

VU Research Portal

De betrouwbaarheid van elektronische gegevens als bewijsmiddel in het Nederlandse, Duitse en Amerikaanse civiele bewijsrecht

van Stekelenburg, M.C.

2010

document version

Publisher's PDF, also known as Version of record

[Link to publication in VU Research Portal](#)

citation for published version (APA)

van Stekelenburg, M. C. (2010). *De betrouwbaarheid van elektronische gegevens als bewijsmiddel in het Nederlandse, Duitse en Amerikaanse civiele bewijsrecht*. Eburon.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

E-mail address:

vuresearchportal.ub@vu.nl

Samenvatting

Hoofdstuk 1

Dit onderzoek gaat over de bewijskracht van elektronische bewijsmiddelen in het Nederlandse, Duitse en Amerikaanse civiele bewijsrecht. Met de toename van elektronische middelen in het maatschappelijk en economisch verkeer, worden deze middelen steeds vaker gebruikt als bewijs om feiten op te baseren en rechten aan te tonen. Nu aan rechters gevraagd wordt dit nieuwe soort bewijsmiddelen op betrouwbaarheid te waarderen is het de vraag welke betrouwbaarheidscriteria zij hierbij aanleggen. Temeer daar de risico's die aan het gebruik van elektronische gegevens als bewijsmiddel niet altijd bekend zijn.

De probleemstelling in dit onderzoek luidt: *welke concrete criteria worden in het Nederlandse, Duitse en Amerikaanse civiele bewijsrecht gesteld aan elektronische gegevens ten aanzien van de borging van de betrouwbaarheid van deze gegevens om de door partijen gestelde feiten te kunnen bewijzen en met welke abstracte criteria moeten ontwikkelaars van gegevensverwerkende/-producerende technologieën daarnaast rekening houden met het oog op het ontwikkelen van nieuwe technologieën zodat de verwerkte/geproduceerde elektronische gegevens voldoende betrouwbaar zijn als bewijsmiddel?* Deze probleemstelling is tweeledig. In de eerste plaats onderzoek ik de concrete criteria die in de huidige wetgeving en jurisprudentie worden gesteld ter beoordeling van elektronische gegevens als bewijsmiddel. In de tweede plaats onderzoek ik door middel van het antwoord op de eerste vraag, welke meer abstracte criteria herleid kunnen worden uit de concrete criteria met het oog op aanbevelingen voor ontwikkelaars.

Centraal in dit onderzoek staat het begrip bewijzen. Een complicerende factor is het feit dat onder Nederlands, Duits en Amerikaans recht het begrip bewijzen verschillende betekenissen kan hebben al gelang het soort nationaal recht. Voor dit onderzoek is dat echter geen probleem. Het beoordelen van bewijsmiddelen op hun betrouwbaarheid is een taak van feitelijke aard. In dit onderzoek maak ik de aanname dat er een gemeenschappelijk idee bestaat over de vraag wanneer een bewijsmiddel voldoende betrouwbaar is en dat rechters bij de beoordeling van bewijsmiddelen op hun betrouwbaarheid dezelfde risico's onderkennen. Aanwijzingen hiertoe zijn te vinden in het feit dat soortgelijke zaken tot soortgelijke uitkomsten hebben geleid op soortgelijke overwegingen in voornamelijk de Duitse en Amerikaanse rechtspraak. In het

Nederlandse recht wordt uitgegaan dat de rechter een “*redelijk mate van zekerheid*” moet hebben verkregen om te kunnen stellen dat feiten zijn bewezen. In het Duitse recht is § 286 ZPO leidend. Dit artikel stelt namelijk: “*den Richter unter Berücksichtigung des gesamten Inhalts der Verhandlungen und des Ergebnisses einer etwaigen Beweisaufnahme nach freier Überzeugung zu entscheiden, ob eine tatsächliche Behauptung für wahr oder für nicht wahr zu erachten sei.(...)*”. Doorslaggevend is hier de overtuiging van de rechter. In het Amerikaanse recht geldt in beginsel de “*preponderance of evidence*”. Hierbij dient de jury te oordelen dat de waarschijnlijkheid van het bestaan van een bepaald feit is groter de waarschijnlijkheid dat dit feit niet bestaat.

