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

De betere byte in de strijd om het gelijk

Een onderzoek naar de betrouwbaarheid van elektronische gegevens als bewijsmiddel in het Nederlandse, Duitse en Amerikaanse civiele bewijsrecht

Maarten van Stekelenburg

VRIJE UNIVERSITEIT

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

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad Doctor aan
de Vrije Universiteit Amsterdam,
op gezag van de rector magnificus
prof.dr. L.M. Bouter,
in het openbaar te verdedigen
ten overstaan van de promotiecommissie
van de faculteit der Rechtsgeleerdheid
op dinsdag 22 juni 2010 om 15.45 uur
in de aula van de universiteit,
De Boelelaan 1105

door

Maarten Christiaan van Stekelenburg

geboren te Arnhem

promotoren: prof.mr. A. Oskamp
prof.dr. F.M.T. Brazier

In estimating the weight of evidence we cannot mark it as so many ounces, pounds, or tons, and yet we know that it may have all degrees of weight from the ligthtest feather to the most absolute moral certainty. All we can do is to note all the facts and circumstances carefully, and estimate its absolute and relative weight by the lights of conscience and experience.

Judge Vredenburg of New Jersey
in
Boylan v. Meeker, 28 N.J.L. 274, 333

ISBN 978 90 5972 378 8

Uitgeverij Eburon
Postbus 2867
2601 CW Delft
tel.: 015-2131484 / fax: 015-2146888
info@eburon.nl / www.eburon.nl

(NL) Omslagontwerp: Maarten van Stekelenburg
(EN) Cover design: Maarten van Stekelenburg

Voorwoord

Dit proefschrift zou niet tot stand zijn gekomen zonder de hulp en medewerking van vele personen. Ik ben hen erg dankbaar voor al hun steun, maar misschien wel het meest voor het geduld dat zij hebben kunnen opbrengen. Bijzondere dank gaat uit naar de volgende personen.

Eerst wil ik mijn promotor en begeleider Anja Oskamp bedanken. Toen zij als hoogleraar verbonden was aan de Radboud Universiteit, heeft zij mij begeleid bij het schrijven van mijn scriptie. Daarna heeft zij mij de kans geboden om te promoveren aan de Vrije Universiteit Amsterdam. Als kritisch begeleider wist zij mij te inspireren en motiveren en met een positief geluid sleepte zij mij door moeilijke momenten.

Ook wil ik mijn tweede promotor Franzes Brazier bedanken voor haar kritische blik op mijn werk en alle aanvullingen en opmerkingen. Ik ben haar zeer erkentelijk voor alle kennis en ideeën die zij heeft gedeeld.

Voorts bedank ik al mijn oud-collega's op de Vrije Universiteit. Zij hebben een toch wel eenzame promotietijd aangenaam gemaakt. Ik kon altijd even binnenlopen om het over serieuze dingen te hebben, maar ook om gewoon even te praten en te lachen. Bijzondere dank gaat daarbij uit naar mijn directe collega en kamergenote Martine Boonk. In de vier jaar die ik op de universiteit heb doorgebracht, was zij de eerste om lief en leed mee te delen. Daarnaast bood zij een luisterend oor voor mijn ideeën en voorzag zij deze van commentaar.

Daarnaast wil ik mijn familie bedanken voor al hun steun die ik heb gehad tijdens mijn leven. De wijze levenslessen van mijn ouders die menig keer van toepassing waren op situaties waarmee ik geconfronteerd werd tijdens mijn onderzoek, hebben mij geholpen dit onderzoek tot een goed einde te brengen.

Dank gaat tevens uit naar de leden van de leescommissie: prof.mr. R.E. van Esch, prof.mr. I. Giesen, prof.dr. C.M. Jonker, mr.dr. A.R. Lodder en prof.mr.drs. C. Stuurman.

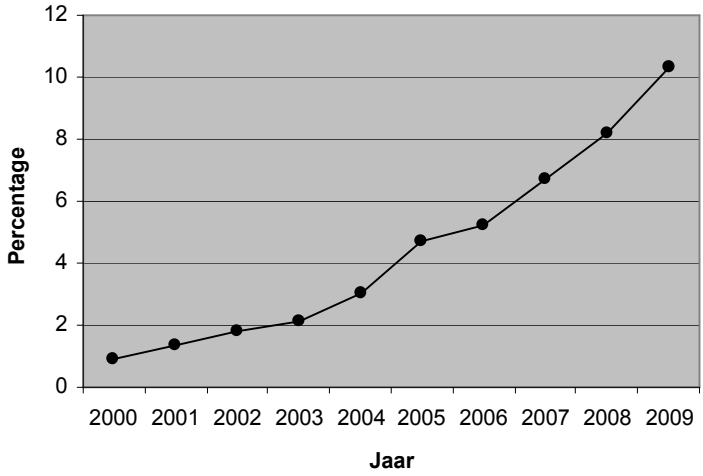
Maarten van Stekelenburg
Amsterdam, 3 april 2010

Inhoudsopgave

1 Inleiding

1.1 Elektronische gegevens als bewijsmiddel

Dit onderzoek gaat over de bewijskracht van elektronische gegevens in het Nederlandse, Duitse en Amerikaanse civiele recht. Elektronische bewijsmiddelen zijn al langere tijd onderwerp van onderzoek en niet geheel zonder reden. Met de komst van elektronische middelen in het maatschappelijk en economisch verkeer, worden deze middelen ook steeds vaker gebruikt als middel ter bewijs (zie afbeelding 1.1).[1]



Afbeelding 1.1: Percentage van alle civiele zaken waarin e-mail een rol speelt t.o.v. alle handelzaken en overige civiele zaken in www.rechtspraak.nl.

Hierdoor wordt van rechters gevraagd zich te buigen over de betrouwbaarheid en de kwaliteit van een voor hen onbekend soort bewijsmiddel waarvan ze de mogelijkheden, maar ook de risico's mogelijk niet altijd kennen.[2] Elektronische bewijsmiddelen staan aan verschillende risico's bloot waardoor de

[1] Zie ook de bijlage (pag. 239).

[2] A.M.Ch. Kemna, 'De vraagstukken van bewijs en bewaring in een elektronische omgeving', in: H. Franken, H.W.K. Kaspersen, A.H. de Wild (red.), *Recht en computer* (Recht en Praktijk), Deventer: Kluwer 2004, p. 214 en 215.

betrouwbaarheid en de kwaliteit niet altijd gewaarborgd kunnen worden. Deze verschillende risico's concentreren zich op drie punten, namelijk: identiteit, integriteit en vertrouwelijkheid.[3] Bij het identiteitsprobleem kan bijvoorbeeld worden gedacht aan het risico dat een derde zich rechtmatig dan wel onrechtmatig toegang verschaft tot een systeem en berichten onder de naam van een andere persoon verzendt of zelfs rechtshandelingen verricht onder de naam van een ander. In dat geval kan de identiteit van de persoon die via het systeem communiceert niet worden gegarandeerd. Ook kan hierbij gedacht worden aan zogenaamde *identity theft* waarbij een persoon de identiteit van een ander aanneemt en zich via elektronische weg toegang verschaft tot gegevens van de persoon voor wie hij zich uitgeeft of de gegevens van derden. Ook zou hij rechtshandelingen kunnen verrichten in naam van de persoon voor wie hij zich uitgeeft. Bij integriteitsproblemen kan bijvoorbeeld gedacht worden aan rechtmatige of onrechtmatige wijzigingen aan het elektronische bewijsmiddel. Hierbij speelt het probleem dat het in de meeste gevallen niet of nauwelijks te achterhalen valt of het bewijsmiddel is gewijzigd en door wie dat gedaan is. In dit geval is de integriteit van het bewijsmiddel niet langer gegarandeerd. Het derde risico raakt het elektronische bewijsmiddel niet direct, maar slechts indirect. Hierbij gaat het om het schenden van de vertrouwelijkheid van informatie door een derde. Als bijvoorbeeld een e-mail inbox gekraakt wordt door een derde kan deze alle e-mails in de inbox kan bekijken. Hij kan dan kennisnemen van vertrouwelijke informatie, zoals wachtwoorden en gebruikersnamen van een gebruikersaccount. Hiermee zou hij zich vervolgens toegang kunnen verschaffen tot de gebruikersaccount en mogelijk gegevens modificeren. Het enkele feit dat de vertrouwelijkheid van informatie is aangetast, betekent echter niet per definitie dat ook de betrouwbaarheid van elektronische gegevens is aangetast. Het vergoot enkel de mogelijkheid dat een derde met deze informatie de identiteit van de oorspronkelijke gebruiker kan aannemen en uit naam van de persoon van wie de gegevens zijn (of op wie de gegevens betrekking hebben) kan handelen (identiteit) of elektronische middelen kan aantasten (integriteit).

De onduidelijkheid met betrekking tot de kwalitatieve waarde van elektronische bewijsmiddelen leidt ertoe dat het vaak niet duidelijk is waar deze bewijsmiddelen aan moeten voldoen om voldoende betrouwbaar te zijn om de feiten die zij ondersteunen als bewezen te kunnen beschouwen. Zo is het de vraag of een e-mail die afkomstig van een e-mailadres welke de naam van een persoon bevat, ook door deze persoon geschreven is. Een andere vraag is of de inhoud van die e-mail wel voldoende betrouwbaar is om met die inhoud de door een partij gestelde feiten aan te tonen. Weer een andere vraag is of systemen die automatisch metingen doen wel voldoende betrouwbare

[3] ECP.nl (M. Durinck, I. Aarts (red.)), Bewaren en bewijzen, Efficiënta Offsetdrukkerij bv, p. 9 en OLG Köln 6.9.2002 – 19 U 16/02. Zie ook paragraaf 3.2.

data opleveren en of deze data als voldoende betrouwbaar kan worden beschouwd. Denk bijvoorbeeld aan een persoon die zijn computer gebruikt om te handelen in aandelen. Daarbij maakt hij gebruik van systemen van een bankinstelling die het mogelijk maken om op grond van instellingen automatisch aandelen te kopen en verkopen. Als in deze systemen iets mis gaat en de aandelen worden tegen een te lage prijs verkocht of tegen een te hoge prijs gekocht, dan kan de handelaar de bank aansprakelijk stellen. Om zijn claims kracht bij te zetten en zijn stellingen te bewijzen, zal hij gebruik moeten maken van de elektronische bewijsmiddelen (als schermafdrukken, gegevens in de database, enzovoorts). De vraag is of deze elektronische gegevens gebruikt kunnen worden als bewijs.

De technologische ontwikkelingen staan niet stil. Er worden nieuwe toepassingen ontwikkeld die nieuwe mogelijkheden bieden en waarvan de juridische consequenties niet altijd helder zijn. Een voorbeeld hiervan is mobiele code.[4] Dit zijn computerprogramma's die zich (laten) verplaatsen van locatie naar locatie om daar een proces te starten en gebruik te maken van de faciliteiten die geboden worden door de machine waar de agent heen 'reist'. *Grid computing* en *agent technology* zijn voorbeelden van mobiele code. Bij *grid computing* geven eigenaars van computers toestemming aan een partij om, al dan niet tegen betaling, gebruik te maken van hun computerfaciliteiten. De vele computers die hiervoor beschikbaar gesteld worden, vormen samen een cluster die gebruikt kan worden voor zeer ingewikkelde berekeningen. Een andere tendens is het gebruik van *agent technology* waarbij autonome computerprogramma's taken voor hun gebruiker uitvoeren. Deze *agents* kunnen op basis van specifieke input geheel of gedeeltelijk autonoom een bepaalde taak uitvoeren voor hun gebruiker. Hierbij kan gedacht worden aan *agents* die zich over een netwerk verplaatsen van locatie naar locatie om zelfstandig informatie te zoeken en te verzamelen, om te onderhandelen (met andere *agents*: computerprogramma's of mensen) of om een product te kopen.

---

[4] Mobiele code kent een aantal voordelen. Ten eerste kunnen met behulp van mobiele code computerprocessen die teveel rekenkracht zouden vragen van een computer of processen die op diezelfde computer te lang zouden duren, uitgevoerd worden op een andere computer. Hiertoe wordt de code gestuurd naar een andere (krachtigere) computer, waar de berekeningen kunnen worden uitgevoerd om vervolgens de resultaten van die berekeningen te sturen naar een andere gewenste locatie (welke meestal de locatie zal zijn waar de code oorspronkelijk van verzonden is). Ten tweede kan mobiele code een oplossing bieden voor het versturen van grote hoeveelheden data en tevens een oplossing bieden voor de bescherming van het auteursrecht. De mobiele code zou bijvoorbeeld verplaatst kunnen worden naar een locatie waar zich bepaalde data bevindt, deze data doorzoeken, om vervolgens slechts de relevante data mee terug te nemen naar de locatie waar deze data benodigd is. Hoewel vele databases reeds doorzoekbaar zijn gemaakt, is een gebruiker hiervan vaak gebonden aan een enkel zoekmechanisme dat op basis van reeds vooraf bepaalde instructies die database doorzoekt. Wil de gebruiker op een andere manier diezelfde database doorzoeken, dan heeft hij hiertoe meestal geen mogelijkheden. Met behulp van mobiele code kan een zoekmechanisme naar de database gestuurd worden om daar uitgevoerd te worden en de database te doorzoeken.

Mobiele code biedt nieuwe mogelijkheden, maar brengt ook nieuwe problemen met zich.[5] Data wordt getransporteerd van en naar verschillende locaties. Daar staat de data bloot aan de risico's van aantasting van integriteit, identiteit en vertrouwelijkheid. De vraag is echter of de concrete criteria waarop de rechter de huidige elektronische middelen onderzoekt op betrouwbaarheid als bewijsmiddel, wel van toepassing zijn op een geheel nieuwe technologie waarbij data wordt blootgesteld aan aantasting door (mobiele) code. Kunnen de concrete eisen die gesteld worden aan elektronische bewijsmiddelen om ze als voldoende betrouwbaar te beoordelen ook gesteld worden aan data van mobiele code of vraagt deze technologie om eigen concrete criteria om de betrouwbaarheid als bewijsmiddel te garanderen?

1.2 Probleemstelling

Samenvattend is de bewijskracht van elektronische bewijsmiddelen niet duidelijk. Dat geldt temeer voor toepassingen waarbij nieuwe elektronische middelen een rol spelen. Het is de vraag wanneer deze voldoende betrouwbaar zijn om de door partijen gestelde feiten te bewijzen. Daarbij is de sterke internationale oriëntatie van het internet van belang. Het gebruik van technologie is juist *niet* aan grenzen gebonden, terwijl daarentegen de diverse landen verschillende bewijsregels hebben in het civiele recht. Hierdoor komt een betrouwbaarheidsoordeel op verschillende manieren tot stand. Bij deze totstandkoming van het betrouwbaarheidsoordeel worden de verschillende risico's van aantasting van de integriteit, identiteit en vertrouwelijkheid onderzocht. Verwezenlijken deze risico's zich, dan kan het zijn dat het bewijsmiddel niet meer als voldoende betrouwbaar kan worden beschouwd. Ook kan slechts de enkele blootstelling aan deze risico's ertoe leiden dat het bewijsmiddel niet als voldoende betrouwbaar kan worden gekwalificeerd.[6] De vraag is aan welke criteria elektronische bewijsmiddelen moeten voldoen om als voldoende betrouwbaar te kunnen worden gekwalificeerd. Hierbij kom ik bij mijn onderzoeksvraag:

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

---

5 R.A. Grimes, *Malicious Mobile Code*, Sebastopol: O'Reilly & Associates, Inc, 2001, p. 2 en 3; D. Gollman, *Computer Security*, Chichester: John Wiley & Sons, Ltd, 2006, p. 308 e.v.

6 Waarbij het niet duidelijk is of het risico zich heeft verwezenlijkt.

technologieën zodat de verwerkte/geproduceerde elektronische gegevens voldoende betrouwbaar zijn als bewijsmiddel?

Mijn onderzoeksvraag omvat twee componenten. In het eerste deel van mijn onderzoeksvraag kijk ik naar de in het verleden aangelegde criteria voor de betrouwbaarheid van elektronische gegevens. Hierbij hanteer ik een positiefrechtelijke aanpak, waarbij ik onderzoek welke concrete criteria er reeds in de wetgeving en in de rechtspraak worden gehanteerd bij het beoordelen van de betrouwbaarheid van elektronische gegevens als bewijsmiddel. Met concrete criteria doel ik op de feitelijke criteria die in specifieke gevallen worden aangelegd om de betrouwbaarheid van elektronische gegevens als bewijsmiddel te beoordelen. Het tweede deel van mijn onderzoeksvraag gebruikt de output van het eerste deel als input om te kijken welke abstracte criteria te herleiden zijn uit de concrete criteria die reeds zijn aangelegd met als doel een richtlijn te geven waaraan nieuwe elektronische gegevens verwerkende/producerende technologieën zouden moeten voldoen om voldoende betrouwbaar te zijn als bewijsmiddel. Met abstracte criteria doel ik op algemene van de concrete criteria afgeleide principes waar elektronische gegevens aan dienen te voldoen om als voldoende betrouwbaar te kunnen worden gekwalificeerd als bewijsmiddel.

Dit onderzoek richt zich dan wel enkel op de criteria die reeds in de wet en jurisprudentie zijn aangelegd, maar dit wil niet zeggen dat dit onderzoek slechts van belang is voor de situatie waarin het tot een rechtszaak komt. Niet alleen de rechter heeft te maken met het waarderen van de bewijskracht van elektronische bewijsmiddelen, ook voor partijen is het van belang te kunnen inschatten wat de bewijskracht van hun elektronische gegevens is teneinde hun bewijspositie te kunnen bepalen. Partijen hebben er belang bij betrouwbare elektronische gegevens te verzamelen en tot stand te brengen met het oog op een mogelijke conflictsituatie. Hierbij worden bewijsmiddelen anticiperend of preventief gebruikt, namelijk om gelijk te krijgen in de fase die normaal vooraf gaat aan de fase waarin een onafhankelijke derde als een rechter of arbiter wordt ingeschakeld. Dit in tegenstelling tot de gang naar deze derde die een geschil dient te beslechten op grond van de gestelde feiten en de aangeboden bewijsmiddelen. In dat laatste geval is er namelijk sprake van een reactief gebruik van bewijsmiddelen.

De onderzoeksvraag kan nader opgedeeld worden in de volgende deelvragen die in de daarbij horende hoofdstukken worden beantwoord:

- Hoofdstuk 2
- Wat wordt verstaan onder elektronische gegevens?
- Hoe zijn elektronische gegevens nader te kwalificeren?

- Welk onderscheid valt er te maken in elektronische gegevens en hoe raakt dit onderscheid mijn onderzoek?

- Hoofdstuk 3
- Welke technische criteria (op functioneel niveau) zijn er om de betrouwbaarheid van elektronische bewijsmiddelen te waarborgen?
- Welke technologieën worden gebruikt om deze functionele criteria te implementeren?

- Hoofdstuk 4, 5 en 6
- Welke uitgangspunten gelden er respectievelijk in het Nederlandse, Duitse en Amerikaanse bewijsrecht?
- Welke criteria worden gesteld aan bewijsmiddelen en in het bijzonder elektronische gegevens die dienen ter bewijs om te bepalen of ze bewijs opleveren van de gestelde feiten in respectievelijk het Nederlandse, Duitse en Amerikaanse bewijsrecht?

- Hoofdstuk 7
- Wanneer zijn elektronische gegevens onvoldoende/voldoende betrouwbaar om als bewijs te dienen?
- Met welke abstracte criteria moeten ontwikkelaars rekening houden bij het ontwikkelen van nieuwe gegevensverwerkende/producerende technologieën?

- Hoofdstuk 8
- Welke concrete maatregelen kunnen getroffen worden om de bewijspositie te versterken bij gebruikmaking van elektronische gegevens als bewijsmiddel?

Dit onderzoek dient twee doelen. Ten eerste moet het een overzicht van concrete criteria opleveren waaraan elektronische gegevens moeten voldoen om als voldoende betrouwbaar gekwalificeerd te kunnen worden om de gestelde feiten te bewijzen. Ten tweede moet het een overzicht met abstracte criteria opleveren waarmee rekening gehouden kan worden bij het ontwikkelen van nieuwe gegevensverwerkende en –producerende toepassingen, zodat de elektronische gegevens voldoende betrouwbaar zijn als bewijsmiddel met het oog op een eventueel te voeren proces.

Om de hoofdvraag te beantwoorden en de doelen te bereiken analyseer ik de drie verschillende civiele bewijsstelsels in Nederland, Duitsland en Amerika. Deze landen zijn niet willekeurig gekozen. De combinatie van juist het Nederlandse, het Duitse en het Amerikaanse bewijsrechtstelsel omvat drie verschillend ingerichte bewijsrechtstelsel met eigenschappen die in meer of mindere mate ook terug zijn te vinden in andere rechtsstelsels. Voordat ik aan

het verschil in inrichting toekom, eerst een belangrijke overeenkomst: de drie verschillende bewijsrechtstelsels maken alle een onderscheid in de bewijstoelating en de bewijswaardering. In ieder stelsel wordt eerst onderzocht of bewijs kan worden toegelaten, om daarna te onderzoeken hoe het toegelaten bewijs kan worden gewaardeerd. Het grote verschil is echter dat de bewijstoelating bij de drie landen verschilt; het Nederlandse recht kent een open stelsel van bewijsmiddelen, wat wil zeggen dat in beginsel alle bewijsmiddelen worden toegelaten. Het Duitse recht kent een gesloten stelsel van bewijsmiddelen, wat inhoudt dat de soorten bewijsmiddelen limitatief in de wet worden opgesomd. Het Amerikaanse recht heeft een geheel eigen aanpak door alle bewijsmiddelen bij de bewijstoelating op een aantal specifieke kwaliteiten te onderzoeken.[7]

Het feit dat ik mij richt op drie verschillende civiele bewijsstelsels heeft als reden dat het object van onderzoek, namelijk elektronische gegevens, vaak niet aan landsgrenzen gebonden is. Elektronische gegevens zijn door de opkomst van het wereldwijde internet steeds vaker onderhevig aan verplaatsing die landsgrenzen overstijgt. Doordat elektronische gegevens zich op verschillende nationale locaties kunnen bevinden, zullen ook verschillende rechtsstelsels van toepassing zijn afhankelijk van de locatie waar de gegevens zich bevinden. Voor het bewijsrecht kan dit een aantal consequenties hebben, want de criteria waaraan een bewijsmiddel moet voldoen om als voldoende betrouwbaar te kunnen worden beschouwd, kunnen verschillen binnen de diverse bewijsrechtsstelsels. Het is daarom van belang om deze criteria nader in kaart te brengen en te onderzoeken welke criteria van belang zijn voor welk stelsel, zodat er rekening kan worden gehouden met het implementeren van specifieke technologieën die de bewijskracht kunnen vergroten, dan wel garanderen. Bij de criteria die voorkomen in alle drie de rechtsstelsels is dit het duidelijkst; deze moeten bij voorkeur geïmplementeerd worden. Bij de verschillen is dat lastiger. Het feit echter dat een bepaald criterium wel of niet gesteld wordt aan elektronische gegevens als bewijs, maakt het in ieder geval mogelijk om een bewuste keuze te maken bij het implementeren van bepaalde technologieën.

Aan bovenstaand doel en het feit dat ik de criteria uit drie verschillende rechtsstelsels onderzoek, ligt een aanname ten grondslag. In dit onderzoek neem ik aan dat er in Nederland, Duitsland en Amerika een gemeenschappelijk idee bestaat wanneer een elektronisch bewijsmiddel voldoende betrouwbaar is om er het gevolg aan te geven dat een feit dat daardoor ondersteund wordt als bewezen kan worden beschouwd. Deze aanname omvat het idee dat dezelfde

[7] Verder in dit onderzoek zal blijken dat deze kwalitatieve eigenschappen ook een rol spelen in het Nederlandse en Duitse recht, maar dat deze kwaliteiten worden meegenomen in de bewijswaardering in plaats van in de bewijstoelating.

risico's worden onderkend die kleven aan bewijsmiddelen en dat bewijsmiddelen niet altijd zijn wat ze lijken. Door deze risico's zijn er criteria ontwikkeld waaraan bewijsmiddelen getoetst moeten worden voordat ze het predicaat 'betrouwbaar' krijgen. Ondanks het feit dat ik uit het Nederlandse, Duitse en Amerikaanse recht put om betrouwbaarheidscriteria te formuleren, is het niet een op zichzelf staand doel om een rechtsvergelijkend onderzoek te doen, hoewel enige vergelijking tussen de verschillende stelsels af en toe wel gemaakt zal worden. Dit is namelijk inherent aan het feit dat verschillende bewijsrechtstelsels in dit onderzoek zijn betrokken.

1.3 Methode van onderzoek

De methode van onderzoek bestaat uit onderzoek naar wetgeving, jurisprudentie en literatuur. Daarbij vindt enige rechtsvergelijking plaats, hoewel dit niet een doel op zich is. In de eerste plaats maak ik gebruik van de meest voorname rechtsbronnen, namelijk in het Nederlandse en Duitse recht voornamelijk de wet en in het Amerikaanse recht in ongeveer gelijke mate de wet en de jurisprudentie. Voor alle drie de bewijsstelsels geldt dat de wet het uitgangspunt is. Voor het Amerikaanse recht geldt echter dat de Federal Rules of Evidence (FRE) een codificatie is van de jurisprudentie. Naast de FRE vormt daarnaast de jurisprudentie nog een belangrijke rechtsbron. Daarom zal in dit onderzoek ook ruim aandacht zijn voor een studie van de voornamelijk vrij recente ontwikkelingen in de jurisprudentie. Naast het uiteenzetten en analyseren van de wet en de jurisprudentie zal gebruik worden gemaakt van literatuur. Hierbij wordt deze literatuur zoveel mogelijk gebruikt als objectieve bron en besteed ik slechts in enkele gevallen aandacht aan opvattingen die door de auteurs verkondigd worden. In de derde plaats zal er enige ruimte zijn voor rechtsvergelijking, hoewel dit niet het hoofddoel van deze studie is. De rechtsvergelijkende component dient zich aan op momenten dat het in het kader van dit onderzoek van belang is om expliciet het contrast aan te geven tussen de verschillende bewijsstelsels.

1.4 Bewijzen in het kader van dit onderzoek

Centraal in dit onderzoek staat het begrip bewijzen. Een belangrijke vraag is daarom wat moet worden verstaan onder bewijzen. Ten eerste dient een onderscheid te worden gemaakt tussen juridisch bewijs voeren en natuurwetenschappelijk of wiskundig bewijs voeren.[8] Natuurwetenschappelijk en wiskundig bewijs zijn erop gericht om sluitend bewijs te verkrijgen voor één

[8] T.R. Hidma, G.R. Rutgers, *Bewijs*, Deventer: Kluwer, 2004, p. 7.

waarheid. Juridisch bewijs laat daarentegen ruimte voor meerdere waarheden. Met juridische bewijsvoering wordt beoogd een feitelijke situatie of gebeurtenis te reconstrueren zodat duidelijk wordt wie welke rechten had of welke juridisch relevante gebeurtenissen hebben plaatsgevonden om daar juridisch relevante consequenties uit te kunnen trekken. Een rechter zal moeten oordelen welke partij welke rechten heeft en hij zal dus moeten werken met een gereconstrueerde waarheid, want de rechter zal in bijna geen enkel geval aanwezig zijn geweest op de momenten dat zich rechtens relevante gebeurtenissen hebben voorgedaan. Bij bewijzen in juridische zin gaat het dus om het reconstrueren van een waarheid op basis van daartoe beschikbare bewijsmiddelen.

Bewijzen speelt een belangrijke rol in bijna iedere rechtszaak. Als er een geschil is of als er getracht wordt door middel van een rechtszaak bepaalde rechtsgevolgen te bewerkstelligen, dan is het niet alleen een kwestie van stellen welke feiten zich hebben voorgedaan en welke rechten iemand toekomen, maar moet degene die deze feiten en rechten stelt deze ook bewijzen.[9] Zonder bewijs kun je deze feiten en rechten niet aantonen en heb je spreekwoordelijk gezegd geen poot om op te staan. Bewijzen is dus van belang in bijna ieder geschil; zowel in het civiele recht, het strafrecht als in het bestuursrecht. In dit onderzoek zal ik mij alleen richten op de bewijsregels die gelden in het civiele bewijsrecht. In het civiele recht spelen geschillen zich af tussen twee of meer burgers en de beslissing van de rechter is een beslissing die geldt tussen de strijdende partijen. In tegenstelling tot het civiele recht kennen het strafrecht en het bestuursrecht geheel eigen regels van bewijsrecht en de bewijsmaatstaf ligt, zeker in het strafrecht, aanzienlijk hoger, omdat geschillen in deze rechtsgebieden zich afspelen tussen een burger en de staat of een overheidsorgaan; daarmee is een heel ander soort rechtsbescherming geboden dan bij geschillen tussen burgers onderling.

Er is in dit onderzoek een complicerende factor bij het definiëren van het begrip bewijzen: het feit dat in dit onderzoek drie verschillende civiele bewijsstelsels worden onderzocht, levert namelijk drie verschillende definities op van het bewijsbegrip. Daarbij komt ook nog dat er per rechtsstelsel meerdere bewijsstelsels naast elkaar kunnen bestaan (zoals voor het strafrecht en het civiele recht). Hierdoor kunnen het strafrecht en het civiele recht binnen één land een ander bewijsbegrip hebben. Daarom zal ik hieronder verder ingaan op de verschillende bewijsbegrippen die het Nederlandse, Duitse en Amerikaanse civiele recht hanteren.

[9] Dit geldt tenminste in het Nederlandse, Duitse en Amerikaanse recht.

De bewijsdefinitie naar Nederlands recht

In het Nederlandse civiele recht is geen definitie gegeven van wat onder bewijzen moet worden verstaan.[10] Art. 149 Rv biedt wel een aanknopingspunt; dit artikel stelt dat de rechter "slechts feiten of rechten aan zijn beslissing ten grondslag leggen, die (…) zijn komen vast te staan". De vraag is nu echter wanneer deze feiten zijn komen vast te staan. Nu de wet verder niets stelt over de overtuigingsgraad van de rechter, ligt het voor de hand om naar de jurisprudentie van de Hoge Raad te kijken. Ook de Hoge Raad echter heeft zich niet uitgelaten over wat hij verstaat onder bewijzen.[11]

Een maatstaf die veel in de literatuur wordt gehanteerd is dat de rechter *een redelijke mate van zekerheid* moet hebben verkregen over de zich afgespeelde feiten.[12] In de literatuur worden tevens nog een aantal andere maatstaven genoemd zoals 'een grote mate van aannemelijkheid', 'een redelijke mate van waarschijnlijkheid' en 'een zekere mate van waarschijnlijkheid',[13] maar deze maatstaven lijken in de laatste decennia toch minder aanhang te hebben dan de maatstaf 'een redelijke mate van zekerheid'. Hoewel, zoals reeds gesteld, deze laatste bewoordingen niet zijn gebruikt in rechtspraak van de Hoge Raad, worden deze wel regelmatig gebruikt in lagere rechtspraak en conclusies van de Advocaat Generaal.[14] Ook in de literatuur wordt de maatstaf 'een redelijke mate van zekerheid' alom gehanteerd en beschouwd als de maatstaf voor wanneer een feit als bewezen kan worden beschouwd of niet.[15]

De bewijsdefinitie naar Duits recht

De Duitse wet kent geen expliciete definitie van bewijzen. Toch kan uit art. 286, lid 1 ZPO worden afgeleid wat onder bewijzen moet worden verstaan, 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.(…)*"[16]

---

10 T.R. Hidma, G.R. Rutgers, *Bewijs*, Deventer: Kluwer, 2004, p. 7. Het strafrecht daarentegen kent wel een basis voor een bewijsdefinitie in art. 338 Sv: de rechter dient de overtuiging te hebben bekomen op basis van wettige bewijsmiddelen.

11 Dit is niet geheel onlogisch, aangezien bewijzen een oordeel geeft over de feiten. De Hoge Raad is cassatierechter en houdt zich niet bezig met het beoordelen van de feiten. De Hoge Raad toetst ingevolge art 79 Wet RO enkel op het verzuim van vormen en schending van het recht.

12 T.R. Hidma, G.R. Rutgers, *Bewijs*, Deventer: Kluwer, 2004, p. 7.

13 I. Giesen, "*De bewijswaardering in civiele zaken: vage noties of scherpe normen?*", Ars Aequi 1999, p. 626; M.L. Kan, *Bewijslast en bewijswaardering*, Amsterdam: N.V. Johannes Müller 1921, p 104

14 Zie bijvoorbeeld *LJN*: AD4006, Hoge Raad, R00/172HR; *LJN*: AR7438, Hoge Raad, R04/030HR; *LJN*: AB0377, Hoge Raad, C99/089HR

15 T.R. Hidma, G.R. Rutgers, *Bewijs*, Deventer: Kluwer, 2004, p. 7.

16 Art. 286, lid 1 ZPO; P. Förschler. *Der Zivilprozess, Ein Lehrbuch für die Praxis mit Aktenfall*, Stuttgart: Kohlhammer 2004, p. 424.

Een feit kan als bewezen worden beschouwd als de rechter overtuigd is van de feiten. Daarbij is de rechter vrij in het waarderen van de bewijsmiddelen die tot die overtuiging van de feiten moeten leiden. De rechtspraak heeft daar het volgende over gezegd:[17] "Eine von allen Zweifeln freie Überzeugung setzt das Gericht dabei nicht voraus. Auf diese eigene Überzeugung des entscheidenden Richters kommt es an, auch wenn andere zweifeln oder ein andere Auffassung erlangt haben würden. Der Richter darf und muß sich aber in tatsächlich zweifelhaften Fällen mit einem für das praktische Leben brauchbaren Grad von Gewißheit begnügen, der den Zweifeln Schweigen gebietet, ohne sie völlig auszuschließen"[18]

Bewijs is geleverd bij volle overtuiging van de rechter. Volle overtuiging neemt echter niet weg dat er bij de rechter niet nog enige twijfel mag bestaan. Er mag enige twijfel blijven bestaan bij de rechter, maar de overtuiging moet de twijfel het zwijgen opleggen. Volle overtuiging is dus niet gelijk aan honderd procent zekerheid. Paragraaf 5.6.2 gaat nader in op de bewijswaardering en het bewijsbegrip.

De bewijsdefinitie naar Amerikaans recht

In het Amerikaanse recht wordt de term '*to prove*' gehanteerd als het gaat over bewijzen. Deze term is echter dubbelzinnig.[19] In de eerste plaats kan er namelijk gedoeld worden op de bewijsmiddelen zelf en op de vraag wie de

---

17 BGHZ 53,245 ff. (Urteil v. 17.02.1970 (Anastasia)). De vorderende partij, grootvorstin Anastasia Nikolajewna Romanow, wilde aanspraak maken op Duitse waardepapieren die van Nicolaus II waren geweest. Mevrouw Romanow was namelijk de jongste dochter van de laatste tsaar Nicolaus II en zij was de enige die de uitmoording van de overige tsarenfamilie op 17 juli 1917 had overleefd. Het Landesgericht en het Beroepsgerecht kwamen tot de conclusie dat mevrouw Romanov niet het benodigde bewijs had geleverd, ondanks een omvangrijke bewijsvoering. Het Bundesgerichtshof in Zivilsachen (BGHZ) kwam echter tot de conclusie dat de bewijsopdracht in het nadeel van Romanov was en dat het Beroepsgerecht bijna onmogelijke bewijsinspanningen verwachtte van Romanov. Het BGHZ stelde dat noch onvervulbare bewijsinspanningen, noch onomstotelijke zekerheid bei de toetsing kan worden verlangd of een bewering waar en bewezen is. Onjuist is de maatstaf waarbij grote waarschijnlijkheid verlangd wordt; art. 286 SPO stelt namelijk dat de rechter zelf de overtuiging moet hebben of een bewering waar of niet waar is. Deze persoonlijke overtuiging is voor een beslissing noodzakelijk en alleen de feitenrechter mag zonder binding aan de wettelijke bewijsregels en is alleen aan zijn geweten onderworpen de beslissing te nemen of hij de twijfel kan overwinnen en zich van een bepaald feit overtuigen kan. Een van alle twijfel vrije overtuiging is niet door de wet verplicht. Het komt aan op de eigen overtuiging van de rechter, ook in de gevallen dat andere twijfel hebben of een ander standpunt verlangd zouden hebben. De rechter mag en moet bij gevallen van daadwerkelijke twijfel, met een voor het praktische leven bruikbare graad van zekerheid genoegen nemen, welke de twijfel het zwijgen oplegt, zonder deze volledig uit te sluiten.

18 Een vrije overtuiging die zonder enige twijfel is, wordt niet door de rechtbank verlangd. Het komt aan op de eigen overtuiging van de rechter, ook in de gevallen dat andere twijfel hebben of een ander standpunt verlangd zouden hebben. De rechter mag en moet bij gevallen van daadwerkelijke twijfel, met een voor het praktische leven bruikbare graad van zekerheid genoegen nemen, welke de twijfel het zwijgen oplegt, zonder deze volledig uit te sluiten.

19 C.B. Mueller, L.C. Kirkpatrick, *Modern Evidence, Doctrine and Practise*, Boston, New York, Toronto, London: Little, Brown and Company 1999, p. 78.

bewijslast draagt om met voldoende bewijs de door hem gestelde feiten te onderbouwen voor een rechter (*burden of producing evidence*). In de tweede plaats kan er worden gedoeld op de vraag wanneer de rechter of de jury kan worden overtuigd van de feiten die door partijen zijn gesteld (burden of persuasion). In dit onderzoek is het tweede punt van belang, namelijk de overtuiging van de rechter of de jury van de feiten.

