag op als de rechtspraak dienaangaande: wat dient te worden verstaan onder 'echtheid van de handtekening'?

Vóór een strikte uitleg van de bepaling van art. 159 lid 2 Rv pleit naar mijn oordeel dat daarin wordt gesproken over de afkomst van de ondertekening in plaats van de afkomst van de handtekening. Ondertekening is het proces van ondertekenen, hetgeen mede omvat het gebruik van de middelen voor het stellen van de handtekening. Het valt op dat de Hoge Raad in zijn arrest van 2019 spreekt over de 'echtheid van de handtekening',<sup>29</sup> hetgeen naar mijn gevoel meer ruimte biedt voor de ruime uitleg van deze bepaling.

Op grond van de tekst van art. 159 lid 2 Rv neig ik tot een strikte uitleg van de bepaling van art. 159 lid 2 Rv. Bij deze uitleg zal de inroeper bij een stellige ontkenning van werktuigelijke ondertekening niet alleen moeten bewijzen dat de middelen van de vermeende ondertekenaar zijn gebruikt voor het zetten van de handtekening, maar ook dat de vermeende ondertekenaar of een daartoe bevoegde deze middelen heeft

gebruikt, wil hij de ondertekende verklaring als onderhandse akte kunnen tegenwerpen aan de vermeende ondertekenaar.

## 10 Gevolgen van de stellige ontkenning van ondertekening voor de bewijskracht

Bij stellige ontkenning van ondertekening levert het ondertekende stuk niet alleen geen dwingende bewijskracht, maar ook geen vrije bewijskracht op totdat de afkomst van de ondertekening is bewezen. De Hoge Raad formuleert het als volgt, dat 'aan het stuk *geen enkele* (cursivering auteur) bewijskracht toekomt, zolang niet bewezen is van wie de handtekening afkomstig is'.<sup>30</sup> Deze overweging van ons hoogste rechtscollege roept de vraag op of hij bedoelt dat aan het ondertekende stuk bij gebrek aan bewijs ten aanzien van de afkomst van de handtekening geen enkele bewijskracht toekomt ten aanzien van welk feit dan ook, of dat het geen enkele bewijskracht toekomt ten aanzien van de waarheid van de ondertekende verklaring. Het antwoord op deze vraag kan bijvoorbeeld van belang zijn als (1) een elektronische verklaring elektronisch is ondertekend, (2) de vermeende ondertekenaar het ondertekenen van deze verklaring stellig ontkent, en (3) het bestand met de elektronische verklaring en de elektronische handtekening wordt ingebracht als middel om te bewijzen dat de middelen voor het aanmaken van elektronische handtekeningen van de vermeende ondertekenaar zijn gebruikt. Eenzelfde belang kan spelen als (1) een schriftelijke verklaring is ondertekend met een handtekeningstempel, (2) de vermeende ondertekenaar de ondertekening stellig ontkent, en (3) het stuk met de gestempelde handtekening wordt ingebracht als middel om te bewijzen dat de handtekeningstempel van de vermeende ondertekenaar is gebruikt om de schriftelijke verklaring te ondertekenen. Of als een ondertekend stuk waarvan de handtekening stellig wordt ontkend, wordt ingebracht om te bewijzen dat het gepersonaliseerd briefpapier van de vermeende ondertekenaar is gebruikt. Om het huidige elektronisch rechtsverkeer niet onnodig te belemmeren, zou het antwoord op de vraag naar mijn oordeel als volgt moeten luiden: een ondertekend stuk waarvan de handtekening stellig wordt ontkend door degene tegen wie het stuk als onderhandse akte wordt ingeroepen, levert geen enkel bewijs op ten aanzien van de waarheid van de ondertekende verklaring, zolang niet is bewezen van wie de ondertekening afkomstig is.