Hoofdstuk 2

In hoofdstuk twee wordt het onderzoeksobject elektronische gegevens nader gedefinieerd en in een kader geplaatst. Elektronische gegevens zijn feiten, concepten of instructies die op elektronische wijze zijn vastgelegd en welke bruikbaar zijn voor communicatie, interpretatie, verwerking of uitvoering door mensen of door een geautomatiseerd werk. De kleinste bouwstenen van elektronische gegevens zijn tekens. Dit zijn symbolen, cijfers, letters en allerlei andere vormen en andere tekens waarmee gegevens kunnen worden weergegeven en verwerkt. Zowel tekens als elektronische gegevens hebben een objectief karakter. Gegevens kunnen informatie vormen als er betekenis aan gegeven wordt. Daarmee krijgt informatie een subjectie karakter.

Elektronische gegevens kunnen de vorm hebben van code en van data. Code bestaat uit instructies die op elektronische wijze zijn vastgelegd en welke bruikbaar zijn voor het initiëren, het op gang houden en het beëindigen van een proces door een geautomatiseerd werk. Data bestaat uit feiten en concepten (echter niet uit instructies) die op elektronische wijze zijn vastgelegd en welke bruikbaar zijn voor communicatie, interpretatie, verwerking of uitvoering door mensen of door een geautomatiseerd werk. De rechtvaardiging voor het onderscheid in code en data ligt in het verschil in functie. Code bevat aansturingregels voor een machine en in de code ligt daarmee het “gedrag” van een machine besloten. Data daarentegen bevat in beginsel slechts informatie. Ook voor het recht is dit onderscheid van belang en dan vooral in verband met de kwalificatie van een geschrift, een *elektronisches Dokument* of een *writing*. Er is ook een kanttekening te plaatsen bij het onderscheid tussen code en data; het onderscheid is namelijk niet altijd even hard. Soms ligt code besloten in data (bijvoorbeeld broncode, hoewel deze zonder compilatie of interpretatie uitvoerbaar is) of ligt data besloten in code (bijvoorbeeld in uitvoerregels of printregels).

Hoofdstuk 3

In hoofdstuk drie ga ik in op de beveiliging van elektronische gegevens. Het rechtsgoed bewijzen staat hier centraal. Om het rechtsgoed bewijzen te

waarborgen, dienen de authenticiteit en de integriteit te worden gewaarborgd. Authenticatie en integriteit staan echter in de computerwetenschap en de rechtswetenschap in een andere verhouding tot elkaar. In de computerwetenschap heeft authenticatie betrekking op mensen en integriteit op gegevens. In de rechtswetenschap kan authenticatie betrekking hebben op zowel mensen als gegevens. Nader gespecificeerd heeft integriteit betrekking op rechtsoBJECTEN (gegevens) en ligt het rechtssubject besloten in de identiteit. Het waarborgen van de authenticatie van personen kan door middel van het bewijzen van de identiteit van een persoon. Klassiek is de indeling die gemaakt wordt in de computerbeveiliging, namelijk: iets dat een persoon weet (wachtwoord, code), iets dat een persoon in zijn bezit heeft (ID-kaart, RFID-chip) en iets dat een persoon is (DNA, vingerafdruk, stem). Het waarborgen van de integriteit van gegevens kan door middel van verschillende soorten van versleuteling, zoals door middel van cryptografische hash functies, symmetrische versleuteling, asymmetrische versleuteling, dubbele asymmetrische versleuteling of een combinatie van de verschillende soorten versleuteling.

Hoofdstuk 4

In hoofdstuk vier onderzoek ik de betrouwbaarheid van elektronische gegevens in het Nederlandse civiele bewijsrecht. De betrouwbaarheidswaardering kan niet onderzocht worden zonder de processuele positie van de rechter te onderzoeken. Een belangrijk uitgangspunt in het civiele procesrecht is de lijdelijkheid van de rechter en de autonomie van partijen. De partijen bepalen de omvang van hun geschil en de rechter is niet bevoegd om de rechtsfeiten aan te vullen; enkel de rechtsgronden mogen door de rechter aangevuld worden. Toch zijn er grenzen aan de autonomie van partijen. Deze grenzen vinden hun weg in de vorm van bewijsvermoedens. De wet of een overeenkomst stelt dan regels betreffende de bewijskracht van bepaalde feitelijke gegevens. Van belang voor dit onderzoek is daarin het bewijsvermoeden van de betrouwbaarheid van de methode van authenticatie van de elektronische handtekening.