In de Amerikaanse rechtspraak zijn slechts enkele uitspraken bekend waarin expliciet een bewijsstandaard voor het civiele recht wordt genoemd.[20] Op grond hiervan noemt Anderson de volgende drie standaarden: Prepon*derance of evidence, clear and convincing / clear / convincing* en de *beyond reasonable doubt*.[21] Vaak wordt gedacht dat '*beyond reasonable doubt'* de maatstaf is voor de overtuiging van de rechter of de jury om de gepresenteerde feiten als waar of onwaar aan te mogen nemen. De woorden "*beyond reasonable doubt*" zijn echter exclusief gereserveerd voor het strafrecht, ondanks het feit dat zowel het strafrecht en het civiele recht gebruik maken van dezelfde bewijsregels. De bewijsmaatstaf die in het civiele recht in de meeste staten wordt gehanteerd, ligt lager dan de maatstaf die in het strafrecht wordt gehanteerd. Deze maatstaf wordt verwoord met de woorden '*proof by a preponderance*' of met de woorden '*by a preponderance of evidence*'.[22] Een meer specifieke betekenis van deze woorden is ook wel: '*greater weight of evidence*' of '*more probable than not'*.[23] Ook Broun geeft aan dat de meest geaccepteerde betekenis van de woorden 'proof of preponderance' is: '*proof which leads the jury to find that the existance of the contested fact is more probable than its nonexistance'*.[24] Toch houdt niet iedere rechtbank zich aan deze geaccepteerde betekenis, omdat zij menen dat er meer voor nodig moet zijn dan slechts een schatting van waarschijnlijkheden. Deze rechtbanken vinden dat er sprake moet zijn dat de jury of rechter "*an actual belief*" hebben of dat deze "*convinced of the truth of the fact*" zijn. Zij lijken daarmee een stringentere maatstaf aan te leggen, waartoe zij overigens gerechtigd zijn. Het feit dat verschillende rechtbanken verschillende maatstaven mogen hanteren komt voort uit het feit dat de Verenigde Staten van Amerika een federale structuur kent, waarbij de verschillende staten autonoom zijn in het vaststellen van bewijsregels. Hoewel deze bewijsregels deels zijn geharmoniseerd door implementatie van de *Federal Rules of Evidence* in een groot aantal staten, ontbreekt er in deze regels

---

20 Zie bijvoorbeeld: Addington v. Texas 441 U.S. 418, 99 S.Ct. 1804; Bourjaily v. U.S. 483 US. 171, 107 S.Ct. 2775, Huddleston v. U.S. 485 U.S. 681, 108 S.Ct. 1496, Colorado v. Connelly 479 U.S. 157, 107 S.Ct. 515. Zie ook: C.B. Mueller, L.C. Kirkpatrick, *Modern Evidence, Doctrine and Practise*, Boston, New York, Toronto, London: Little, Brown and Company 1999, p. 80 en p. 183.

21 T. Anderson, D Schum, W. Twining, *Analysis of Evidence*, New York: Cambridge University Press 2005, p. 242 en 243.

22 G.C. Lilly, *Principles of Evidence*, St. Paul: Thomson West 2006, p. 387.

23 G.C. Lilly, *Principles of Evidence*, St. Paul: Thomson West 2006, p. 387.

24 K.S. Brown (red.), *McCormick ON EVIDENCE*, St Paul: Thomson West 2006, p. 568; zie ook: Devitt, Blackmar, Wolff, *Federal Jury Practise and Instructions* ff 72.01, 4h edition, 1987.

een bewijsmaatstaf die antwoord geeft op de vraag wanneer feiten als bewezen kunnen worden beschouwd.

In civiele zaken wordt naast de '*preponderance*' maatstaf nog een tweede maatstaf aangelegd die wordt verwoord met de woorden *'by clear and convincing evidence', 'clear, convincing and satisfactory"* of *'clear, unequivocal, satisfactory and convincing'*.[25] Deze maatstaf die ergens lijkt in te hangen tussen de 'preponderance' maatstaf en de 'beyond reasonable doubt' maatstaf, is gereserveerd voor gevallen waarin geen sprake is van strafrechtelijke vervolging, maar waarin een aantal belangrijke burgerrechten aan iemand worden ontnomen,[26] zoals in gevallen van een dwangbevel tot opname in een psychiatrische inrichting, ontzetting uit de ouderlijke macht of denaturalisatie of deportatie.[27]

1.5 Opbouw van dit onderzoek

Dit onderzoek is als volgt opgebouwd. In het tweede hoofdstuk introduceer ik de definities van elektronische gegevens, informatie, kennis, data en code.

Hoofdstuk drie gaat nader in op het te beschermen rechtsgoed van dit onderzoek, namelijk "bewijzen" en wordt onderzocht welke technische oplossingen er bestaan om dit rechtsgoed te waarborgen. Hierbij worden authentificerende methoden en integriteitswaarborgende methoden beschreven.

In hoofdstuk vier behandel ik het Nederlandse civiele bewijsrecht. Het Nederlandse bewijsrecht kenmerkt zich door haar open stelsel van toelating van bewijsmiddelen en een vrije bewijswaardering door de rechter. Na een inleiding op het Nederlandse bewijsrecht en de algemene regels die ten grondslag liggen aan bewijstoelating en bewijswaardering zal nader onderzocht worden welke specifieke criteria er gesteld worden aan elektronische bewijsmiddelen. Vervolgens zal ook nader worden ingegaan op de elektronische handtekening en de elektronische onderhandse akte en zal bekeken worden welke betekenis deze middelen kunnen hebben voor de bewijskracht van elektronische documenten. Het hoofdstuk zal, overigens net als hoofdstuk vijf en zes (Duitse en Amerikaanse bewijsrecht), worden afgesloten met een opsomming van criteria waaraan elektronische gegevens

---

25 K.S. Brown (red.), *McCormick ON EVIDENCE*, St Paul: Thomson West 2006, p. 568 en 569.

26 C.B. Mueller, L.C. Kirkpartick, *Modern Evidence, Doctrine and Practise, Boston*, New York, Toronto, London: Little, Brown and Company 1999, p. 183.

27 K.S. Brown (red.), *McCormick ON EVIDENCE*, St Paul: Thomson West 2006, p. 570.

aan zouden moeten voldoen om met voldoende betrouwbaarheid de feiten te kunnen bewijzen.

Hoofdstuk vijf behandelt het Duitse civiele bewijsrecht. Dit kent, in tegenstelling tot het Nederlandse civiele bewijsrecht, een gesloten stelsel van bewijsmiddelen; dat wil zeggen dat de bewijsmiddelen limitatief in de wet zijn opgesomd. De bewijswaardering is daarentegen, net als in het Nederlandse recht vrij. Toch bestaat er bij de vrije bewijswaardering een belangrijk verschil: de Duitse rechter krijgt expliciet de opdracht om de bewijswaardering te motiveren in het vonnis. Ook in dit hoofdstuk zal ik beginnen met een uiteenzetting van het algemene bewijsrecht, om daarna te onderzoeken welke rol het Elektronische Signatur, de Urkunde en de elektronische Urkunde kunnen spelen bij de betrouwbaarheid van elektronische gegevens als bewijsmiddel.

Het zesde hoofdstuk gaat uitvoerig in op het Amerikaanse bewijsrecht.[28] De Amerikaanse regels die handelen over bewijs, geven een opsomming van kwalitatieve eigenschappen waar bewijsmiddelen aan dienen te voldoen om deze toe te laten. Deze eigenschappen zullen worden onderzocht en er zal gekeken worden welke criteria gesteld kunnen worden aan bewijsmiddelen en in het bijzonder elektronische gegevens.

In hoofdstuk zeven neem ik de juridische criteria die geformuleerd zijn in de hoofdstukken vier, vijf en zes als uitgangspunt om te onderzoeken waar de verschillen en overeenkomsten liggen bij het betrouwbaarheidsoordeel van elektronische gegevens. Ik trek conclusies waarbij ik een antwoord formuleer op de vraag welke concrete criteria worden gesteld in het Nederlandse, Duitse en Amerikaanse civiele bewijsrecht aan elektronische gegevens ten aanzien van de borging van de betrouwbaarheid van deze gegevens om de door partijen gestelde feiten te kunnen bewijzen. Daarnaast zal de vraag worden beantwoord met welke abstracte criteria ontwikkelaars van gegevensverwerkende/-producerende technologieën rekening moeten houden met het oog op het ontwikkelen van nieuwe technologieën zodat de verwerkte/geproduceerde elektronische gegevens voldoende betrouwbaar zijn als bewijsmiddel?

In hoofdstuk acht doe ik nog een aantal aanbevelingen met het oog op gebruikers van elektronische gegevens. Eenvoudige aanpassingen in werkwijze kunnen ertoe leiden dat hun elektronische gegevens betrouwbaarder worden beoordeeld en dat deze in het geval van een procedure een hogere bewijswaarde kunnen hebben.

---

[28] Ik hanteer hier met opzet niet de term Amerikaanse civiele bewijsrecht, maar Amerikaanse bewijsrecht.

2 Elektronische gegevens

2.2 Inleiding

In dit onderzoek staan elektronische gegevens centraal. Afhankelijk van de benadering van het begrip elektronische gegevens valt er een onderscheid te maken in verschillende soorten elektronische gegevens. In het recht heeft het de voorkeur elektronische gegevens functioneel te benaderen.[29] Er wordt dan gekeken welke functie(s) de elektronische gegevens hebben, namelijk of de gegevens objectief of subjectief zijn, of ze verklaringen bevatten, of de gegevens opdrachten ten behoeve van de aansturing van computers bevatten, enzovoort. Een belangrijk functioneel onderscheid is de splitsing van elektronische gegevens in code en data. In dit hoofdstuk vindt eerst een verkenning plaats van de begrippen 'gegevens', 'code' en 'data'. Het onderscheid in code en data is niet alleen van belang om het object van onderzoek nader te specificeren, maar moet in de volgende hoofdstukken ook bijdragen aan het verschaffen van duidelijkheid of code en/of data gekwalificeerd kunnen worden als de juridische belangrijke begrippen 'geschrift', '*elektronisches dokument*' en '*writing'*. Deze begrippen zullen in dit hoofdstuk verder niet aan de orde komen, maar worden nader uitgewerkt in de hoofdstukken die handelen over de bewijsproblematiek van de drie verschillende rechtssystemen die ik onderzoek.[30]

2.2 Elektronische gegevens

Niet alleen binnen de informatica, maar ook in andere onderzoeksvelden wordt regelmatig van gegevens gesproken. Gegevens kunnen verschillende vormen aannemen, zoals een teken op papier, een geluid, een kleur of, zoals we veel data tegenwoordig kennen: als een reeks bits of bytes op een gegevensdrager of als elektronische signalen.[31] In dit onderzoek beperk ik me tot de elektronische variant van gegevens.[32] Er lijkt overeenstemming te bestaan over

---

29 H.W.K. Kaspersen, *Strafbaarstelling van computermisbruik* (diss. Amsterdam VU), Deventer: Kluwer 1990, p. 45.

30 Zie de hoofdstukken 4, 5 en 6.

31 R.J.J. Westerdijk, *Produktenaansprakelijkheid voor software* (diss. Amsterdam VU), 1995, p. 21.

32 Data en gegevens worden vaak uitwisselbaar gebruikt, aangezien gegevens een Nederlands en data een Engels woord is. De term data wordt echter binnen de informatica ook gebruikt als een

wat onder gegevens moet worden verstaan zowel binnen de rechtswetenschap als binnen de *computer security*,[33] hoewel de definities soms niet helemaal aan elkaar gelijk zijn. Binnen de rechtswetenschap hanteren Oskamp, Apistola en De Mulder als definitie: "Gegevens zijn rechtstreeks waarneembaar: getallen, namen, adressen. Ze kunnen digitaal of anderszins zijn vastgelegd en zijn te zien als patronen die informatie kunnen bevatten".[34] Kaspersen en Westerdijk hanteren de definitie die door het ISO wordt gebruikt: "*A representation of facts, concepts or instructions in a formalized manner suitable for communication, interpretation or processing by human beings or by automatic means.*"[35] Binnen de computer security worden gegevens omschreven als: "*Physical phenomena chosen by convention to represent certain aspects of our conceptual and real world.*"[36] Mijn voorkeur gaat uit naar het begrip zoals gedefinieerd door het ISO aangezien dit begrip expliciet instructies erkend die door middel van geautomatiseerde gegevensverwerkende eenheden kunnen worden uitgevoerd of verwerkt.

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.

Gegevens staan in relatie tot de begrippen 'tekens' en 'informatie' en 'kennis'. Om een nader beeld te schetsen waar code en data zijn te plaatsen, ga ik kort in op de verhouding tussen deze begrippen.

Gegevens bestaan uit symbolen, cijfers, letters en allerlei andere vormen en tekens waarmee gegevens kunnen worden weergegeven en verwerkt. De ISO definieert een *character*: "A character is a member of a set of elements upon which agreement has been reached and that is used for the organisation, control or representation of data."[37] Een teken is dus het kleinste bouwblok van een gegeven met zelfstandige betekenis.

Zoals verschillende tekens gegevens vormen, zo vormen verschillende gegevens informatie. Gegevens zijn dus te beschouwen als de bouwblokken

---

subset van gegevens om een functioneel onderscheid te maken tussen data en code. Verderop in deze paragraaf zal ik dit onderscheid ook maken en in het kader van dit onderzoek aanhouden.

33 M. Weggeman, *Kennismanagement - Inrichting en besturing van kennisintensieve organisaties*, Schiedam: Scriptum Management 1997, p. 30.

34 A. Oskamp, A.R. Lodder, *Informatietechnologie voor Juristen*, Deventer: Kluwer 2002, p. 168.

35 H.W.K. Kaspersen, *Strafbaarstelling van computermisbruik* (diss. Amsterdam VU), Kluwer: Deventer 1990, p. 42. R.J.J. Westerdijk, *Produktenaansprakelijkheid voor software* (diss. Amsterdam VU), 1995, p. 21.

36 D. Gollman, *Computer Security*, Chichester: John Wiley & Sons, Ltd, 2006, p. 26.

37 ISO 5138/9, 09.03.01; ISO 2382/4, 04.02.01; [IEC 60050-702 702-05-10]

van informatie. Ook over de definitie van informatie bestaat overeenstemming in de rechtswetenschap en in de *computer security*. In de rechtswetenschap word informatie gedefinieerd als: "gegevens waar betekenis aan kan worden toegekend."[38] Binnen de *computer security* wordt informatie gedefinieerd als "*the meanings we assign to data*"[39] en "*collated and processed data presented so as to yield a significant content*."[40] Het toekennen van betekenis aan gegevens is van essentieel belang voor het ontstaan van informatie en de menselijke factor is daarmee onderdeel van het informatiebegrip. Pas als gegevens worden waargenomen en in verband zijn te brengen met andere gegevens, kan er sprake zijn van informatie.[41]

In tegenstelling tot de begrippen 'tekens', 'gegevens' en 'informatie' bestaat er over de betekenis van het begrip kennis geen overeenstemming.[42] Een aantal definities die in de literatuur wordt genoemd: "een persoonlijk vermogen, het product van informatie, ervaring, vaardigheid en attitude van iemand;[43] hetgeen waarmee gegevens geïnterpreteerd kunnen worden en waarmee informatie toegepast kan worden;[44] en begrijpen plus de vaardigheid om het om te zetten in vaardigheden.[45]" Aangezien het begrip kennis verder niet van belang is voor mijn onderzoek, [46] zal ik hier niet verder op in gaan.

In dit onderzoek worden twee soorten gegevens onderscheiden, namelijk code en data. De begrippen code en data komen uit de informatica waar deze begrippen als vanzelfsprekend beschouwd worden. Het zijn misschien wel begrippen die voor informatici zo voor zichzelf spreken als de begrippen 'zaak' en 'goed' dat doen voor juristen. Toch lijkt het begrip data niet altijd eenduidig te worden gebruikt, omdat de term data soms betrekking heeft op alle soorten gegevens (inclusief code), maar soms enkel op niet uitvoerbare gegevens (gegevens exclusief code). Het begrip 'gegevens' bevat in het kader van dit onderzoek feiten, objectieve concepten en/of instructies en omvat daarmee zowel code als data waarbij code en data twee verschillende soorten gegevens zijn. De definitie van data zoals ik die voor dit onderzoek zal aanhouden bestaat

---

38 A. Oskamp, A.R. Lodder, *Informatietechnologie voor Juristen*, Kluwer Deventer, tweede druk, 2002, p. 168; M. Apistola, *Advocaat & Kennismanagement* (diss. Amsterdam VU), 2007, p. 36.

39 D. Gollman, *Computer Security*, Chichester: John Wiley & Sons, Ltd, 2006, p. 26.

40 T. Daler, R. Gulbrandsen, B. Melgård, T. Sjølstad, *Security of Information and Data*, Chichester: Ellis Horwood Ltd, p. 1989, p. 16.

41 H.W.K. Kaspersen, *Strafbaarstelling van computermisbruik* (diss. Amsterdam VU), Kluwer: Deventer 1990, p. 41.

42 M. Apistola, *Advocaat & Kennismanagement* (diss. Amsterdam VU), 2007, p. 37.

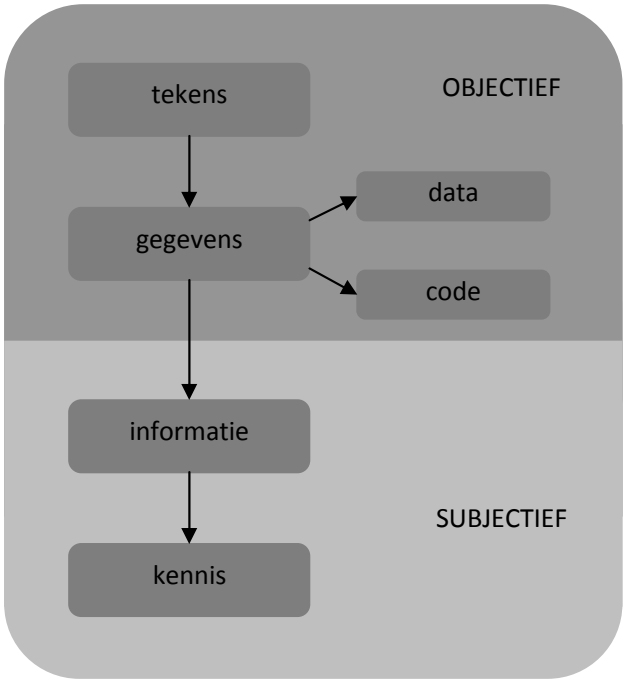
43 M. Weggeman, *Kennismanagement - Inrichting en besturing van kennisintensieve organisaties*, Schiedam: Scriptum Management 1997, p. 33.

44 R. Florijn, M. van Gurchom & M. van der Meulen, *Kennis leren managen. De theorie an praktijk van kennismanagement*, Den Haag: Ten Hagen & Stam 2000, p. 22.

45 S.K.Th Boersma, *Management van kennis. Een creatieve onderneming*, Assen: Koninklijke Van Gorcum 2002, p. 22.

46 Buiten het schetsen van een kader voor het begrip 'gegevens'

namelijk uit gegevens exclusief code (zie figuur 1). Als data beschouw ik dan ook die gegevens die door een processor verwerkt kunnen worden maar welke zelf geen instructies voor de processor bevatten. Het onderscheid wordt ook duidelijk aan de hand van de terminologie die ik hanteer: data kan worden verwerkt, maar niet worden uitgevoerd. Code kan zowel worden uitgevoerd en onder omstandigheden ook worden verwerkt. Hierop ga ik in de twee volgende paragrafen nader in.



Afbeelding 1.1: Verhouding van gehanteerde begrippen

2.3 Code

Een computer is een machine die als wezenlijk kenmerk heeft dat deze instructies uitvoert. Een computer gebruikt ingevoerde gegevens om volgens formele regels logische conclusies te trekken. Het uitvoeren van instructies, ook wel een proces genoemd, is dus een essentiële eigenschap van computers. De instructies, ook wel aangeduid als code of software, worden uitgevoerd met behulp van een processor, ook wel de *CPU* of *central processing unit* genoemd. In moderne computers liggen de instructies in eerste instantie vast op een

gegevensdrager.[47] Code onderscheidt zich van data door de instructies die zij bevat om de processor aan te sturen. Deze instructies zijn opgesteld in een taal die de processor kan 'begrijpen', zodat de processor de instructies kan uitvoeren. Niet iedere processor kan ook iedere code uitvoeren; de processor moet namelijk wel in staat zijn de code uit te voeren. In tegenstelling tot een mens heeft een processor geen vermogen tot leren; een processor is een onveranderlijk ding en zijn architectuur ligt vast.

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.

2.4 Data

Strikt genomen zijn data gegevens. Daarbij worden onder deze gegevens meestal verstaan de gegevens die vervat zijn als bits op een gegevensdrager. Binnen de informatica wordt ook wel een onderscheid gemaakt in data inclusief code en data exclusief code. In de meeste gevallen wordt dit onderscheid impliciet gemaakt, maar voor dit onderzoek is het van belang om dit onderscheid expliciet in kaart te brengen omdat code en data (exclusief code) verschillende functies hebben. Data exclusief code zijn gegevens die geen mogelijkheid hebben om te executeren. De gegevens bevatten geen instructies om de processor aan te sturen. Het adressaat van deze data is dan in de meeste gevallen een persoon voor wie deze data betekenis heeft, kan hebben of die er betekenis aan kan geven. Ook kan data als adressaat de computer hebben, maar de computer kan de data in enge zin niet executeren. Wel kan de computer de data met behulp van code nader verwerken. Deze verwerking wordt echter door het proces uitgevoerd welke aangestuurd wordt door code en niet door de data zelf.

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.

Data kan op twee verschillende manieren tot stand gebracht (gegenereerd) worden, namelijk door mensen en door computers. Dit onderscheid lijkt in eerste instantie misschien kunstmatig, maar het is een juridisch relevant

[47] In oudere computers waren de instructies meestal deel van het ontwerp van de rekeneenheid zelf.

onderscheid. In de volgende drie hoofdstukken zal blijken dat dit onderscheid gemaakt wordt in alle drie de onderzochte rechtsstelsels.

Data komt niet zomaar tot stand; data wordt gecreëerd. Er is een actie nodig die een (elektrisch of licht) signaal genereert. Dit signaal kan vervolgens worden vastgelegd op een gegevensdrager. Het meest eenvoudige voorbeeld is waarschijnlijk de door mensen gebruikte toetsenborden en de muis. Door middel van toetsaanslagen, muisklikken en het bewegen van de muis krijgt de computer een invoersignaal waarmee deze wat kan doen. Of de computer er iets mee doet hangt af van de instructies die de computer uitvoert. Of ook merkbaar is dat de computer iets met de invoer doet, hangt daarbij tevens af van de uitvoerapparatuur, zoals een beeldscherm, luidsprekers of andere apparatuur die uitvoer produceren die door menselijke zintuigen kan worden waargenomen. Als bij het werken met een tekstverwerker de toetsen die corresponderen met de letters M a a r t e n worden ingedrukt (invoer), verschijnt het woord Maarten op het scherm (uitvoer). Bij het maken van een foto met een digitale camera (ervan uitgaande dat deze gereed is om een foto te maken), geef ik door middel van de druk op de knop een signaal om het licht dat op een lichtgevoelige chip valt, vast te leggen op een gegevensdrager. In bovenstaande gevallen is de initiator van het vastleggen van de gegevens een persoon.

Steeds meer taken worden echter automatisch door machines verricht. Hierbij valt te denken aan allerlei meetapparatuur die constant de omgeving 'waarneemt'. Zo staat overal ter wereld meetapparatuur opgesteld om constant variabelen te meten en de waarden als data op te slaan in databases. In koelwagens wordt periodiek de temperatuur gemeten met als doel een signaal te geven als de temperatuur bepaalde waarden overschrijdt en om de temperatuurgegevens op te slaan. De apparatuur die automatisch gegevens meet en vastlegt werkt niet zomaar. Ergens moet een persoon een handeling hebben verricht om de machine aan te zetten. Is echter eenmaal de machine aangezet, dan blijft deze observeren tot een signaal komt dat de machine de acties niet langer hoeft te verrichten.

2.5 Rechtvaardiging onderscheid code en data

In dit onderzoek maak ik een hard onderscheid tussen code en data.[48] Dit onderscheid is niet arbitrair.[49] Code en data liggen dan wel beide vast in

[48] In dit onderzoek zal ik de term data gebruiken voor elektronische data. Indien ik niet elektronische data bedoel, zal ik dit expliciet noemen.

[49] Voor een nadere verhandeling over de oorsprong van het onderscheid in code en data zie ook: H. Franken (Kapsersen, Wild) , *Recht en Computer Recht en Praktijk*, 5e druk, Kluwer, 2004, p. 3 t/m 6.

eenzelfde vorm, maar vertonen in hun gedrag een aantal belangrijke verschillen. Meer specifiek kan gesteld worden dat het grote verschil tussen code en data is dat code wel gedrag vertoont of kan aansturen (in de vorm van een proces), terwijl data geen gedrag kan vertonen of aansturen.[50]

Aangezien code en data elk een specifieke functie hebben, brengen beide ook specifieke problematiek met zich mee. Code stuurt gedrag aan door middel van een proces. Dit gedrag is niet altijd van menselijk handelen te onderscheiden en het kan lijken alsof een mens handelt of heeft gehandeld. Machines die in naam van / ten behoeve van mensen rechtshandelingen verrichten zijn dan ook een belangrijk onderzoeksgebied geweest voor juristen.[51] Ook data heeft juristen bezig gehouden. Data onderscheidt zich van code doordat de gegevens die vervat zijn in die data een ander adressaat hebben. De gegevens die in de code zijn vervat, zijn gericht tot een machine die bepaalde instructies dient uit te voeren. Bij data zijn deze gegevens vaak niet meer dan een elektronische codering van gegevens die ook op papier, film, foto, geluidsdrager, enzovoorts zouden kunnen bestaan. Het betreft daarbij dus niet de werking van die gegevens. Vanzelfsprekend is de juridische problematiek die bij data speelt dan ook een andere dan bij code. Bij data hebben de rechtsvragen veelal betrekking op authenticiteit, integriteit en vertrouwelijkheid.[52] In een behoorlijk aantal gevallen betreft het vragen met betrekking tot de bewijsvoering.

Het onderscheid tussen code en data is ook van invloed op de kwalificatie van het bewijsmiddel als geschrift, *elektronisches Dokument* of als *writing*. Om bepaalde informatie als een geschrift, *elektronisches Dokument* of *writing* te kunnen kwalificeren dient er te zijn voldaan aan een aantal eigenschappen. In respectievelijk de paragrafen 4.11, 5.5 en 6.10 zal aan de orde komen waarom mijns inziens zuivere code wel of niet gekwalificeerd kan worden als *geschrift*, *elektronisches Dokument* of *writing*. Data kan naar mijn mening onder omstandigheden wel worden gekwalificeerd als *geschrift*, *elektronisches Dokument* en de *writing*. Als gevolg van de kwalificatie als *geschrift*, *elektronisches Dokument* of *writing* zal er een verschil zijn in de bewijskracht van code en data.[53] Hierdoor kan de bewijskracht van code anders zijn dan de bewijskracht van data.

---

50 Het onderscheid in code en data wordt al gemaakt door Von Neumann in 1945 in het model van de programeerbare computer. Het onderscheid tussen code en data is niet langer een fysiek onderscheid, maar slechts van conceptuele aard. Zie: H. Franken (Kapsersen, Wild) , R*echt en Computer*, 5e druk, Kluwer, 2004, p. 4 en 5.

51 Zo heeft van Esch onderzoek gedaan naar de vraag of EDI-systemen rechtshandelingen kunnen verrichten, hoe deze tot stand komen en wie gebonden is in R. van Esch, *Electronic data interchange (EDI) en het vermogensrecht*, (diss. Nijmegen), Deventer: W.E.J. Tjeenk Willink 1999.

52 De trits integriteit, vertrouwelijkheid en beschikbaarheid is ontleend aan de informatiebeveiligingseisen die door informatici gehanteerd worden. Authenticiteit is een belangrijk begrip bij het bepalen of informatie wel van een bepaalde persoon afkomstig is. Zie ook: H. Franken (Kapsersen, Wild) , *Recht en Computer*, 5e druk, Kluwer, 2004

53 Zie hiervoor hoofdstuk 4 en 5.

2.6 Kanttekeningen op de strikte scheiding van code en data

In veel gevallen zijn er kanttekeningen te plaatsen bij de scheiding die ik heb aangebracht tussen code en data. Deze kanttekeningen zal ik hieronder toelichten aan de hand van een aantal concrete voorbeelden. Ik onderscheid hier een fysieke en functionele scheiding van code en data.

De fysieke scheiding houdt in dat code en data strikt gescheiden entiteiten zijn. Code en data zijn echter bijna nooit compleet fysiek van elkaar gescheiden. Code en data liggen in de meeste gevallen vast in een bestand (file), ook wel document genoemd. De meeste bestanden bestaan echter niet uit alleen code of alleen data, maar bevatten zowel code als data. Zo bevat veel executeerbare code regels die niet uitvoerbaar zijn, maar enkel gegevens die als input worden gebruikt om te worden verwerkt door de code of het bevat gegevens in elektronische vorm. Hierbij kan gedacht worden aan printregels die teksten op een scherm doen verschijnen, geluidsfragmenten en video. Het omgekeerde is ook het geval: code wordt opgenomen binnen data. Hierbij valt te denken aan macro's die in tekstverwerkingsprogramma's en spreadsheets kunnen worden geactiveerd.

In de tweede plaats is er de functionele scheiding die soms toch minder hard lijkt dan dat deze wordt voorgesteld. Zo is bijvoorbeeld broncode vaak niet meer dan data.[54] De broncode zelf kan zonder compilatie of interpretatie niet worden uitgevoerd. Het omgekeerde kan ook het geval zijn. Machinecode kan ook worden behandeld als data.[55] Zo is het bijvoorbeeld mogelijk om machinecode door middel van een computerprogramma te analyseren en te onderzoeken, zonder dat de code zelf ook wordt uitgevoerd. Ook kan deze geopend worden als tekstbestand. Ook bij het transport van code (kopiëren (downloaden, uploaden)) wordt code behandeld als data.

Op grond van bovenstaande kan gesteld worden dat de functionele en fysieke scheiding in code en data minder hard is dan deze in eerste instantie lijkt. Enige relativering is daarom op zijn plaats. De vraag is nu hoe om te gaan met deze relativering in het kader van dit onderzoek. Naar mijn mening geniet het de voorkeur om elektronische gegevens praktisch en functioneel te benaderen. Dient bepaald te worden of elektronische gegevens als code of data moeten worden beschouwd, dan moet onderzocht worden welke functie de elektronische gegevens hebben (gehad). Op grond van de uitkomst kan dan gesteld worden of de juridische problematiek betrekking heeft op code of op data.

---

[54] Broncode: de code geschreven in een voor de mens eenvoudig te begrijpen syntax.

[55] Machinecode: gecompileerde broncode die door een computer kan worden uitgevoerd. Voor de meeste mensen is deze code niet begrijpelijk.

2.8 Samenvatting

Elektronische gegevens kunnen functioneel worden onderscheiden in code en data. Code kan verschillende verschijningsvormen hebben. Machinecode kan direct door een computer worden uitgevoerd, maar is voor mensen nauwelijks te begrijpen. Broncode is voor mensen begrijpelijk, maar kan niet door een computer worden uitgevoerd. Data kan niet worden uitgevoerd, maar kan met behulp van een proces worden verwerkt. Data bevat gegevens niet zijnde code. Voor dit onderzoek is een onderscheid van belang in data gegenereerd door mensen en data gegenereerd door computers. Het belang van dit onderscheid zal aan de orde komen in de volgende hoofdstukken en houdt verband met ondertekende geschriften. De functionele en fysieke scheiding in code en data is vaak niet heel duidelijk. Aan de hand van de functie zal bepaald moeten worden of het om code of data gaat.

3 Beveiliging van elektronische gegevens

3.1 Inleiding

De omgang met elektronische gegevens is in het hedendaagse leven zo normaal geworden dat het voor veel mensen niets vreemds meer is om te werken met deze gegevens. Het is dan ook verwonderlijk dat de overheid slechts mondjesmaat lijkt te reageren op de risico's die het gebruik van elektronische gegevens met zich meebrengt. De wetgeving die vervolgens wel wordt ingevoerd is in de meeste gevallen slechts een implementatie van Europese regelgeving en stelt een aantal functionele criteria die vertaald naar technische oplossingen de lat hoog lijken te leggen. Zo ook in het bewijsrecht. Bij de bewijskracht van de elektronische handtekening wordt alleen dwingend rechtsgevolg verleend aan de gekwalificeerde elektronische handtekening. De wetgever heeft gelukkig de vrije bewijskracht niet aangetast en ruimte gelaten aan de rechter om elektronische gegevens als bewijsmiddel te waarderen. Binnen deze vrije bewijskracht kan de rechter zelf bepalen welke waarde hij aan elektronische gegevens als bewijsmiddel hecht en op grond waarvan hij dat doet. In de volgende hoofdstukken zal blijken dat de rechter in de praktijk vaak helemaal geen uitspraak doet over bewijsmiddelen waarbij zware en ingewikkelde technische methoden worden ingezet om de betrouwbaarheid van de gegevens als bewijsmiddel te vergroten dan wel te garanderen. Overigens is het ook maar de vraag of hij deze wel onder ogen krijgt. Toch ga ik in dit hoofdstuk in op een aantal van deze beveiligingsmethoden, omdat de literatuur deze vaak noemt. Ik zal deze slechts beschrijven op een functioneel niveau en aangeven welke beschermingsmogelijkheden deze beveiligingsmethoden bieden. De technische details laat ik in het kader van dit onderzoek achterwege. In paragraaf 3.2 beschouw ik het te beschermen rechtsgoed binnen dit onderzoek. Technische middelen worden namelijk niet zomaar geïmplementeerd, maar dienen een doel: ze bieden bescherming tegen een aantal risico's. In de literatuur die handelt over *computer security* worden deze risico's genoemd. Echter, in het kader van dit onderzoek dat zich enkel richt op de betrouwbaarheid van elektronische gegevens als bewijsmiddel, zijn niet alle risico's die in de *computer security* genoemd worden van belang. In paragraaf 3.3 ga ik vervolgens in op de authentificatie van personen, waarbij de belangrijkste methoden van authentificatie van personen worden genoemd. In paragraaf 3.4 ga ik vervolgens in op het waarborgen van de integriteit van elektronische gegevens. In de laatste paragraaf ga ik nog kort in op de

verschillende mogelijkheden die de combinatie van de in paragraaf 3.3. en 3.4 besproken beveiligingsoplossingen.

3.2 Het te beschermen rechtsgoed volgens de literatuur

Over informatiebeveiliging ten behoeve van de betrouwbaarheid van bewijsmiddelen is in de juridische literatuur wel het een en ander geschreven, zij het slechts mondjesmaat. De meeste literatuur gaat in op de wetgeving die zich concentreert op middelen die een hoge beschermingsgraad hebben. Een voorbeeld is de elektronische handtekening die ingevolge art. 3:15, lid 2 BW (a) op unieke wijze aan de ondertekenaar moet zijn verbonden, (b) het mogelijk moet maken de ondertekenaar te identificeren, (c) tot stand moet zijn gekomen met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden, (d) de integriteit moet waarborgen, (e) gebaseerd moet zijn op een gekwalificeerd certificaat en (f) gegenereerd moet zijn door een veilig middel als bedoeld in de Telecommunicatiewet. De literatuur beschrijft vervolgens een aantal technieken dat deze functionele criteria via technische weg kan waarborgen.[56] Het doel van de regelgeving betreffende de elektronische handtekening is namelijk om een betrouwbare methode te hebben om de authenticiteit van de persoon en de integriteit van de gegevens vast te stellen. In het bewijsrecht is het ook vaak van belang om een persoon te authentificeren. In het Amerikaanse recht is dit zelfs een expliciete toelatingseis voor bewijsmiddelen en het is niet onaannemelijk dat de Nederlandse en Duitse rechters dit ook doen, zij het impliciet.

Elektronische gegevens dienen voldoende betrouwbaar te zijn om als bewijs te dienen.[57] In de literatuur zijn er criteria aangelegd om deze betrouwbaarheid vorm te geven. Zo spreekt Franken over de algemene beginselen van behoorlijk ICT-gebruik,[58] waarbij de sleutelwoorden beschikbaarheid, vertrouwelijkheid, integriteit, flexibiliteit en transparantie zijn. Om deze betrouwbaarheid te vergroten, dan wel te garanderen kan er gebruik worden gemaakt van verschillende technische oplossingen. Hierbij valt te denken aan verschillende soorten van versleuteling en het gebruik van wachtwoorden. De criteria die worden gesteld in de literatuur voorzien een breed spectrum aan beveiligingsmethoden. Deze zijn vanuit allerlei vraagstukken ingegeven en passen in een breed beveiligingsbeleid. Zo zal bijvoorbeeld het garanderen van

---

56 Bijvoorbeeld: A.R. Lodder, J. Dumortier, S. Bol, *Het recht rond elektronische handtekeningen*, Deventer, Kluwer: 2005, p. 11 t/m 21.

57 A.M.Ch. Kemna, 'De vraagstukken van bewijs en bewaring in een elektronische omgeving', in: H. Franken, H.W.K. Kaspersen, A.H. de Wild (red.), *Recht en computer* (Recht en Praktijk), Deventer: Kluwer 2004, p. 215.