## 11 De stellige ontkenning van elektronische ondertekening

Een stellige ontkenning van een elektronische ondertekening kan net als bij de stellige ontkenning van een schriftelijke ondertekening inhouden dat (1) de elektronische handtekening niet de handtekening is van de vermeende ondertekenaar, of (2) zij niet is gesteld door de vermeende ondertekenaar of iemand die bevoegd was om de middelen te gebruiken om de elektronische handtekening van de vermeende ondertekenaar aan te maken.

25. Zie bijv. HR 12 april 2019, ECLI:NL:HR:2019:572, r.o. 3.3.2.

26. ECLI:NL:GHSGR:2012:BY2903, r.o. 5.1.

27. ECLI:NL:GHARL:2019:2299, r.o. 5.6.

28. Zie bijv. H.L.G. Dijksterhuis-Wieten, *Bewijsrecht in civiele procedures*, Deventer: Kluwer 1992, p. 52-53; Pitlo/Hidma & Rutgers 2004/53; *Asser Procesrecht/Asser 3* 2017/250.

29. HR 12 april 2019, ECLI:NL:HR:2019:572, r.o. 3.3.2.

30. HR 12 april 2019, ECLI:NL:HR:2019:572, r.o. 3.3.2. Zie ook randnr. 3.3 van de conclusie van A-G Wissink bij HR 12 april 2019, ECLI:NL:PHR:2019:238.

In uitzonderlijke gevallen zal de vermeende ondertekenaar met de stellige ontkenning van de elektronische ondertekening bedoelen dat de elektronische handtekening niet van hem is. Wordt bijvoorbeeld een elektronische verklaring ondertekend doordat de ondertekenaar door middel van zijn vingerafdruk zich de verklaring toe-eigent, dan kan degene tegen wie het elektronisch bestand als onderhandse akte wordt ingeroepen, stellen dat de vingerafdruk die is gebruikt om te ondertekenen niet de kenmerken heeft van zijn vingerafdruk. Het gebruik van een andere vingerafdruk kan bijvoorbeeld tijdens het proces van ondertekenen onopgemerkt blijven als de kenmerken van de vingerafdruk in de template die wordt gebruikt om de echtheid van de elektronische handtekening te controleren, is vervangen door de kenmerken van de andere vingerafdruk die is gebruikt voor ondertekening. Er zal dan sprake zijn van een vorm van identiteitsfraude, vergelijkbaar met het vervangen van een foto op een paspoort door een andere foto.

Ik verwacht dat in het informatiemaatschappelijk verkeer een vermeende ondertekenaar in de regel de elektronische ondertekening stellig zal ontkennen door te stellen dat iemand anders dan hij of een bevoegde zijn middelen heeft gebruikt voor het aanmaken van de elektronische handtekening. Denk aan het betalingsverkeer en phishing. Zo'n stellige ontkenning kan naar mijn oordeel worden gelijkgesteld met de ontkenning dat een handtekeningstempel van de vermeende ondertekenaar is gebruikt door hemzelf of een daartoe bevoegd persoon.

## 12 De gevolgen van de stellige ontkenning van elektronische ondertekening van een elektronische verklaring

Uit art. 159 lid 2 Rv volgt dat bij stellige ontkenning van de ondertekening de inroeper moet bewijzen van wie de ondertekening *afkomstig is*, wil aan het ondertekende stuk enige bewijskracht kunnen worden toegekend. Hoe moet deze rechtsregel worden toegepast als het gaat om het geval dat een vermeende ondertekenaar een elektronische ondertekening stellig ontkent?

Houdt de stellige ontkenning in dat de elektronische handtekening niet de handtekening van de vermeende ondertekenaar is, dan heeft de inroeper naar mijn oordeel een gerede kans dat hij zal slagen in de bewijsopdracht als de middelen voor en de methode van elektronisch ondertekenen voldoende betrouwbaar zijn. Het zal voor hem moeilijker worden om hieraan te voldoen als de middelen en/of de methode onvoldoende betrouwbaar zijn. Denk aan het geval dat de verificatie van de identiteit van de ondertekenaar aan de hand van de vingerafdruk plaatsvindt op basis van slechts een paar kenmerken van de vingerafdruk, of dat er bij de verificatie een hoge zogenoemde *false acceptance rate* wordt gehanteerd om te voorkomen dat te vaak een vingerafdruk bijvoorbeeld als gevolg van een beschadiging van de huid van de vinger ten onrechte als onecht wordt afgewezen. In dat geval is er een grotere kans dat een andere vingerafdruk tijdens de ondertekening is herkend als de vingerafdruk van degene tegen wie het elektro-