Een tweede belangrijk uitgangspunt in het Nederlandse bewijsrecht is de theorie van de vrije bewijsleer. Deze leer omvat twee principes, namelijk een open stelsel van bewijsmiddelen als het de toelating van bewijs betreft en het principe van de vrije bewijswaardering. Een open stelsel van bewijsmiddelen houdt in dat alle bewijs wordt toegelaten om feiten of rechten aan te tonen. De vrije bewijswaardering houdt in dat de rechter vrij is om de bewijsmiddelen ambtshalve op betrouwbaarheid te waarderen. Als in de jurisprudentie gezocht wordt naar aanknopingspunten waarom een rechter bewijs voldoende betrouwbaar (of juist onvoldoende betrouwbaar) acht om feiten als aangetoond te beschouwen, dan zijn hiervoor geen criteria te vinden. De oorzaak hiervan kan gelegen zijn in de motiveringsplicht van het bewijsoordeel

die de rechter alleen heeft als het debat van partijen daartoe aanleiding geeft. Een tweede oorzaak kan gelegen zijn in de processuele houding die de rechter heeft. Dit maakt het moeilijk te achterhalen welke criteria een rechter ten grondslag legt aan zijn bewijswaardering. De weinige jurisprudentie concentreert zich op de vraag wie moet aantonen en met welke middelen of een e-mail is ontvangen. De jurisprudentie is eenduidig: het is bij betwisting dat een e-mail ontvangen is, aan de verzendende partij om te bewijzen dat de wederpartij de e-mail heeft ontvangen. Slechts in één door mij gevonden uitspraak geeft een rechter expliciet een drietal criteria op grond waarvan de rechter voldoende overtuigd is van de ontvangst van de gegevens. Deze zijn:

- verzender heeft een e-mail ontvangen welke is verzonden vanaf hetzelfde e-mailadres als waar zij een eerdere e-mail heeft gezonden.
- verzender heeft een e-mail ontvangen met dezelfde referentie als de e-mail die zij heeft verzonden.
- verzender heeft een e-mail ontvangen met een inhoud die moeilijk anders te begrijpen is dan als een reactie op de door haar gezonden e-mail.

In de wet zijn enkele aanknopingspunten te vinden die de bewijskracht van elektronische bewijsmiddelen regelen of beïnvloeden. Ten eerst regelt art. 6:227a BW de voorwaarden waaronder ook door middel van gebruikmaking van elektronische gegevens aan een wettelijk eis van schriftelijkheid kan worden voldaan als het overeenkomsten betreft. Het blijft echter onduidelijk of aan het schriftelijkheidsvereiste kan worden voldaan door gebruik te maken van elektronische gegevens in die gevallen waarin art. 6:227a BW niet van toepassing is. Zonder te motiveren stelt de Rechtbank Amsterdam dat voldaan is aan de schriftelijkheidsvereiste van art. 6:82 BW als een ingebrekestelling per e-mail wordt gedaan.⁵⁰⁵

Een tweede artikel dat van belang is, is art. 3:15a BW dat de elektronische handtekening definieert en een abstracte invulling geeft aan de criteria waaraan de methode van authenticatie moet voldoen om voldoende betrouwbaar te zijn. Is eenmaal vastgesteld dat de methode van authenticatie voldoende betrouwbaar is, dan worden de rechtsgevolgen van de elektronische handtekening gelijkgesteld met de rechtsgevolgen van een handgeschreven handtekening. Echter, de rechter heeft de bevoegdheid om de rechtsgronden ambtshalve aan te vullen. Art. 3:15 BW geeft de rechter onder omstandigheden de mogelijkheid om ambtshalve de methode van authenticatie te beoordelen. Daarmee kan de rechter invloed uitoefenen op de uitkomst of de elektronische handtekening dezelfde rechtsgevolgen krijgt als de handgeschreven handtekening en daarmee tevens invloed hebben op de vraag of er een elektronische onderhandse akte tot stand is gekomen. De zekerheid die de

⁵⁰⁵ Rb. Amsterdam van 21 november 2007, *LJN* BC0337, r.o. 4.11 (Canon Nederland N.V. / G-SUS Wholesale and Design B.V.)

elektronische onderhandse akte als bewijsmiddel met dwingende bewijskracht zou moeten bieden, is daarmee een schijnzekerheid.