58 *Beschikken en automatiseren, pre-advies voor de Vereniging voor Administratief Recht, VAR*, nr. 110, Alphen aan den Rijn, 1993.

de beschikbaarheid ertoe dienen om altijd de juiste gegevens op het gewenste moment beschikbaar te hebben op de juiste plaats. Het garanderen van de vertrouwelijkheid zal ertoe dienen om te zorgen dat niet iedereen bij gevoelige informatie kan komen (bijvoorbeeld persoonsgegevens). In dit onderzoek staan deze genoemde gebieden echter niet centraal. In dit onderzoek staat het onderwerp bewijzen centraal. Juist omdat ik mij enkel richt op de bewijsproblematiek in het civiele recht, zal een deel van de voor de expert bekende beveiligingstechnieken buiten beschouwing blijven. De reden hiervoor is dat die technieken niet of slechts in ondergeschikte mate bijdragen aan het optimaliseren van de betrouwbaarheid van elektronische gegevens als bewijsmiddel. Hier doel ik op het rechtsgoed privacy of de bescherming van persoonsgegevens en de daarmee verbonden beveiligingsoplossingen die de vertrouwelijkheid kunnen garanderen. Dit onderwerp is slechts zijdelings verbonden met bewijsvoering. In paragraaf 3.4 komt dan wel de vertrouwelijkheid aan de orde bij *two way* versleuteling, maar de reden hiervoor is dat deze vorm van versleuteling ook de integriteit van elektronische gegevens garandeert. Integriteit is wel nauw verbonden met het rechtsgoed bewijs. Ook binnen de *computer security* zijn vertrouwelijkheid en integriteit twee verschillende onderwerpen.[59]

In het rapport 'bewaren en bewijzen' gaat het ECP in op het bewijzen met behulp van elektronische gegevens. Daarbij neemt het ECP het begrip historiciteit als uitgangspunt voor de betrouwbaarheid van elektronische gegevens als bewijsmiddel Op basis van deze historiciteit worden de begrippen integriteit, authenticiteit en controleerbaarheid geïntroduceerd.[60] Zoals in de hoofdstukken 4, 5 en 6 blijkt, hebben vooral de begrippen authenticiteit en integriteit ook al lange tijd hun weg hebben gevonden in de rechtspraak en wetgeving. In mijn conclusie zal ik ook ingaan op de onderlinge verhouding van deze begrippen. Ook vanuit beveiligingperspectief wordt onderkend dat authentificatie een belangrijk begrip is in de beveiliging.[61]

Zoals gesteld, is het voor de betrouwbaarheid van elektronische gegevens als bewijsmiddel belangrijk om de authenticiteit en de integriteit te waarborgen. Van belang is het om te weten dat binnen de rechtswetenschap onder authentificatie verschillende dingen worden verstaan al naar gelang het object of subject waar de authentificatie betrekking op heeft. Heeft authentificatie betrekking op rechtsobjecten (waaronder ook elektronische gegevens), dan gaat het erom of het object ook daadwerkelijk dat object is als wordt beweerd. In dat geval is het de vraag of het object integer is; dat wil zeggen dat het niet is

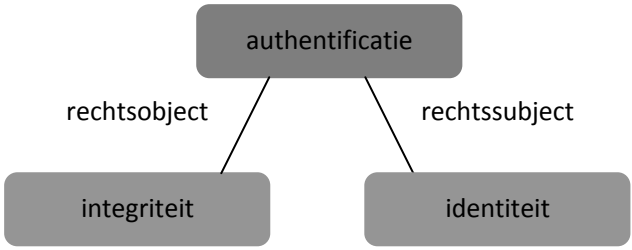
---

59 D. Pei, *Authentication Codes and Combinatorial Designs*, Boca Raton: Chapman & Hall/CRC 2006, p. 1. Zie ook C.P. Pfleeger, *Security in Computing*, New Jersey: Prentice Hall International, Inc. 1997, p. 4 t/m 6.

60 ECP.nl (M. Durinck, I. Aarts (red.)), Bewaren en bewijzen, Efficiënta Offsetdrukkerij bv, p. 9.

61 F. Stajano, *Security for Ubiquitous Computing*, Chichester: John Wiley & Sons, Ltd, 2002, p. 85.

gemodificeerd. Heeft de authenticiteit daarentegen betrekking op rechtssubjecten dan gaat het enerzijds om de vraag of de persoon inderdaad de persoon is waarvan gesteld wordt dat deze het is en anderzijds de vraag of een bepaald iets (handtekening, geschrift, vingerafdruk, enzovoorts) inderdaad afkomstig is van deze persoon. Hier is meteen een onderscheid te zien in de betekenis zoals deze in de technische en in de juridische literatuur wordt gemaakt. In de technische literatuur heeft authentificatie enkel betrekking op de laatste vraag. Daarbij handelt het bij authentificatie dus over een persoon. Voor de authentificatie van objecten wordt het begrip integriteit gebruikt (zie afbeelding 3.1). In het bewijsrecht wordt daarentegen gesproken over de authentificatie of authenticiteit van personen en objecten.[62]



Afbeelding 3.1: Verhouding van authentificatie tot integriteit en identiteit

In de volgende paragrafen zal ik nader ingaan op een aantal technieken die ingezet kunnen worden voor het authentificeren van personen en het authentificeren van elektronische gegevens (oftewel het garanderen van de integriteit).[63]

3.3 Authentificatie van personen

De authentificatie van personen is het proces van vaststellen of een bepaald persoon ook daadwerkelijk degene is voor wie hij zich uitgeeft.[64] Het authentificeren van personen is bijvoorbeeld van belang bij het verlenen van toegang tot bepaalde gegevens en de vraag wie wat met welke gegevens mag

---

62 Zie paragraaf 6.8.3. Zie ook: P.R. Rice, *Electronic Evidence, Law and Practice*, Chicago: ABA Publishing 2008, p. 335.

63 Sommige informatici hebben het echter ook over authenticatie van elektronische gegevens als ze het hebben over de integriteit van deze gegevens. Zie hiervoor bijvoorbeeld: D. Pei, *Authentication Codes and Combinatorial Designs*, Boca Raton: Chapman & Hall/CRC 2006, p. 1 en D.E.R. Denning, *Cryptography and Data Security*, Reading: Addison-Wesley Publishing Company, p. 4. Overigens is Schneier het niet eens met deze opvatting. Hij beschouwt authentificatie en integriteit als twee verschillende dingen: B. Schneier, *Secrets & Lies, Digital Security in a Networked World*, New York: John Wiley & Sons, Inc., 2000, p. 73.

64 F. Stajano, *Security for Ubiquitous Computing*, Chichester: John Wiley & Sons, Ltd, 2002, p. 75.

doen, zoals de gegevens bekijken, creëren, verwijderen en/of wijzigen. Authentificatie van een persoon kan op basis van verschillende kenmerken. Daarbij worden traditioneel drie criteria onderscheiden, namelijk iets dat een persoon weet, iets dat een persoon heeft en iets dat een persoon is.[65]

1. Iets dat een persoon weet

De informatie die een persoon heeft, wordt veel gebruikt om iemand te authentificeren. Informatie of gegevens kunnen door een persoon worden onthouden, zodat een fysieke opslag van deze gegevens buiten de persoon die ze onthoudt, niet nodig is. Gebruikersnamen en wachtwoorden (passwords) zijn op dit moment misschien wel de meest gebruikte vormen van authentificatie. Een ander voorbeeld is de PIN-code zoals deze gebruikt wordt bij bankpassen en creditcards. Wachtwoorden hebben als zwakste schakel de persoon die het wachtwoord toebehoort. Als deze zijn wachtwoord niet geheim houdt, dan is het bij het authentificeren van de gebruiker van het wachtwoord, minder zeker of dat ook de persoon is aan wie het wachtwoord oorspronkelijk is meegedeeld.

2. Iets dat een persoon in zijn bezit heeft

Een persoon kan iets in zijn bezit hebben, waarmee hij zich kan authentificeren. Hierbij kan gedacht worden aan een identificatiekaart, al dan niet voorzien van elektronische gegevens, maar ook aan een RFID-chip. Een nadeel is dat het object dat authentificerend werkt kan worden verloren of gestolen. Een ander die het in zijn bezit krijgt, kan dan gebruik maken van bevoegdheden die hem niet zijn verleend. Het wordt daarom steeds gebruikelijker een object dat authentificerend kan werken, te voorzien van andere kenmerken die onder nummer 1, 3, 4 en 5 zijn genoemd. Zo heeft een bankpas een pincode (iets waarvan een persoon informatie heeft) en worden de nieuwste paspoorten voorzien van biometrische informatie (eigenschappen van een persoon zelf), zoals een vingerafdruk en gelaatskenmerken.[66]

3. Iets dat een persoon is

Een persoon heeft specifieke eigenschappen, waarvan sommige eigenschappen zo uniek zijn dat deze een persoon kunnen identificeren of een groep personen (met overeenkomstige eigenschappen) kunnen identificeren. Het betreft hier biometrische gegevens.[67] Hier kan bijvoorbeeld gedacht worden aan een vingerafdruk, een irisscan, DNA, stemherkenning, een thermogram van een

---

65 B. Schneier, *Secrets & Lies, Digital Security in a Networked World*, New York: John Wiley & Sons, Inc., 2000, p. 136. Gollman onderscheidt overigens vijf middelen op basis waarvan een persoon kan worden geauthentificeerd. Zie hiervoor: D. Gollman, *Computer Security*, Chichester: John Wiley & Sons, Ltd, 2006, p. 44 e.v.

66 D. Gollman, *Computer Security*, Chichester: John Wiley & Sons, Ltd, 2006, p. 45.

67 S. Baase, *A Gift of Fire, Social, Legal, and Ethical Issues for Computing and the Internet*, New Jersey: Pearson, Prentice Hall, 2009, p. 297.

gezicht, oorvorm,[68] enzovoorts. Afhankelijk van het soort kenmerk zijn deze in meer of mindere mate uniek voor een persoon. Een combinatie van deze eigenschappen levert een nog unieker patroon op waarmee een persoon kan worden geïdentificeerd. Ook handelingen en gedragingen van een persoon kunnen eigenschappen omvatten die uniek of ten minste onderscheidend zijn voor een persoon. Een handtekening is een voorbeeld van een eigenschap van een gedraging die wordt vastgelegd. Het probleem met de handtekening op papier is dat enkel degene die observeert kan beoordelen hoe de handtekening gezet wordt. Dit levert maar een klein deel van de eigenschappen van het zetten van de handtekening op. Met moderne middelen kunnen meer eigenschappen vastgelegd worden. Op dit moment wordt bijvoorbeeld steeds meer gebruik gemaakt van een elektronisch *pad* dat een aantal eigenschappen kan registreren die niet met het menselijk oog waarneembaar zijn, zoals de druk die wordt uitgeoefend en de snelheid waarmee de handtekening wordt geplaatst. Ook bij invoer via een toetsenbord kan sprake zijn van het registreren van de druk die een persoon uitoefent op de toetsen en de snelheid van de toetsaanslag.[69]

Gollman onderscheidt ook authentificatie op basis van de locatie waar een persoon zich bevindt.[70] Een klassiek voorbeeld is dat slechts computers die zich binnen een bepaald netwerk of terminal bevinden toegang geven tot bepaalde elektronische gegevens. Met de komst van moderne technieken en mobiele computers, kunnen ook andere locatiebepalende methoden ingezet worden. Hierbij kan dan gedacht worden aan diensten via het Global Positioning System (GPS), waarbij de locatie van het apparaat waarmee een persoon zich probeert te authentificeren bepalend is voor de authentificatie van de persoon.[71] Deze methode van authentificatie is echter niet erg betrouwbaar, omdat niet altijd een persoon kan worden gekoppeld aan de locatie. De locatie is dan wel duidelijk, maar niet de persoon. Hiermee ontbeert het de juist zo belangrijke eigenschap dat de identiteit van een persoon komt vast te staan.

De eerste en tweede vorm van authentificatie geven maar deels zekerheid over de identiteit van een persoon. Iets wat een persoon weet, blijkt namelijk niet altijd in het hoofd van deze persoon. Deze kan bijvoorbeeld zijn wachtwoord opschrijven of vertellen aan iemand anders. Iets wat een persoon heeft zoals een toegangspas met gegevens, kan gestolen worden of aan iemand anders gegevens worden. Daarom wordt vaak gewerkt met zogenaamde *two factor* authentificatie.[72] Dit wil zeggen dat er gebruik wordt gemaakt van een dubbele

---

68 R. Anderson, Security Engineering, *A Guide to Building Dependable Distributable Distributed Systems*, New York: Wiley Compter Publishing, p. 262 t/m 273.

69 D. Gollman, *Computer Security*, Chichester: John Wiley & Sons, Ltd, 2006, p. 47.

70 D. Gollman, *Computer Security*, Chichester: John Wiley & Sons, Ltd, 2006, p. 47.

71 D. Gollman, *Computer Security*, Chichester: John Wiley & Sons, Ltd, 2006, p. 47.

72 C.P. Pfleeger, *Security in Computing*, New Jersey: Prentice Hall International, Inc. 2003, p. 209.

authentificatie, zoals zowel een pasje met elektronische gegevens (iets dat iemand heeft) als een wachtwoord (iets dat iemand weet) of van zowel een wachtwoord (iets dat iemand weet) als een gebruikersnaam (iets dat iemand weet).

3.4 Versleuteling van elektronische gegevens

Al lange tijd bestaat er behoefte om te communiceren zonder dat derden de te communiceren gegevens kunnen onderscheppen en deze te wijzigen. Het versleutelen van gegevens (encryptie) [73] gaat minstens terug tot de Egyptenaren, maar waarschijnlijk maakten ook culturen daarvoor al gebruik van het versleutelen van gegevens.[74] Deze behoefte bestaat nog steeds. Nog steeds willen personen en organisaties gegevens versturen zonder dat deze kunnen worden gelezen en begrepen door derden en kunnen worden gewijzigd. Het leger beschermt gegevens en ook in commerciële organisaties is het van belang dat bepaalde strategische gegevens vertrouwelijk blijven en de integriteit niet kan worden aangetast. Hieronder ga ik in op een aantal cryptografische methoden die ingezet kunnen worden bij het waarborgen van de authenticiteit, de integriteit en/of de vertrouwelijkheid.

Cryptografische hash functies[75]

Als (vooral Amerikaanse) juristen spreken over het authentificeren van elektronische gegevens lijkt dit misschien in eerste instantie vreemd, omdat informatici alleen over authentificeren spreken als het gaat over personen. Elektronische gegevens vertonen op het eerste gezicht geen kenmerken, zoals een persoon. Persoonlijke kenmerken (zoals een vingerafdruk, kennis van zaken, stemgeluid, irisscan, gelaatsherkenning, enzovoorts) die kunnen worden gebruikt bij het authentificeren zijn er dan ook niet. Toch is het authentificeren van elektronische gegevens mogelijk. Het gaat hier dan in feite om het vaststellen van de integriteit van de gegevens. Dit kan bijvoorbeeld door deze te vergelijken met een kopie van deze gegevens die is gemaakt op een eerder moment of door te vergelijken met een 'vingerafdruk' van de gegevens.[76] In tegenstelling tot wat bij de authentificatie van personen het geval is, hebben de elektronisch gegevens niet zomaar een middel om geauthentificeerd te worden. Echter, de elektronische gegevens hebben wel degelijk kenmerken op basis waarvan een 'vingerafdruk' kan worden gecreëerd. Een van de middelen die kan worden gecreëerd is het creëren van een zogenaamde cryptografische

---

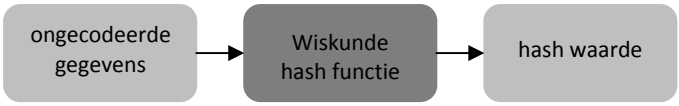
73 *Encryptie* komt van het Griekse word *kryptos*, dat verbergen betekent.

74 T.H. Barr, *Invitation to Cryptology*, New Jersey: Prentice Hall, 2002, p. vii (p. 1 t/m 55 voor een complete historie); A. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, Boca Raton: CRC Press 1997, p. 1.

75 Bijvoorbeeld SHA en MD5.

76 F. Stajano, *Security for Ubiquitous Computing*, Chichester: John Wiley & Sons, Ltd, 2002, p. 70.

hash waarde. Een *hash* waarde kan gezien worden als een vingerafdruk van een elektronisch bericht.[77] Om een *hash* waarde te genereren wordt uit een elektronisch bericht door middel van een wiskundige functie een *hash* waarde berekend die uniek is voor dat bericht (zie afbeelding 3.2).



Afbeelding 3.2: Functionele benadering van totstandkomen van een *hash* waarde

Een cryptografische *hash* functie moet specifieke eigenschappen bezitten. Ten eerste moet deze slechts één richting op kunnen werken.[78] Dat will zeggen dat uit de elektronische gegevens wel een *hash* waarde kan worden gecreëerd, maar dat uit de *hash* waarde nooit het originele bericht kan worden gegenereerd.[79] Ten tweede moet de hash waarde *collision free* zijn.[80] Als gegevens A leiden tot een *hash* waarde A, dan moet de kans heel klein zijn dat ook de gegevens B, C, D, enzovoorts, leiden tot de *hash* waarde van A. Ten derde mogen *hash* waardes van bijna gelijke gegevens, niet bijna gelijk aan elkaar zijn. Als er slechts één letter of cijfer verandert, dan dient de *hash* waarde ook ingrijpend te verschillen van de waarde van het oorspronkelijke bericht.

Als eenmaal uit het originele bericht een *hash* functie is berekend kan het verstuurd worden. Hierbij wordt de *hash* waarde ofwel via een andere weg ofwel door middel van encryptie gestuurd naar de ontvanger van het bericht. Als deze ontvanger zowel het bericht als de *hash* waarde heeft ontvangen kan deze met de coderingsmethode opnieuw de *hash* waarde berekenen.[81] Is deze niet identiek aan de ontvangen *hash* waarde en staat vast dat er geen fouten zijn gemaakt bij het creëren van de *hash* waardes, dan kan met zekerheid geconcludeerd worden dat het bericht en/of de *hash* waarde zijn gemodificeerd.[82]

---

77 F. Stajano, *Security for Ubiquitous Computing*, Chichester: John Wiley & Sons, Ltd, 2002, p. 70; B. Schneier, *Secrets & Lies, Digital Security in a Networked World*, New York: John Wiley & Sons, Inc., 2000, p. 94.

78 A. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, Boca Raton: CRC Press 1997, p. 33.

79 R. Anderson, Security Engineering, *A Guide to Building Dependable Distributable Distributed Systems*, New York: Wiley Computer Publishing, p. 78.

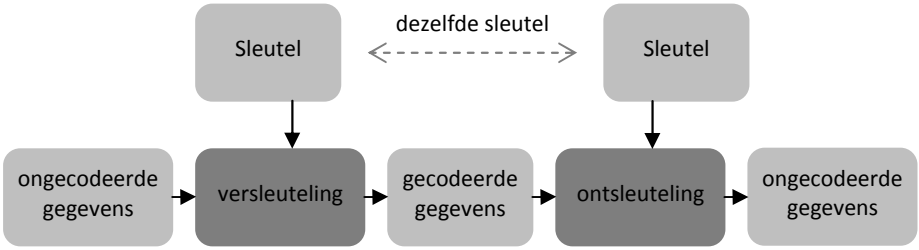
80 D. Gollman, *Computer Security*, Chichester: John Wiley & Sons, Ltd, 2006, p. 191.

81 D.R. Stinson, Cryptography, Theory and Practise, Boca Raton: CRC Press 1995, p. 1.

82 C.P. Pfleeger, *Security in Computing*, New Jersey: Prentice Hall International, Inc. 1997, p. 97.

Symmetrische versleuteling[83]

De eerste versleuteling werd ingezet om de vertrouwelijkheid van gegevens te vergroten.[84] Hierbij werd enkel gebruik gemaakt van een coderingssysteem om gegevens onleesbaar en onherkenbaar te maken voor derden (zie afbeelding 3.3). Het coderingssysteem bestaat uit een algoritme en een sleutel. Het algoritme is openbaar. Daarbij wordt gebruikgemaakt van één sleutel die partijen delen.



Afbeelding 3.3: Symmetrische versleuteling

Een bekende vorm van symmetrische versleuteling is de methode waar Gaius Julius Caesar gebruikt van maakte. Zijn methode van versleuteling was eenvoudig. Iedere letter werd vervangen door een letter drie plaatsen verderop in het alfabet. Hierdoor wordt de A een D, B een E, C een F enzovoorts.[85] De laatste drie letters werden vervangen voor de eerste drie letters van het alfabet (zie afbeelding 3.4).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Afbeelding 3.4: Coderingssysteem gebruikt door Caesar

Een boodschap die luidt:'Onze nieuwste telefoon zal begin maart gelanceerd worden' zal dan worden:

'Rqch qlhxzvwh whohirrq cdo ehjlq pdduw jhodqfhhug zrughq.'

De caesariaanse vorm van versleuteling, ook wel *shift encryptie* (verplaatsings versleuteling) genoemd is vrij eenvoudig te kraken, omdat de sleutel niet heel moeilijk te achterhalen is.

---

83 Bijvoorbeeld het verouderde, maar nog steeds gebruikte DES (dat in pinautomaten wordt gebruikt) en het op dit moment veel gebruikte AES (dat vaak in webwinkels wordt gebruikt).

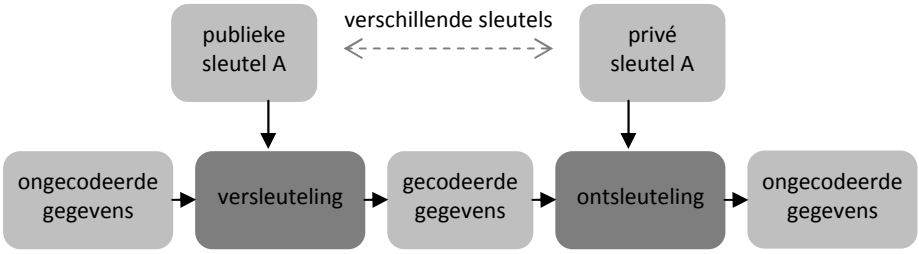
84 B. Schneier, *Secrets & Lies, Digital Security in a Networked World*, New York: John Wiley & Sons, Inc., 2000, p. 103 t/m 106.

85 T.H. Barr, *Invitation to Cryptology*, New Jersey: Prentice Hall, 2002, p. 5.

Het zwakke punt bij symmetrische versleuteling is dat beide partijen één sleutel delen. Als de sleutel van een van de partijen wordt gestolen of de partij maakt de sleutel per ongeluk openbaar of bekend aan anderen, dan is het bericht niet meer vertrouwelijk.

Asymmetrische versleuteling[86]

Een andere vorm van versleuteling is asymmetrische versleuteling. Deze vorm van versleuteling dient niet alleen de vertrouwelijkheid van de gegevens, maar ook de integriteit.[87] Tevens wordt er tegemoet gekomen aan het bezwaar dat kleeft aan het feit dat beide partijen één sleutel delen zoals dat bij symmetrische versleuteling het geval is. Bij asymmetrische versleuteling bestaat het coderingssysteem uit een combinatie van een sleutel (code) en een algoritme.[88] Het algoritme is in veel gevallen openbaar.[89] De sleutels echter zijn geheim. Er wordt een sleutelpaar gegenereerd waarvan 1 sleutel een privésleutel is en de andere sleutel de publieke sleutel is. Met zowel de privé sleutel als de publieke sleutel kunnen elektronische gegevens worden versleuteld en ontsleuteld. Echter, de met de privé sleutel versleutelde gegevens kunnen alleen met de publieke sleutel ontsleuteld worden en de met de publieke sleutel versleutelde gegevens kunnen alleen met de privé sleutel ontsleuteld worden. De privé sleutel is slechts bekend bij persoon A. De publieke sleutel kan verspreid worden onder één of meerdere personen (B, C, D, enz.). De personen B, C en D kunnen allemaal een bericht versturen naar A en daarbij gebruikmaken van de publieke sleutel van A. Zij versleutelen het bericht dan met de privé sleutel van A en sturen dan hun versleutelde berichten naar A. A kan het bericht met zijn eigen privé sleutel ontsleutelen. B, C en D kunnen er zeker van zijn dat alleen A het bericht kan lezen. De vertrouwelijkheid en de integriteit van het bericht zijn op deze manier gegarandeerd.



Figuur 3.5: Asymmetrische versleuteling / ontsleuteling

86 Bijvoorbeeld RSA.

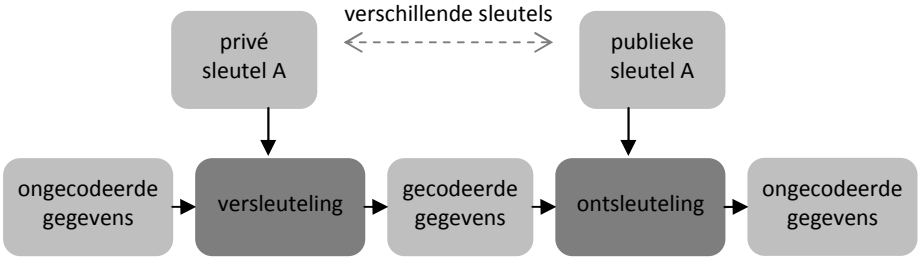
87 C.P. Pfleeger, *Security in Computing*, New Jersey: Prentice Hall International, Inc. 1997, p. 21.

88 T. Daler, R. Gulbrandsen, B. Melgård, T. Sjølstad, *Security of Information and Data*, Chichester: Ellis Horwood Ltd, p. 1989, p. 82.

89 Het idee van openbare algoritmen komt van Kerckhoffs en staat nu ook wel bekend als Kerkhoffs principle. Zie ook: D. Gollman, *Computer Security*, Chichester: John Wiley & Sons, Ltd, 2006, p. 188.

Het zwakke punt van dit systeem is dat A wel integere gegevens ontvangt die niet door andere gelezen konden worden, maar dat het onzeker blijft of de gegevens wel daadwerkelijk van B en C en D afkomstig zijn. De berichten zouden ook best door persoon F, persoon G en persoon H verstuurd kunnen zijn. Met andere woorden: er ontbreekt een methode om de afzender te authentificeren.

Stel nu dat de methode omgekeerd zou functioneren (zie afbeelding 3.5; deze afbeelding lijkt op afbeelding 3.4, maar de privé en de publieke sleutels zijn omgedraaid.). De privé sleutel is slechts bekend bij persoon A. De publieke sleutel kan worden verspreid onder één of meerdere personen (B, C, D, enz.). A kan een bericht versturen naar B en daarbij gebruikmaken van zijn privé sleutel. A versleutelt het bericht dan met zijn privé sleutel en stuurt het versleutelde bericht naar B. B kan het bericht met de publieke sleutel van A ontsleutelen. B kan er behoorlijk zeker van zijn dat het bericht van A afkomstig is. Met andere woorden: de authenticiteit van A is gewaarborgd. Omdat de authenticiteit van de verzender gewaarborgd wordt, noemt men deze vorm van versleuteling ook wel signing of digitale handtekening.



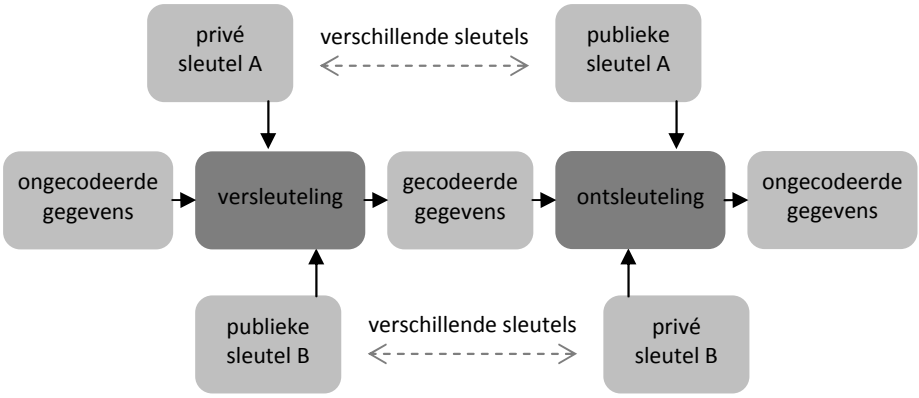
Figuur 3.6: Asymmetrische versleuteling / ontsleuteling (signing / digitale handtekening)

Ook in dit systeem zit echter een zwak punt: iedereen die de publieke sleutel van A bezit, kan het bericht ontsleutelen. Als de personen C en D ook een publieke sleutel hebben, dan kunnen ook zij het bericht ontsleutelen. Hierdoor is het bericht niet langer vertrouwelijk.

Dubbele asymmetrische versleuteling

Om aan de bezwaren van bovenstaande bezwaren die kleven aan enkele asymmetrische versleuteling (of wel authenticiteit en geen vertrouwelijkheid, of wel vertrouwelijkheid en geen authenticiteit) kan er gebruik worden gemaakt van dubbele asymmetrische versleuteling. Hiervoor is een tweede sleutelpaar noodzakelijk. Van dit tweede sleutelpaar heeft B de privé sleutel en kunnen andere personen zoals A, C en D de publieke sleutel in bezit hebben. A kan het oorspronkelijke bericht versleutelen met de eigen privé sleutel en daarna nogmaals versleutelen met de publieke sleutel van B. Als B het bericht

ontvangt dan kan alleen hij het bericht ontsleutelen met zijn eigen privé sleutel en de publieke sleutel van A. Niet alleen zijn nu de vertrouwelijkheid en de integriteit gewaarborgd, maar tevens kan er gesteld worden dat het bericht afkomstig is van persoon A en alleen door persoon B gelezen kan worden.



Figuur 3.7: Dubbele asymmetrische versleuteling / ontsleuteling

Wordt er gebruik gemaakt van dubbele asymmetrische versleuteling, dan zijn zowel de authenticiteit, de integriteit en de vertrouwelijkheid in behoorlijke mate beschermd. Hoe groot deze bescherming is, hangt mede af van het coderingssysteem (welke en de lengte van de sleutels en welke algoritme zijn gebruikt)[90].

Combinatie van verschillende methoden
De methoden die hierboven beschreven zijn kunnen in combinatie met elkaar worden toegepast. Een nadeel van asymmetrische versleuteling is namelijk dat het veel tijd (lees: geld) kost om te berekenen. Daarom worden vaak niet alle gegevens asymmetrisch versleuteld, maar wordt bijvoorbeeld eerst een *hash* waarde berekend en wordt deze *hash* waarde vervolgens asymmetrisch versleuteld. Op deze manier kan een boodschap die niet vertrouwelijk behandeld hoeft te worden, maar waar de authenticiteit en de integriteit gewaarborgd moeten worden, worden verstuurd.

3.5 Samenvatting

Vanuit de literatuur wordt zwaar ingezet op technische oplossingen om de bewijskracht van elektronische gegevens te vergroten dan wel te garanderen.

[90] B. Schneier, *Secrets & Lies, Digital Security in a Networked World*, New York: John Wiley & Sons, Inc., 2000, p. 103 t/m 106.

Om de betrouwbaarheid van elektronische gegevens als bewijsmiddel te vergroten, is het van belang de authenticiteit en de integriteit van de gegevens te vergroten dan wel te garanderen. Een aantal veelgebruikte oplossingen die dit kunnen bewerkstelligen zijn in dit hoofdstuk besproken. Dit zijn de gebruikmaking van wachtwoorden of andere identificerende middelen, *hashing* en verschillende vormen van versleuteling. Deze verschillende methoden kunnen al dan niet in combinatie met elkaar worden gebruikt.

4 Elektronische gegevens als bewijsmiddel in het Nederlandse civiele recht

4.1 Inleiding

Als twee partijen een geschil hebben over feiten of rechten, dan kunnen zij naar de rechter stappen. Deze zal vervolgens alle gestelde feiten en rechten afwegen, een oordeel vormen en komen tot een beslissing. Bij deze afweging is de rechter lijdelijk. Art. 149, lid 1 Rv stelt namelijk: *"Tenzij uit de wet anders voortvloeit, mag de rechter slechts die feiten of rechten aan zijn beslissing ten grondslag leggen, die in het geding aan hem ter kennis zijn gekomen of zijn gesteld en die overeenkomstig de voorschriften van deze afdeling zijn komen vast te staan. Feiten of rechten die door de ene partij zijn gesteld en door de wederpartij niet of niet voldoende zijn betwist, moet de rechter als vaststaand beschouwen, behoudens zijn bevoegdheid bewijs te verlangen, zo vaak aanvaarding van de stellingen zou leiden tot een rechtsgevolg dat niet ter vrije bepaling van partijen staat."* De door partijen betwiste feiten dienen hard gemaakt te worden door middel van bewijs. Art. 150 Rv stelt namelijk: "*De partij die zich beroept op rechtsgevolgen van door haar gestelde feiten of rechten, draagt de bewijslast van die feiten of rechten, tenzij uit enige bijzondere regel of uit de eisen van redelijkheid en billijkheid een andere verdeling van de bewijslast voortvloeit.*" Uit art. 150 Rv volgt dan ook het belang van bewijsmiddelen en het hebben daarvan. Als een partij zich met succes wil kunnen beroepen op de rechtsgevolgen van gestelde feiten, dient deze partij deze feiten te bewijzen. Zij draagt de bewijslast, tenzij enige bijzondere regel of de eisen van redelijkheid en billijkheid een uitzondering vormen op de hoofdregel van bewijslastverdeling. Het is van belang dat de partijen zich tijdens hun handelen bewust zijn van deze bewijslastregel. Dit geldt in het bijzonder voor handelingen waarbij bepaalde rechtsgevolgen van belang zijn voor de partijen. Het is dan ook niet verwonderlijk dat veel partijen bewijs vergaren ook al is er geen strijd om de rechtsfeiten. Het vastleggen, verzamelen en bewaren van bewijsstukken maakt voor veel zakelijke partijen een substantieel deel uit van hun werkzaamheden.

Artikel 150 Rv geeft een, naar mijn mening, positieve opdracht tot bewijslevering. Hiermee bedoel ik dat artikel 150 Rv slechts de positieve opdracht geeft de door de stellende partij gestelde feiten te bewijzen. Art. 150 Rv geeft in beginsel niet de ruimte voor een negatieve bewijsopdracht waarbij de niet-stellende partij de door de stellende partij gestelde feiten dient te ontkrachten. In beginsel, want door het betwisten van de feiten zoals gesteld

door de stellende partij, maakt de niet-stellende partij een begin met het ontkrachten. Daarnaast kan een negatieve bewijsopdracht in een enkel aantal gevallen worden afgeleid uit enige bijzondere regel of uit de eisen van redelijkheid en billijkheid. Meer concreet kan dan gedacht worden aan bewijsvermoedens.

Dit onderzoek is gericht op criteria die in de wetgeving en rechtspraak worden gesteld aan elektronische gegevens die dienen als bewijsmiddel. Als een partij die elektronische gegevens gebruikt, wil aantonen welke feiten zich hebben voorgedaan, dan is het in het licht van art. 150 Rv van belang om voldoende bewijsmiddelen te creëren, vast te leggen, te verzamelen en te bewaren, om zo de gestelde feiten te kunnen bewijzen. Al het gecreëerde en verzamelde bewijs kan dan worden gebruikt voor het onderzoek ter zitting naar de feiten. Een belangrijke vraag is nu hoe het Nederlandse recht omgaat met bewijsmateriaal. Welke middelen worden toegelaten en hoe worden deze gewaardeerd? Zijn er daarbij middelen aan welke een grotere dan wel dwingende bewijswaarde worden toegekend en onder welke voorwaarden hebben deze een hogere dan wel dwingende bewijswaarde?

Het Nederlandse bewijsstelsel kent een aantal specifieke kenmerken waarmee het zich onderscheidt van andere bewijsstelsels. Deze kenmerken en vraagstukken zullen in dit hoofdstuk aan de orde komen. In de volgende paragrafen zal ik ingaan op de plaats van het civiele bewijsrecht in het Nederlandse recht. In de derde paragraaf zullen twee belangrijke uitgangspunten in het Nederlandse bewijsrecht besproken worden, namelijk de autonomie van partijen en de lijdelijkheid van de rechter. De vierde paragraaf gaat vervolgens nader in op de stelplicht, de bewijslast en bewijsvermoedens. Daarna zal in de vijfde paragraaf de theorie van de vrije bewijsleer nader beschouwd worden. Centraal binnen deze leer staan het open stelsel van bewijsmiddelen en de vrije bewijswaardering, op welke nader ingegaan zal worden in paragraaf zes en zeven. Paragraaf acht gaat over elektronische gegevens in de jurisprudentie. In aansluiting daarop zal in paragraaf negen onderzocht worden waarom er zo weinig explicietgemaakte bewijscriteria te vinden zijn in de jurisprudentie. Het Nederlandse recht kent, evenals het Duitse recht en in tegenstelling tot het Amerikaanse recht, uitzonderingen op de hoofdregel van vrije bewijswaardering, namelijk: de dwingende bewijskracht die aan akten moet worden toegekend. Een belangrijke rol is hierbij weggelegd voor de elektronische onderhandse akte, het elektronische geschrift en de elektronische handtekening. De elektronische handtekening is van speciaal belang, omdat deze niet alleen een vereiste is voor de totstandkoming van een onderhandse akte in elektronische vorm, maar tevens een authentificatiefunctie heeft, waardoor deze mogelijk ook voor andere toepassingen dan de akte een niet onbelangrijke rol in het bewijsrecht kan spelen. Op dit alles zal in de paragrafen tien tot en met veertien nader worden

ingegaan. Vervolgens is in paragraaf vijftien aandacht voor de bewijsovereenkomst. Dit middel is niet van invloed op de betrouwbaarheid van bewijsmiddelen, maar kan wel de bewijspositie van partijen in belangrijke mate reguleren. Als laatste zal ik in paragraaf zestien de belangrijkste punten samenvatten en de conclusies geven. Deze conclusies bevatten een opsomming van de juridische vereisten die aan bewijsmiddelen gesteld worden in het Nederlandse recht met het oog op het definiëren van betrouwbaarheidseisen die gesteld kunnen worden aan elektronische gegevens.