nisch bestand als onderhandse akte wordt ingeroepen en zal het voor de inroeper moeilijker zijn om te bewijzen dat de handtekening afkomstig is van de vermeende ondertekenaar.

In die gevallen dat de stellige ontkenning inhoudt dat een onbevoegde de middelen van de vermeende ondertekenaar heeft gebruikt voor het aanmaken van de elektronische handtekening, zal het lastig, zo niet onmogelijk worden om bij een strikte uitleg van de bepaling van art. 159 lid 2 Rv en met name het woord 'afkomstig' daarin aan deze wettelijke bewijsopdracht te voldoen. Professionele fraudeurs op afstand plegen geen sporen achter te laten, zodat meestal niet kan worden bewezen wie de handtekening heeft gesteld.

Ik ben er een voorstander van om art. 159 lid 2 Rv aldus uit te leggen dat een elektronisch ondertekende elektronische verklaring bij stellige ontkenning van ondertekening elke bewijskracht ontbeert *ten aanzien van de waarheid van de verklaring*, totdat de inroeper bewezen heeft welke middelen er gebruikt zijn voor het aanmaken van de elektronische handtekening en wie die middelen heeft gebruikt. Deze uitleg laat onverlet dat het bestand met de elektronische handtekening vrije bewijskracht toekomt ten aanzien van andere feiten dan de waarheid van de verklaring, zoals welke middelen er zijn gebruikt om de elektronische handtekening aan te maken. Aldus wordt de inroeper de mogelijkheid geboden om de eerste stap te zetten naar de rechtsvraag of het misbruik van de middelen kan worden toegerekend aan de vermeende ondertekenaar.

## 13 Toerekening van misbruik van middelen voor ondertekening en bewijs

Is een handtekening van een vermeende ondertekenaar op werktuigelijke wijze gesteld op een stuk, zoals met behulp van een handtekeningstempel, dan staat de echtheid van de handtekening vast, in die zin dat het de handtekening van de vermeende ondertekenaar is. Kan niet worden bewezen wie de handtekening heeft gesteld, dan kan als uitgangspunt gelden dat de handtekening niet is gesteld door de vermeende ondertekenaar of een daartoe bevoegde. Dan rijst de vraag wie in de rechtsverhouding tussen de vermeende ondertekenaar en de inroeper het risico draagt van misbruik van de middelen voor het op werktuigelijke wijze stellen van de handtekening. Deze vraag kan bijvoorbeeld rijzen als een elektronische verklaring is ondertekend met behulp van middelen voor het aanmaken van elektronische handtekeningen van de vermeende ondertekenaar, maar niet kan worden bewezen wie die middelen heeft gebruikt. Draagt de vermeende ondertekenaar het risico, dan kan de inroeper de vermeende ondertekenaar aan de ondertekende verklaring houden. Draagt de inroeper het risico, dan heeft de ondertekende verklaring geen werking.

Neem het voorbeeld van een bestelling op internet die is ondertekend met middelen (bijvoorbeeld mobiele telefoon en code) die toebehoren aan X. Als de verkoper kan bewijzen dat de middelen waarmee de elektronische handtekening is aangeemaakt, toebehoren aan X, maar niet kan bewijzen door wie die middelen zijn gebruikt, kan ervan worden uitgegaan dat deze middelen ook door een onbevoegde kunnen zijn gebruikt en

kan de vraag rijzen of de verkoper X aan de koopovereenkomst kan houden.