Zowel het open stelsel van bewijsmiddelen en de vrije bewijswaardering kennen enkele wettelijke uitzonderingen. Een voor dit onderzoek belangrijke uitzondering op de vrije bewijswaardering is de elektronische variant van de onderhandse akte. Deze kan tot stand komen door een hiervoor genoemde overeenkomst die in elektronische vorm is opgemaakt (art 6:277a BW) te ondertekenen met een (geavanceerde/gekwalificeerde) elektronische handtekening (art 3:15a BW). De gelijkstellingsbepaling van art. 6:227a BW maakt het mogelijk om via elektronische weg aan het schriftelijkheidsvereiste te voldoen, terwijl art. 3:15a BW de rechtsgevolgen van de elektronische handtekening onder omstandigheden gelijkschakelt met de rechtsgevolgen van een gewone handtekening. De combinatie van de elektronische varianten van het geschrift en de handtekening kunnen een elektronische onderhandse akte vormen waaraan dwingende bewijskracht moet worden toegekend.

Naast de elektronische onderhandse akte kan er gebruik worden gemaakt van bewijsovereenkomsten. Door middel van de bewijsovereenkomst kan ingegrepen worden in het wettelijke bewijsrecht. Zo kan bijvoorbeeld worden overeengekomen dat logbestanden worden uitgesloten als bewijsmiddel, dat aan communicatie tussen computers dwingende bewijskracht wordt gegeven of dat een bepaalde partij de bewijslast heeft indien software inbreuk maakt op rechten van die partij. Gezien het feit dat het partijen vrij staat om bewijsovereenkomsten af te sluiten, kunnen zij zelf de inhoud van de bewijsovereenkomst regelen.

Hoofdstuk 5

Het Duitse civiele bewijsrecht is onderdeel van het civiele procesrecht en is gecodificeerd in de *ZPO*. Uitgangspunt in het procesrecht is de lijdelijkheid van de rechter en de autonomie van partijen. Deze hebben hun weg gevonden in een aantal maximen en in de heersende leer is sprake van een sterk *Dispositionmaxime* en een *Beibringungsmaxime*. Uitzonderingen hierop kunnen gevonden worden in de wet en in verschillende soorten *Beweisvermutungen*.

In het Duitse recht is sprake van een gesloten stelsel van bewijsmiddelen, ook wel *Strengbeweis* genoemd. Dit wil zeggen dat in beginsel alleen bewijsmiddelen die vallen onder de wettige bewijsmiddelen worden toegelaten om feiten aan te tonen. Slechts voor het vaststellen van feiten waarover partijen niet van mening verschillen en die niet de kern van de zaak betreffen (zoals het vaststellen van procedurele eisen, procedurele vragen en de behandeling van de voorwaarden voor vergoeding van proceskosten) worden niet bij wet omschreven bewijsmiddelen worden toegelaten, oftewel dan is er

sprake van *Freibeweis*. Ook indien er sprake is van zogenaamde *Glaubhaftmachung*, geldt het *Freibeweis*. Binnen het stelsel van wettige bewijsmiddelen (*Strengbeweis*) bestaan vijf bewijsmiddelen: het *Augenscheinsbeweis* (zintuiglijke waarneming door de rechter), *Zeugensbeweis* (getuigenbewijs), *Sachverständigenbeweis* (deskundigenbewijs), *Urkundenbeweis* (akten) en *Parteivernehmung* (getuigenis door de procespartijen). Voor de toelating dienen code en data gekwalificeerd te worden als een van de vijf soorten wettelijk bewijsmiddelen. Zowel code als data kunnen worden gekwalificeerd als *Augenscheinsbeweis*. Daarbij kunnen zowel code als data gekwalificeerd worden als *elektronisches Dokument*, dat een species is van de *Augenschein*. Deze laatste kwalificatie is van belang voor de bewijswaardering.

Als een bewijsmiddel eenmaal is toegelaten, zal dit bewijsmiddel door de rechter gewaardeerd moeten worden op betrouwbaarheid. In beginsel geldt dat de rechter op grond van § 286 ZPO vrij is in de beoordeling van het bewijs. De rechter dient daarbij persoonlijk overtuigd te zijn van de waarheid of onwaarheid van de feiten. Een enkele (hoge) waarschijnlijkheid is niet voldoende. Onder invloed van meer recente rechtspraak lijkt de jurisprudentie echter steeds meer aan te sturen op een symbiose van de subjectieve en persoonlijke overtuiging van de rechter en objectieve waarschijnlijkheid.