4.2 Plaats van het Nederlandse civiele bewijsrecht

Het Nederlandse civiele bewijsrecht is geregeld in het Wetboek van Burgerlijke Rechtsvordering (Rv) in de negende afdeling van de tweede titel van het eerste boek in de artikelen 149 tot en met 207. Deze artikelen zijn ondergebracht in acht paragrafen, namelijk: 1) algemene bepalingen van bewijsrecht, 2) akten en vonnissen, 3) openlegging van boeken, bescheiden en geschriften, 4) getuigen, 5) voorlopig getuigenverhoor, 6) deskundigen, 7) plaatsopneming en bezichtiging en 8) voorlopig bericht of verhoor van deskundigen, voorlopige plaatsopneming en bezichtiging.

Het civiele bewijsrecht is onderdeel van het civiele recht en is uitsluitend van toepassing op rechtsbetrekkingen in een horizontale verhouding; daarbij staan twee civiele partijen tegenover elkaar. Deze civiele partijen zijn niet altijd natuurlijke personen of rechtspersonen als verenigingen, stichtingen en vennootschappen, maar kunnen ook bestaan uit rechtspersonen met een publiekrechtelijk karakter zoals gemeenten, provinciën en de staat. In een geding waarbij een rechtspersoon met een publiekrechtelijk karakter tegenover een natuurlijk persoon of een rechtspersoon met privaatrechtelijk karakter staat, zijn tevens een aantal regels uit het publiekrecht van toepassing.[91] Deze vallen buiten het bestek van dit onderzoek en daar zal ik verder ook niet op ingaan.

4.3 Lijdelijkheid van de rechter in het civiele bewijsrecht

Indien partijen een geschil hebben, kunnen zij zich tot de rechter wenden en de rechter kan beslissen welke rechten aan de partijen toekomen. Om tot een beslissing te komen, is er een aantal regels dat door de partijen en de rechter in acht genomen dient te worden. De rechter heeft geen ongebreidelde macht om in alle vrijheid tot een beslissing te komen; de rechter wordt namelijk aan verschillende wettelijke regels en beginselen gebonden. Een belangrijk beginsel

[91] Zie hiervoor art. 3:1, lid 2 Awb.

in het burgerlijk procesrecht is het uitgangspunt dat de rechter zich lijdelijk dient op te stellen.[92] De lijdelijkheid van de rechter vloeit voort uit de partijautonomie die geldt in het burgerlijk proces; partijen bepalen de opzet en de omvang van het geschil.[93] De lijdelijkheid van de rechter is echter niet absoluut. In verschillende gevallen krijgt de rechter de bevoegdheid om zich ambtshalve met het proces te bemoeien.[94] Daarnaast is de rechterlijke lijdelijkheid onderhevig aan veranderende opvattingen over de rol van de rechter en partijen. Ten gevolge hiervan is er de afgelopen decennia een trend waarneembaar waarbij gepleit wordt voor meer invloed van de rechter in het geding.[95] Echter vooralsnog geldt nog steeds als uitgangspunt dat partijen de aanvang/beëindiging van het proces bepalen en partijen zelf de rechtsfeiten in dienen te brengen.

De lijdelijkheid van de rechter is voor het bewijsrecht vastgelegd in art. 149, lid 1 Rv. De eerste zin van art. 149, lid 1 Rv ziet op de rechtsfeiten en rechten waarop de rechter zijn beslissing baseert. Deze mogen namelijk niet ambtshalve door de rechter worden aangevuld. Enkel de feiten en de rechten die door de partijen in het geding zijn gebracht mogen door de rechter worden gebruikt om zijn beslissing op te baseren.[96] De tweede zin ziet op de gevolgen van het niet betwisten of het niet voldoende betwisten van de feiten die door een partij gesteld zijn. De rechter kan bij niet of onvoldoende betwisting door de wederpartij de feiten als vaststaand aannemen zonder dat bewijs wordt verlangd. Slechts indien aanvaarding van de stellingen zou leiden tot een rechtsgevolg dat niet ter vrije bepaling van partijen staat, bijvoorbeeld als er sprake is van dwingend recht of onweerlegbare bewijsvermoedens, mag de rechter bewijs verlangen van de stellende partij.

De lijdelijkheid van de rechter is van grote invloed op de inbreng van bewijsstukken. Zoals blijkt uit art. 149, lid 1 Rv behoeven feiten of rechten die

---

92 De lijdelijkheid en partijautonomie van partijen wordt echter steeds meer teruggedrongen. Met de invoering van het nieuwe bewijsrecht heeft de rechter een aantal middelen in handen gekregen om het proces te sturen. Zie hiervoor: G.R. Rutgers (red.), *Parlementaire geschiedenis van het bewijsrecht in civiele zaken*, Deventer: Kluwer 1988, p. 63 e.v.; H.J. Snijders geeft aan dat dit beginsel steeds meer ter discussie wordt gesteld. Zie hiervoor: M.L Hendrikse, A.W. Jongbloed (red.), *De Toekomst van het Nederlands burgerlijk procesrecht*, Deventer: Kluwer 2004, p. 27.

93 G.R. Rutgers (red.), *Parlementaire geschiedenis van het bewijsrecht in civiele zaken*, Deventer: Kluwer 1988, p. 64.

94 Zie bijvoorbeeld de ambtshalve bevolen comparitie in art. 191 Rv.

95 Zie: W.D.H. Asser, H.A. Groen, J.B.M. Vranken, I.N. Tzankova, *Een nieuwe Balans: Interim-rapport Fundamentele herbezinning Nederlands Burgerlijk Procesrecht*, Den Haag 2003, p. 79. Voor Ingelse blijft de partijautonomie uitgangspunt. Zie hiervoor: P. Ingelse (red.), *Commentaren op fundamentele herbezinning*, Nijmegen: Ars Aequi Libri 2004, p.45 t/m 49. Zie ook: J.M.J. Chorus, *De lijdelijkheid van de rechter. Historie van een begrip* (oratie Leiden), Deventer: Kluwer 1987, p. 1 en M.L Hendrikse, A.W. Jongbloed (red.), *De Toekomst van het Nederlands burgerlijk procesrecht*, Deventer: Kluwer 2004, p. 27.

96 Overigens is dit iets anders dan het ambtshalve aanvullen van de rechtsgronden. Hiertoe is de rechter wel bevoegd op grond van art. 25 Rv.

niet of niet voldoende betwist worden in beginsel geen bewijs. De rechter zal in dat geval het feit of het recht als waar moeten aannemen, aangezien hij lijdelijk is. Pas als een feit of recht betwist wordt, zal de rechter toekomen aan het verlangen van bewijs. Nu zal een rechter bijna altijd toekomen aan het verlangen van bewijs daar juist een conflict over het bestaan van de gestelde feiten of rechten heeft geleid tot de stap naar de rechter. Bewijs zal daarom ook bijna altijd een rol spelen om te bepalen of de gestelde feiten of rechten de stellende partij ook daadwerkelijk toekomen.

De vraag of het tot een bewijsopdracht komt, hangt af van welke bewijsstukken partijen reeds in het geding hebben gebracht. Als partijen meteen bewijsstukken inbrengen om de door hen gestelde feiten en rechten aan te tonen, kan de rechter meteen uitspraak doen. Slechts in gevallen waarin bewijsmiddelen die zijn ingebracht de rechter onvoldoende overtuigen van de gestelde feiten en deze bewijsmiddelen geen dwingend bewijs opleveren van deze feiten,[97] zal aanvullend bewijs mogen worden geleverd in de vorm van een bewijsaanbod. Overigens mag in alle gevallen tegenbewijs ingebracht worden, dus ook waar het dwingend bewijs betreft. De rechter heeft de bevoegdheid om bewijsmiddelen ambtshalve te waarderen.[98] Indien hij een bewijsmiddel niet betrouwbaar vindt, staat het hem vrij het bewijsmiddel dan ook als onvoldoende betrouwbaar te waarderen. Het feit of recht is daarmee niet bewezen en aanvullend bewijs zal het feit of recht moeten aantonen. Mochten zich nieuwe feiten voordoen of ter sprake komen, dan kan de rechter ook een bewijsopdracht geven.

4.4 Stelplicht, bewijslast en bewijsvermoedens

In paragraaf 1 van dit hoofdstuk haal ik het belang van de stelplicht en de bewijslast voor het civiele bewijsrecht aan. De bewijslast is gebaseerd op de gematigd-objectiefrechtelijke leer welke is vervat is art. 150 Rv: "*De partij die zich beroept op rechtsgevolgen van door haar gestelde feiten of rechten, draagt de bewijslast van die feiten of rechten, tenzij uit enige bijzondere regel of uit de eisen van redelijkheid en billijkheid een andere verdeling van de bewijslast voortvloeit.*" Aan de keuze voor de gematigd-objectiefrechtelijke leer is een lange discussie voorafgegaan. Aanhangers van twee theorieën, namelijk de procesrechtelijke of billijkheidstheorie en de objectiefrechtelijke theorie streden lange tijd met elkaar welke leer het meest rechtvaardig was.[99] De

---

97 Zoals akten en in kracht van gewijsde gegane strafvonnissen.

98 Art. 152, lid 2 Rv. Zie ook: J.E. Bosch-Boesjes, *Lijdelijkheid in geding* (diss. Groningen), Kluwer, Deventer: 1991, p. 159.

99 De procesrechtelijke of billijkheidstheorie gaat uit van gelijkheid van partijen. Dit leidt tot een bewijslastverdeling op grond van billijkheid in het concrete geval. Voor meer hierover zie: C. Asser, A. Anema, P.J. Verdam, *Handleiding tot de beoefening van het Nederlands Burgerlijk Recht, Vijfde*

wetgever heeft uiteindelijk gekozen voor de gematigde-objectiefrechtelijke leer. Met de keuze voor deze leer heeft de wetgever naar mijn mening een afweging gemaakt tussen rechtszekerheid en rechtvaardigheid. Partijen weten namelijk vooraf reeds wie wat dient aan te tonen en kunnen met het oog hierop reeds in een vroeg stadium anticiperen door het creëren en bewaren van bewijsmiddelen. In een aantal gevallen echter kan de objectiefrechtelijke bewijslastverdeling onrechtvaardig uitpakken. Daarom is deze leer gematigd; de rechter kan op grond van een bijzondere regel of op grond van de eisen van redelijkheid en billijkheid een andere bewijslast nodig achten.

Bijzondere regels of eisen van redelijkheid en billijkheid kunnen dus tot gevolg hebben dat er afgeweken wordt van de normale bewijslastverdeling. Een andere manier om in te grijpen in de bewijslast van partijen kan door middel van bewijsvermoedens. Opgemerkt dient te worden dat bewijsvermoedens geen omkering van de bewijslast inhouden, maar slechts een verlichting van de bewijslast.[100] Dit in tegenstelling tot bijzondere regels of eisen van redelijkheid en billijkheid.

Bewijsvermoedens zijn "*gevolgtrekkingen welke de wet of de regter uit eene bekende tot eene onbekende daadzaak afleidt*".[101] Ze stammen uit het oud BW waar deze vermoedens expliciet geregeld werden in het bewijsrecht. De bewijsvermoedens zijn met het nieuwe Rv en nieuw BW niet geheel verdwenen; er wordt zelfs expliciet rekening gehouden met bewijsvermoedens getuige het gebruik van bepaalde terminologie.[102] Zo kent het BW bepalingen als "wordt vermoed" of "wordt geacht". Ook worden bewijsvermoedens nog steeds in nieuwe wetgeving opgenomen (bijvoorbeeld art. 3:15a BW dat nader zal worden besproken).

Bewijsvermoedens bestaan uit wettelijke vermoedens en feitelijke vermoedens. Wettelijke vermoedens zijn "dezoodanige welke, uit kracht eener bijzondere wetsbepaling, met zekere handelingen of met zekere daadzaken verbonden zijn." [103] Ze worden ook wel omschreven als "voorschriften waarin de

---

deel – van Bewijs, Zwolle: W.E.J. Tjeenk Willink 1953, p. 80 t/m 86; C.W. Star Busmann, L.E.H. Rutten, *Hoofdstukken van burgerlijke rechtsvordering*, De Erven F. Bohn N.V.: Haarlem 1972, nr. 213 t/m 215, p. 180 t/m 185. De objectiefrechtelijke theorie gaat daarentegen uit van het toepassen van objectieve rechtsregels op het concrete geval, waarbij op iedere partij de bewijslast rust van de feiten waaraan het objectieve recht de ingeroepen rechtsgevolgen heeft verbonden. Zie ook: Pitlo, Hidma, T.R., Rutgers, G.R., *Het Nederlands burgerlijk recht: Bewijs, deel 7*, Deventer: Kluwer 2004, p. 32.

100 H.J. Snijders, C.J.M. Klaassen, G.J. Meijer, *Nederlands burgerlijk procesrecht, Deventer*: Kluwer 2007, p. 224.

101 Art. 1952, lid 1 BW (oud).

102 A.S. Hartkamp, *Compendium van het vermogensrecht volgens het nieuwe Burgerlijk Wetboek*, Deventer: Kluwer 1999, nr. 11, p. 11.

103 Art. 1953 BW (oud).

bewijskracht van bepaalde feitelijke gegevens is geregeld".[104] Feitelijke vermoedens zijn niet nader gedefinieerd, maar uit art. 1959 BW (oud) kan worden afgeleid dat dit vermoedens zijn "welke niet op de wet zelve gegrond zijn". Het verschil tussen wettelijke vermoedens en feitelijke vermoedens is dat bij wettelijke vermoedens een redenering en de gevolgen daarvan niet worden overgelaten aan het oordeel van de rechter (hier loopt de rechter dus tegen de grenzen van zijn discretionaire bevoegdheid aan), maar in de wet zijn genoemd. Bij feitelijke vermoedens daarentegen mag de rechter op grond van zijn discretionaire bevoegdheid gevolgtrekkingen doen naar eigen oordeel. Het betreft vermoedens waarbij de rechter tot vaststelling van een rechtsfeit komt door middel van algemene ervaringsregels dan wel feiten van algemene bekendheid.[105] De rechter mag dan bijvoorbeeld feiten als waar aannemen, ook al zijn deze feiten zelf niet bewezen, maar enkel aannemelijk op grond van andere wel bewezen feiten. Dit onderzoek zal in beginsel alleen ingaan op de wettelijke bewijsvermoedens, omdat de feitelijke bewijsvermoedens niet in de wet zijn opgenomen en afhankelijk zijn van de omstandigheden; feitelijke vermoedens worden in dit onderzoek behandeld alleen voor zoverre deze in de jurisprudentie aan de orde komen en van belang zijn in het kader van dit onderzoek naar elektronische gegevens als bewijsmiddel.

De wettelijke bewijsvermoedens bestaan uit weerlegbare vermoedens en onweerlegbare vermoedens. Weerlegbare vermoedens laten de partij die door een bewijsvermoeden in een benadeelde positie gesteld wordt, de mogelijkheid om het bewijsvermoeden te ontkrachten door tegenbewijs in te brengen. Weerlegbare bewijsvermoedens worden veelal consequent aangeduid met de woorden ' wordt vermoed'.[106] Onweerlegbare vermoedens kunnen daarentegen niet worden weerlegd; de wetgever heeft reeds op voorhand willen ingrijpen in de bewijspositie van partijen. Deze soorten bewijsvermoedens wordt veelal aangeduid met woorden als "worden geacht",[107] "heeft te gelden als" en "wordt aangemerkt als".

In het kader van dit onderzoek is het weerlegbare wettelijke bewijsvermoeden, dat is neergelegd in art. 3:15a BW, van belang. Hierbij wordt in lid 2 gesteld: "Een in lid 1 bedoelde methode wordt vermoed voldoende betrouwbaar te zijn, indien een elektronische handtekening voldoet aan de volgende eisen: (…)". In paragraaf 4.12 zal nader worden ingegaan op art. 3:15a BW.

---

104 Pitlo, Hidma, T.R., Rutgers, G.R., *Het Nederlands burgerlijk recht: Bewijs, deel 7*, Deventer: Kluwer 2004, p. 39.

105 H.J. Scheltema, *Nederlandsch burgerlijk bewijsrech*t, Zwolle: W.E.J. Tjeenk Willink 1939, p. 112 t/m 114.

106 Pitlo, Hidma, T.R., Rutgers, G.R., *Het Nederlands burgerlijk recht: Bewijs, deel 7*, 8e druk, Kluwer Deventer 2004, nr. 23, p. 41 en 42. Zie bijvoorbeeld: art. 3:15a BW.

107 Bijvoorbeeld in art. 3:34, lid 1 BW.

4.5 Theorie van de vrije bewijsleer

Uitgangspunt bij de toelating van bewijs en de bewijswaardering is de theorie van de vrije bewijsleer. Deze leer combineert twee principes welke in onderlinge samenhang beschouwd dienen te worden,[108] namelijk het principe van het open stelsel van bewijsmiddelen als het de toelating van bewijs betreft en het principe van de vrije bewijswaardering als het de bewijswaardering betreft. Het is dan ook geen toeval dat beide principes zijn gecodificeerd in art. 152 in lid 1 en lid 2 Rv. Wat beide principes betekenen en wat de gevolgen zijn voor bewijsmiddelen, en in het bijzonder elektronische bewijsmiddelen, zal in de volgende paragrafen aan de orde komen.

De theorie van de vrije bewijsleer is geënt op het idee dat de rechter in het civiele proces zoveel mogelijk de materiële waarheid dient te achterhalen en dat dit niet mag worden beperkt door formele bepalingen die op negatieve wijze ingrijpen in het proces om de materiële waarheid te achterhalen. Toch kent de Nederlandse wet beperkingen op de vrije bewijsleer door grenzen te stellen aan het open stelsel van bewijsmiddelen en de vrije bewijswaardering.[109] Deze grenzen zijn volgens de Staatscommissie voor de Nederlandse Burgerlijke Wetgeving ingegeven door het bestaan van een "polaire spanning" tussen het belang van de rechtszekerheid en het belang van een soepele toepassing van het bewijsrecht.[110] Deze commissie geeft aan dat met een te grote vrijheid de rechtszekerheid in gevaar komt, waarbij de uitkomst van een procedure onvoorspelbaar wordt. Daartegenover staat dat met een meer gesloten stelsel van bewijsmiddelen en een minder grote vrije bewijswaardering de rechtszekerheid groter wordt, maar het achterhalen van de materiële waarheid soms problematisch kan worden. De uitkomst van een gerechtelijke procedure zal dan leiden tot een formele waarheid. Dit laatste werd als onwenselijk beschouwd.

Aan de positie van technische middelen is in de voorverkenning van het wetsontwerp van het nieuwe burgerlijke bewijsrecht in de Tweede Kamer ook aandacht besteed. Technische middelen verdienen, ondanks dat deze middelen niet altijd even betrouwbaar zijn, geen uitzondering op de vrije bewijswaardering of op het principe dat ook slechts één bewijsmiddel voldoende bewijs kan opleveren om feiten aan te tonen. Men heeft voldoende vertrouwen in het inzicht en de integriteit van de rechter.[111]

---

108 Pitlo, Hidma, T.R., Rutgers, G.R., *Het Nederlands burgerlijk recht: Bewijs, deel 7*, achtste druk, Kluwer Deventer 2004, p. 65.

109 Art. 152, lid 1 en lid 2: de woorden "tenzij de wet anders bepaalt" duiden hierop.

110 G.R. Rutgers (red.), *Parlementaire geschiedenis van het bewijsrecht in civiele zaken*, Deventer: Kluwer 1988, p. 98.

111 G.R. Rutgers (red), *Parlementaire geschiedenis van het bewijsrecht in civiele zaken*, Deventer: Kluwer 1988, p. 99.

Zoals reeds gesteld in de voorgaande alinea's, kent het recht toch een aantal uitzonderingen op het beginsel van de vrije bewijsleer en in het bijzonder de vrije bewijswaardering; voorbeelden hiervan zijn de akte en het strafvonnis. Deze worden namelijk dwingende bewijskracht toegekend. Daarentegen kan een verklaring van de partijgetuige geen bewijs in het voordeel van haarzelf opleveren, tenzij de verklaring strekt ter aanvulling van onvolledig bewijs.[112] Juist in het licht van het feit dat er in het bijzonder ingegaan wordt op technische bewijsmiddelen is het interessant om te zien welke ontwikkelingen zich hebben voorgedaan een aantal decennia later. In 2003 is met de implementatie van richtlijn 1999/93/EG in de Nederlandse wet erkenning gekomen van de elektronische handtekening en de gelijkstelling van een analoog geschrift met een elektronisch geschrift, waardoor er sprake kan zijn van een elektronische akte waaraan dwingende bewijskracht kan worden toegekend. Hier is dus een ontwikkeling te zien waarbij de voortschrijdende techniek en veranderde inzichten in deze techniek een duidelijke invloed hebben gehad op de betrouwbaarheid die wordt toegekend aan technische middelen als bewijs. Werden er bij de parlementaire behandeling van het nieuwe bewijsrecht nog expliciet vragen gesteld of de vrije bewijswaardering misschien niet teveel ruimte gaf om technische middelen te snel als voldoende betrouwbaar te waarderen, anno 2003 wordt er aan technische bewijsmiddelen onder omstandigheden dwingende bewijskracht toegekend. De elektronische onderhandse akte is hiervan een voorbeeld. Hierop zal in paragraaf 4.14 nader worden ingegaan.

4.6 Toelating van bewijs

4.6.1 Toelating van bewijsmiddelen in het algemeen

Zoals reeds is gegeven in de vorige paragraaf, is de toelating van bewijsmiddelen in het Nederlandse recht geregeld in art. 152, lid 1 Rv. In dit artikel wordt gesteld: *"Bewijs kan worden geleverd door alle middelen, tenzij de wet anders bepaalt"*[113] In beginsel kunnen gestelde feiten bewezen worden door alle middelen. Het feit dat alle middelen worden toegelaten in het Nederlandse bewijsrecht duidt op een open stelsel van bewijsmiddelen.[114] Dit

112 Zie art. 164, lid 2 Rv.

113 Art. 152, lid 1 Rv.

114 Een tegenhanger van het open stelsel van bewijsmiddelen is het gesloten stelsel van bewijsmiddelen. Het Duitse recht kent middels het zogenaamde strengbeweis een gesloten stelsel van bewijsmiddelen; de bewijsmiddelen die worden toegelaten tot een rechtszaak worden limitatief in de wet opgesomd. Daarnaast bestaat er het Angelsaksisch stelsel, dat niet uitgaat van een open of gesloten stelsel, maar waarbij de bewijsmiddelen aan een aantal kwalitatieve eigenschappen moeten voldoen om te worden toegelaten tot een rechtszaak. Zie hoofdstuk 1 (inleiding) voor een vergelijking en hoofdstuk 5 (Duits recht) en 6 (Amerikaans recht) voor het gesloten en Angelsaksisch stelsel.

stelsel legt in beginsel geen restricties op aan de toelating van bewijsmiddelen. In beginsel, want de wet kan namelijk anders bepalen. Met de bewoordingen "tenzij de wet anders bepaalt", wordt uitgesloten dat andere rechtsvormende instanties kunnen ingrijpen in de bewijstoelating. De rechter mag dan wel toetsen of bewijsmiddelen zijn toegelaten, maar de rechter is hierbij gebonden aan wettelijke bewijsregels. Het staat de rechter niet vrij op eigen houtje en buiten de wettelijke regels om te bepalen dat bewijs niet is toegelaten.

Uit de bewoordingen van art. 152, lid 1 Rv kan dan wel worden opgemaakt dat de wet anders kan bepalen, maar geheel duidelijk is deze regel naar mijn mening niet. De regel lijkt namelijk bewijsmiddelen in zijn geheel niet toe te laten als de wet anders bepaalt. Dit is echter niet het geval. Art 152, lid 1 RV moet mijns inziens zo gelezen worden dat bepaalde feiten slechts door een bewijsmiddel dat expliciet in de wet genoemd is, kunnen worden bewezen en andere bewijsmiddelen niet worden toegelaten om die feiten te bewijzen. Dit sluit overigens niet uit dat diezelfde bewijsmiddelen wel worden toegelaten om andere feiten, waarvoor geen bewijsmiddelen door de wet worden voorgeschreven, te bewijzen. Het bewijsmiddel heeft dus beperkte bewijskracht in plaats van geheel geen bewijskracht.

De uitzondering dat niet voor alle feiten alle bewijsmiddelen gebezigd kunnen worden, hangt samen met het feit dat de wetgever sommige feiten dusdanig belangrijk acht dat deze alleen bewezen kunnen worden door een bepaald bewijsmiddel. Voorbeelden hiervan zijn het bewijzen van het bestaan van een in Nederland gesloten huwelijk door middel van een huwelijksakte en het bewijzen van het buiten de gemeenschap houden van goederen.[115] Ingevolge het tweede deel van de bepaling kan slechts de wet anders bepalen. Daarmee wordt de rechterlijke macht de mogelijkheid ontnomen om zelfstandig te bepalen welke middelen wel of niet worden toegelaten om bepaalde feiten te bewijzen.

4.6.2 Toelating van elektronische gegevens als bewijsmiddel

In beginsel vormt de wet geen beletsel om elektronische gegevens (code en data) toe te laten als bewijsmiddel. Bewijs kan namelijk geleverd worden door alle middelen. Voor elektronische en technische bewijsmiddelen geldt dan ook geen uitzondering, wat tevens bevestigd wordt in de parlementaire geschiedenis.[116] Ook Wieten stelt dat onder "alle middelen" moderne technische middelen, zoals foto's, films, geluidsbanden, videobanden, floppies,

[115] Art 1:78 BW en art 1:130 BW.

[116] G.R. Rutgers (red), *Parlementaire geschiedenis van het bewijsrecht in civiele zaken*, Deventer: Kluwer 1988, p. 99.

faxen, bloedproeven, fotokopieën en microfilms moeten worden verstaan. Zij geeft ook aan dat het voordeel van een open systeem is dat middelen die nu nog niet bestaan maar in de toekomst door de ontwikkeling van de techniek wèl aan de bestaande kunnen worden toegevoegd zonder dat een wetswijziging nodig is.[117] Voor elektronische gegevens als bewijsmiddel geldt hetzelfde. Slechts in enkele gevallen die in de wet omschreven zijn, kunnen feiten niet aangetoond worden met behulp van elektronische gegevens. Deze kunnen bijvoorbeeld niet ingezet worden om een in Nederland gesloten huwelijk te bewijzen. Dit geldt overigens voor alle middelen; technische en elektronische middelen als elektronische gegevens vormen dan ook hier geen uitzondering.

Zoals hierboven beschreven, stelt de wet soms dat bepaalde feiten slechts bewezen kunnen worden door een specifiek bewijsmiddel. Wat de wetgever in feite doet is het definiëren van een feit en het bewijsmiddel dat dit feit kan aantonen. In deze gevallen is het niet alleen van belang te kijken naar het bewijsmiddel zelf, maar ook naar het gedefinieerde feit. Als het aannemelijk is dat het desbetreffende feit eenvoudig met behulp van elektronische gegevens bewezen kan worden, dan zou misschien wel de vraag mogen worden opgeworpen of de wet de bewijsvoering met behulp van elektronische gegevens moet openstellen. In het kader van dit onderzoek zal ik mij echter niet richten op deze vraag naar de wenselijkheid van elektronische bewijsmiddelen. De wetgever heeft bepaald dat voor het vaststellen van sommige feiten slechts een specifiek bewijsmiddel kan worden toegelaten. De wetgever maakt weinig gebruik van regelingen die een specifiek bewijsmiddel toelaten en als zij dit al doet, dan is het enkel in bijzondere gevallen waar meestal belangen van derden in het geding zijn.

4.7 Bewijswaardering

4.7.1 Vrije bewijswaardering en de bewijsmaatstaf

Naast een open stelsel van bewijsmiddelen maakt het principe van vrije bewijswaardering onderdeel uit van de theorie van de vrije bewijsleer. Het principe van vrije bewijswaardering door de rechter is vervat in art. 152, lid 2 Rv: *"De waardering van het bewijs is aan het oordeel van de rechter overgelaten, tenzij de wet anders bepaalt."*[118]

Nadat het bewijs is toegelaten in een rechtszaak is het aan de rechter om het bewijs te waarderen. Daarbij is het oordeel van de rechter in beginsel bepalend

[117] H.L.G. Wieten, *Bewijs, Studiereeks burgerlijk procesrecht*, Kluwer: Deventer 2004, p. 14.
[118] Art. 152, lid 2 Rv.

voor de waardering van het bewijs. Het draait daarbij om de subjectieve en innerlijke overtuiging van de rechter.[119] Is de rechter overtuigd van de geloofwaardigheid van het bewijsmiddel of geeft het bewijsmiddel de rechter juist niet voldoende overtuiging?[120]

Vervolgens is de vraag in welke mate de rechter overtuigd moet zijn, zodat hij tot het oordeel kan komen dat een feit bewezen is. De Hoge Raad heeft zich nog nooit over de bewijsmaatstaf uitgelaten. Echter de Advocaat Generaal en lagere rechters gebruiken in veel gevallen de maatstaf "*een redelijke mate van zekerheid*".[121] Zoals ook in paragraaf 1.4 is aangegeven worden in de literatuur ook andere maatstaven verdedigd zoals '*een grote mate van aannemelijkheid*', '*een redelijke mate van waarschijnlijkheid*' en '*een zekere mate van waarschijnlijkheid*',[122] maar deze maatstaven lijken gezien de jurisprudentie in de laatste decennia toch minder aanhang te hebben dan de maatstaf '*een redelijke mate van zekerheid*'.

Naast de maatstaf '*een redelijke mate van zekerheid*' bestaat er volgens Giesen nog een tweede maatstaf, namelijk (voorhandse) aannemelijkheid. Deze komt neer op een waarschijnlijkheid die minder is dan '*een redelijke mate van zekerheid*', maar waarbij een feit meer zeker moet zijn dan onzeker. Hoewel met de maatstaf van aannemelijkheid de feiten niet bewezen zijn, geeft de rechter alvast aan dat een partij een betere bewijspositie heeft. De rechter geeft dan aan de wederpartij de opdracht tegenbewijs te leveren. In dat geval hoeft die wederpartij niet de tegenovergestelde feiten hard te maken, maar enkel het bewijs dat leidt tot aannemelijkheid van de feiten, 'zacht' te maken. Indien de wederpartij niet slaagt in het leveren van tegenbewijs, zal de rechter dan de (voorhandse) aannemelijkheid omzetten tot een bewezenverklaring.[123]

De vraag is wanneer de rechter acht te zijn voldaan aan de maatstaf 'een red*elijke mate van zekerheid*'. Giesen heeft een poging gedaan om deze maatstaf in percentages van overtuigingsgraad onder te brengen.[124] Hierbij komt hij tot de conclusie dat sprake is van aannemelijkheid als een rechter meer dan 50% overtuigd is van het bestaan van het feit. Bij een

---

119 I. Giesen, "De bewijswaardering in civiele zaken: vage noties of scherpe normen?", *Ars Aequi* 1999-9, p. 625; zie ook paragraaf 4.9.2.

120 *Parlementaire geschiedenis van het bewijsrecht in civiele zaken*, Deventer: Kluwer 1988, p. 76. Zie ook: H.J. Scheltema, *Nederlandsch burgerlijk bewijsrech*t, Zwolle: W.E.J. Tjeenk Willink 1939, p. 101.

121 T.R. Hidma, G.R. Rutgers, *Bewijs*, Deventer: Kluwer, 2004, p. 7. Zie ook: Zie bijvoorbeeld *LJN*: AD4006, Hoge Raad, R00/172HR; *LJN*: AR7438, Hoge Raad, R04/030HR; *LJN*: AB0377, Hoge Raad, C99/089HR.

122 I. Giesen, "De bewijswaardering in civiele zaken: vage noties of scherpe normen?", *Ars Aequi* 1999, p. 626; M.L. Kan, *Bewijslast en bewijswaardering*, Amsterdam: N.V. Johannes Müller 1921, p. 104.

123 I. Giesen, De bewijswaardering in civiele zaken: vage noties of scherpe normen?', *Ars Aequi* 1999-9, p. 629 en 630.

124 Hoewel Giesen dit niet expliciet maakt, ga ik er vanuit dat de overtuigingsschaal loopt van: zonder enige twijfel niet overtuigd (0%) tot zonder enige twijfel volledig overtuigd (100%).

overtuigingsgraad van meer dan 75% (tot 98,8%) is er sprake van een redelijke mate van zekerheid.[125] In de volgende paragraaf zal deze verdeling door middel van een tabel nader in het perspectief van dit onderzoek geplaatst worden.

4.7.2 Gewenste bewijswaardering en bewijsmaatstaf in het kader van dit onderzoek

De keuze voor de vrije bewijsleer door de wetgever heeft tot gevolg dat de rechter een discretionaire bevoegdheid krijgt om in de fase van bewijswaardering de bewijsmiddelen naar eigen inzicht te waarderen. Een discretionaire bevoegdheid brengt in de regel met zich dat als van deze bevoegdheid gebruik wordt gemaakt, de beslissing met redenen wordt omkleed. Met het motiveren van een beslissing legt de rechter namelijk verantwoording af aan partijen en wordt inzichtelijk gemaakt welke overwegingen ten grondslag liggen aan zijn beslissing. Als een discretionaire bevoegdheid een motiveringsplicht met zich meebrengt,[126] dan zou het in de lijn der verwachtingen liggen, dat in gerechtelijke uitspraken steeds gemotiveerd wordt waarom de aangeboden bewijsmiddelen wel of niet voldoende betrouwbaar zijn om de gestelde feiten te bewijzen. In de motivering van de rechter zouden dan aanknopingspunten te vinden moeten zijn over de betrouwbaarheid van deze bewijsmiddelen.[127]

Voor dit onderzoek is van belang welke eigenschappen van elektronische gegevens als bewijsmiddel van belang zijn om deze gegevens aan te merken als voldoende of onvoldoende betrouwbaar. Als duidelijkheid bestaat over de eigenschappen die ertoe leiden dat elektronische gegevens als voldoende betrouwbaar worden gekwalificeerd kunnen partijen zich hierop instellen bij het vergaren en creëren van bewijsmiddelen. Partijen kunnen zo reeds in een vroeg stadium rekening houden met het vergaren van betrouwbaar bewijs.

Het beoordelen van bewijs is naar mijn mening niet zwart-wit; bewijs is niet volledig betrouwbaar of helemaal onbetrouwbaar. De betrouwbaarheid kan blijken uit verschillende omstandigheden en is mogelijk ook afhankelijk van de feiten die aangetoond moeten worden. De betrouwbaarheid is dan een glijdende schaal. Als een bewijsmiddel onder de vrije bewijswaardering van de rechter valt, dan is het voor een partij van belang dat zijn bewijsmiddelen dusdanig betrouwbaar zijn dat de rechter rechtsgevolgen verbindt aan het

---

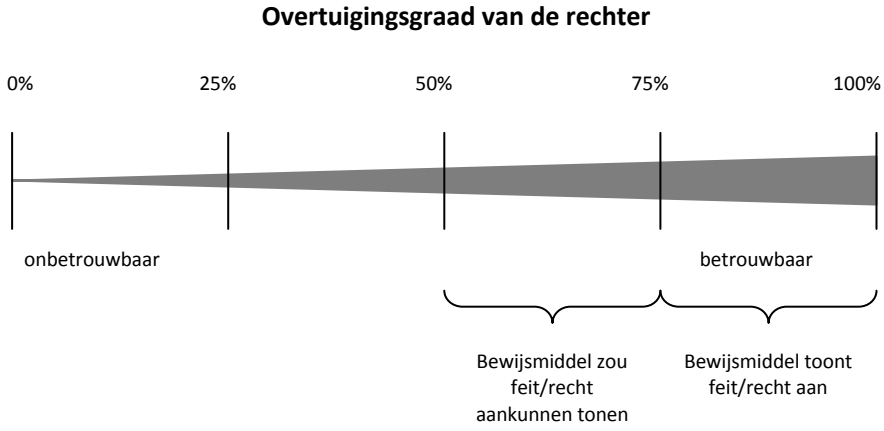
125 I. Giesen, De bewijswaardering in civiele zaken: vage noties of scherpe normen?', *Ars Aequi* 1999-9, p. 630.

126 I. Giesen, De bewijswaardering in civiele zaken: vage noties of scherpe normen?', *Ars Aequi* 1999-9, p. 625.

127 Dat deze motiveringsplicht ziet op een juridisch oordeel en slechts in zeer beperkte mate op het bewijsoordeel, zal ik verdedigen in paragraaf 4.9.2.

bewijsmiddel door de gestelde feiten als waar aan te nemen of aan te nemen dat bepaalde rechten waar de partij zich op baseert aan deze toekomen.

Willen partijen hun bewijspositie veilig stellen dan is het van belang dat zij bewijsmiddelen vergaren met die eigenschappen die ervoor zorgen dat ze als betrouwbaar beoordeeld worden. Het is van belang dat de rechter op zijn minst tot het oordeel komt dat de bewijsmiddelen tot de conclusie leiden dat de gestelde feiten aannemelijk zijn, maar veel beter nog '*een redelijke mate van zekerheid*' verschaffen. Schematisch gezien komt dit neer zoals te zien is in schema 4.1. Voor partijen is het van belang dat hun bewijsmiddel zich wat betrouwbaarheid betreft, bevindt aan de meest rechterkant van de glijdende schaal.



Afbeelding 4.1: Schaal vande overtuigingsgraad van de rechter in combinatie met de betrouwbaarheid van het bewijsmiddel.