Voor de beantwoording van de vraag wie in een concreet geval het risico draagt van misbruik van middelen voor het aanmaken van elektronische handtekeningen is de bewijsrechtelijke bepaling van art. 159 lid 2 Rv niet direct van belang. Niet kan worden gezegd dat uit deze bepaling volgt dat de inroeper het risico van misbruik van de middelen voor het aanmaken van elektronische handtekeningen draagt zolang niet is bewezen van wie de ondertekening afkomstig is. Deze bepaling heeft slechts betrekking op de bewijskracht van een ondertekend stuk waarvan de ondertekening stellig wordt ontkend. Hoe je haar ook uitlegt, als degene die zich beroept op het ondertekende stuk kan bewijzen dat de middelen voor het aanmaken van elektronische handtekeningen van een bepaald persoon zijn gebruikt voor het ondertekenen van het stuk en de vermeende ondertekenaar ontkent zelf die middelen te hebben gebruikt, of een ander deze heeft laten gebruiken voor het ondertekenen van de betreffende verklaring, kan de vraag rijzen of dit gebruik kan worden toegerekend aan de vermeende ondertekenaar.

Uit het *COVA*-arrest<sup>31</sup> volgt dat de vraag wie het risico draagt van misbruik van middelen voor het aanmaken van een elektronische handtekening moet worden beantwoord aan de hand van de concrete omstandigheden van het geval, waarbij in het bijzonder van belang is aan wie valt toe te rekenen dat de middelen in de macht van de onbevoegde gebruiker daarvan zijn gekomen. Is de onbevoegde in dienst van de vermeende ondertekenaar of staat hij anderszins in relatie tot de vermeende ondertekenaar, waardoor hij gemakkelijker dan willekeurige derden toegang tot de middelen heeft kunnen verkrijgen, dan zal er in het algemeen grond zijn voor een dergelijke toerekening aan de vermeende ondertekenaar, nu dan in beginsel mag worden aangenomen dat het misbruik aan gebrek aan diens zorg te wijten is. Dit zal slechts anders zijn in door de vermeende afzender te stellen en te bewijzen omstandigheden die een zodanig gebrek aan zorg uitsluiten. Partijen kunnen ter zake een afwijkende afspraak maken.

Stelt de inroeper dat het misbruik van de middelen voor het aanmaken van elektronische handtekeningen moet worden toegerekend aan de vermeende ondertekenaar en dat de vermeende ondertekenaar gebonden is aan de ondertekende verklaring, dan zal hij omstandigheden moeten stellen en zo nodig bewijzen die deze stelling kunnen dragen. Zo zal hij bijvoorbeeld om de stelling te kunnen onderbouwen dat onder de gegeven omstandigheden toerekening aan de vermeende ondertekenaar in het licht van het *COVA*-arrest op haar plaats is, de feitenrechter er zo nodig van moeten kunnen overtuigen dat:

- a. voor het aanmaken van de elektronische handtekening gebruik is gemaakt van middelen die toebehoren aan de vermeende ondertekenaar; en

- b. deze middelen zijn misbruikt door een medewerker van de vermeende ondertekenaar of iemand die in zodanige relatie tot de vermeende ondertekenaar stond dat hij gemakkelijker dan willekeurige derden toegang tot de middelen heeft kunnen krijgen (zoals een echtgenoot of een partner van de vermeende ondertekenaar).

Als de inroeper de feitenrechter ervan moet overtuigen dat zich omstandigheden hebben voorgedaan die toerekening van het misbruik van de middelen voor ondertekening aan de vermeende ondertekenaar rechtvaardigen, kan hij bij stellige ontkening van de elektronische ondertekening door degene aan wie deze middelen toebehoren, als bewijsmiddel het bestand met de ondertekende verklaring inbrengen. Denk aan het geval dat in een elektronische betaalopdracht het betaalrekeningnummer en de naam van een medewerker van de vermeende ondertekenaar als rekeningnummer en naam van de begunstigde staan vermeld. Dat zou erop kunnen wijzen dat de betreffende medewerker de middelen heeft gebruikt, en bij onbevoegdheid heeft misbruikt, om de elektronische betaalopdracht te (laten) ondertekenen.