In de rechtspraak blijft het voor wat betreft de de bewijswaardering van code stil. Voor wat betreft data zijn er wel enige aanknopingspunten te vinden in de rechtspraak. Vooral met betrekking tot de identificatie van personen wordt het volgende duidelijk. Indien een persoon een account heeft (e-mail / eBay) welke niet van extra beveiligingseisen is voorzien, dan kan daarmee niet bewezen worden dat de persoon die het account gebruikte ook daadwerkelijk de persoon is van wie het account is. De veiligheidsstandaard is namelijk niet hoog genoeg. In gevallen waarbij meerdere elementen tot de conclusie kunnen leiden dat degene die een bepaalde verklaring heeft gestuurd daadwerkelijk degene is van wie gesteld wordt dat deze de verklaring heeft geschreven, dan kan een rechter de data wel als voldoende betrouwbaar kwalificeren. Bij deze omstandigheden kan gedacht worden aan een combinatie van de inhoud van het bericht, de namen onder het bericht, de kennis die partijen hebben, feiten en gebeurtenissen die spelen buiten het elektronische berichtenverkeer om, enzovoorts. De bewijskracht hangt niet af van één element, maar wordt groter naarmate meerdere elementen in hun onderlinge samenhang tot de conclusie kunnen leiden dat het bewijsmiddel voldoende betrouwbaar is en zodoende voldoende bewijskracht heeft dat deze de gestelde feiten kan onderbouwen.

Op de hoofdregel dat de rechter vrij is in het waarderen van het bewijs is de *Urkunde* een wettelijke uitzondering. Daarbij wordt een onderscheid gemaakt in *öffentliche Urkunden* en *private Urkunden* die is ondertekend. Voordat

bewijskracht wordt toegekend geldt voor beide dat deze geen gebreken mogen vertonen en dat er een controle op echtheid plaatsvindt. Ook het *elektronisches Dokument* neemt een bijzondere plaats in binnen het Duitse recht. Als bewijsmiddel wordt deze toegelaten onder het *Augenscheinsbeweis*, maar binnen de bewijswaardering krijgt deze, als deze is voorzien van een gekwalificeerde elektronische handtekening, dwingende bewijskracht. Als een *elektronisches Dokument* niet voorzien is van een gekwalificeerde elektronische handtekening dan is het aan de rechter om op grond van § 286 ZPO dit bewijsmiddel te waarderen.

Als de code of data voorzien is van een gekwalificeerde elektronische handtekening dan zijn de regels betreffende de *private Urkunde* voorzien van handtekening van toepassing op het *elektronisches Dokument*. Het krijgt dan dwingende (formele) bewijskracht. In de gevallen waarin code en data niet voorzien is van een gekwalificeerde elektronische handtekening mogen deze door de rechter gewaardeerd worden op hun betrouwbaarheid

Tot slotte kan de bewijsovereenkomst een rol spelen om de bewijspositie te versterken. In tegenstelling tot het Nederlandse recht is de bewijskrachtovereenkomst in strijd met de bevoegdheid van de rechter om bewijs naar alle vrijheid en eigen inzicht te waarderen. Er kan alleen gebruik worden gemaakt van de bewijsmiddelenovereenkomst, de bewijslastovereenkomst en het regelen van tegenbewijs.

Hoofdstuk 6

Het Amerikaanse civiele bewijsrecht is in tegenstelling tot het Nederlandse en Duitse en bewijsrecht niet enkel onderdeel van het civiele procesrecht, maar kent een eigen bestaan en is van toepassing op zowel het civiele, het administratieve als ook het strafrecht. Het Amerikaanse rechtstelsel kent haar oorsprong in het Engelse recht. De afgelopen eeuwen heeft zij haar eigen ontwikkeling doorgemaakt, maar toch zijn een groot aantal bewijsregels nog steeds terug te vinden in het moderne Amerikaanse bewijsrecht. In 1971 zijn de bestaande rechtsregels uit de jurisprudentie gecodificeerd en samengebracht in de *Federal Rules of Evidence (FRE)*.

Van groot belang voor de ontwikkeling van het Amerikaanse bewijsrecht is de juryrechtspraak geweest. Daardoor heeft zich een stelsel kunnen ontwikkelen waarbij de rechter tijdens de bewijstoelatingsfase uitgebreid kan onderzoeken of de bewijsmiddelen voldoen aan wettelijke eisen, waarna de jury in de bewijstoelatingsfase nader kan ingaan op de bewijswaardering.