De vraag is nu welke criteria de rechter hanteert om bewijs als voldoende betrouwbaar te waarderen. In paragraaf 4.9 zal ik daarom nader ingaan op de motivering van het bewijsoordeel, de oorzaken van het ontbreken daarvan in veel gevallen en de gevolgen die dat voor dit onderzoek heeft.

4.7.3 Wettelijke uitzonderingen op de hoofdregel: dwingend bewijs

Een uitzondering op het principe van vrije bewijswaardering wordt, naast de in paragraaf 4.15 te bespreken bewijsovereenkomst, gevormd door het zogenaamde dwingend bewijs en beperkt bewijs.[128] Dwingend bewijs houdt in dat: *"de rechter verplicht is de inhoud van bepaalde bewijsmiddelen als waar*

[128] Beperkt bewijs zal in het kader van dit onderzoek niet verder worden beproken.

aan te nemen dan wel verplicht is de bewijskracht te erkennen die de wet aan bepaalde gegevens verbindt".[129]

De discretionaire bevoegdheid van de rechter wordt dus beperkt bij het gebruik van een aantal in de wet omschreven bewijsmiddelen, waarbij onder andere wordt gedoeld op de akte. Het feit dat de rechter de bewijskracht moet erkennen van de inhoud van bepaalde bewijsmiddelen wil echter niet zeggen dat het de rechter niet vrij staat om te oordelen over eventueel aangeboden tegenbewijs.[130] De feiten die getracht worden te bewijzen met het dwingend bewijs worden, als het tegenbewijs slaagt, niet langer beschouwd als bewezen door het dwingend bewijs.

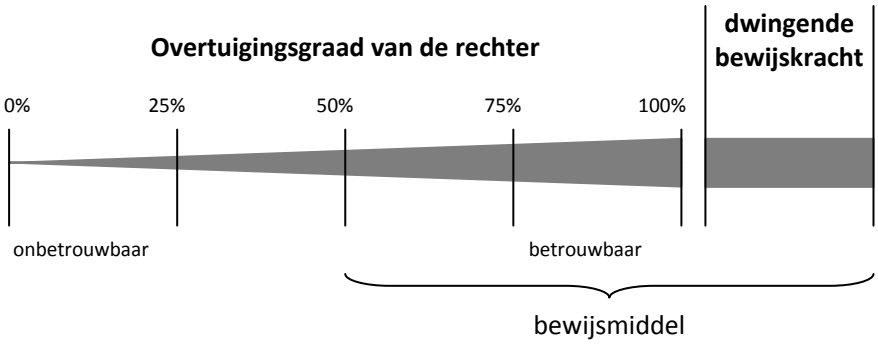
In de voorgaande subparagraaf is de vrije bewijswaardering onderzocht en het blijkt dat de rechter geen criteria expliciet maakt. In het Nederlandse recht bestaat er naast de vrije bewijswaardering de dwingende bewijskracht. Bij vrije bewijskracht staat het de rechter vrij het bewijs te waarderen op betrouwbaarheid; bij dwingende bewijskracht heeft de rechter deze bevoegdheid niet, tenzij aangeboden tegenbewijs slaagt.

Bij het vergaren van betrouwbare bewijsmiddelen is het van belang dat de bewijskracht van elektronische bewijsmiddelen zo hoog mogelijk is of dat deze dwingende bewijskracht worden toegekend. In die gevallen is de kans het grootst dat een rechter de door het bewijs onderbouwde feiten als waar aangenomen worden. In afbeelding 4.1 is al geschetst waar op de schaal van betrouwbaarheid zich een bewijsmiddel zou moeten bevinden, zodat deze als voldoende betrouwbaar kan worden gewaardeerd. In afbeelding 4.2 is deze schaal aan de rechterkant uitgebreid met een deel voor dwingende bewijskracht.

De bewijskracht van elektronische gegevens kan vergroot worden door ervoor te zorgen dat deze gegevens gekwalificeerd worden als een bewijsmiddel waar de wet dwingende bewijskracht aan toekent. Deze dwingende bewijskracht kan echter alleen worden toegekend als deze elektronische gegevens aan bepaalde eisen voldoen. De belangrijkste soorten dwingend bewijs worden gevormd door de akten en in kracht van gewijsde gegane vonnissen waarbij de Nederlandse strafrechter bewezen heeft verklaard dat iemand een feit heeft begaan. In dit onderzoek zal ik verder slechts ingaan op de akte, omdat deze opgemaakt kan worden door partijen onderling en de inhoud ter vrije beschikking staat van deze partijen. Bij het strafvonnis bepaalt de rechter de inhoud van het vonnis en daarom is de dwingende bewijskracht van het strafvonnis niet interessant voor dit onderzoek.

---

129 Art. 151, lid 1 Rv.
130 Art. 151, lid 2 Rv.



Afbeelding 4.2: Schaal van betrouwbaarheid binnen de vrije bewijswaardering en dwingende bewijskracht

4.8 Elektronische gegevens in de jurisprudentie

Op grond van de theorie van de vrije bewijsleer kan gesteld worden dat e-mail in beginsel in de meeste gevallen toegelaten kan worden als bewijsmiddel. Ook blijkt dat rechters in de fase van bewijswaardering geen moeite hebben met het toekennen van bewijswaarde aan elektronische gegevens.

Allereerst constateer ik dat rechters steeds vaker gebruik maken van elektronische gegevens (en dan voornamelijk e-mail) om gestelde feiten als waar aan te nemen. Er is een behoorlijke hoeveelheid aan jurisprudentie aanwezig waaruit blijkt dat de rechter geen moeite heeft feiten te baseren op e-mail.[131] Dat een rechter e-mail als voldoende betrouwbaar waardeert, kan

[131] Zie bijvoorbeeld: Hof Leeuwarden 8 november 2009, *LJN* BJ7622:" De e-maildiscussie maakt immers duidelijk dat (…)"; Rb. Middelburg 10 maart 2009, *LJN* BJ2001: "Tot slot heeft X bij e-mailbericht van 7 augustus 2008 nog nadrukkelijk gevraagd of er nog iets aan de huurprijs te doen valt. Dit duidt erop dat de prijs nog niet definitief was vastgesteld."; Rb. Middelburg 10 maart 2009, *LJN* BI0345:" Uit het (…) e-mailbericht van Ultimo d.d. 15 januari 2009, waarin zij stelt dat Intres (…) formeel weliswaar niet gemachtigd was namens gedaagden, maar wel sprak namens gedaagden, blijkt naar het voorlopig oordeel van de voorzieningenrechter dat Ultimo met het ontbreken van de volmacht bekend was." ; Rb. Haarlem 27 februari 2008, *LJN* BC8136:" Dit blijkt uit de e-mail van [A] van Ebrex maar ook uit de e-mail van [B], aldus nog steeds Mairon." ; Rb. Rotterdam 16 mei 2007, *LJN* BA6212: "betreffende de huurvergoeding geldt dat uit de hiervoor onder 2.10 weergegeven e-mail van [directeur] blijkt dat hierover wel is gesproken" ; Rb. Middelburg 24 september 2008, *LJN* BG 5275:" Zo hebben partijen blijkens de door hen over en weer verzonden e-mails van 20, 21 en 23 juni 2006 (…) " ; Rb. Leeuwarden 12 maart 2008, *LJN* BC8079:" (…) De rechtbank wijst daartoe bijvoorbeeld op de e-mail van 30 maart 2005 van Koga." ; Hof Amsterdam 4 maart 2008, *LJN* BF5982: "Vast is komen te staan dat [appellante] de in de appendix genoemde werkzaamheden heeft verricht. Dit kan worden afgeleid uit de e-mail van [persoon A], waarin zij verwijst naar de appendix." ; Rb. Roermond 13 januari 2009, *LJN* BG9737:" Uit de door gedaagde overgelegde e-mails leidt de kantonrechter af dat eiseres gedaagde in ieder geval tot driemaal toe

echter alleen worden opgemaakt uit de conclusie dat feiten als waar worden aangemerkt. De reden waarom de elektronische gegevens klaarblijkelijk als voldoende betrouwbaar worden aangemerkt, blijft in bijna alle gevallen onduidelijk. De waardering is niet met redenen omkleed en vind waarschijnlijk impliciet plaats. Slechts in één zaak heb ik aanknopingspunten gevonden waarbij de bewijswaardering expliciet werd gemaakt. Het betreft echter de vraag waarom de stelling dat een e-mail niet ontvangen is, niet aannemelijk is.[132] Deze zal ik verder bespreken onder de volgende paragraaf.

Verzending en ontvangst van elektronische gegevens

Het verzenden en het ontvangen van elektronische gegevens komt geregeld als onderwerp terug in de jurisprudentie. Het betreft het niet direct de inhoud van de gegevens, maar het bewijs van het feit of elektronische gegevens zijn aangekomen en/of verzonden.

In LJN BC6016 stelt appellant dat een e-mail hem niet heeft bereikt. Bij deze ontkenning, zal Nike bewijs moeten oveleggen om aan te tonen dat appellant de door Nike gestuurde e-mail wel heeft ontvangen. De rechtbank stelt het volgende betreffende Nike's bewijsvoering: "De stelling van Appellant dat de e-mail van 3 augustus 2006 hem niet heeft bereikt is in het licht van de door Nike overgelegde producties niet aannemelijk. Het hof wijst in dit verband met name op de door Nike als productie 6 overgelegde e-mail van Appellant aan haar van 16 augustus 2006. Deze is niet alleen verzonden vanaf hetzelfde e-mailadres als dat waarnaar de e-mail van Nike is verzonden (xxx@post.cz), doch vermeldt dezelfde referentie ("Re: Nike smiouva") en valt ook qua inhoud moeilijk anders te begrijpen dan als een reactie op de e-mail van Nike."

In LJN AV3919 is aan de orde dat een opzegging van een abonnement niet zou zijn ontvangen per e-mail door Lis BV.[133] Het is aan gedaagde om aan te tonen dat Lis BV zijn opzegging per e-mail zou hebben ontvangen. Gedaagde kan voor zijn stelling dat hij de opzegging heeft verstuurd enkel twee getuigen aandragen. Deze kunnen echter alleen getuigen dat gedaagde de opzegging heeft verstuurd, maar niet dat Lis BV de opzegging heeft ontvangen. Ook een ontvangstbevestiging heeft gedaagde niet. Gedaagde kan dus niet aantonen dat Lis BV zijn opzegging heeft ontvangen.

Bovenstaande uitspraken zijn ook in lijn met Sagro Aannemingsmaatschappij Zeeland B.V. / Van Diemen Asbestverwijdering B.V. waarin Sagro stelt een e-mail met voorwaarden naar Van Diemen te hebben gestuurd, echter welke

heeft laten weten dat het voor hem niet meer mogelijk was om de digitale ontvanger te retourneren (…)" ;

132 Hof Amsterdam 6 maart 2008, *LJN* BC 6016.

133 Rb. Amsterdam 6 maart 2006, *LJN* AV3919.

door Van Diemen niet is ontvangen.[134] De rechter overweegt dan alsvolgt: "*Aan de hand van de productie die Sagro ter onderbouwing van haar stelling heeft overgelegd kan niet worden geconcludeerd dat het stuk met de algemene voorwaarden daadwerkelijk op genoemde datum per e-mail aan Van Diemen verstuurd is en dat het door Van Diemen is ontvangen. Ook blijkt uit deze productie niet dat het betreffende stuk en de algemene voorwaarden daadwerkelijk als bijlage bij de e-mail waren gevoegd. Derhalve kan niet worden geconcludeerd dat de toepasselijkheid van de algemene voorwaarden door Sagro aan Van Diemen is voorgesteld.*" Welke producties wel en niet zijn ingebracht blijkt helaas niet uit de uitspraak.

Eenzelfde lijn wordt gehanteerd in LJN BD2165.[135] Verweerder beweert een e-mail met een adreswijzing te hebben gestuurd naar eiser. Eiser stelt echter dat hij deze e-mail nooit ontvangen heeft en deze betwisting (en gebrek aan overig bewijs) slaagt. Verweerder had moeten aantonen dat de eiser de e-mail ontvangen had.

Met betrekking tot de bevestiging en ontvangst van elektronische gegevens is het bij betwisting van de ontvanger dat deze de gegevens zou hebben ontvangen aan de verzender om aan te tonen dat ontvanger de gegevens heeft ontvangen. Het enkel aantonen dat de gegevens zijn verzonden is daarvoor niet voldoende. In hoofdstuk 8 zal ik nader ingaan op de mogelijkheden om te anticiperen door bewijsmateriaal voor de ontvangst van de gegevens te verzamelen.

Strijd met redelijkheid: bericht wel ontvangen maar niet op de overeengekomen wijze, maar per e-mail.

Niet alleen bij wet kunnen vormvereisten gesteld worden; ook bij overeenkomst kan een vormvereiste gesteld worden. Hoewel vormvereisten een formele eis inhouden en niet zien op de betrouwbaarheid van bewijsmiddelen zal ik hier toch kort op ingaan.

In LJN BI1212 werd een vormvereiste gesteld in een koopovereenkomst onder ontbindinde voorwaarde die partijen waren aangegaan. Indien een van partijen zich op de ontbindende voorwaarde zou beroepen, dan zou dit de wederpartij kenbaar gemaakt moeten worden "*bij aangetekende brief met bericht met handtekening retour*" of "*telefaxbericht met verzendbevestiging*". Echter, gedaagden beroepen zich op de ontbindende voorwaarde en stelt eisers op de hoogte door middel van een e-mailbericht. Eisers stellen dat gedaagden "*aan deze e-mail geen rechten kunnen ontlenen en dat de overeenkomst daardoor niet is ontbonden*." De rechter is het hiermee oneens en stelt: "*De strekking van*

[134] Rb. Middelburg 24 juni 2009, *LJN* BK8790.
[135] Rb. Roermond 23 april 2008, *LJN* BD2165.

de e-mail van 3 december 2007 laat aan duidelijkheid niet te wensen over. Eisers hebben niet gesteld dat zij niet hebben begrepen dat gedaagden zich wilden beroepen op de ontbindende voorwaarde, omdat zij de financiering niet rond konden krijgen. Vast staat dat het bericht de verkopers heeft bereikt en dat de inhoud hen duidelijk was. Daarom wordt geoordeeld dat eisers in redelijkheid geen beroep kunnen doen op het voornoemde formele vereiste." Als bepaald is dat een specifiek communicatiemiddel wordt gebruikt om het beroep op een ontbindende voorwaarde kenbaar te maken en er wordt vervolgens gebruik gemaakt van e-mail, terwijl dit niet het communicatiemedium is zoals overeengekomen, dan is het in strijd met de redelijkheid als voor de ontvangers de ontbindende voorwaarde kenbaar gemaakt is, maar zij zich toch daarop beroepen op de ongeldigheid omdat niet aan de formele eis is voldaan. In bovenstaand geval gaat het om een e-mail. Ik zie niet in waarom bovenstaande regel niet zou opgaan voor allerlei andere vormen van elektronische gegevens waarmee gecommuniceerd kan worden. De rechter geeft als enkele grond dat het beding in strijd is met de redelijkheid dat het bericht de verkopers heeft bereikt en dat de inhoud hen duidelijk was. Als dit de enige gronden zijn, dan ligt het in de rede om te stellen dat als bij overeenkomst een communicatiemedium wordt gekozen om een beroep op een ontbindende voorwaarde kenbaar te maken en het bericht vervolgens via een ander medium wordt gecommuniceerd, dit een beroep op het beding altijd in strijd is met de redelijkheid zolang het bericht de wederpartij heeft bereikt en de inhoud deze partij duidelijk is. Dezelfde lijn wordt gehanteerd in LJN BJ3831.[136] De rechtbank overweegt het volgende: "*Dat gedaagden een beroep op de ontbindende voorwaarde hebben gedaan door middel van een e-mailbericht en niet op de in artikel 6.1 van de koopovereenkomst voorgeschreven wijze (namelijk schriftelijk, gericht aan de verkoper en diens makelaar, per aangetekende brief met bericht van ontvangst of per deurwaardersexploot), maakt niet dat het beroep op de ontbindende voorwaarde rechtsgevolg mist. Het gaat er om dat eiser binnen de overeengekomen termijn op de hoogte is gebracht van het inroepen van de ontbindende voorwaarde. Dat is gebeurd met de e-mail van 9 april 2008, waarvan de ontvangst niet is betwist.*" Ook daar wordt gesteld dat indien niet op overeengekomen wijze een beroep wordt gedaan op een ontbindende voorwaarde, er toch ontbinding volgt indien de wederpartij binnen de overeengekomen termijn op de hoogte is gebracht van het inroepen van de ontbindende voorwaarde.

[136] Rb. Middelburg 21 januari 2009, *LJN* BJ3831.

4.9 Oorzaken van het ontbreken van jurisprudentie

4.9.1 Inleiding

In deze paragraaf ga ik in op de oorzaken waarom het ontbreekt aan expliciete criteria waaraan elektronische gegevens zouden moeten voldoen. In de vorige paragraaf constateerde ik al dat explicite criteria waaraan de betrouwbaarheid van elektronische gegevens moeten voldoen ontbreken. Twee algemene oorzaken kunnen hier naar mijn mening aan ten grondslag liggen. Ten eerste de beperkte motiveringsplicht die de feitenrechter heeft. Hierop ga ik in paragraaf 4.9.2 nader in. De tweede reden is de processuele rol die de rechter heeft, dan wel zich aanmeet. Hierover gaat paragraaf 4.9.3.

4.9.2 Beperkte motiveringsplicht

Het inhoudelijk beoordelen van bewijs is niet altijd een eenvoudige aangelegenheid, want het is de vraag op welke gronden kan worden gesteld dat bewijs voldoende betrouwbaar is of juist onvoldoende betrouwbaar. De beoordeling van bewijs op de betrouwbaarheid is een handeling van feitelijke aard en is daarom slechts voorbehouden aan de rechter die over de feiten oordeelt; in civiele zaken zal dit de Rechtbank of het Hof zijn. De Hoge Raad kan slechts beoordelen of de feitenrechter alle vormen in acht heeft genomen en of er geen schending van het recht is.[137] Een inhoudelijke beoordeling van bewijsmiddelen ligt dus bij de feitenrechter.[138]

De rechter heeft ingevolge art. 152, lid 2 Rv in beginsel de bevoegdheid om bewijs te waarderen naar eigen inzicht. Deze vrijheid is echter niet ongelimiteerd; de rechter dient namelijk wel verantwoording af te leggen over de gronden en de feiten waarop de beslissing rust. Art. 121 Gw bepaalt namelijk: *"Met uitzondering van de gevallen bij de wet bepaald vinden terechtzittingen in het openbaar plaats en houden vonnissen de gronden in waarop zij rusten. De uitspraak geschiedt in het openbaar."*

Vervolgens bepaalt art. 30 Rv: "*Vonnissen, arresten en beschkkingen houden de gronden in waarop zij rusten, tenzij uit de wet anders voortvloeit*". Ook art. 230, lid 1, onder e Rv bepaalt dat: *"Het vonnis vermeldt: (…) de gronden van de beslissing, waaronder begrepen de feiten waarop de beslissing rust".* Tevens bevat art. 5, lid 1 Wet RO de bepaling dat "*de uitspraak van vonnissen en arresten in burgerlijke zaken (…) bevatten (..) de gronden waarop zij berusten*."

---

137 Art. 79, lid 1 RO.

138 W.D.H. Asser, *Monografieën Nieuw BW, Bewijslastverdeling*, Deventer: Kluwer 1992, p. 13 en 14.

Art. 121 Gw, art. 30 Rv, art. 230 Rv en art 5 Wet RO stellen dat de gronden van de beslissing waaronder begrepen de feiten, moeten worden opgenomen in het vonnis. Hier wordt gesproken over de "*gronden (…) waarop zij berusten*" en de "*gronden van de beslissing*". Houden deze gronden ook in de gronden die het bewijsoordeel raken of slechts de gronden die het feitelijk oordeel van het vonnis inhouden?

Allereerst moet een onderscheid gemaakt worden tussen het bewijsoordeel en het rechtsoordeel.[139] Dit onderscheid is namelijk van belang voor het vaststellen van de motiveringsplicht die de rechter heeft.[140] Het bewijsoordeel is namelijk van feitelijke aard, terwijl het rechtsoordeel van juridische aard is en totstandkomt op grond van juridische argumentatie.[141]

Het rechtsoordeel is onderworpen aan de motiveringsplicht van art 121 Gw, art. 30 Rv, art. 230 Rv en art. 5 Wet RO. Een rechter dient inzicht te geven in de gedachtengang die hij volgt en dient zijn argumentatie expliciet in zijn oordeel te beschrijven. Zoals hiervoor gesteld dient het bewijsoordeel van het rechtsoordeel te worden onderscheiden.

Het bewijsoordeel is een oordeel wat gebaseerd is op een discretionaire bevoegdheid van de rechter. De rechter heeft namelijk grote vrijheid om op grond van art. 152, lid 2 Rv geheel zelfstandig het bewijs te waarderen. Lange tijd heeft de rechter geen motiveringsplicht gehad bij beslissingen waarbij hij gebruik maakte van zijn discretionaire bevoegdheid.[142] Dit is echter niet langer in alle gevallen zo. De Hoge Raad heeft in een aantal arresten in de jaren negentig bepaald dat een rechter een beperkte motiveringsplicht kan hebben. De HR heeft bepaald dat als het debat van partijen daartoe aanleiding geeft, de rechter zal moeten motiveren waarom hij in bepaalde zin van zijn beoordelingsvrijheid gebruik maakt.[143]

Eerst in Finkenburgh/van Mansum geeft de HR meer duidelijkheid over de gronden waarop de motiveringsplicht betreffende het bewijsoordeel wordt gebaseerd, namelijk op grond van het grondbeginsel van een behoorlijke

---

139 W.D.H. Asser, *Monografieën Nieuw BW, Bewijslastverdeling*, Deventer: Kluwer 1992, p. 13.

140 W.D.H. Asser, *Monografieën Nieuw BW, Bewijslastverdeling*, Deventer: Kluwer 1992, p. 14.

141 D.J. Veegens, E. Korthals Altes, H.A. Groen, *Cassatie in burgerlijke zaken*, Deventer: Kluwer 2005 , nr. 117 t/m 121, p. 259 t/m 272. Zie ook: W.D.H. Asser, *Monografieën Nieuw BW, Bewijslastverdeling*, Deventer: Kluwer 1992, p. 14.

142 D.J. Veegens, E. Korthals Altes, H.A. Groen, *Cassatie in burgerlijke zaken*, Deventer: Kluwer 2005 , nr. 117 t/m 121, p. 259 t/m 272. Zie ook verschillende jurisprudentie: HR 23 december 1943, *NJ* 1944, 130; HR 30 november 1945, *NJ* 1946, 88; HR 31 oktober 1986, *NJ* 1987, 207.

143 HR 6 maart 1992, *NJ* 1992, 373 (Micherna Beheer / Kamerbeek):"Wel dient hij indien het debat van aprtijen daartoe aanleiding geeft in zijn beschikking rekenschap af te leggen van de wijze waarop hij van die vrijheid gebruik heeft gemaakt."

rechtspleging:[144] *"Het Hof, als rechter die over de feiten oordeelt, was weliswaar vrij in de waardering van de in het geding gebrachte stukken, maar ook ten aanzien van het oordeel of het bewijs is geleverd, geldt het grondbeginsel van een behoorlijke rechtspleging dat elke rechterlijke beslissing tenminste zodanig moet worden gemotiveerd dat zij voldoende inzicht geeft in de aan haar ten grondslag liggende gedachtegang om de beslissing zowel voor partijen als voor derden – in het geval van openstaan van hogere voorzieningen: de hogere rechter daaronder begrepen – controleerbaar en aanvaardbaar te maken"*[145]

Hoewel de Grondwet en het Wetboek van Burgerlijke rechtsvordering niet expliciet een motivering van het bewijsoordeel lijken te eisen, maar enkel de motivering van hoe de feiten tot een beslissing leiden, leidt de Hoge Raad uit het grondbeginsel van een behoorlijke rechtspleging een motiveringsplicht van het bewijsoordeel af. Hij stelt dat de feitenrechter vrij is in de waardering van het bewijs, maar ondanks dat zij hierin vrij is, dient zij het bewijsoordeel dusdanig te motiveren dat zij voldoende inzicht geeft in de aan haar ten grondslag liggende gedachtegang om de beslissing voor partijen als voor derden (inclusief de hogere rechter) controleerbaar en aanvaardbaar te maken.[146]

---

144 HR 16 oktober 1998, *NJ* 1999, 7 (Finkenburgh / van Mansum): Tussen Finkenburgh en Rimo NV bestaat een schriftelijke overeenkomst waarbij is overeengekomen dat Finkenburg kinderzitjes produceert, daarbij zorg draagt dat deze aan de veiligheidseisen voldoen en zorg draagt dat het TNO goedkeuringsmerk zal blijven gelden. Rimo zal de producten verkopen. De overeenkomst is mede ondertekend door van Mansum die zorg draagt voor de research en ontwikkeling van de kinderzitjes. In de overeenkomst is tevens bepaald dat van Mansum een bedrag per verkocht product ontvangt. Nadat de kinderzitjes is een vergelijkend warenonderzoek als onvoldoende veilig waren gekwalificeerd heeft TNO geen goedkeuringsmerk meer afgegeven en valt de omzet terug. Van Mansum betrekt Finkenburg in rechte wegens wanprestatie. De Rechtbank wijst de vordering van Van Mansum af; het Hof wijst de vordering toe op grond van de volgende overwegingen:"19. Finkenburg heeft de door Van Mansum gestelde wanprestatie voldoende gemotiveerd bestreden. Derhalve draagt Van Mansum als partij, die zich beroept op de rechtsgevolgen van die door hem gestelde wanprestatie, in beginsel de bewijslast daarvan. 20. Gelet op de inhoud van de door partijen overlegde producties, beschouwd in onderling verband en samenhang is, behoudens door Finkenburgh te leveren bewijs van het tegendeel, afdoende bewezen dat Finkenburgh jegens Van Mansum wanprestatie heeft gepleegd. 21. Finkenburgh heeft geen bewijs terzake voormeld aangeboden. 22. Derhalve is komen vast te staan dat Finkenburgh jegens Van Mansum wanprestatie heeft gepleegd."

145 Deze maatstaf is reeds neergelegd in HR 4 juni 1993, *NJ* 1993, 659: "Ook in kort geding gelden de grondbeginselen van een goede procesorde waartoe behoort dat elke rechterlijke beslissing tenminste zodanig moet worden gemotiveerd dat zij voldoende inzicht geeft in de daaraan ten grondslag liggende gedachtengang om de beslissing zowel voor partijen als voor derden- in het geval van hogere voorzieningen: de hogere rechter daaronder begrepen – controleerbaar en aanvaardbaar te maken."

146 Deze maatstaf wordt tevens aangehaald in HR 4 juni 1993, *NJ* 1993, 659 (Motiveringsplicht bewijsbeslissing in kort geding), HR 7 april 1995, *NJ* 1997, 21 (Motiveringsplicht bewijsbeslissing bij faillietverklaring) en HR 29 juni 2001, *NJ* 2001, 495 (Motiveringsplicht bewijsbeslissing bij alimentatie). Zie ook: E. Korthals Altes, 'Het motiveringsvereiste in burgerlijke zaken als toetsingsgrond in cassatie', in: P.A. Wackie Eysten (e.a. (red.), *Gemotiveerd gehuldigd*, Zwolle: W.E.J. Tjeenk Willink 1993, p. 96 t/m 103.

Naar mijn mening heeft de Hoge Raad hiermee een eerste stap in de juiste richting gezet. Hij zou echter verder moeten gaan door in het geval van gebruikmaking van een discretionaire bevoegdheid niet enkel een motiveringsplicht op te leggen als het debat van partijen daartoe aanleiding geeft, maar juist de motiveringsplicht uit te breiden. In Nederland is de staatsmacht verdeeld over de wetgevende macht, de bestuurlijke macht en de rechtgevende macht.[147] De wetgever ontleent haar macht aan de kiezer.[148] Door middel van verkiezingen wordt zijn macht steeds op democratische wijze voor een termijn van maximaal 4 jaar gelegitimeerd.[149] De bestuurlijke macht ontleent haar handelingsbevoegdheid aan de wetgever die bepaalt hoever de bevoegdheden van het bestuur gaan bij de uitoefening van haar uitvoerende taak. Daar waar een bestuursorgaan een discretionaire bevoegdheid krijgt (in de vorm van beleidsvrijheid of beoordelingsvrijheid), heeft zij tevens een motiveringsplicht als zij gebruik maakt van deze discretionaire bevoegdheid.[150] Op deze manier legt het orgaan verantwoording af aan de betrokken partijen. De rechterlijke macht ontleent haar handelingsbevoegdheid aan art. 112 en 113 Gw.[151] Zoals reeds hierboven uiteengezet is, heeft de rechterlijke macht ook een motiveringsplicht. Deze ziet echter alleen op het rechtsoordeel. Indien de rechter gebruikmaakt van een discretionaire bevoegdheid, geldt sinds nog geen twee decennia slechts een zeer beperkte motiveringsplicht.

Juist daar waar het de uitoefening van overheidsmacht betreft zou naar mijn mening verwacht mogen worden dat het machtsuitoefenende orgaan uitermate zorgvuldig omgaat met haar bevoegdheden. Onderdeel van deze zorgvuldigheid is het afleggen van verantwoording aan de betrokken partijen. Het zou daarom toch in de lijn der verwachtingen mogen liggen dat daar waar de rechter bij het waarderen van bewijs grote discretie toebedeeld krijgt, deze toch tenminste een motiveringsplicht krijgt, waardoor een beslissing gebaseerd op deze bevoegdheid altijd met redenen is omkleed. Zoals echter reeds is geconcludeerd, is deze motiveringsplicht beperkt tot gevallen waarin het debat van partijen daartoe aanleiding geeft. Mijns insziens wordt daarmee onrecht gedaan aan het afleggen van verantwoording bij het uitoefenen van staatsmacht. Daarnaast doet het onrecht aan de partijen die een rechter hebben gevraagd een oordeel te geven. De rechter kan zich ontrekken aan een zorgvuldig met redenen omkleed bewijsoordeel met een beroep op een

147 G.J. Wiarda, *Drie typen van rechtsvinding*, Deventer: Kluwer 1999, p77 t/m 82; zie ook: C.L. Montesquieu, *Over de geest van de wetten*, Amsterdam: Boom 2006.

148 Art. 54 en 55 Gw.

149 Art. 52 en 53 Gw; zie ook: A.F.M. Brenninkmeijer, 'De plaats van de rechter in onze constitutionele rechtsorde', in: R.H.M. Jansen, J. Godrie (red.), *De rechter als dictator?*, Lochem: J.B. van den Brink & Co. 1987, p. 62 en 63.

150 H.D. van Wijk, W. Konijnenbelt, *Hoofdstukken van bestuursrecht*, Den Haag: Elsevier Juridisch 2008 , p.238 en 239.

151 D.J. Veegens, E. Korthals Altes, H.A. Groen, *Cassatie in burgerlijke zaken*, Deventer: Kluwer 2005, nr. 117 t/m 121, p. 261.

beperkte motiveringsplicht die hij in het geval van een discretionaire bevoegdheid heeft.

4.9.3 De rol van de rechter bij de bewijswaardering

Ondanks het feit dat elektronische middelen steeds meer ingeburgerd raken, is er geen of nauwelijks gepubliceerde jurisprudentie beschikbaar waarbij de rechter oordeelt over de betrouwbaarheid van elektronische bewijsmiddelen.[152] Het feit dat in veel uitspraken een motivering van de bewijswaardering ontbreekt, wordt ook onderkend door Kemna. Zij stelt "in veel uitspraken wordt het aspect van de precieze bewijswaardering niet geadresseerd".[153] Daarbij worden twee voorbeelden uit de jurisprudentie aangehaald. In de eerste plaats noemt zij een telexcode welke als technisch identificatiemiddel werd gebruikt bij een banktransactie. Daarbij gaat de aandacht van de Hoge Raad uit naar de vraag waar het risico van misbruik van een modern identificatiemiddel dient te liggen in plaats van zich te richten op de motivering van de waardering van het ingebrachte bewijsmiddel.[154] Ook zijn er uitspraken bekend van enkele strafrechtelijke arresten waar faxkopieën een rol speelden, maar ook hier ontbreekt het aan expliciete betrouwbaarheidscriteria.[155]

Kemna gaat ook in op de redenen waarom expliciete waarderingscriteria ontbreken in de rechtspraak. Zij voert de onderstaande redenen aan.

In de eerste plaats noemt zij het feit dat elektronische middelen eenvoudigweg niet worden ingebracht als bewijs. In dat geval komen deze middelen ook niet voor de rechter, met als gevolg dat er nooit iets gezegd wordt over deze middelen. Deze reden ging misschien op ten tijde dat Kemna haar stuk schreef, maar gezien de enorme ontwikkeling van elektronische gegevens die ingebracht worden als bewijsmiddel, gaat mijns inziens dit argument niet langer op.

Een tweede reden is dat ingebrachte middelen niet of onvoldoende worden betwist door partijen. De rechter krijgt de middelen wel onder ogen, maar de lijdelijkheid van de rechter in civiele zaken brengt vervolgens met zich dat de rechter de bewijsmiddelen zal aannemen. Deze oorzaak lijkt mij heel

---

152 A.M.Ch. Kemna, 'De vraagstukken van bewijs en bewaring in een elektronische omgeving', in: H. Franken, H.W.K. Kaspersen, A.H. de Wild (red.), *Recht en computer* (Recht en Praktijk), Deventer: Kluwer 2004, p. 214.

153 A.M.Ch. Kemna, 'De vraagstukken van bewijs en bewaring in een elektronische omgeving', in: H. Franken, H.W.K. Kaspersen, A.H. de Wild (red.), *Recht en computer* (Recht en Praktijk), Deventer: Kluwer 2004, p. 214.

154 HR 19 november 1993, *NJ* 1994, 622 (COVA/Internationale Bank).

155 HR 13 september 1988, *NJ* 1989, 12.

waarschijnlijk. Uit mijn jurisprudentie-onderzoek blijkt namelijk dat rechters weldegelijk elektronische gegevens gebruiken als bewijsmiddel. Hierbij betreft het voornamelijk e-mail. Rechters accepteren e-mail in veel gevallen zonder een expliciet betrouwbaarheidsoordeel te geven. Volledig uit het oog lijkt te worden verloren dat e-mail niet altijd even betrouwbaar hoeft te zijn.[156] Rechters lijken hier volledig aan voorbij te gaan, aangezien in alle door mij onderzochte uitspraken de rechter nooit ingaan op de gevaren die ten grondslag liggen aan e-mailverkeer zoals de autentificatie van personen en de authentificatie van de elektronische gegevens. Ondanks hun discretionaire bevoegdheid om de bewijsmiddelen te waarderen op betrouwbaarheid,[157] lijkt de rechter zijn lijdelijke rol door te trekken naar de bewijswaardering. Echter, juist waar het bewijswaardering betreft, is de rechter niet lijdelijk. De rechter heeft een discretionaire bevoegdheid en mag het bewijs waarderen naar eigen inzicht. Daar staat zijn lijdelijke rol niet aan in de weg. Bij een gebrek aan expliciete bewijswaardering van elektronische gegevens lijkt het er sterk op dat de rechter uit gaat van de betrouwbaarheid van bewijs, tenzij één van de partijen stelt dat het bewijsmiddel niet betrouwbaar is. Zolang partijen de betrouwbaarheid van een bewijsmiddel niet betwisten, gaat de rechter in de alle door mij onderzochte gevallen uit van de betrouwbaarheid. De rechter laat na om zelfstandig en uit eigen beweging de betrouwbaarheid van bewijs te beoordelen.

Een derde reden zou kunnen zijn dat de rechter een impliciete waardering maakt van de bewijsmiddelen. Er wordt dan wel toegekomen aan een waardering, maar deze waardering is een proces dat zich afspeelt in het hoofd van de rechter en een explicitatie op papier ontbreekt. De hoeveelheid uitspraken waarin een rechter wel feiten aanneemt op basis van enkel e-mailverkeer in combinatie met het feit dat er daarentegen juist geen expliciete waardering plaatsvindt, duidt er volgens mij op dat er wel een waardering plaatsvindt, maar dat deze impliciet gebeurt.

Als vierde reden noemt Kemna het feit dat de rechter zijn oordeel reeds baseert op ander bewijs zodat het elektronische bewijsmiddel verder buiten beschouwing wordt gelaten. Dit is een mogelijkheid, maar in de door mijn onderzochte uitspraken ben ik hiervan niets tegengekomen.

Tenslotte wordt als vijfde reden gegeven dat betreffende rechters misschien niet voldoende op de hoogte zijn van de manipulatiemogelijkheden van ogenschijnlijk betrouwbare ingebrachte elektronische middelen. Ook deze

---

156 J. Koëter, A.M.Ch. Kemna, C. Stuurman, 'E-mail: bewijzen, bewaren, vormvoorschriften en contracteren', in: H.W.K. Kaspersen en C. Stuurman, *Juridische aspecten van e-mail*, Deventer: Kluwer 2001, p. 46.

157 M.E.M.G. Peletier, *Rechterlijke vrijheid en partij-autonomie* (diss. Amsterdam VU), Den Haag: Boom Juridische Uitgevers 1999, p. 203.

mogelijkheid acht ik zeer goed mogelijk. In geen van alle door mij onderzochte uitspraken wordt ook maar gewezen op het feit dat elektronische gegevens eenvoudig te manipuleren zijn.