Ik wijs in dit verband ook op de bijzondere wettelijke regeling voor betalingstransacties. Art. 7:528 BW brengt mee dat de betaaldienstverlener van de betaler de debitering van de betaalrekening van de betaler ongedaan moet maken als blijkt dat de betaalopdracht zonder instemming van de betaaldienstgebruiker is gegeven. Krachtens art. 7:529 BW geldt een afwijkende regeling als de verliezen met betrekking tot niet-toegestane betalingstransacties zich hebben voorgedaan doordat de betaler frauduleus heeft gehandeld of opzettelijk of met grove nalatigheid een of meer verplichtingen uit hoofde van art. 7:524 BW niet is nagekomen. Art. 7:524 BW bevat onder meer de verplichting van de betaaldienstgebruiker om, zodra hij een betaalinstrument ontvangt, in het bijzonder alle redelijke maatregelen te nemen om de veiligheid van de persoonlijke beveiligingskenmerken ervan te waarborgen. Tot de veiligheidskenmerken van het betaalinstrument horen ook middelen die worden gebruikt om een betaalopdracht elektronisch te ondertekenen, zoals de pincode.

Uit art. 7:528-529 BW vloeit voort dat misbruik van de middelen voor het elektronisch ondertekenen van een betaalopdracht voor rekening van de betaaldienstverlener komt, tenzij deze de omstandigheden als bedoeld in art. 7:529 BW stelt en zo nodig bewijst die toerekening van het misbruik aan de betaaldienstgebruiker rechtvaardigen. In wezen is dit een toerekeningsregeling die ruimer is dan de toerekeningregel verwoord door de Hoge Raad in het hiervoor besproken *COVA*-arrest. In de praktijk komt deze wettelijke regeling erop neer dat de betaaldienstverlener van de betaler het risico van misbruik van betaalinstrumenten draagt, tenzij hij kan aantonen dat de betaler frauduleus heeft gehandeld of grof nalatig is geweest als het gaat om de bescherming van het betaalinstrument tegen onbevoegd gebruik.

31. HR 19 november 1993, ECLI:NL:1993:ZC1148, NJ 1994/622, r.o. 5.2.



#### 14 Afrondend

In de titel van dit artikel stel ik de vraag: 'Is art. 159 lid 2 Rv toe aan modernisering?' Deze vraag zou ik thans ontkennend willen beantwoorden. Ik denk dat toepassing van deze bepaling tot billijke uitkomsten kan leiden, ook als er sprake is van een stellige ontkenning van elektronische ondertekening, mits haar reikwijdte wordt beperkt tot de waarheid van de verklaring vervat in het ondertekende stuk c.q. elektronische bestand waarmee de elektronische handtekening verbonden is.

Het zou naar mijn oordeel wel aanbeveling verdienen om nogmaals te overwegen of in art. 159 Rv een bepaling dient te worden opgenomen met betrekking tot de stellige ontkenning van de elektronische handtekening, dit ter bevordering van de rechtszekerheid in het huidige informatiemaatschappelijk verkeer.

Ik verwacht niet dat art. 159 Rv zal worden aangepast. In het advies van de expertgroep Modernisering Burgerlijk Bewijsrecht van april 2017 staat in paragraaf 4.4.1 (randnummer 163): 'Ten aanzien van de bewijskracht van akten van en van de bewezenverklaring in een strafvonnis bevat deze afdeling in § 2 voorschriften die naar onze mening geen herziening vergen.' Het ter consultatie gepubliceerde Voorstel tot aanpassing van het Wetboek van Burgerlijke Rechtsvordering in verband met de vereenvoudiging en modernisering van het bewijsrecht bevat geen voorstel tot wijziging van art. 159 Rv. Blijkbaar wordt de behoefte aan het creëren van meer rechtszekerheid met betrekking tot de stellige ontkenning van een elektronische ondertekening door de wetgever niet gevoeld.