Het Amerikaanse recht kent voor de toelating een open stelsel van kwalitatieve bewijsmiddelen. Dit wil zeggen dat alle ingebrachte bewijsmiddelen door de rechter worden getoetst aan een aantal kwalitatieve eisen, namelijk: *relevancy*,

exclusion, hearsay, authentication en best evidence.

Relevancy (Rule 401 FRE e.v.) houdt in dat een bewijsmiddel enkel wordt toegelaten als deze heeft *“any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.”* Aangezien het sterk afhankelijk is van de feiten, vallen er op basis van deze regel geen algemene uitspraken te doen waaraan bewijsmiddelen moeten voldoen.

Exclusion (Rule 403 FRE e.v.) houdt in dat onder bepaalde omstandigheden bewijsmiddelen die relevant zijn, toch uitgesloten kunnen worden. Hiervoor noemen de FRE een aantal uitsluitingsgronden, namelijk: *“if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.”* Enkel op basis van deze gronden kunnen bewijsmiddelen uitgesloten worden. Net als bij *relevancy* is hierbij het probleem dat het sterk afhangt van de feiten of een bewijsmiddel wordt uitgesloten of niet.

Hearsay (Rule 801 FRE e.v.) houdt in dat bewijs enkel mag worden toegelaten als er geen sprake is van een *“a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted.”* De ratio van deze regel is dat verklaringen gedaan buiten de rechtszaal per definitie onbetrouwbaar zijn; aangenomen wordt dat er ruis optreedt als een persoon gebeurtenissen observeert, onthoudt en verklaart. Verklaringen dienen daarom te worden afgelegd onder ede, ten overstaan van een jury of rechter en met de mogelijkheid van ondervraging door de tegenpartij. Enkel op grond van in de *FRE* genoemde uitzonderingen mogen verklaringen afgelegd buiten de rechtszaal worden meegenomen in de rechtszaak. Voor code en door computers gegenereerde data geldt dat er geen problemen zijn om deze toe te laten, omdat er geen sprake kan zijn van *hearsay*.⁵⁰⁶ Voor het toelaten van door mensen gegenereerde data geldt dat deze niet als *hearsay* mag worden gekwalificeerd of dat (als er sprake is van *hearsay*) deze onder een uitzondering als genoemd onder *Rule 803 FRE* of *Rule 804 FRE* moet vallen. Door elektronische documenten is hier sprake van als:

- De verklaring direct nadat de gebeurtenis zich heeft voorgedaan worden opgetekend. Wat onder direct wordt verstaan is niet geheel duidelijk. Ik kan mij voorstellen dat dit afhankelijk is van de omstandigheden. In één van de onderzochte zaken geldt dat onder direct ook werd verstaan de optekening die 23 minuten na de gebeurtenis werd gedaan (*Rule 803(1) FRE*).

⁵⁰⁶ Enkel moet aangetoond worden dat de computer correct werkte.

- De verklaring gaat over de geestelijke gesteldheid, emotie of fysieke conditie (als intentie, plan, motief, ontwerp, mentaal gevoel, pijn and lichamelijke gezondheid) van de declarant. Hieronder mogen geen verklaringen zijn welke gaan over het geheugen of overtuiging om een gesteld feit te bewijzen, tenzij gerelateerd aan de uitvoering, herroeping of identificatie van de wil van de declarant. (Rule 803(3) FRE) .
- Verklaringen welke door de getuige zijn opgetekend en die de getuige (deels) is vergeten (Rule 803(5) FRE).
- De verklaringen vallen onder de business record exception: ze zijn opgemaakt tijdens de gebruikelijke werkzaamheden van het bedrijf, gelijktijdig met de met deze gebruikelijke werkzaamheden en het moet gebruikelijk zijn voor het bedrijf om hiervan aantekeningen te maken (Rule 803(6) FRE).
- De verklaring aan te merken is als een market report of een commercial publication waarop het publiek mag vertrouwen ((Rule 803(17) FRE).