4.9.4 Tussenconclusie

Er lijken globaal beschouwd twee hoofdredenen te zijn waarom het ontbreekt aan expliciete criteria waaraan elektronische bewijsmiddelen moeten voldoen om als voldoende betrouwbaar gewaardeerd te worden. In de eerste plaats de beperkte verplichting aan de rechter om expliciet te motiveren welke criteria hij aanlegt bij het waarderen van bewijsmiddelen. In de tweede plaats de processuele en voornamelijk lijdelijke rol die de rechter heeft in het civiele proces. Deze redenen zien op het ontbreken van bewijscriteria voor zoverre het de vrije bewijswaardering door de rechter betreft. Er zijn echter ook bewijsmiddelen waarbij de bewijswaardering niet aan de rechter is overgelaten. In de volgende paragraaf zal verder onderzocht worden welke bijdrage bewijsmiddelen met dwingende bewijskracht kunnen leveren aan de criteria waaraan elektronische bewijsmiddelen zouden moeten voldoen.

4.10 Dwingend bewijs: de akte

4.10.1 Inleiding

In de vorige paragraaf is gesteld dat een akte dwingende bewijskracht kan hebben; er moet dan sprake zijn van een onderhandse akte (dwingende bewijskracht tussen partijen) of een authentieke akte (dwingende bewijskracht jegens derden). In subparagrafen 4.10.2 en 4.10.3 zal ik nader ingaan op respectievelijk de vereisten om een akte te constitueren en de bewijskracht van de onderhandse en de authentieke akte. Dit met als doel om in paragraaf 4.13 de elektronische varianten van de onderhandse en de authentieke akte te onderzoeken.

4.10.2 De definitie van de akte

"Akten zijn ondertekende geschriften, bestemd om tot bewijs te dienen", aldus art. 156, lid 1 Rv. Uit deze definitie blijkt dat er pas sprake is van een akte als er cumulatief aan drie voorwaarden is voldaan, namelijk schriftelijkheid, ondertekening en een bewijsfunctie.

Ten eerste moet er sprake zijn van een geschrift. De wet kent geen definitie van het begrip geschrift en ook de rechtspraak geeft geen definitie van het begrip

geschrift. In de literatuur wordt gesteld dat een geschrift is:"*iedere drager van verstaanbare leestekens die een gedachte-inhoud vertolken*."[158] Het is niet nodig dat het geschrift op papier is gesteld. Andere dragers die leestekens bevatten kunnen ook als geschrift worden gekwalificeerd, zoals hout of klei. De leestekens moeten verstaanbaar zijn. Het maakt daarbij niet uit welke taal of codering is gebruikt om de gedachte-inhoud vast te leggen. Zoals ik Hidma en Rutgers lees gaat het hier dan eigenlijk om de mogelijkheid dat de tekens verstaanbaar zijn. Of iemand de tekens daadwerkelijk begrijpt is dan niet van belang; het gaat om de mogelijkheid dat er mensen zijn die de tekens wel begrijpen. Ook hoeven de leestekens niet met het blote oog leesbaar te zijn, aangezien Hidma en Rutgers hieronder ook gegevens op een microfilm verstaat. Daarbij wordt door Van Esch wel opgemerkt dat leestekens op een gegevensdrager discussie kunnen opleveren.[159] Als argument voor het feit dat elektronische gegevens (die leestekens representeren) op een elektronische gegevensdrager als verstaanbare leestekens moeten worden aangemerkt valt te noemen dat deze net als microfilm door middel van een apparaat leesbaar worden gemaakt. Een argument tegen deze stelling is dat elektronische gegevens door een computer omgezet moeten worden naar een leesteken. De leestekens zijn namelijk niet meer dan een reeks van elektrische ladingen of deukjes (putjes) op een gegevensdrager. Het betreft dan niet slechts een vergroting, maar er is een mechanisme noodzakelijk dat de elektronische gegevens interpreteert en er een leesteken van maakt en deze door middel van een uitvoerapparaat toont op een scherm of ander uitvoerapparaat. Als de coderingstabel de elektronische gegevens anders 'vertaalt' is het mogelijk dat een ander leesteken wordt getoond. Tenslotte dienen de leestekens een gedachte-inhoud te vertolken. Als de leestakens geen gedachte-inhoud vertolken is er ook geen sprake van een geschrift in juridische zin. Zo vertolken meetgegevens geen gedachte-inhoud en kunnen daarom ook niet als geschrift worden gekwalificeerd.

Ten tweede dient het geschrift te zijn ondertekend.[160] Net als bij het begrip geschrift kent het Nederlandse recht geen definitie van het begrip 'ondertekening' of 'handtekening'. Wel valt uit oudere rechtspraak af te leiden dat onder ondertekenen het plaatsen van een naam die de ondertekenaar draagt of heeft, met of zonder toevoeging van de voornaam.[161] Hierbij is het plaatsen van een kruisje niet voldoende.[162] Dit ligt in de lijn met de

---

158 T.R. Hidma, G.R. Rutgers, *Pitlo. Het Nederlands burgerlijk recht. Deel 7. Bewijs*, Deventer: Kluwer 2003, nr. 47 , p. 82.

159 Zie voor deze discussie: R.E. van Esch, *Electronic Data Interchange (EDI) en het vermogensrecht* (diss. Nijmegen), W.E.J. Tjeenk Willink, Deventer: 1999, p. 170, noot 7.

160 C. Asser, A. Anema, P.J. Verdam, *Handleiding tot de beoefening van het Nederlands Burgerlijk Recht, Vijfde deel – van Bewijs*, Zwolle: W.E.J. Tjeenk Willink 1953, p. 160.

161 HR 17 december 1885, *Weekblad van het recht* 1886-5251, p. 1; HR 6 mei 1910, *Weekblad van het recht* 1910-9025, p. 1.

162 HR 21 januari 1898, *Weekblad van het recht* 7078.

authentificerende functie die wordt bedeeld aan de handtekening. Mijns inziens gaat het er bij een handtekening dan ook om, om aan te kunnen tonen wie het geschrift heeft ondertekend.

Ten derde moet het doel van de akte zijn dat deze als bewijs kan dienen. Veel afspraken (overeenkomsten) zijn ook geldig zonder dat deze schriftelijk zijn opgemaakt.[163] Echter om het bestaan van deze afspraken te bewijzen, is een akte een van de meest geschikte middelen, zo niet het meest geschikte middel. De bewijsfunctie van de akte is een constitutioneel vereiste. Dit wil zeggen dat de bewijsfunctie heeft moeten bestaan vanaf het moment dat het geschrift is ondertekend.[164] Het kan zijn dat de bewijsfunctie pas op een later moment wordt gegeven aan het ondertekende geschrift.[165] De bewijsfunctie geldt logischerwijs alleen ten aanzien van bewijs dat de ondertekenaar tegen zichzelf schept.[166] Een ondertekenaar kan met zijn eigen verklaring niet een ander binden.[167]

Naast bovenstaande eisen die gelden voor de onderhandse akte gelden er voor de authentieke akte aanvullende eisen. De authentieke akte moet ingevolge art. 156, lid 2 Rv bevoegdelijk zijn opgemaakt door ambtenaren aan wie bij of krachtens de wet is opgedragen op die wijze te doen blijken van door hem gedane waarneming of verrichtingen of aan anderen indien de wet dit opdraagt. Onder deze ambtenaren vallen de notaris, de deurwaarder en de ambtenaar van de burgerlijke stand.[168]

4.10.3 De bewijskracht van de akte

Zowel de authentieke als de onderhandse akte hebben dwingende rechtskracht. Het is echter van het soort akte afhankelijk jegens wie de akte rechtskracht heeft en of de bewijskracht materieel, formeel of uitwendig van aard is. Hieronder wordt daarom eerst ingegaan op de vraag jegens wie de akte rechtskracht heeft. Vervolgens wordt behandeld welke soort rechtskracht (materieel, formeel, uitwendig) aan de onderhandse en de authentieke aktes toekomt.

---

163 Dit is natuurlijk anders als de wet schriftelijkheid als vereiste noemt voor het constitueren van een rechtshandeling.

164 C.A. Kraan, *De authentieke akte* (diss. UvA), Arnhem: Goude Quint BV, p. 39 t/m 41.

165 C. Asser, A. Anema, P.J. Verdam, *Handleiding tot de beoefening van het Nederlands Burgerlijk Recht, Vijfde deel – van Bewijs*, Zwolle: W.E.J. Tjeenk Willink 1953, p. 160; T.R. Hidma, G.R. Rutgers, *Pitlo. Het Nederlands burgerlijk recht. Deel 7. Bewijs*, Deventer: Kluwer 2003, nr. 47, p. 86 en 87.

166 P.A. Stein, A.S. Rueb, Burgerlijk Procesrecht, Deventer: Kluwer 2003, p. 128.

167 T.R. Hidma, G.R. Rutgers, *Pitlo. Het Nederlands burgerlijk recht. Deel 7. Bewijs*, Deventer: Kluwer 2003, nr. 47, p. 88.

168 T.R. Hidma, G.R. Rutgers, *Pitlo. Het Nederlands burgerlijk recht. Deel 7. Bewijs*, Deventer: Kluwer 2003, nr. 47, p. 101.

Voor authentieke akten regelt art. 157, lid 1 Rv de rechtskracht: *'Authentieke akten leveren tegen een ieder dwingend bewijs op van hetgeen de ambtenaar binnen de kring van zijn bevoegdheid omtrent zijn waarnemingen en verrichtingen heeft verklaard*'. De authentieke akte levert bewijs op jegens een ieder voor zoverre de ambtenaar binnen de kring van zijn bevoegdheid heeft bepaald. Daarmee heeft de authentieke akte dus dwingende rechtskracht jegens derden. Hierbij moet opgemerkt worden dat deze derdenwerking slechts geldt voor zoverre de ambtenaar binnen de kring van zijn bevoegdheid handelt en enkel de verklaring van de betreffende ambtenaar heeft dwingende rechtskracht.

Voor onderhandse akten en authentieke akten regelt art. 157 lid 2 Rv de rechtskracht: *'Een authentieke of onderhandse akte levert ten aanzien van de verklaring van een partij omtrent hetgeen de akte bestemd is ten behoeve van de wederpartij te bewijzen, tussen partijen dwingend bewijs op van de waarheid van die verklaring, tenzij dit zou kunnen leiden tot een rechtsgevolg dat niet ter vrije bepaling van partijen staat. Onder partij wordt begrepen de rechtverkrijgende onder algemene of bijzondere titel, voor zover het desbetreffende recht is verkregen na het opmaken van de akte*.' De rechtskracht van zowel de onderhandse als de authentieke akte heeft alleen tussen partijen rechtskracht en dat voor zoverre het rechtsgevolgen betreft die ter vrije bepaling van partijen staan. Dit geldt ook voor rechtverkrijgenden onder algemene of bijzondere titel, voor zover het desbetreffende recht is verkregen na het opmaken van de akte. Jegens derden heeft de akte vrije bewijskracht.[169] Het is dan aan de rechter welke bewijswaarde hij toekent aan de akte.

Materiële bewijskracht

Zowel de authentieke akte als de onderhandse akte leveren tussen partijen dwingende rechtskracht op van datgene wat in de akte staat. Hierbij gaat de wet uit van de materiële bewijskracht van de akte.[170] Dit wil zeggen dat de rechter bij een akte uit moet gaan van de waarheid van de verklaring in de akte. Pas als de echtheid van de handtekening in de akte wordt bestreden, wordt de dwingende rechtskracht doorbroken.[171] Het is dan aan de rechter om het geschrift te waarderen.

---

169 P.A. Stein, A.S. Rueb, *Burgerlijk Procesrecht*, Deventer: Kluwer 2003, p. 128.

170 *Parlementaire geschiedenis van het bewijsrecht in civiele zaken*, Deventer: Kluwer 1988, p. 144. Zie ook: C. Asser, A. Anema, P.J. Verdam, *Handleiding tot de beoefening van het Nederlands Burgerlijk Recht, Vijfde deel – van Bewijs*, Zwolle: W.E.J. Tjeenk Willink 1953, p. 112 – 124.

171 Art. 159, lid 2 Rv.

Formele bewijskracht

De onderhandse akte heeft materiële rechtskracht, maar ontbeert formele rechtskracht.[172] Bij de formele rechtskracht gaat het om de verhouding van datgene wat is verklaard en datgene wat in de onderhandse akte is opgetekend, oftewel om de vraag: is het waar dát er zo is verklaard. Dit heeft tot gevolg dat als een rechter twijfelt dat de opgetekende verklaring niet overeenkomt met datgene wat is verklaard, hij deze verklaring ook niet dwingend aan hoeft te nemen.[173] Echter, zodra vaststaat dat wat partijen hebben verklaard ook in de onderhandse akte staat (ook al is dit in strijd met de waarheid), dan staat ook de materiële rechtskracht vast. Voor de authentieke akte geldt, dat deze wel formele rechtskracht heeft. Juist omdat er een derde (onafhankelijke) partij is, namelijk de ambtenaar, die speciaal wordt belast met het opmaken van de authentieke akte en deze tevens een controlefunctie heeft, staat de formele rechtskracht voor de authentieke akte vast.[174]

Uitwendige bewijskracht

Bij de uitwendige bewijskracht gaat het om de vraag of een stuk dat het uiterlijk heeft van een akte ook als akte moet worden gekwalificeerd.[175] Dit is niet het geval bij de onderhandse akte.[176] De rechter is geheel vrij om te beoordelen of een stuk dat eruit ziet als een onderhandse akte te onderzoeken en wel of niet te kwalificeren als onderhandse akte. Daarentegen heeft de authentieke akte ingevolge art. 159, lid 1 Rv wel dwingende bewijskracht.[177] Indien een geschrift het uiterlijk heeft van een authentieke akte, dan geldt deze als zodanig behoudens bewijs van het tegendeel.

---

172 T.R. Hidma, G.R. Rutgers, *Pitlo. Het Nederlands burgerlijk recht. Deel 7. Bewijs*, Deventer: Kluwer 2003, nr. 47, p. 88.

173 G.R. Rutgers (red.), *Parlementaire geschiedenis van het bewijsrecht in civiele zaken*, Deventer: Kluwer 1988, p. 152. Lange tijd is het tegenovergestelde verdedigd. Zie hiervoor bijvoorbeeld: C. Asser, A. Anema, P.J. Verdam, *Handleiding tot de beoefening van het Nederlands Burgerlijk Recht, Vijfde deel – van Bewijs*, Zwolle: W.E.J. Tjeenk Willink 1953, p. 112 – 124. H.J. Scheltema, *Nederlandsch burgerlijk bewijsrech*t, Zwolle: W.E.J. Tjeenk Willink 1939, p. 260 t/m 262.

174 T.R. Hidma, G.R. Rutgers, *Pitlo. Het Nederlands burgerlijk recht. Deel 7. Bewijs*, Deventer: Kluwer 2003, nr. 47, p. 88.

175 G.R. Rutgers (red.), *Parlementaire geschiedenis van het bewijsrecht in civiele zaken*, Deventer: Kluwer 1988, p. 152.

176 C. Asser, A. Anema, P.J. Verdam, *Handleiding tot de beoefening van het Nederlands Burgerlijk Recht, Vijfde deel – van Bewijs*, Zwolle: W.E.J. Tjeenk Willink 1953, p. 160; T.R. Hidma, G.R. Rutgers, *Pitlo. Het Nederlands burgerlijk recht. Deel 7. Bewijs*, Deventer: Kluwer 2003, nr. 43, p. 90 t/m 92.

177 G.R. Rutgers (red.), *Parlementaire geschiedenis van het bewijsrecht in civiele zaken*, Deventer: Kluwer 1988, p. 152. Zie ook: C. Asser, A. Anema, P.J. Verdam, *Handleiding tot de beoefening van het Nederlands Burgerlijk Recht, Vijfde deel – van Bewijs*, Zwolle: W.E.J. Tjeenk Willink 1953, p. 112 t/m 124.

4.11 Het elektronisch geschrift

Zoals in paragraaf 4.10.2 al is opgemerkt is het de vraag of onder de definitie van 'geschrift' ook elektronische gegevens moeten worden verstaan. Van Esch gaat nader in op deze vraag en concludeert dat er in de literatuur verdeeldheid heerst(e).[178] Hierbij moet worden opgemerkt dat dit de stand van zaken was in 1999. In de tussentijd is art. 6:227a BW toegevoegd. Dit artikel voorziet in een oplossing om daar waar een wettelijke schriftelijkheidseis wordt gesteld hieraan ook te kunnen voldoen met gebruikmaking van elektronische gegevens. Daarnaast is er de eerste jurisprudentie met betrekking tot schriftelijkheid en elektronische gegevens.

In sommige gevallen stelt de wet een schriftelijkheidsvereiste. In het geval dat het de totstandkoming van overeenkomsten betreft is art. 6:227a BW van toepassing. Op de vraag of elektronische gegevens als geschrift moeten worden beschouwd doet art. 6:227a BW geen uitspraak. Enkel wordt gesteld dat in bepaalde gevallen aan de eis van schriftelijkheid wordt voldaan indien gebruik wordt gemaakt van de elektronische weg. Art 6:227a BW stelt in lid 1: "Indien uit de wet voortvloeit dat een overeenkomst slechts in schriftelijke vorm geldig of onaantastbaar tot stand komt, is aan deze eis tevens voldaan indien de overeenkomst langs elektronische weg is tot stand gekomen en:
a. raadpleegbaar door partijen is;
b. de authenticiteit van de overeenkomst in voldoende mate gewaarborgd is;
c. het moment van totstandkoming van de overeenkomst met voldoende zekerheid kan worden vastgesteld; en
d. de identiteit van de partijen met voldoende zekerheid kan worden vastgesteld."
De wetgever heeft met deze bepaling de mogelijkheid gegeven om in gevallen waar een wettelijke schriftelijkheidseis wordt gesteld voor het geldig of onaantastbaar totstandkomen van een overeenkomst, ook aan deze eis wordt voldaan als deze overeenkomst langs elektronische weg wordt gesloten en er voldoende zekerheid bestaat over de onder a t/m d genoemde onderwerpen.

Sub a van art. 6:227a, lid 1 BW stelt dat de overeenkomst raadpleegbaar is voor partijen. Dit dient te zijn 'vóór of op het moment van het sluiten van de overeenkomst als ter latere kennisneming.'[179] De bestendigheid van de gegevensdrager is echter niet dwingend voorgeschreven. Partijen kunnen kiezen voor een duurzame gegevensdrager waarbij de data waarin de

[178] R.E. van Esch, *Electronic Data Interchange (EDI) en het vermogensrecht* (diss. Nijmegen), W.E.J. Tjeenk Willink, Deventer: 1999, p. 184 t/m 185

[179] *Kamerstukken II*, 2000/2001, 28197, p. 6.

overeenkomst opgetekend ligt niet of moeilijk gewijzigd kan worden, maar ook mogen partijen kiezen voor minder bestendige gegevensdrager.[180]

Sub b van art. 6:227a, lid 1 BW stelt dat de authenticiteit van de overeenkomst in voldoende mate gewaarborgd is. In beginsel komt dit er (ook volgens de minister) op neer dat de overeenkomst tijdens de verzending geen wijzigingen meer heeft ondergaan.[181] Het gebruik van een elektronische handtekening of een andere techniek is niet voorgeschreven. Het is volgens de minister aan partijen om ervoor te zorgen dat de authenticiteit in voldoende mate gewaarborgd is. Hoewel de minister verder niet ingaat op welke maatregelen partijen zouden kunnen treffen, zou er naar mijn mening gebruik kunnen worden gemaakt van minder zware technische middelen. Te denken valt aan gebruikmaking van derde partijen (*trusted third parties (TTP*)) of het meermaals versturen dan wel het toevoegen van extra gegevens waaruit de authenticiteit kan blijken. Zolang maar voldoende zekerheid komt te bestaan over de authenticiteit van partijen. Overigens wordt er gesproken over 'de authenticiteit van de overeenkomst'. Naar mijn mening moet hier gesproken worden over de authenticiteit van de data (of het document) waarin de overeenkomst is vastgelegd.

Sub c van art 6:227a, lid 1 BW eist dat het moment van totstandkoming van de overeenkomst met voldoende zekerheid kan worden vastgesteld. Volgens de minister dient het tijdstip van totstandkoming in die mate vast te staan zoals dat ook het geval hoort te zijn bij een niet schriftelijke overeenkomst.[182] De vraag hoe partijen dit kunnen regelen, wordt verder niet beantwoord.

Als laatste dient voldaan te zijn aan sub d van art. 6:227a, lid 1 BW; de identiteit van partijen kan met voldoende zekerheid worden vastgesteld. Met de bewoordingen 'met voldoende zekerheid' wordt de parallel getrokken met de 'gewone' schriftelijke overeenkomst. De identeit moet vaststaan in dezelfde mate als dat het geval zou zijn bij een schriftelijke overeenkomst. Hoe partijen aan deze eis tegemoet komen, staat de partijen vrij. De minister geeft ook aan dat zelfs al zou er onduidelijkheid bestaan over de identiteit van partijen, dan nog kan de identiteit op andere wijze met voldoende mate zekerheid worden vastgesteld. Bedacht moet worden dat ondertekening slechts één van de manieren is waarop de identiteit van partijen kan worden vastgesteld.[183]

De criteria a t/m d van art. 6:227, lid 1 BW zijn abstracte criteria. De vraag hoe deze concreet gemaakt kunnen worden, wordt niet beantwoord en het is dan ook aan partijen om aan deze abstracte criteria invulling te geven. Echter bij

180 *Kamerstukken II*, 2000/2001, 28197, p. 7.
181 *Kamerstukken II*, 2000/2001, 28197, p. 7
182 *Kamerstukken II*, 2000/2001, 28197, p. 8.
183 *Kamerstukken II*, 2000/2001, 28197, p. 8.

gebrek aan jurisprudentie is het niet duidelijke welke concrete criteria als voldoende betrouwbaar worden beschouwd.[184]

Een aantal specifieke onderwerpen is uitgesloten van de schriftelijkheidgelijkstelling van art. 6:227a. lid 1 BW.[185] De wetgever heeft gekozen voor een tussenoplossing om enerzijds de wens tussen partijen om elektronisch te contracteren niet in de weg te staan en om anderzijds niet teveel vooruit te lopen of de technische ontwikkelingen om te voorkomen dat langs elektronische weg niet dezelfde waarborgen zouden kunnen worden geboden als in de analoge wereld.[186] Het betreft hier de in lid 2 en 3 van art 6:227a BW genoemde onderwerpen. Dit zijn ten eerste overeenkomsten die rechten doen ontstaan of overdragen ten aanzien van onroerende zaken, met uitzondering van huurrechten (art. 6:227a, lid 2, onder a BW). Ten tweede overeenkomsten waarbij persoonlijke of zakelijke zekerheden worden verstrekt door personen die niet handelen in de uitoefening van een beroep of bedrijf; voor zover de aard van de overeenkomst of van de rechtsbetrekking waarvan zij deel uitmaakt zich daartegen verzet (art. 6:227a, lid 2, onder b BW). Ten derde overeenkomsten waarvoor de wet de tussenkomst voorschrijft van de rechter, een overheidsorgaan of een beroepsbeoefenaar die een publieke taak uitoefent (art. 6:227a, lid 3, onder a BW). Ten vierde overeenkomsten die onder het familierecht of het erfrecht vallen (art. 6:227a, lid 3, onder b BW).

Een vijfde beperking is niet te vinden in lid 2 of lid 3 van art. 6:227a BW, maar ligt besloten in lid 1. Ik vind het opvallend dat hele bepaling van art. 6:227a BW enkel ziet op overeenkomsten die slechts in schriftelijke vorm geldig of onaantastbaar tot stand komen. Daarmee wordt de eenzijdige rechtshandeling uitgesloten van de gelijkstelling voor wat betreft het schriftelijkheidvereiste en een schakelbepaling die de regeling ook van toepassing verklaart op eenzijdige rechtshandelingen ontbreekt. Nu verplicht de De minister geeft in de Memorie van Toelichting aan dat dit artikel geen dwingendrechtelijke regeling geeft ten aanzien van overeenkomsten waarvoor geen wettelijke vormvereisten gelden.[187] Dit is met het oog gericht op de achtergrond van de regeling, namelijk belemmeringen van het vormvereiste van schriftelijkheid weg te nemen begrijpelijk, maar heeft vanuit bewijsrechtelijk oogpunt een naar mijn mening onwenselijke (en waarschijnlijk onvoorziene) bijwerking. Het rechtvaardigt mijns inziens niet dat eenzijdige rechtshandelingen worden uitgesloten.

---

184 Jurisprudentie niet bekend in het maandblad Computerrecht. Ook de database op rechtspraak.nl bevat geen uitspraken die nader ingaan op deze criteria (laatst geraadpleegd op 01-02-2010).

185 Richtlijn nr. 2000/31/EGvan het Europees Parlement en de Raad van de Europese Unie betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (richtlijn inzake de elektronische handel) geeft hiertoe de ruimte.

186 *Kamerstukken II*, 2000/2001, 28197, p. 54 en 55; *Kamerstukken II*, 2007-2008, 31358, nr. 3, p. 8.

187 *Kamerstukken II*, 2000/2001, 28197, nr. 3. p. 51 en 52.

Rechtvaardig of niet, de wetstekst van art. 6:227a BW ziet alleen op overeenkomsten en sluit eenzijdige rechtshandelingen uit.[188] Desondanks kwam de Rechtbank Amsterdam toch tot een ander oordeel in het geval dat een ingebrekestelling als bedoeld in art. 6:82 BW niet schriftelijk, maar via e-mail was geschied.[189] De rechtbank overwoog: "*De rechtbank is met G-sus van oordeel dat het onder 2.8. vermelde e-mailbericht van 21 maart 2006 voldoet aan de vereisten voor ingebrekestelling als vermeld in artikel 6:82 van het Burgerlijk Wetboek (BW)*." Uit de uitspraak blijkt echter nergens op grond waarvan zij de e-mail accepteert als ingebrekestelling (welke volgens de wet schriftelijk dient te geschieden). Zo kan het zijn dat hij van oordeel is dat art. 6:227a BW analoge toepassing dient te vinden op enkelzijdige rechtshandelingen. Echter, indien art. 6:227a BW analoge toepassing zou hebben gevonden, zou de rechter toch op zijn minst moeten toetsen aan de criteria van art. 6:227a, lid 1 BW en dit is niet gebeurd. Daarom ligt een andere verklaring in de rede. De rechter heeft de e-mail zelf als schriftelijk aangemerkt. Mijns inziens gaat de rechter hiermee in tegen de bedoeling van de wetgever die met art. 6:227a BW juist eisen heeft willen stellen aan elektronische gegevens voordat deze gelijkgesteld kunnen worden aan een schriftelijk stuk. De rechter heeft mijns inziens het recht onjuist toegepast.

4.12 De elektronische handtekening

Het tweede vereiste voor een akte is de ondertekening met een naam of handtekening. De belangrijkste functies van de handtekening, namelijk de identificatiefunctie en de authentificatiefunctie, zijn van belang om de persoon die het geschrift heeft ondertekend, aan te kunnen wijzen.[190] Samen met een elektronisch geschrift kan de elektronische handtekening gekwalificeerd worden als akte en daarmee bestaat er dwingende bewijskracht van die akte. In deze paragraaf wordt nader ingegaan op de wettelijke regeling betreffende de elektronische handtekening, zoals neergelegd in art. 3:15a BW.

De elektronische handtekening is niet alleen van belang als vereiste voor de akte. De authentificatiefunctie die de elektronische handtekening heeft, kan dienen als een digitale *fingerprint*. Door gebruik te maken van deze

---

188 Tot deze conclusie komt ook Martius in H.P.A.J. Martius, *Elektronisch Handelsrecht* (diss. Heerlen), Zutphen: Paris 2008, p. 107 1/m 109.

189 Rb. Amsterdam van 21 november 2007, *LJN* BC0337, r.o. 4.11 (Canon Nederland N.V. / G-SUS Wholesale and Design B.V.). Zie ook: E.C. Kraan-Beekman, 'Leerstukken – Elektronisch contracteren, maar toch de pen (moeten) hanteren?', *Contracteren* 2009-3, p. 80 en 81.

190 Deze functies worden ook onderscheiden door van Esch in R.E. van Esch, *Electronic Data Interchange (EDI) en het vermogensrecht*, (diss. Nijmegen), Deventer: W.E.J. Tjeenk Willink 1999, p. 136 – 139.

elektronische handtekening kan aangetoond worden wie welke handelingen heeft verricht. Deze bewijsfunctie is eveneens van belang in dit onderzoek.

Het recht laat na de handtekening nader te definiëren. Voor dit onderzoek is een definitie van een handtekening niet van groot belang, omdat dit onderzoek zich richt op elektronische bewijsmiddelen en daarmee de handgeschreven handtekening buiten beschouwing laat. Voor dit onderzoek is de elektronische equivalent van de handtekening van belang: in juridische termen heet dit equivalent de elektronische handtekening. De elektronische handtekening wordt in art. 3:15a, lid 4 BW gedefinieerd als: *"een handtekening (…) die bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens die worden gebruikt als middel voor authentificatie."*

Bovenstaande definitie beschrijft twee groepen gegevens. Ten eerste een handtekening die bestaat uit elektronische gegevens en ten tweede andere elektronische gegevens.[191] In de eerste plaats zijn de gegevens elektronisch van vorm. Dit lijkt het intrappen van een open deur, maar als de gegevens niet in elektronische vorm bestaan is er geen sprake van een elektronische handtekening. Vervolgens moet de eerste groep gegevens die de elektronische handtekening vormen, zijn vastgehecht aan of logisch geassocieerd zijn met andere gegevens. Dit wil zeggen dat een elektronische handtekening bestaat uit een aantal elektronische gegevens welke samen met de andere elektronische gegevens zodanige toegangkenmerken bevatten, dat de computer die deze kenmerken vergelijkt, vaststelt dat zij bij elkaar horen.[192] Ten derde moeten de elektronische gegevens gebruikt worden ter authentificatie, oftewel als bewijs dat de gegevens daadwerkelijk van degene komen als waarvan gesteld wordt dat ze afkomstig zijn. De eisen die aan gegevens gesteld worden om als elektronische handtekening beschouwd te kunnen worden, zijn daarmee ruim geformuleerd. Zo is een pincode ook een elektronische handtekening, want de pincode bestaat uit elektronische gegevens die zijn vastgehecht of logisch geassocieerd met de gegevens die gelezen worden van de bankpas en deze gegevens worden gebruikt om een persoon te identificeren.[193] Ook wachtwoorden om fysieke of "cybertoegang" te krijgen tot ruimtes of gegevens zijn bedoeld om te identificeren en kunnen beschouwd worden als elektronische handtekening.

De elektronische handtekening heeft juridische status gekregen met de bepaling die is vervat in art. 3:15a, lid 1 BW. Dit artikel stelt: *"Een elektronische handtekening heeft dezelfde rechtsgevolgen als een handgeschreven*

---

191 A.R. Lodder, J. Dumortier, S.H. Bol, *Het recht rond elektronische handtekeningen, Richtlijn 1999/93/EG en de omzetting in België en Nederland*, Deventer, Kluwer: 2005, p. 23 en 24.

192 *Kamerstukken II*, 2000/2001, 27743, nr. 3. p. 16.

193 Het proces van identificatie wordt ook wel authentificatie genoemd.

handtekening, indien de methode die daarbij is gebruikt voor authentificatie voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval."

De rechtsgevolgen van een elektronische handtekening worden gelijk gesteld met de rechtsgevolgen van een handgeschreven handtekening als de methode van authentificatie voldoende betrouwbaar is. Bij het bepalen van de betrouwbaarheid dienen twee uitgangspunten in acht genomen te worden: het doel waarvoor de elektronische gegevens werden gebruikt en alle overige omstandigheden van het geval. Deze twee uitgangspunten zijn bewust "open" geformuleerd "om de nodige flexibiliteit in het elektronisch rechtsverkeer mogelijk te maken en aldus aan partijen een grote mate van vrijheid te bieden om het voor de tussen hen te gebruiken elektronische handtekening gewenste veiligheids- en betrouwbaarheidsniveau zelf te bepalen".[194]

De authentificatiefunctie neemt, evenals bij de handgeschreven handtekening een belangrijke plaats in. Dit blijkt ook wel uit het feit dat in bijna alle leden van artikel 3:15a BW de methode van authentificatie centraal wordt gesteld. Art. 3:15a BW regelt voor een deel de eisen die gesteld kunnen worden aan de methode van authentificatie om te bepalen of die methode betrouwbaar genoeg is om de elektronische handtekening dezelfde rechtsgevolgen te kunnen verlenen als de handgeschreven handtekening.

De leden 2 en 3 van art. 3:15a BW geven vervolgens een nadere invulling van wat onder de betrouwbaarheid en onbetrouwbaarheid van "de methode van authentificatie" moet of kan worden verstaan. "Moet worden verstaan", omdat in lid 2 van art. 3:15a BW een wettelijk bewijsvermoeden is neergelegd dat stelt dat de in lid 1 genoemd methode voor authentificatie wordt vermoed voldoende betrouwbaar te zijn indien er cumulatief aan een zestal in lid 2 genoemde eisen voldaan is. "Kan worden verstaan", omdat art. 3:15a, lid 3 BW stelt dat deze methode voor authentificatie niet als onvoldoende betrouwbaar kan worden aangemerkt op de enkele grond dat deze niet voldoet aan de gronden gesteld in lid 3 van art. 3:15a BW[195] In het geval dat aan geen of slechts aan de eerste vier van de zes in lid 2 genoemde eisen is voldaan geldt niet van rechtswege het vermoeden van de betrouwbaarheid van de methode van authentificatie.[196] Echter ook het vermoeden van onbetrouwbaarheid geldt niet van rechtswege. Het is aan de rechter om te beoordelen of de methode van authentificatie voldoende betrouwbaar is.

---

194 *Kamerstukken II*, 2000/2001, 27743, nr. 6. p. 2.

195 Twee van deze drie eisen worden tevens genoemd in het reeds genoemde art. 3:15a, lid 2 BW.

196 Deze drie eisen worden verderop in deze paragraaf besproken. Zie ook: A.R. Lodder, J. Dumortier, S. Bol, *Het recht rond elektronische handtekeningen*, Deventer, Kluwer: 2005, p. 91.

Lid 2 van art 3:15a BW stelt dat een in lid 1 bedoelde methode (van authentificatie) wordt vermoed voldoende betrouwbaar te zijn, indien een elektronische handtekening voldoet aan de volgende 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 middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; en
d. zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;
e. zij is gebaseerd op een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss, van de Telecommunicatiewet;
f. zij is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen als bedoeld in artikel 1.1, onderdeel vv, van de Telecommunicatiewet."

In lid 2 van art. 3:15a BW wordt een bewijsvermoeden neergelegd. Het bewijsvermoeden (zie paragraaf 4.4) is in dit geval een wettelijk weerlegbaar bewijsvermoeden. De methode van authentificatie die wordt genoemd in lid 1 van de elektronische handtekening die voldoet aan het zestal vereisten (onderdeel a t/m f), wordt vermoed voldoende betrouwbaar te zijn. De bewijslast om de betrouwbaarheidswaardering van de rechter te beïnvloeden wordt daarmee echter niet omgekeerd; het is alleen aan de wederpartij tegenbewijs te leveren. De rechter dient de betrouwbaarheid aan te nemen, tenzij de wederpartij erin slaagt met tegenbewijs het vermoeden dat de methode van authentificatie voldoende betrouwbaar is onderuit te halen.[197] De vraag is hoe de zinsnede "gelet op het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval" en de in lid 2 genoemde vereisten zich verhouden. Deze zinsnede geeft namelijk twee criteria waarbij rekening moet worden gehouden bij de waardering van de betrouwbaarheid van de methode van authentificatie. Lid 2 legt echter een bewijsvermoeden neer wat de waardering van de betrouwbaarheid van de methode van authentificatie lijkt te ontnemen. De Europese regeling waarop de Wet op de elektronische handtekening is gebaseerd schrijft geen dwingende bewijskracht voor.[198] Met implementatie van de richtlijn in de Nederlandse wet is met lid 2 van art. 3:15a BW een weerlegbaar wettelijk bewijsvermoeden neergelegd waar de rechter, behoudens geslaagd tegenbewijs, aan gehouden is.[199] Ik ben dan ook van mening dat het in lid 2 neergelegde bewijsvermoeden het criterium "gelet op

197 *Kamerstukken II*, 2000/2001, 27743, nr. 3. p. 16.
198 Art. 5, lid 1, onder b van Richtlijn nr. 1999/93/EG (PbEG 2000 L13/12).
199 Er wordt dus niet ingegrepen in de bewijskracht, maar er wordt afgeweken van de verdeling van de bewijslast met een bewijswettelijk weerlegbaar bewijsvermoeden. T.R. Hidma, G.R. Rutgers, *Pitlo. Het Nederlands burgerlijk recht. Deel 7. Bewijs*, Deventer: Kluwer 2003, nr. 21, p. 39.

het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval" uit lid 1, op grond van specialiteit derogeert. Het bewijsvermoeden is namelijk van dusdanig dwingende aard, dat de rechter niet via lid 1 alsnog de bevoegdheid heeft om het doel waarvoor de elektronische gegevens werden gebruikt en alle overige omstandigheden van het geval in het betrouwbaarheidoordeel te betrekken.

Een elektronische handtekening die voldoet aan de eisen a t/m f wordt dus in beginsel voldoende betrouwbaar geacht als bewijsmiddel. Om de bewijspositie te versterken biedt een elektronische handtekening die voldoet aan de eisen a t/m f van art. 3:15, lid 2 BW daarom de grootst mogelijke bewijszekerheid. De eisen a t/m d zijn bijna één-op-één overgenomen uit de richtlijn betreffende een gemeenschappelijk kader voor elektronische handtekeningen en bij de bespreking van deze onderdelen zal ik de Richtlijn betrekken.