Authentication (Rule 901 FRE e.v.) betekent dat een bewijsmiddel is “*sufficient to support a finding that the matter in question is what it proponent claims*”. Aangevoerd moet worden dat een bewijsmiddel daadwerkelijk is wat gesteld wordt dat het is en dat aangetoond wordt van wie het afkomstig is. Authenticatie kan op vele manieren plaatsvinden. *Rule 901(b) FRE* geeft daartoe een groot aantal voorbeelden, die overigens niet limitatief zijn. In paragraaf 6.8 wordt nader uitgewerkt welke kwaliteiten van een bewijsmiddel maken dat deze aan authenticatie voldoen. De wijze van authenticeren en identificeren van een bewijsmiddel is sterk afhankelijk van het bewijsmiddel en daarom bestaat er niet één methode van *authentication*. Aangezien code en data verschillende functies hebben en op verschillende wijze tot stand komen, kunnen beide op verschillende wijze worden geauthenticeerd. Methoden van *authentication* worden in de FRE genoemd, maar deze zijn niet uitputtelijk. Daarom moeten methoden van authenticatie zowel in de FRE als in de jurisprudentie gezocht worden. De FRE noemt een aantal methoden van *authentication*, waarvan de volgende voor zowel code als data van belang zijn: *testimony of witness with knowledge* (Rule 901(b)(1) FRE), *comparison by trier or expert witnesses* (Rule 901(b)(3) FRE), *distinctive characteristics and the like* (Rule 901(b)(4) FRE), *process or system* (Rule 901(b)(9) FRE). Voor enkel data zijn ook de *public records or reports* (Rule 901(b)(7) FRE) van belang. In de rechtspraak zijn methoden van authenticatie ontwikkeld die in het verlengde liggen van bovengenoemde methoden of methoden die juist geheel op zichzelf staan. Kenmerkend in de rechtspraak is dat *authentication* en *identification* veelal worden beoordeeld aan de hand van meerdere kenmerken en dan vaak in hun onderling verband. Daar de rechtspraak ziet op concrete juridische problemen, is er een onderscheid gemaakt op grond van de toepassingen als elektronisch bewijsmiddel worden ingezet. Paragraaf 6.8.6 gaat nader in op de eisen die aan *authentication* en *identification* worden gesteld. Deze zullen in

hoofdstuk 6 nader worden geanalyseerd.

Best evidence (Rule 1001 FRE e.v.) is de regel die ziet op het feit dat in beginsel alleen originele *writings, recordings* en *photographs* worden toegelaten. *Duplicates* en secundaire bewijsmiddelen worden toegelaten als het origineel niet kan worden overlegd en dan alleen onder voorwaarden die in de *FRE* omschreven zijn. In beginsel dient het meest originele *writing, recording* of *photograph* ingebracht te worden als bewijsmiddel. *Duplicates* worden pas toegelaten als daarvoor in de *FRE* omschreven gronden voor bestaan. Hoewel er bezwaren zouden kunnen bestaan voor elektronische kopieën van *writings, recordings* of *photographs*, omdat deze beschouwd kunnen worden als *duplicates*, zijn er in de rechtspraak geen problemen te vinden die het zijn van *duplicate* als argument gebruiken om te voorkomen dat deze niet toegelaten worden als bewijsmiddel. Van belang is daarbij echter dat er geen oprechte twijfel mag zijn over de authenticiteit van het origineel of het onrechtvaardig zou zijn het *duplicate* toe te laten in plaats van het *original*.

Bewijswaardering en bewijstoelating zijn in het Amerikaanse recht strikt van elkaar gescheiden, onder invloed van het systeem waarbij de rechter en de jury ieder hun eigen taken hebben in een rechtszaak. In het Amerikaanse recht worden geen regels gesteld aan de bewijswaardering. De bewijswaardering is geheel vrij aan de jury (of aan de rechter in het geval dat de zaak volledig door de rechter wordt behandeld) en beperkingen, zoals bijvoorbeeld dwingende bewijskracht van bepaalde bewijsmiddelen zoals het Nederlandse en Duitse recht kennen, bestaan niet in het Amerikaanse recht.

Ook de bewijsovereenkomst is een fenomeen dat in het Amerikaanse recht zo goed als niet voorkomt en mocht deze voorkomen dan is deze waarschijnlijk nietig op grond van strijd met het recht (strijd met de bevoegdheden van de rechter) en/of het feit dat de rechter niet gebonden kan worden aan afspraken tussen partijen.

Elektronische bewijsmiddelen dienen aan een vijftal eisen te voldoen, namelijk: relevancy, exclusion, hearsay, authentication en best evidence. Voor zowel code als data geldt dat aan de eisen van relevancy en exclusion vooraf geen eisen gesteld kunnen worden omdat relevancy en exclusion afhankelijk zijn van het feitencomplex en deze eisen geen aanknopingspunten geven voor de intrinsieke kwaliteiten van bewijsmiddelen.

Hoofdstuk 7

In hoofdstuk zeven worden de conclusies getrokken. Uit de jurisprudentie en de wetgeving wordt duidelijk dat het bij de betrouwbaarheid vooral gaat om de authenticatie van personen. Elektronische gegevens zijn wel voldoende betrouwbaar als dit blijkt uit meerdere kenmerken zoals: de naam van de

ondertekenaar, het bevatten van de naam van de verzender in het e-mailadres, het bevatten van de naam van de verzender in het replyadres, het gebruik van een nickname door een bepaald persoon, het gebruik van afkortingen van de naam van de persoon, het gebruik van een voor de persoon kenmerkende schrijfstijl, een inhoud die alleen aan de schrijver en de ontvanger bekend is, de inhoud verwijst naar specifieke informatie waar een selecte groep mensen kennis van heeft, een verzoek van de ontvangende partij wordt door de verzendende partij opgevolgd en dat blijkt uit de gegevens, verklaring dat eerdere gegevens ontvangen zijn, getuigenis van een persoon die heeft gezien dat de verzender inderdaad de aangewezen persoon is. Om aan te tonen dat gegevens van een aangewezen persoon afkomstig zijn, is een enkel feit of gegeven niet voldoende. Het minimaal aantal aanknopingspunten om het bewijsmiddel voldoende betrouwbaar te achten is niet met zekerheid te stellen, maar lijkt een glijdende schaal te zijn. In een enkel geval zijn twee omstandigheden voldoende, maar meestal moeten er minstens drie verschillende omstandigheden zijn waaruit moet blijken of een bewijsmiddel voldoende betrouwbaar is. Dit is in lijn met het principe van *two factor identification* uit de computersecurity.

De bewijskracht kan ook dwingend zijn. In Nederland is sprake van materiële rechtskracht en in Duitsland van formele rechtskracht. Deze geldt voor elektronische geschriften en *elektronische Dokumenten* die ondertekend zijn met een gekwalificeerde elektronische handtekening. Voor het Nederlandse recht heeft de wet de mogelijkheid opengelaten om gebruik te maken van de geavanceerde of zelf de gewone elektronische handtekening.

Bewijs kan ook onvoldoende betrouwbaar zijn. De bewijsmiddelen betreffen dan gegevens die verstuurd zijn vanaf accounts waarbij er onvoldoende zekerheid bestaat van wie de gegevens afkomstig zijn. Hierbij betreft het accounts welke onder een pseudoniem zijn aangemaakt, maar ook accounts waarbij wel duidelijk is aan wie het account toebehoort, maar er twijfel kan bestaan over wie het account gebruikt heeft. Een andere categorie bestaat uit de betrouwbaarheid van gegevens zoals deze gevonden zijn op websites.

In een klein aantal gevallen blijft het onduidelijk wat de bewijskracht is of kan zijn van elektronische gegevens. In Nederlandse en Duitse wetgeving is nog niet duidelijk wat de bewijskracht van een gewone elektronische handtekening en een geavanceerde elektronische handtekening is.

Het belangrijkste criterium, welke een rode draad vormt in dit onderzoek, is authenticatie. Dat ziet bij rechtsubjecten op de vraag of iemand daadwerkelijk is wie hij stelt te zijn en op rechtobjecten op de vraag of deze ongemodificeerd zijn.

In de literatuur wordt gesteld dat het belangrijk is om de zwaarste technische middelen in te zetten om juridische problemen te voorkomen. In de praktijk blijkt echter dat rechters prima met elektronische bewijsmiddelen overweg kunnen en er geen moeite mee hebben om deze als bewijs te accepteren en er feiten op baseren.

Hoofdstuk 8

In hoofdstuk acht komen enkele aanbevelingen aan de orde om de betrouwbaarheid van elektronische gegevens als bewijsmiddel te vergroten.

Dit zijn:

- gebruikmaking van een geavanceerde elektronische handtekening met gekwalificeerd certificaat;
- gebruikmaking van een geavanceerde elektronische handtekening;
- gebruikmaking van een gewone elektronische handtekening;
- gebruikmaking van cryptografische *hash* functies;
- het gebruiken van de naam van de ondertekenaar;
- het gebruikte (e-mail)adres / het domein van het e-mailadres;
- de inhoud van een elektronisch bericht;
- het werken met ontvangstbevestigingen;
- het (automatisch) aanmaken van logs;
- het maken van één of meerdere back ups;
- inschakelen van derden.