Ingevolge onderdeel a van art. 3:15a, lid 2 BW moet de elektronische handtekening op unieke wijze aan de ondertekenaar verbonden zijn. In de eerste plaats moet er sprake zijn van een ondertekenaar. Dit is degene die *"een middel voor het aanmaken van elektronische handtekeningen als bedoeld in artikel 1.1 onderdeel uu van de Telecommunicatiewet gebruikt"*. [200] De ondertekenaar hoeft ingevolge deze definitie niet degene te zijn die de handtekening zet; het is degene die het middel om handtekeningen aan te maken gebruikt en daarmee de eigenaar van de handtekening bindt. Een ondertekenaar is dus niet degene die de handtekening zet, maar degene die beschikt over het middel voor het aanmaken van handtekeningen. [201] Onderdeel van de definitie van ondertekenaar is de eis, welke gesteld wordt in art. 1.1, onderdeel uu Telecommunicatiewet, dat er sprake is van een middel voor het aanmaken van elektronische handtekeningen. Art. 1.1, onderdeel uu Telecommunicatiewet spreekt echter niet over een middel, maar geeft een definitie van "certificatiedienstverlener". Bedoeld wordt waarschijnlijk echter art. 1.1, onderdeel vv Telecommunicatiewet dat een definitie geeft van "middel". [202] Onder middel wordt verstaan: "geconfigureerde software of hardware die wordt gebruikt om de gegevens voor het aanmaken van elektronische handtekeningen te implementeren". Hoewel de Nederlandse wet niet verder ingaat op een definitie van "*gegevens voor het aanmaken van elektronische handtekeningen*" zegt de richtlijn hierover in art. 2, lid 4 dat dit zijn "unieke gegevens, zoals codes of cryptografische privé-sleutels, die door de

---

200 Art. 3:15a, lid 5 BW.

201 A.R. Lodder, J. Dumortier, S. Bol, *Het recht rond elektronische handtekeningen*, Deventer, Kluwer: 2005, p. 27.

202 Waarschijnlijk is bij de wijziging van de Telecommunicatiewet in verband met de implementatie van richtlijn 2004/108/EG in de Wet van 28 december 2006, Stb. 2007, 21 vergeten om de verlettering van art 1.1, onderdeel kk. t/m zz. naar ll. t/m aaa. tevens door te voeren in art. 3:15a BW.

ondertekenaar worden gebruikt om een elektronische handtekening aan te maken." De tweede eis die gesteld wordt, is dat de elektronische handtekening aan de ondertekenaar verbonden moet zijn en wel op unieke wijze. Dit houdt in dat niemand anders dan de ondertekenaar in verband moet kunnen worden gebracht met de elektronische handtekening.

Onderdeel b van art. 3:15a, lid 2 BW stelt dat elektronische handtekening het mogelijk maakt de ondertekenaar te identificeren. Met de handtekening moet het mogelijk zijn om de identiteit van de persoon die de handtekening heeft gezet, te kunnen vaststellen. Het gaat hier dus ook weer om de ondertekenaar (degene die beschikt over het middel voor het aanmaken van handtekeningen) en niet om degene die de eigenaar is van de handtekening, maar degene die het middel om de elektronische handtekening aan te maken, heeft gebruikt.

Onderdeel c van art. 3:15a, lid 2 BW geeft aan dat de elektronische handtekening tot stand komt met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden. Hierbij wordt weer gedoeld op middelen als in art. 2, lid 5 van de richtlijn.[203] Dit zijn de middelen als bedoeld in art. 1.1 onderdeel vv Telecommunicatiewet, hoewel hier niet expliciet naar verwezen wordt. De ondertekenaar moet de geconfigureerde software of hardware die wordt gebruikt om de gegevens voor het aanmaken van elektronische handtekeningen te implementeren onder zijn uitsluitende controle kunnen houden. De wet stelt echter niet hoe dit in de praktijk mogelijk zou moeten zijn.

Art. 3:15a, lid 2 onder d BW stelt dat de elektronische handtekening op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft is verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord. Hier wordt gedoeld op de integriteit van de gegevens waarmee de elektronische handtekening is verbonden. Iedere modificatie van de gegevens moet kunnen worden opgespoord zodat kan worden vastgesteld of de gegevens nog wel betrouwbaar zijn.

In onderdeel e van art. 3:15a, lid 2 BW wordt gesteld dat een elektronische handtekening is gebaseerd op een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss (bedoeld wordt tt), van de Telecommunicatiewet. Dit certificaat heeft als functie dat misbruik van elektronische handtekeningen zoveel mogelijk wordt tegengegaan door een publieke sleutel aan de hantekening toe te voegen.[204] Een gekwalificeerd certificaat is een certificaat dat voldoet aan de eisen, gesteld krachtens artikel 18.15, tweede lid

---

[203] A.R. Lodder, J. Dumortier, S. Bol, *Het recht rond elektronische handtekeningen*, Deventer, Kluwer: 2005, p. 28.

[204] A.R. Lodder, J. Dumortier, S. Bol, *Het recht rond elektronische handtekeningen*, Deventer, Kluwer: 2005, p. 95 en 96. Voor (publieke) versleuteling zie paragraaf 3.4 en voor de eisen die gesteld worden zie paragraaf 4.12.

Telecommunicatiewet, en is afgegeven door een certificatiedienst die voldoet aan de eisen, gesteld krachtens artikel 18.15, eerste lid Telecommunicatiewet. Zowel in art. 18.15, lid 1 als lid 2 Telecommunicatiewet wordt verwezen naar een algemene maatregel van bestuur die eisen stelt aan een gekwalificeerd certificaat en aan een certificatiedienst. Deze eisen zijn echter niet van direct belang voor dit onderzoek. In paragraaf 4.13 zal ik voor de volledigheid kort ingaan op de functies van de certificaatdienstverlener, het gekwalificeerd certificaat en het veilige middel.

Art 3:15a, lid 2 onderdeel f BW stelt dat de elektronische handtekening is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen als bedoeld in artikel 1.1 onderdeel vv (bedoeld wordt ww) van de Telecommunicatiewet. Dit is een middel voor het aanmaken van elektronische handtekeningen dat voldoet aan de eisen gesteld krachtens artikel 18.17, eerste lid. Art. 18.17 Telecommunicatiewet kent echter geen eerste lid. Het geeft echter wel eisen die gesteld worden aan een veilig middel: "Degene die een veilig middel voor het aanmaken van elektronische handtekeningen op de markt brengt, zorgt ervoor dat het veilig middel voldoet aan de bij of krachtens algemene maatregel van bestuur te stellen eisen en, ten behoeve daarvan, dat het veilig is voorzien van een verklaring van een door Onze Minister aangewezen instelling als bedoeld in artikel 18.17a of van een verklaring van een instelling die is aangewezen door de bevoegde autoriteiten van een andere lidstaat van de Europese Gemeenschap dan wel van een van de overige staten die partij zijn bij de Overeenkomst betreffende de Europese Economische Ruimte, dat het middel voldoet aan de eisen."

Art. 3:15a, lid 3 BW geeft aan wanneer de methode van authentificatie zoals bedoeld in lid 1, niet als voldoende betrouwbaar kan worden beschouwd, namelijk op de enkele grond dat deze:

- niet is gebaseerd op een gekwalificeerd certificaat als bedoeld in art. 1.1, onderdeel ss van de Telecommunicatiewet;
- niet is gebaseerd op een door een certificatiedienstverlener als bedoeld in art. 18.16 eerste lid van de Telecommunicatiewet afgegeven certificaat of;
- niet met een veilig middel voor het aanmaken van elektronische handtekeningen is aangemaakt als bedoeld in art. 1.1 onderdeel vv van de Telecommunicatiewet.

Mocht een elektronische handtekening wel voldoen aan de eisen a t/m d van lid 2 van art. 3:15a BW, maar niet aan de eisen e of f (dit zijn de eerste en tweede eisen die genoemd worden in lid 3 van art. 3:15a BW) of niet met een veilig middel zijn aangemaakt, dan heeft dit niet tot gevolg dat de methode van authentificatie op grond daarvan onbetrouwbaar wordt. Daar zullen dan nog andere feiten voor moeten worden aangetoond. Het bewijsvermoeden van de betrouwbaarheid van de methode van authentificatie (uit lid 2) blijft gelden.

Wordt namelijk niet aan één van de voorwaarden onder e of f voldaan of wordt de elektronische handtekening niet met een veilig middel aangemaakt, dan is dit enkele feit niet voldoende om het bewijsvermoeden weg te nemen. Echter, indien aan meerdere van deze voorwaarden niet is voldaan of er andere bijkomende omstandigheden zijn, dan kunnen deze het bewijsvermoeden doorbreken. Dit heeft tot gevolg dat de rechter weer volledig van zijn discretionaire bevoegdheid gebruik kan maken om de betrouwbaarheid van de methode van authentificatie van de elektronische handtekening te waarderen.

Net als bij lid 2 van art. 3:15 BW is het de vraag hoe art. 3:15a, lid 3 BW zich verhoudt tot de maatstaf "*gelet op het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval*" in art. 3:15a, lid 1 BW. Art. 3:15a, lid 3 BW stelt dan wel dat als niet voldaan is aan één of meer van de drie genoemde gronden de handtekening niet per definitie onbetrouwbaar is, maar daarmee wordt niets gezegd over de betrouwbaarheid van deze elektronische handtekening.[205] De betrouwbaarheid van de methode van authentificatie van een elektronische handtekening die wel voldoet aan de eisen a t/m d van lid 2 van art. 3:15a BW, maar niet aan de eisen e **of** f **of** niet met een veilig middel zijn aangemaakt, is een specifieke regel. Deze gaat voor de algemene regel in lid 1. Lid 3 derogeert in dat geval daarmee lid 1.

Echter als een elektronische handtekening die wel voldoet aan de eisen a t/m d van lid 2 van art. 3:15a BW, maar niet aan **twee of meer** van de eisen e, f **o*f*** niet met een veilig middel zijn aangemaakt, of er sprake is van **één** van deze eisen **en** er bijkomende omstandigheden zijn waar met succes een beroep op wordt gedaan, dan zal de specialiteit van de regel doorbroken worden en zal de rechter terugvallen op zijn discretionaire bevoegdheid. In beginsel wordt lid 1 dan ook gederogeerd door lid 3. Echter lid 3 zal dan niet meer voorschrijven dat de methode van authentificatie wel of niet voldoende betrouwbaar is, waardoor de rechter binnen zijn discretionaire bevoegdheid geheel kan terugvallen op lid 1 en de betrouwbaarheid van de methode van authentificatie beoordelen "*gelet op het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval*".

Art 3:15a BW lijkt een zekerheid te willen bieden, maar biedt deze zekerheid mijns insziens enkel voor het geval dat voldaan is aan alle zes de eisen van lid 2. De rechter behoudt veel ruimte om zelf te oordelen of hij de methode van authentificatie voldoende betrouwbaar acht en aan de elektronische handtekening dezelfde rechtsgevolgen verleent als de handgeschreven handtekening heeft.

---

[205] Dit in tegenstelling wat gesteld wordt pagina 86 in A.R. Lodder, J. Dumortier, S. Bol, *Het recht rond elektronische handtekeningen*, Deventer, Kluwer: 2005.

4.13 Het (gekwalificeerd) certificaat, de certificaatdiensverlener en het veilige middel

Een betrouwbaarheid van de methode van authentificatie van de elektronische handtekening is afhankelijk van verschillende factoren.[206] Drie van deze factoren zijn de certificaatdienstverlener, het gekwalificeerd certificaat en het veilige middel. De eisen waaraan deze moeten voldoen zijn opgenomen in de artikelen 2, 3 en 5 van het Besluit elektronische handtekeningen. Er moet cumulatief voldaan worden aan respectievelijk negentien, negen en vier eisen die rechtstreeks zijn overgenomen uit Bijlage I van de richtlijn. Aangezien deze eisen niet direkt zien op de kwaliteiten van de elektronische handtekening zelf zijn deze opgenomen in bijlage 1. Om de in de voorgaande paragraaf geschetste eisen aan de elektronische handtekening nader toe te lichten, zal ik wel kort ingaan op de functie van het (gekwalificeerd) certificaat, de certificaatdienstverlener en het veilige middel.

Het certificaat is in feite een elektronische bevestiging van de identiteit van de afzender. In het geval van een gewone elektronische handtekening wordt een specifieke code verbonden aan de eigenaar van de handtekening. Deze code kan online verkregen worden, zonder dat daar enige identificatie aan vooraf is gegaan. De betrouwbaarheid laat daarom te wensen over. Een gekwalificeerd certificaat kan worden gebruikt bij de geavanceerde elektronische handtekening. Het gekwalificeerd certificaat komt dan in de vorm van een publieke sleutel die aan de ondertekenaar verbonden. De ondertekenaar verkrijgt een gekwalificeerd certificaat pas als deze zich heeft geïdentificeerd bij de uitgever van het gekwalificeerd certificaat: de certificaatdienstverlener. Juist doordat deze zich heeft gelegitimeerd, staat met veel grotere zekerheid vast dat degene die gebruik maakt van het certificaat ook degene is aan wie het certificaat is uitgegeven. De betrouwbaarheid van dit certificaat is daardoor veel groter.

De certificaatdienstverlener is een natuurlijk persoon of rechtspersoon die certificaten afgeeft of andere diensten in verband met elektronische handtekeningen verleent. Het is in feite een derde partij (ook wel TTP of Trusted Third Party genoemd) die het vertrouwen van de afnemers van zijn diensten moet hebben. De certificaatdienstverlener die voldoet aan alle eisen zoals gesteld in art. 2 van het Besluit elektronische handtekeningen is bevoegd om gekwalificeerde certificaten af te geven. Hiervoor behoeft hij verder geen accreditatie.

Een veilig middel is een middel waarmee elektronische handtekeningen kunnen worden aangemaakt en waarbij specifieke eisen in acht zijn genomen zodat de

[206] Zie paragraaf 4.12.

vertrouwelijkheid van de elektronische handtekening gegarandeerd is en deze beschermd is tegen vervalsing. Het veilig middel waarborgt tevens dat de gegevens voor het aanmaken van elektronische handtekeningen kunnen worden beschermd tegen gebruikt door anderen. Ook laat het de te ondertekenen gegevens ongewijzigd en belet het niet dat die gegevens voor de ondertekening aan de ondertekenaar worden voorgelegd.

4.14 De elektronische onderhandse akte

4.14.1 Vereisten voor de elektronische onderhandse akte

Rechtshandelingen (en daarmee overeenkomsten) kunnen in een groot aantal gevallen vormvrij tot stand komen.[207] Het verrichten van rechtshandelingen langs elektronische weg is dan ook een mogelijkheid die partijen vrij stond reeds vóór de inwerkingtreding van de Wet elektronische handtekeningen en de Aanpassingswet richtlijn inzake elektronische handtekeningen. [208] Rechtshandelingen konden wel verricht worden en overeenkomsten konden tot stand komen, maar in de bewijspositie van het bestaan van die overeenkomsten stonden partijen minder sterk. Er bestond namelijk grote twijfel of aan een elektronisch bericht de status van onderhandse akte kon worden verleend, omdat niet duidelijk was of dit soort berichten geschriften waren en of de ondertekening wel voldoende waarde had om als handtekening te kunnen worden beschouwd. Daarmee ontbeerde het elektronisch bericht dwingende bewijskracht. Hoewel nog verdedigd kon worden dat aan het schriftelijkheidsvereiste voldaan was,[209] was het moeilijk om te verdedigen dat aan het ondertekeningsvereiste werd voldaan. Met de implementatie van de Richtlijn 1999/93/EG en Richtlijn 2000/31/EG in de Wet elektronische handtekeningen en de Aanpassingswet richtlijn inzake elektronische handel is er meer duidelijkheid gekomen over de invulling van het schriftelijkheidsvereiste en het ondertekeningsvereiste voor het ontstaan van een onderhandse akte via elektronische weg.

---

207 Art. 3:37, lid 1 BW.

208 De Wet elektronische handtekeningen, Stb. 2003, 199 (implementatie van Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen) en de Aanpassingswet richtlijn inzake elektronische handel (implementatie van Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ("richtlijn inzake elektronische handel")).

209 Zie voor een overzicht van deze verschillende standpunten R.E. van Esch, *Electronic Data Interchange (EDI) en het vermogensrecht*, (diss. Nijmegen), Deventer: W.E.J. Tjeenk Willink 1999, p. 170 – 195.

Het eerste vereiste is het in subparagraaf 4.11 aangehaalde vereiste van een geschrift. Art. 6:277a lid 1 BW bepaalt dat *"indien uit de wet voortvloeit dat een overeenkomst slechts in schriftelijke vorm geldig of onaantastbaar totstandkomt, aan deze eis tevens voldaan is indien de overeenkomst langs elektronische weg is totstandgekomen en (a) raadpleegbaar door partijen is; (b) de authenticiteit van de overeenkomst in voldoende mate gewaarborgd is; (c) het moment van totstandkoming van de overeenkomst met voldoende zekerheid kan worden vastgesteld; en; (d) de identiteit van de partijen met voldoende zekerheid kan worden vastgesteld."* De tweede eis waaraan een akte dient te voldoen is het ondertekeningsvereiste. In paragraaf 4.12 is behandeld dat in een elektronische omgeving aan het ondertekeningsvereiste kan worden voldaan door gebruikmaking van een elektronische handtekening.

Kan nu aan een overeenkomst, gesloten langs elektronische weg met daaraan gekoppeld een elektronische handtekening, de status van akte verleend worden? Daar art. 6:227a BW de schriftelijkheidseis voor het totstandkomen van overeenkomsten ook onder de in dat artikel beschreven omstandigheden van toepassing verklaart op overeenkomsten die langs elektronische weg gesloten zijn en art. 3:15a BW de rechtsgevolgen van een elektronische handtekening gelijk stelt met de gevolgen van een handgeschreven handtekening, kan gesteld worden dat een elektronische onderhandse akte tot stand kan komen. Deze opvatting is tevens door de minister verdedigd in de Parlementaire Geschiedenis naar aanleiding van kamervragen. Hierbij stelt de minister:"*binnen de grenzen van de artikelen 3:15a BW en 6:227a BW zal inderdaad voldaan kunnen worden aan de voor een akte gestelde eisen van ondertekening en schriftelijkheid (art. 156, eerste lid, Rv). Gelijkstelling met een akte ligt dan derhalve in de rede, met inbegrip van de daaraan toekomende – binnen de grenzen van art. 157, tweede lid, Rv dwingende – bewijskracht.*"[210] Hoewel niet iedere auteur het met deze opvatting eens lijkt te zijn,[211] ben ik er van overtuigd dat de artikelen 6:227a BW en 3:15a BW voldoende ruimte bieden om aan het schriftelijkheidsvereiste en het ondertekeningsvereiste te voldoen voor het constitueren van een elektronische variant van de onderhandse akte.[212] Mijn overtuiging dat een elektronische onderhandse akte tot stand kan komen binnen de grenzen van art. 6:227a BW en art. 3:15a BW, vindt steun in de opvatting van de minister en de opvattingen van Kemna en

---

210 *Kamerstukken I* 2002-2003, 27743, nr. 35, p. 10; Zie ook: H. Franken, H.W.K. Kaspersen, A.H. de Wild (red.), *Recht en computer*, Deventer: Kluwer 2004, p. 212 en R.E. van Esch, 'De betrekkelijke waarde van de Wet elektronische handtekeningen voor de elektronische handel', *Computerrecht* 2003, p. 344.

211 J.H.M. ter Haar, E.D.C. Neppelenbroek, 'Het elektronisch ondertekend document: wel, niet of zoiets als een akte', *Weekblad voor Privaatrecht, Notariaat en Registratie* 2006, p. 152 en 153.

212 Voor de argumenten waarom er voldaan is aan de eisen van schriftelijkheid en ondertekening zie paragraaf 4.11 respectievelijk 4.12.

Van Esch.[213] In het vervolg van dit onderzoek versta ik dan ook onder de elektronische onderhandse akte een akte welke is opgemaakt binnen de grenzen van art. 6:227a BW en art. 3:15a BW.

Overigens kan voor de (recente) toekomst wetsvoorstel 31358 van belang zijn voor de totstandkoming van de elektronische onderhandse akte.[214] In dit wetsvoorstel wordt de mogelijkheid van het opmaken van elektronische onderhandse aktes bevestigd door middel van toevoeging van art. 156a aan het Wetboek van Burgerlijke Rechtsvordering. Dit artikel stelt in lid 1 expliciet dat een onderhandse akte op andere wijze dan bij geschrift kan worden opgemaakt. Hiermee wordt de weg die reeds is ingeslagen met art. 6:227a BW bevestigd en verbreed.[215]

4.14.2 Twee opmerkelijk bewijsrechtelijke consequenties van de elektronische handtekening op de elektronische onderhandse akte

Dwingende bewijskracht (of toch niet)?

Zoals ik in paragraaf 4.7 reeds behandelde, kent het Nederlandse bewijsrecht in civiele procedures het beginsel van vrije bewijswaardering. Hierop wordt een aantal uitzonderingen gemaakt, zoals in het geval van aktes;[216] de rechter zal de inhoud van een akte voor waar moeten aannemen, zolang deze inhoud niet wordt betwist.[217] Voor elektronische onderhandse aktes geldt hetzelfde als voor "gewone" onderhandse aktes. Toch lijkt er mij iets vreemd aan de hand met de dwingende bewijskracht van de elektronische onderhandse akte. De rechter krijgt via art. 3:15a, lid 1 BW namelijk een discretionaire bevoegdheid om de betrouwbaarheid van de elektronische handtekening te onderzoeken.[218] Daarbij kan hij tot twee conclusies komen: de elektronische handtekening is niet betrouwbaar of de elektronische handtekening is wel betrouwbaar. Komt de rechter tot de conclusie dat de elektronische handtekening wel

---

213 Kemna in H. Franken, H.W.K. Kaspersen, A.H. de Wild (red.), *Recht en computer*, Deventer: Kluwer 2004, p. 212 en R.E. van Esch, 'De betrekkelijke waarde van de Wet elektronische handtekeningen voor de elektronische handel', *Computerrecht* 2003, p. 344.

214 *Kamerstukken II*, 2007-2008, 31358 (Wetsvoorstel 31358: 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 elektronische verkeer).

215 Ik gebruik hier het woord "verbreed", omdat art. 6:227a BW alleen betrekking heeft op overeenkomsten. Het nieuwe art. 156a Rv ziet daarentegen op het schriftelijkheidsvereiste ook niet zijnde overeenkomsten. Dit heeft tot gevolg dat bijvoorbeeld een ontvangstbevestiging in elektronische vorm en voorzien van elektronische handtekening de status van akte kan krijgen; iets wat met 6:227a BW niet mogelijk was daar een (elektronische) ontvangstbevestiging geen overeenkomst is.

216 Zie paragraaf 4.10.

217 Dit wordt ook wel de materiele bewijskracht van de akte genoemd.

218 *Kamerstukken I*, 2002-2003, 27743, nr. 35, p. 9

betrouwbaar is, dan heeft dat tot gevolg dat deze in combinatie met het geschrift kan worden beschouwd als onderhandse akte in de zin van art. 156, lid 1 j° lid 3 Rv, waardoor de inhoud van de akte dwingende bewijskracht heeft. Komt de rechter echter tot de conclusie dat de elektronische handtekening niet betrouwbaar is, dan heeft dat tot gevolg dat het geschrift niet kan worden beschouwd als onderhandse akte; de inhoud van de akte heeft dan geen dwingende bewijskracht.

De rechter heeft zich in beginsel te houden aan de dwingende bewijskracht van aktes. Toch lijkt dit beginsel doorbroken te worden door de toetsing op betrouwbaarheid van de methode van authentificatie door de rechter. De rechter is namelijk vrij om die methode op betrouwbaarheid te waarderen. Via het waarderen van betrouwbaarheid van de methode van authentificatie van de elektronische handtekening, kan de rechter invloed uitoefenen of hij het geschrift als akte kwalificeert en daarmee op de uitkomst of er sprake is van dwingende bewijskracht. Dit lijkt mij in strijd met de dwingende bewijskracht die aan de akte is toegekend door de wetgever. De wetgever heeft in het geval van de akte geen discretionaire bevoegdheid toegekend aan de rechter om de akte vrijelijk te waarderen. Via een omweg kan deze nu toch de dwingende bewijskracht van de elektronische onderhandse akte omzeilen.

Bovenstaande redenering heeft als gevolg dat de rechtszekerheid, die getracht wordt te verschaffen met de dwingende bewijskracht van aktes, niet wordt gediend door de elektronische handtekening die onder een elektronische onderhandse akte staat. De rechter heeft ruimte gekregen van de wetgever om een keuze te maken om wel of juist niet dwingende bewijskracht toe te kennen aan de elektronische onderhandse akte. Dat de rechtszekerheid hier niet mee wordt gediend is misschien wel een understatement, er is naar mijn mening namelijk helemaal geen sprake meer van enige rechtszekerheid in het geval van de elektronische onderhandse akte.

Vooralsnog ben ik van mening dat de elektronische onderhandse akte wel als akte in de zin van art. 156 lid 1 Rv beschouwd kan en mag worden. Dit ondanks de consequentie dat er voor de rechter mogelijkheden zijn om via de waardering van de methode van betrouwbaarheid van de elektronische handtekening in te grijpen in de dwingende bewijskracht. Ik vermoed dat de wetgever zich niet ten volle bewust was van deze consequentie toen zij art. 3:15a BW opnam in de wet.

Lijdelijkheid (of toch niet)?

Zoals ik paragraaf 4.10.3 reeds aangaf, heeft de rechter zich in beginsel te houden aan de dwingende bewijskracht van aktes. De rechter heeft in het geval van een “gewone” onderhandse akte ook geen actieve rol in het onderzoeken van de echtheid van het geschrift en de handtekening. De lijdelijkheid van de

rechter brengt met zich dat de rechter pas onderzoek doet als de partij tegen wie de handtekening wordt ingeroepen deze aanvecht. Zolang partijen niet betwisten dat een bewijsmiddel niet betrouwbaar is, zal de rechter geen onderzoek naar de rechtsfeiten mogen doen; met andere woorden: de rechter mag niet ambtshalve de rechtsfeiten aanvullen.[219] Ook uit art 159, lid 2 Rv kan opgemaakt worden dat een partij eerst actief moet handelen voordat de rechter gevolgen moet trekken uit dit optreden. Art 159, lid 2 Rv stelt namelijk dat indien een onderhandse akte waarvan de ondertekening door de partij, tegen welke zij dwingend bewijs zou leveren, stellig wordt ontkend, geen bewijs oplevert, zolang niet bewezen is van wie de ondertekening afkomstig is. De partij moet dus in het geval van art. 159, lid 2 Rv eerst stellig ontkennen voordat de rechter daar gevolgen aan moet verbinden.

De lijdelijkheid van de rechter wordt echter in art. 3:15a BW doorbroken doordat de rechter zelfstandig onderzoek moet doen naar de betrouwbaarheid van de methode van authentificatie van de elektronische handtekening.[220] Dit zelfstandig onderzoek is naar mijn mening niet in strijd met de rechterlijke lijdelijkheid, daar art. 24 Rv de lijdelijkheid van de rechter kan beperken. Dit blijkt uit de laatste woorden van art. 24 Rv "*tenzij uit de wet anders voortvloeit*." Ik meen dat hiervan sprake is in art. 3:15 BW. De rechter dient namelijk het recht toe te passen en bij de toepassing van het recht geeft art. 3:15 BW hem opdracht de methode van authentificatie op betrouwbaarheid te beoordelen. Naar de redenen waarom de rechter hier de bevoegdheid krijgt om zich toch met de rechtsfeiten te mogen bemoeien, zonder dat hiervoor de betrouwbaarheid door een van de partijen in twijfel moet worden getrokken, blijft het gissen. Dit wordt namelijk niet duidelijk uit de wetshistorie.

4.14.3 Dwingende bewijskracht van elektronische gegevens

De eisen die gesteld worden aan de elektronische onderhandse akte zijn (1) de schriftelijkheid van een overeenkomst, (2) ondertekening met een elektronische handtekening en (3) het hebben van een bewijsfunctie. Het antwoord op de vraag of data en code als elektronische onderhandse akte kan worden geclassificeerd, hangt voornamelijk af van het criterium 'geschrift'. Een geschrift wordt in de literatuur gedefinieerd als "iedere drager van verstaanbare leestekens die een gedachte-inhoud vertolken."[221] Deze vertolking van een gedachte-inhoud is dus essentieel voor de totstandkoming van een elektronische onderhandse akte. Code bevat, zoals reeds in paragraaf 2.3 is aangegeven per definitie geen gedachte-inhoud. Daarom kan code geen

---

219 De grondslag hiervoor is verwoord in art. 24 Rv.

220 *Kamerstukken I*, 2002-2003, 27743, nr. 35, p. 9.

221 T.R. Hidma, G.R. Rutgers, *Pitlo. Het Nederlands burgerlijk recht. Deel 7. Bewijs*, Deventer: Kluwer 2003, nr. 47 , p. 82. Zie ook subparagraaf 4.8.1.

dwingende bewijskracht worden toegekend, ook al zou deze ondertekend zijn met een elektronische handtekening. Data kan echter onder omstandigheden wel dwingende bewijskracht toekomen. Hiervoor geldt dat deze door mensen moet zijn gegenereerd en dan binnen de grenzen van art 6:227a BW. De data moet een overeenkomst bevatten, deze moet opgetekend zijn door een persoon en er is geen sprake van situaties als bedoeld in art. 6:227a, lid 3 en 4 BW.

4.15 De bewijsovereenkomst

4.15.1 Inleiding

Om de bewijswaarde van elektronische gegevens te verhogen kan gebruik worden gemaakt van bewijsovereenkomsten. Hierbij kan van de wettelijke bewijsregels afgeweken worden door in te grijpen in de toelating van elektronische gegevens, de waardering van deze gegevens of door de bewijslast om te keren.[222] Ik tracht in deze paragraaf om op een zo volledig en systematisch mogelijke wijze te onderzoeken welke mogelijkheden tot afwijking van de wettelijke bewijsregels bestaan. Hoewel binnen dit onderzoek voornamelijk wordt ingegaan op de technische eigenschappen die de bewijswaarde vergroten vind ik dat de bewijsovereenkomst, niet helemaal buiten beschouwing mag blijven, omdat de bewijsovereenkomst wel degelijk de bewijspositie van partijen kan beïnvloeden.

Het onderwerp bewijsovereenkomsten kan betrekking hebben op de inhoud van de bepalingen die zijn opgenomen in de bewijsovereenkomst en op de totstandkoming van de bewijsovereenkomst.

In de volgende paragraaf zal ik alleen nader ingaan op de vraag wat een bewijsovereenkomst is en de inhoud van de bewijsovereenkomst. De vraag naar de totstandkoming van de bewijsovereenkomst, welke een species is van het genus overeenkomsten, zal ik niet nader bespreken. Het leerstuk van de totstandkoming van overeenkomsten langs elektronische weg is een leerstuk dat op zichzelf staat. Ik zal daarom volstaan met het maken van enige kanttekeningen in subparagraaf 4.15.5 en het formuleren van problemen die kunnen spelen in het kader van totstandkoming van bewijsovereenkomsten via elektronische weg.

---

[222] De wet geeft in art. 153 Rv ruimte voor bewijsovereenkomsten. Eerder is de mogelijkheid tot het afsluiten van bewijsovereenkomsten bevestigd in Hof Amsterdam 28 juni 1920, NJ 1921, 864. Zie ook: F.G. Scheltema, H.J. Scheltema, *Nederlandsch burgerlijk bewijsrecht*, Zwolle: W.E.J. Tjeenk Willink 1940, p. 76-77.

4.15.2 Definitie bewijsovereenkomst

De Nederlandse recht kent niet een expliciet in de wet opgenomen definitie van de bewijsovereenkomst. De enige bepaling die de wet kent met betrekking tot de bewijsovereenkomst is art. 153 Rv: *"Overeenkomsten waarbij van het wettelijke bewijsrecht wordt afgeweken, blijven buiten toepassing, wanneer zij betrekking hebben op het bewijs van feiten waaraan het recht gevolgen verbindt, die niet ter vrije bepaling van partijen staan, zulks onverminderd de gronden waarop zij krachtens het Burgerlijk Wetboek buiten toepassing blijven."*[223]

De bewijsovereenkomst wordt hier kortweg gedefinieerd als een overeenkomst "waarbij van het wettelijke bewijsrecht wordt afgeweken". Enkele auteurs, waaronder Hidma en Rutgers houden een iets andere definitie aan, welke zij ontlenen aan de Memorie van Toelichting: "De bewijsovereenkomst is de contractuele regeling, waarbij partijen met het oog op een mogelijk proces afspraken maken omtrent hun bewijspositie, met dien verstande dat bijvoorbeeld bepaalde bewijsmiddelen worden uitgesloten, dwingende bewijskracht aan een bepaald bewijsmiddel wordt toegekend of een afwijkende verdeling van de bewijslast wordt toegekend of een afwijkende verdeling van de bewijslast wordt overeengekomen, al dan niet met beperking of uitsluiting van tegenbewijs."[224] Wieten stelt dat de bewijsovereenkomst is: "een van het wettelijk bewijsrecht afwijkende overeenkomst, die wordt gesloten met het oog op een eventueel later tussen partijen te voeren geding."[225] Ik sluit me aan bij de definitie van Wieten, omdat deze expliciet stelt dat er met de overeenkomst wordt afgeweken van het wettelijke bewijsrecht. De tweede reden is dat de definitie van Hidma en Rutgers ook ingaat op de verschillende methoden die bestaan om van het wettelijke bewijsrecht af te wijken. Deze hoeven naar mijn mening niet expliciet te worden genoemd in een definitie.

4.15.3 De inhoud van de bewijsovereenkomst

Een bewijsovereenkomst kan een instrument zijn waarmee de bewijswaarde kan worden vergroot van elektronische gegevens door van het wettelijke bewijsrecht af te wijken. Zoals ook in de definitie van Hidma en Rutgers is aangegeven kan hierbij gedacht worden aan het uitsluiten van bewijsmiddelen, het toekennen van dwingende bewijskracht aan een bepaald bewijsmiddel of

---

223 Art. 153 Rv.

224 Pitlo, Hidma, T.R., Rutgers, G.R., *Het Nederlands burgerlijk recht: Bewijs, deel 7*, achtste druk, Kluwer Deventer 2004, p. 71 en 72. Zie ook: G.R. Rutgers (red.), *Parlementaire geschiedenis van het bewijsrecht in civiele zaken*, Deventer: Kluwer 1988, p. 110.

225 H.L.G. Wieten, *Bewijs, Studiereeks burgerlijk procesrecht*, Kluwer: Deventer 2004, p. 18.

het maken van afspraken omtrent de bewijslast. Het is echter van belang te onderzoeken welke grenzen het Nederlandse bewijsrecht stelt aan de afspraken die partijen kunnen en mogen overeenkomen. De grenzen van de bewijsovereenkomst worden gevormd door de bepalingen in art 153 Rv, namelijk "in het geval dat zij betrekking hebben op het bewijs van feiten waaraan het recht gevolgen verbindt die niet ter vrije bepaling van partijen staan" en "in het geval van gronden waarop zij krachtens het Burgerlijk Wetboek buiten toepassing blijven." Op deze laatste zal ik ingaan in paragraaf 4.15.4.

In de vorige paragraaf is bij het behandelen van de definitie van Hidma en Rutgers een aantal manieren belicht hoe de bewijsovereenkomst de bewijspositie kan wijzigen van het wettelijke bewijsrecht. Hier worden genoemd: bewijsuitsluiting, het toekennen van dwingende bewijskracht, een afwijkende verdeling van de bewijslast overeenkomen en dit alles al of niet met uitsluiting van tegenbewijs.

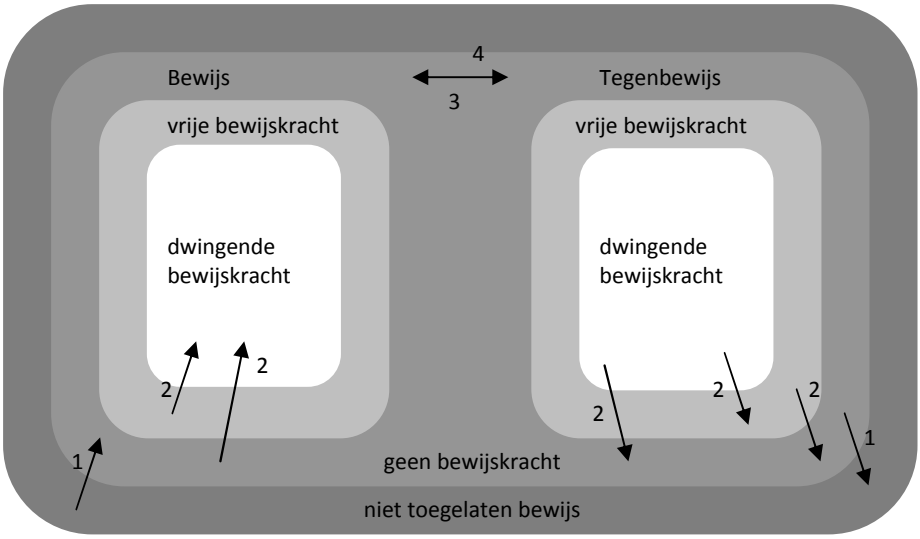
Het wettelijke bewijsrecht geeft regels omtrent (1) toelating van bewijs (art. 152, lid 1 Rv), (2) de waardering van bewijs (art. 152, lid 2 Rv) en (3) de verdeling van de bewijslast (art. 150 Rv). Daarbij kan er sprake zijn van tegenbewijs. Dit onderscheid wordt ook gemaakt door Scheltema die de contractuele regels die afwijken van bovenstaande wettelijke regels van bewijsrecht aanduidt als respectievelijk de bewijsmiddelenovereenkomst (ad 1), de bewijskrachtovereenkomst (ad 2) en de bewijslastovereenkomst (ad 3) en de overeenkomst waarbij tegenbewijs wordt uitgesloten (ad 4).[226] De toelating en de bewijswaardering zijn opgenomen in onderstaand schema.

Ad 1: Bewijsmiddelenovereenkomst
De hoofdregel (art. 152, lid 1 Rv) is dat bewijs kan worden geleverd door alle middelen, tenzij de wet anders bepaalt. Om de eigen bewijspositie te versterken lijkt het in eerste instantie een mogelijkheid te regelen dat bewijs dat wettelijk niet toegelaten wordt, toch als bewijs kan dienen. Een bepaling die deze strekking heeft blijft echter buiten toepassing, omdat deze in strijd is met datgene wat bepaald is in art 153 Rv, namelijk dat een dergelijke regeling niet ter vrije bepaling van partijen staat.[227] Daarvoor is juist de wet voorzien van een dwingendrechtelijke bepaling. Omgekeerd staat er naar mijn mening geen rechtsregel in de weg om te bepalen dat bewijs dat wettelijk wel toegelaten wordt tot de rechtszaak, wordt uitgesloten van toelating voor zover art 153 Rv dit toe laat. De grenzen "in het geval dat zij betrekking hebben op het bewijs van feiten waaraan het recht gevolgen verbindt die niet ter vrije

[226] F.G. Scheltema, H.J. Scheltema, *Nederlandsch burgerlijk bewijsrecht*, Zwolle: W.E.J. Tjeenk Willink 1934-1940, p. 97 en 102.

[227] B.T.M. van der Wiel, "De bewijsovereenkomst", *Weekblad voor Privaatrecht, Notariaat en Registratie 2002-2*, p.223.

bepaling van partijen staan" en "in het geval van gronden waarop zij krachtens het Burgerlijk Wetboek buiten toepassing blijven" zijn hierin doorslaggevend. De volgende paragraaf zal verder ingaan op deze grenzen.



Afbeelding 4.3: :Schematisch overzicht van de afwijkingen die partijen van het wettelijke bewijsrecht kunnen maken (toelichting hieronder).

Ad 2: Bewijskrachtovereenkomst

Het is mogelijk om per overeenkomst te bepalen dat eenmaal toegelaten bewijs dat onderhevig is aan de bewijswaardering door de rechter, dwingende bewijskracht wordt toegekend. Het omgekeerde kan ook het geval zijn: de dwingende bewijskracht wordt ontnomen door vrije bewijskracht toe te kennen aan het bewijsmiddel of door te bepalen dat het bewijsmiddel geheel geen bewijskracht heeft.[228] De vraag is echter in hoeverre bewijsmateriaal waarvan vaststaat dat ermee is geknoeid door een van beide partijen nog dwingende bewijskracht kan hebben in het geval dat bepaald is dat aan dat bewijsmiddel dwingende bewijskracht moet worden toegekend. Het zou mogelijk kunnen zijn dat een contractuele bepaling als deze in strijd is met de tweede uitzondering die geformuleerd is in art 153 Rv, namelijk dat er sprake is van gronden waarop zij krachtens het Burgerlijk Wetboek buiten toepassing blijft. De grond die hiervoor in het Burgerlijk Wetboek gevonden kan worden is het in strijd zijn met de goede trouw.[229]

[228] Dit in tegenstelling tot het Duitse recht, waarbij het niet toegestaan is om bewijskrachtovereenkomsten te sluiten. Zie hiervoor paragraaf 5.10.3.

[229] Vergelijk HR 7 december 1934, *NJ* 1935, p. 443.

Naast het vergroten van de bewijswaarde van het bewijs, kan het verbeteren van de eigen bewijspositie ook door het verkleinen van de bewijskracht van het tegenbewijs. Dit kan op twee manieren. De eerste mogelijkheid is dat er wordt afgeweken van dwingende bewijskracht door de dwingende bewijskracht te ontnemen en het bewijsmiddel slechts vrije bewijskracht toe te kennen en de tweede mogelijkheid is dat er bepaald wordt dat het desbetreffende bewijsmiddel helemaal geen bewijskracht toe zal komen. Ook hier worden de grenzen weer bepaald door art 153 Rv.

Ad 3: Bewijslastovereenkomst
De bewijslastovereenkomst is een overeenkomst die de bewijslast van partijen regelt. De regels van bewijslastverdeling kennen niet het bewijs als object, maar regelen de bewijslast van partijen. Hoe of door welke middelen de feiten bewezen dienen te worden wordt niet bepaald in de bewijslastovereenkomst; enkel wordt bepaald wie welke feiten dient te bewijzen.

Ad 4: Tegenbewijs
In een bewijsovereenkomst kunnen bepalingen opgenomen zijn die betrekking hebben op het tegenbewijs. De eigen bewijspositie wordt dan versterkt of verzwakt door de bewijstoelating, de bewijskracht . Om de eigen bewijspositie te versterken zou bepaald kunnen worden dat bepaald tegenbewijs niet toelaatbaar is als bewijsmiddel of dat bepaald tegenbewijs geen bewijskracht toe komt. Gezien het feit dat de bepalingen betrekking hebben op het bewijs zelf en niet op de bewijslast, zullen alleen de bewijstoelating en de bewijskracht geregeld kunnen worden. Overigens moet bij het uitsluiten van tegenbewijs art. 7A:900, lid 3 BW in acht genomen worden. Bij het uitsluiten van tegenbewijs in een bewijsovereenkomst staat deze bewijsovereenkomst gelijk aan een vaststellingsovereenkomst. De ratio is dat als wordt bepaald dat tegenbewijs wordt uitgesloten, er eigenlijk geen sprake meer is van enkel een bewijsovereenkomst, maar van een overeenkomst waar slechts de feiten worden vastgesteld. In dat geval gelden van rechtswege de wettelijke regels die gesteld worden aan de vaststellingsovereenkomst.[230]

4.15.4 Beperkingen aan de bewijsovereenkomst

Hoewel bewijsovereenkomsten in grote mate van vrijheid tussen partijen kunnen worden afgesloten en een rechter gebonden is aan de rechtsgevolgen die de bewijsovereenkomst schept, zijn er wel degelijk grenzen aan de bewijsovereenkomst.

[230] Pitlo, Hidma, T.R., Rutgers, G.R., *Het Nederlands burgerlijk recht: Bewijs, deel 7*, achtste druk, Kluwer Deventer 2004, p. 75.

De eerste uitzondering ziet op het bewijs van feiten waaraan het recht gevolgen verbindt die niet ter vrije bepaling van partijen staan. Hierbij moet gedacht worden aan bepalingen van dwingend recht. De bepalingen die onder dwingend recht vallen moeten overigens niet gelijk gesteld worden met bepalingen waarbij slechts een wettelijk bepaald bewijsmiddel gehanteerd kan worden om de feiten aan te tonen.[231]

In de wet zijn vele bepalingen opgenomen waarvan niet bij overeenkomst kan worden afgeweken. De wetgever heeft het nodig geacht dat bepaalde partijen (economisch zwakkere partijen, derden, enz.) beschermd dienen te worden door de wet. Afwijking van de dwingendrechtelijke bepalingen is daarom niet toegestaan en is nietig of vernietigbaar.[232]

De tweede beperking aan de vrijheid van partijen om van het wettelijke bewijsrecht af te wijken, is vastgelegd in de woorden "de gronden waarop zij krachtens het Burgerlijke Wetboek buiten toepassing blijven". Hierbij wordt volgens de Memorie van Toelichting gedoeld op de bewijsovereenkomst die in strijd met de goede trouw is.[233] Te denken valt aan het toekennen van dwingende bewijskracht aan een middel, waarbij ieder tegenbewijs wordt uitgesloten en vervolgens blijkt dat met het middel dat dwingende bewijskracht wordt toegekend, vervalst is.

4.15.5 Probleemverkenning voor de totstandkoming van de bewijsovereenkomst

De bewijsovereenkomst is zoals de naam al aangeeft, geen regeling die op grond van de wet geldt, maar een regeling die tussen partijen wordt overeengekomen. Dit brengt een aantal vraagstukken met zich mee van een andere aard dan het bewijsrecht, namelijk vraagstukken van vermogensrechtelijke aard.

In de eerste plaats is er de totstandkoming van de bewijsovereenkomst. Een bewijsovereenkomst kan als raamovereenkomst worden afgesloten.[234] Dit kan bijvoorbeeld gedaan worden tussen partijen die regelmatig met elkaar handel drijven via elektronische weg. Meestal zal de bewijsovereenkomst de vorm hebben van bepalingen die de bewijsrechtelijke positie van partijen regelen en die zijn opgenomen in algemene voorwaarden. De vraag is echter of (semi-

---

231 Zie daarvoor ook: toelating van bewijs (paragraaf 3.5).

232 Zie art. 3:40, lid 2 BW.

233 G.R. Rutgers (red.), *Parlementaire geschiedenis van het bewijsrecht in civiele zaken*, Deventer: Kluwer 1988, p. 110.

234 R.E. van Esch, *Electronic Data Interchange (EDI) en het vermogensrecht* (diss. Nijmegen), W.E.J. Tjeenk Willink, Deventer: 1999, p. 50 en 51.

)autonome computerprogramma's die zich over netwerken verplaatsen voor partijen overeenkomsten aan kunnen gaan en of gebruikers gebonden zijn aan die overeenkomst inclusief de algemene voorwaarden. Zeker als er geen sprake is van een raamovereenkomst, maar als de bewijsbepalingen zijn opgenomen in de algemene voorwaarden, is het niet duidelijk of de bepalingen ook tussen partijen komen te gelden.[235]

4.16 Samenvatting en conclusie

Het Nederlandse bewijsrecht maakt deel uit van het Nederlandse civiele procesrecht. Een belangrijk uitgangspunt hiervan is de lijdelijkheid van de rechter; partijen bepalen de omvang van hun geschil en de rechter is niet bevoegd om de rechtsfeiten aan te vullen, maar enkel de rechtsgronden. 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 betrouwbaarheid van de methode van authentificatie van de elektronische handtekening (zie verderop in deze paragraaf).

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 bijna geen criteria te vinden. De oorzaak hiervan kan gelegen zijn in de beperkte motiveringsplicht die de rechter heeft als het het bewijsoordeel betreft. 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

[235] Voor meer informatie hierover volsta ik hier met een verwijzing naar het proefschrift dat op het moment van afronding van dit proefschrift in voorbereiding is bij mijn collega Martine Boonk.

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 schriftelijkheideis van art. 6:82 BW als een ingebrekestelling per e-mail wordt gedaan.[236]

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 authentificatie moet voldoen om voldoende betrouwbaar te zijn. Is eenmaal vastgesteld dat de methode van authentificatie 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 ambthalve de methode van authentificatie 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 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

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

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.

5 Elektronische gegevens als bewijsmiddel in het Duitse civiele recht

5.1 Inleiding

Zoals blijkt uit het vorige hoofdstuk zijn er in de Nederlandse jurispudentie geen concrete aanwijzingen te vinden hoe elektronische gegevens als bewijsmiddel worden gewaardeerd. De vraag is of het Duitse jurisprudentie meer aanknopingspunten biedt aangezien het Duitse recht op een aantal punten verschilt van het Nederlandse recht. Dit verschil komt in de eerste plaats tot uitting in het gesloten systeem van toelating van bewijsmiddelen. Niet ieder bewijsmiddel wordt toegelaten, maar alleen de bewijsmiddelen die te kwalificeren zijn als één van de vijf door de wet erkende bewijsmiddelen. In de tweede plaats heeft de Duitse wetgever het begrip *elektronisches Dokument* geïntroduceerd in de wetgeving, waardoor er meer duideljkheid zou kunnen bestaan over de bewijskracht van deze *elektronische Dokumenten*. Verder lijkt de Duitse rechter een zwaardere motiveringsplicht van zijn bewijsbeslissing te hebben dan de Nederlandse rechter. Daarom zou het Duitse civiele bewijsrecht wel eens een geschikter stelsel kunnen zijn om in het kader van dit onderzoek de betrouwbaarheidscriteria van elektronische gegevens te onderzoeken.

De tweede paragraaf gaat in op de plaats van het bewijsrecht binnen het Duitse recht. Daarna wordt in de derde paragraaf nader onderzocht welke verhouding er bestaat tussen de autonomie van partijen en de lijdelijkheid van de rechter. In paragraaf vier ga ik daarna verder in op de toelating van het bewijs, waarbij zal blijken dat er een onderscheid bestaat tussen het zogenaamde *Strengbeweis* en het *Freibeweis*. Tevens zal daarbij ingegaan worden op de gevolgen die dit onderscheid met zich meebrengt. In de vijfde paragraaf wordt vervolgens ingegaan op de vijf wettelijke bewijsmiddelen en de toelating van elektronische bewijsmiddelen. Nadat de bewijsmiddelen de toets van toelating hebben doorstaan, zal de rechter een betrouwbaarheidsoordeel moeten geven over de bewijsmiddelen in de fase van bewijswaardering. Dit is waar paragraaf zes nader aandacht aan besteedt. Hoewel ook in het Duitse recht in beginsel de vrije bewijswaardering geldt, waarbij de rechter persoonlijk moet zijn overtuigd van de waar- of onwaarheid van de feiten, bestaan er in bepaalde bij wet omschreven gevallen uitzonderingen op deze overtuiging; de bewijslast is dan dwingend of kent juist een minder hoge drempel. Op het bewijsmiddel met

dwingende bewijskracht gaat paragraaf zeven nader in. De *Urkunde* is een bewijsmiddel welke onder omstandigheden dwingende bewijskracht krijgt toegekend. Ook bestaat er in het Duitse recht het zogenaamde *elektronisches Dokument* waarop onder omstandigheden dwingende bewijskracht van toepassing is. Vervolgens ga ik in de achtste paragraaf in op de rol die de bewijsovereenkomst kan spelen bij het verbeteren dan wel regelen van de bewijspositie om ten slotte in paragraaf negen te komen met een aantal criteria waaraan elektronische bewijsmiddelen in het Duitse recht aan moeten voldoen om als voldoende betrouwbaar te kunnen worden beoordeeld.

5.2 Plaats van het civiele bewijsrecht binnen het Duitse recht

Het civiele bewijsrecht in Duitsland is geregeld in de *Zivilprozessordnung* (*ZPO*) en maakt deel uit van het Duitse civiele recht. Hoewel de meeste bepalingen over bewijsrecht zijn opgenomen in boek twee, hoofdstuk een, titel vijf tot en met titel twaalf, is een aantal bepalingen opgenomen in andere delen van de *ZPO*. Zo regelt § 286 *ZPO* de bewijswaardering door de rechter en is de regeling over partijautonomie binnen het proces opgenomen in het algemene deel van de procesrechtelijke regels, zoals *§ 138, lid 3 ZPO*.[237]

De *ZPO* bevat, net als het Nederlandse Wetboek van Burgerlijke Rechtsvordering, regels voor het gehele procesrecht, het bewijsrecht inbegrepen. Hiermee onderscheiden de Nederlandse en Duitse regelingen zich van de Amerikaanse *Federal Rules of Evidence* en de *Federal Rule of Civil Procedure*, waarbij een scheiding is aangebracht tussen het procesrecht en het bewijsrecht.[238]

5.3 Lijdelijkheid van de rechter

5.3.1 De hoofdregel / de leer van de *Prozessmaximen*

De rol van de civiele rechter in Duitsland heeft in de literatuur nadere uitwerking gekregen in de leer van *Prozessmaximen*.[239] Onderscheiden worden de *Prozessmaximen* die de aanvang en beëindiging van het proces inhouden, ook wel het *Dispositionsmaxime*/*Offizialmaxime* en de *Prozessmaximen* die het bewijsaanbod omvatten, ook wel het *Beibringungsmaxime*/*Inquisitionsmaxime*.

---

237 Hoewel ik geen verklaring heb kunnen vinden voor de plaats van deze artikelen in de ZPO, vermoed ik dat dit te maken heeft met het onderwerp waarop § 286 *ZPO en* § 138, lid 3 ZPO betrekking hebben.

238 De *FRE* stelt enkel regels over bewijsmiddelen en bewijskwesties en de *FRCP* stelt de regels met betrekking tot het civiele procesrecht.

239 R. Oberheim, *Zivilprozessrecht für Refendare*, Neuwied: Werner Verlag 2007, p. 14.

De lijdelijkheid van de Duitse rechter blijkt uit de keuze voor het *Dispositionsmaxime* en het *Beibringungsmaxime.*

Het D*ispositionsmaxime* houdt in dat partijen autonoom zijn in het bepalen of en wanneer zij een proces aanvangen of beëindigen. Partijen zijn eigen baas in hun burgerlijke verhoudingen en zij mogen zelf bepalen of zij een proces beginnen als zij hun recht willen halen. Niemand kan de partijen ertoe dwingen om recht te halen door hen een proces op te dringen. Tegenover het *Dispositionsmaxime* staat het *Offizialmaxime*: hierbij wordt het wel of niet starten en beëindigen van een proces door de staat bepaald; vertegenwoordigers van de bestuurlijke macht of de rechterlijke macht bepalen of er een proces tussen partijen zal plaatsvinden. Partijen hebben dan niet langer de vrijheid om te procederen als zij vinden dat hun rechten zijn aangetast. Zij kunnen dan een proces opgedrongen krijgen terwijl zij hier niet om vragen of juist geen proces beginnen, terwijl hier bij partijen wel behoefte aan bestaat. Uitgangspunt in het burgerlijk proces is het *Dispositionsmaxime*. De ideeën van het *Dispositionsmaxime* sluiten aan bij het burgerlijke procesrecht, waarbij de verhoudingen tussen burgers onderling geregeld worden. Toch kent het Duitse recht geen hard *Dispositionsmaxime*; er zijn namelijk uitzonderingen en dan vooral als het gevallen van familierechtelijke aard betreft of gevallen waar rechten van derden in het geding komen.[240] In die gevallen kan een proces aan partijen worden opgelegd.[241]

Niet alleen de beslissing voor de aanvang en beëindiging van het proces ligt in handen van de procespartijen, maar ook tijdens het proces is het enkel aan partijen om feiten en bewijs aan te voeren. Dit principe wordt het *Beibringungsmaxime* genoemd. Slechts de partijen mogen feiten en bewijsmiddelen aanvoeren. Feiten die niet door partijen gesteld zijn en bewijs dat niet door partijen aangevoerd is, mogen niet gebruikt worden in het oordeel en de beslissing. Evenals in Nederland mag de rechter niet ambtshalve de feiten aanvullen. Zelfs als partijen feiten aanvoeren die anders zijn dan de werkelijkheid, maar partijen het met elkaar eens zijn over de onware feiten, dient de rechter deze feiten als waar aan te nemen, zelfs al weet deze dat de feiten geen reflectie zijn van de waarheid. Tegenover het *Beibringungsmaxime* staat het *Inquisitionsmaxime*. Dit houdt in dat de rechter zich mag mengen in de juistheid van de feiten en dat de rechter zelfstandig bewijs mag gaan zoeken, zelfs al zijn deze niet ingebracht door partijen. In het Duitse recht geldt het *Beibringungsmaxime*.[242] De opvatting dat partijen zelf de omvang van hun proces bepalen sluit hier aan bij de vrijheid die partijen hebben in hun

---

240 R. Oberheim, *Zivilprozessrecht für Refendare*, Neuwied: Werner Verlag 2007, p. 14.

241 R. Oberheim, *Zivilprozessrecht für Refendare*, Neuwied: Werner Verlag 2007, p. 14, BGH NJW 1951, 517.

242 Zie hiervoor ook: J.E. Bosch-Boesjes, *Lijdelijkheid in geding* (diss. Groningen), Kluwer, Deventer: 1991, p. 10 t/m 13.

onderlinge burgerlijke verhoudingen. De rechter dient zich te schikken naar de door partijen gestelde feiten en het door partijen ingebrachte bewijs.

Voor het inbrengen van bewijsmiddelen, daaronder ook begrepen elektronische bewijsmiddelen, wil dit zeggen dat als partijen zich niet beroepen op bepaalde feiten die van belang kunnen zijn voor de beslissing van de rechter en/of als partijen geen bewijs aandragen, de rechter dit bewijs niet zal meenemen in zijn beslissing. Ook als de rechter weet dat feiten die niet gesteld zijn, maar die wel bestaan en bewijs dat niet is aangevoerd, maar wel bestaat, van invloed kunnen zijn op zijn beslissing, mag de rechter deze niet inbrengen of aanvoeren.

5.3.2 Uitzonderingen op de hoofdregel

Op de rechterlijke lijdelijkheid bestaan twee soorten uitzonderingen, namelijk specifieke wettelijke uitzonderingen welke de rechter de bevoegdheid geven om in te grijpen in de voortgang van het proces en de bewijsvermoedens die ingrijpen in de door partijen aangevoerde feiten. Deze uitzonderingen zullen in deze paragraaf verder besproken worden.

In de eerste plaats is er een aantal specifieke wettelijke uitzonderingen. Het gaat te ver om deze allemaal te behandelen, maar ik zal volstaan met een aantal voorbeelden. Zoals in paragraaf 5.3.1 al is aangegeven, kan de rechter een actieve rol aannemen als het gevallen van familierechtelijke aard betreft, gevallen waar rechten van derden in het geding komen en gevallen waar de wet de rechter ambtshalve de bevoegdheid verleend om een actieve niet-lijdende rol aan te nemen. Bij deze laatste kan bijvoorbeeld gedacht worden aan een uitspraak over de vergoeding van proceskosten.[243] De tweede uitzondering bestaat uit de *Beweisvermutungen* of, vrij vertaald, bewijsvermoedens. Ondanks dat verschillende wettelijke bepalingen gebruik maken van *Beweisvermutungen*, wordt in de wet niet nader gedefinieerd wat het onder het begrip *Beweisvermutungen* moet worden verstaan. Uit de literatuur wordt evenwel duidelijk dat een *Beweisvermutung* een wettelijke of niet-wettelijke regel is die de bewerings- en de bewijslast in specifieke gevallen omkeert.[244] *Beweisvermutungen* hoeven niet te worden bewezen, echter tegenbewijs staat ingevolge § 292 *ZPO* open: *"Stellt das Gesetz für das Vorhandensein einer Tatsache eine Vermutung auf, so ist der Beweis des Gegenteils zulässig, sofern nicht das Gesetz ein anderes vorschreibt (…)."*

[243] § 308 II ZPO: "Über die Verpflichtung, die Prozesskosten zu tragen, hat das Gericht auch ohne Antrag zu erkennen."

[244] K. Schellhammer, *Zivilprozess, Gesetz – Praxis – Fälle*, Heidelberg: C.F. Müller Verlag, 2004, p. 182, nr. 395; O. Jauernig, *Zivilprozessrecht*, München: Verlag C.H. Beck, 2007, p. 167.

Ingevolge § 292 *ZPO* zijn de *Vermutungen* weerlegbaar, tenzij de wet dit uitdrukkelijk uitsluit.

Het Duitse recht maakt in de literatuur een onderscheid in *gesetzliche* en *ungesetzliche Vermutungen* (hetzelfde onderscheid wordt gemaakt in het Nederlandse recht waarbij de *gesetzliche Vermutungen* worden vertaald als wettelijke vermoedens en de *ungesetzliche Vermutungen* als feitelijke vermoedens[245]).[246]

De *gesetzliche Vermutungen* worden verdeeld in *Tatsachenvermutungen* en *Rechtsvermutungen*,[247] oftewel vermoedens van feiten en vermoedens van rechten. *Tatsachenvermutungen* zijn rechtsregels die stellen dat er sprake is van bepaalde rechtsfeiten als zich een bepaalde feitelijke toestand voordoet.[248] Bij *Tatsachenvermutungen* behoeven de feiten waar het vermoeden op toeziet geen bewijs. De bewijslast wordt echter niet omgedraaid. De wederpartij tegen wie de *Beweisvermutung* wordt ingeroepen hoeft alleen twijfel te zaaien bij het gerecht en niet volledig het tegendeel te bewijzen. Ook hoeft degene ten wiens gunste de *Beweisvermutung* dient, zich niet expliciet te beroepen op deze rechtsregel.[249] *Rechtsvermutungen* zijn rechtsregels welke stellen dat een partij bepaalde rechten heeft. Deze regels vinden hun oorsprong niet in een feitelijke toestand, maar enkel in het feit dat de wet een vermoeden van het bestaan van rechten stelt. De stellende partij hoeft in het geval van een *Rechtsvermutung* niet zijn gelijk aan te tonen. De wederpartij die zich daarentegen beroept op het niet bestaan van die rechten, dient aan te tonen dat de stellende partij deze rechten inderdaad niet heeft, aangezien hij het vermoeden tegen zich heeft. Een Rechtsvermutung breng dus een omkering van de bewijslast mee.[250]

De *ungesetzliche Vermutungen* zijn door de rechterlijke macht ontwikkeld om in te kunnen grijpen in gevallen waarbij de wettelijke bewijslastverdeling leidt tot ongerechtvaardigde toewijzing van de aansprakelijkheid.[251] In hoeverre dit geeigend is, is niet geheel duidelijk De *ungesetzliche Vermutungen* betreffen de aansprakelijkheid van adviseurs en de aansprakelijkheid van artsen. Aangezien de wet in deze gevallen geen regels geeft, kan er niet meer gesproken worden van uitleg van de wet of rechtsontwikkeling. Door in deze gevallen in te grijpen

---

245 K. Schellhammer, *Zivilprozess, Gesetz – Praxis – Fälle*, Heidelberg: C.F. Müller Verlag, 2004, p. 182-186, nr. 395-404.

246 O. Jauernig, *Zivilprozessrecht*, München: Verlag C.H. Beck, 2007, p.167.

247 L. Rosenberg, K.H. Schwab, P. Gottwald, *Zivilprozessrecht*, München, C.H. Beck 1993, p. 763 en 764.

248 R. Oberheim, *Zivilprozessrecht für Refendare*, Neuwied: Werner Verlag 2007, p. 379.

249 Wat mij logisch voorkomt daar de rechter van ambtswege het recht toepast.

250 Dit in tegenstelling tot het Nederlandse recht, waar geen bewijslastomkering plaatsvindt. Zie ook: K. Schellhammer, *Zivilprozess, Gesetz – Praxis – Fälle*, Heidelberg: C.F. Müller Verlag, 2004, p. 182, nr. 395.

251 O. Jauernig, *Zivilprozessrecht*, München: Verlag C.H. Beck, 2007, p. 167.

in de bewijslast, veranderen de rechters het materiële recht en handelen in strijd met *§ 20 III Grundgesetz*.

In het kader van dit onderzoek spelen bewijsvermoedens een rol bij de toets betreffende de echtheid van verschillende soorten *Urkunden*. De *Urkunde* zal besproken worden in paragraaf 5.5.2.

5.4 Toelating van bewijs

Het Duitse bewijsrecht kent van oorsprong een gesloten stelsel van bewijsmiddelen. Dit betekent dat het een aantal limitatief in de wet omschreven bewijsmiddelen hanteert, waarmee feiten bewezen kunnen worden. Dit gesloten stelsel van bewijsmiddelen wordt ook wel *Strengbeweis* genoemd. Naast het *Strengbeweis* heeft zich een tweede vorm van bewijstoelating ontwikkeld. Dit is het zogenaamde *Freibeweis* en het kenmerkt zich doordat het bij het toelaten van bewijsmiddelen niet gebonden is aan de wettelijke bewijsregels, maar de rechter zich in bepaalde gevallen van ieder bewijsmiddel mag bedienen.

De wettige bewijsmiddelen zoals de Duitse wet deze kent onder het *Strengbeweis* zijn:
- *Augenscheinsbeweis* (waarneming door het gerecht)
- *Zeugenbeweis* (getuigenbewijs);
- *Sachverständigebeweis* (deskundigenbewijs)
- *Urkundenbeweis* (bewijs door middel van akten)
- *Parteivernehmung* (getuigenis door partijen)

Als een bewijsmiddel niet kan worden gekwalificeerd als een van bovenstaande genoemde bewijsmiddelen dan wordt het niet toegelaten. Daarnaast is erkend dat sommige bewijsmiddelen, die wel als wettig bewijsmiddel te kwalificeren zijn, niet worden toegelaten op andere gronden. Hierbij kan gedacht worden aan bij overeenkomst uitgesloten bewijs.[252] De grond voor uitsluiting van bewijsmiddelen, om redenen anders dan het niet zijn van wettig bewijsmiddel, is meestal gelegen in een oordeel dat bij de verkrijging van het bewijs inbreuk is gemaakt op de door de grondwet beschermde persoonlijke levenssfeer, procedurele vormen zijn verzuimd of dat een andere ernstige schending van het recht heeft plaatsgevonden met het toelaten van een bepaald bewijsmiddel. Of er sprake is van het niet toelaten van bewijs op deze gronden,

[252] Zie paragraaf 5.10.

moet van geval tot geval worden beoordeeld en voor iedere regel afzonderlijk worden bepaald.[253]

Hoewel er vijf wettelijke bewijsmiddelen zijn, stelt de wet geen van de bewijsmiddelen boven de andere bewijsmiddelen; alle bewijsmiddelen zijn gelijkwaardig en het is aan de rechter om de bewijsmiddelen te selecteren en te waarderen op betrouwbaarheid.[254] Zoals in paragraaf 5.6 zal blijken is de rechter hierin vrij, maar heeft deze wel een motiveringsplicht. In paragraaf 5.5 zal ik eerst de vijf wettelijke bewijsmiddelen nader onderzoeken, waarbij de nadruk zal liggen op de bewijsmiddelen die van betekenis zijn voor de bewijstoelating van elektronische bewijsmiddelen.

Het *Freibeweis* is, in tegenstelling tot het *Strengbeweis*, een vorm van bewijs die niet geregeld is in de *ZPO* of in een andere wet. In eerste instantie was *Freibeweis* een begrip in het strafrecht, maar dit begrip heeft zijn weg gevonden naar het civiele recht.[255] Hoewel het *Freibeweis* nergens expliciet in de wet wordt genoemd en door een enkeling deze vorm van bewijs wordt beschouwd als zijnde in strijd met de wet, is het *Freibeweis* algemeen geaccepteerd en ook het *Bundesgerichtshof* heeft deze vorm van bewijs erkend.[256] In tegenstelling tot het *Strengbeweis* is een rechter bij het hanteren van het *Freibeweis* niet gebonden aan de wettelijke bewijsmiddelen en ook niet aan de formele bewijsprocedures. Het *Freibeweis* wordt enkel gehanteerd 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. Voor het vaststellen van feiten waarover partijen het oneens zijn en die de kern van de zaak betreffen geldt niet het *Freibeweis*, maar het *Strengbeweis*. Het *Freibeweis* heeft dus een ondergeschikte rol in het Duitse civiele recht.

Het *Strengbeweis* en het *Freibeweis* moeten beide leiden tot de volle overtuiging van het gerecht dat de bewijsmiddelen de waarheid van de feiten aantonen. Het verschil kan echter aan de hand van de gevolgen duidelijk worden gemaakt. Stel dat een rechter zich bedient van *Freibeweis* om bepaalde feiten aan te tonen, dan kan ieder bewijsmiddel ingebracht worden om deze feiten aan te tonen. Als de rechter er echter voor kiest om *Strengbeweis* toe te

---

253 Europese Commissie, Europees jusititieel netwerk, *Verkrijging van bewijs en bewijsvoering – Duitsland*, hs 3 onder 8.

254 H.-J. Musielak, M. Stadler, *Grundfragen des Beweisrechts*, München, C.H. Beck'schen Buchdruckerei Nördlingen: 1984, p. 79, nr. 152.

255 Schneider. *Beweis und Beweiswürdigung*, Verlag Vahlen, 5. Auflage, p. 339.

256 BGH *NJW* 1951, 442: "(…) Bei der Prüfung von Prozeβvoraussetzungen ist das Gericht an die Vorschriften der ZPO über das Beweisverfahren nicht gebunden und auf die dort vorgesehenen Beweismittel nicht beschränkt (sog. Freibeweis)(….)"

passen, dan kan de rechter zich enkel bedienen van de wettelijke bewijsmiddelen om de feiten aan te tonen.[257]

Het is de vraag of en in hoeverre elektronische gegevens als bewijsmiddel worden toegelaten in het Duitse recht. In ieder geval zal er geen twijfel over bestaan dat elektronische gegevens als bewijs kunnen worden toegelaten onder het *Freibeweis*. Elektronische gegevens kunnen worden toegelaten om feiten waar partijen niet over van mening verschillen aan te tonen. Maar juist in de kern van de zaak, waar partijen het niet eens zijn over de feiten is het belangrijk om elektronische gegevens als bewijsmiddel toegelaten te krijgen om aan te kunnen tonen welke feiten zich hebben voorgedaan en welke rechten er bestaan.[258] In dat geval is het stelsel van *Strengbeweis* van toepassing en is de rechter gebonden aan de wettelijke bewijsregels. In de volgende paragraaf zal ik daarom nader ingaan op het toelaten en de waardering van de wettige bewijsmiddelen in het Duitse recht.

5.5 De wettelijke bewijsmiddelen

Het Duitse bewijsrecht kent vijf soorten bewijsmiddelen, namelijk het *Augenscheinsbeweis* (waarneming door het gerecht), *Zeugenbeweis* (getuigenbewijs), *Sachverständigebeweis* (deskundigenbewijs), *Urkundenbeweis* (bewijs door middel van akten) en *Parteivernehmung* (getuigenis door partijen). In het kader van dit onderzoek zijn alleen het *Augenscheinsbeweis* en het *Urkundenbeweis* van belang. Om deze reden zal ik deze twee soorten bewijsmiddelen eerst behandelen en aan het einde van deze paragraaf slechts kort ingaan op de overige soorten bewijsmiddelen.

5.5.1 *Augenscheinsbeweis*

De *Augenschein* of *Augenscheinseinnahme* is geregeld in titel zes van boek twee van de *ZPO*. Een definitie van *Augenschein* ontbreekt echter in de wet. Letterlijk vertaald betekent *Augenschein* ogenschijn of ogenschouw en meer vrij vertaald betekent het waarneming of onderzoek.[259] Hoewel het hier lijkt te gaan om een visuele opname door het gerecht, is de *Augenschein* of de

---

257 W. Kilian, 'Zweck und Inhalt des deutschen EDI-Rahmenvertrages', *Computer und Recht* 1994 pag. 657:"(…) daβ nach geltendem deutschen Zivilprozeβrecht ein elektronisches Dokument nicht als Beweismittel für den Strengbeweis sondern nur für den Freibeweis in Betracht kommt (…)" Zie ook: W. Kilian, 'EDI Forschungsprojekt 'ELTRADO' – Juristische Aspekte', in: Alt, Rainer; Schmid, Beat F.; Zbornik, Stefan, *EM - Electronic Markets*, Vol. 4 , No. 1, April. 1994.

258 M. Bergfelder, *Der Beweis im elektronischen Rechtsverkehr* (diss. Freiburg), Verlag Dr. Kovač, Hamburg 2006, p. 118.

259 *Van Dale, Groot Woordenboek Duits – Nederlands*, pag. 129

Augenscheinsaufnahme niet beperkt tot visuele bezichtiging, maar houdt deze ook de zintuigelijke waarneming via andere zintuigen in; de *Augenschein* wordt daarom in de literatuur ook wel aangeduid als: "*jede unmittelbare sinnliche Wahrnehmung des Gerichts*" [260] of "*jede unmittelbare Wahrnehmung der Beschaffenheit von Personen, Sachen oder elektronische Dokumenten mittels der Sinnesorgane des Richters*"[261]

Augenscheinsbeweis kan bestaan uit het bekijken van beeldmateriaal, het beluisteren van geluidsmateriaal, maar ook alle andere manieren om informatie op te nemen, zoals geur, smaak en tast.[262] Het *Augenscheinsbeweis* is ook een krachtig bewijsmiddel. Het is namelijk een direct middel waarbij de rechter uit eigen waarneming het bewijsmiddel kan aanschouwen. Daarbij wordt voorkomen dat de subjectieve waarneming en de subjectieve verklaring van derden een vertekend beeld kunnen geven aan de rechter.[263] Hoewel in de literatuur wordt gesteld dat dit middel vooral van belang is voor processen op het gebied van ongevallen, bouw en burenruzies, zie ik hier ook een rol weggelegd voor elektronische systemen. De werking van deze systemen kan op papier omschreven worden of op video zijn vastgelegd, maar van een aanschouwing door de rechter, eventueel aangevuld met uitleg door een deskundige, gaat naar mijn mening ook een grote rechtskracht uit. De rechter kan dan direct waarnemen hoe een systeem werkt en hoeft niet te vertrouwen op een omschrijving op papier of een verklaring van een derde.

Het genus *Augenschein* heeft een bijzondere species, namelijk het *elektronische Dokument*. Dit blijkt uit de plaatsing van § 371a ZPO in de afdeling die het *Augenscheinsbeweis* regelt. Het *elektronisches Dokument* moet dus juridisch gezien geclassificeerd worden als *Augenscheinsbeweis*,. Echter, § 371, eerste zin ZPO stelt: "*Auf private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, finden die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung.*" [264] Bovenstaand artikel verklaart dat de regels met betrekking tot de bewijskracht van *private Urkunden* ook van toepassing zijn op *private elektronische Dokumente* die zijn voorzien van een gekwalificeerde elektronische handtekening, ook al vallen deze onder het *Augenscheinsbeweis*. Het feit dat de regels van de *private Urkunde* ook van toepassing zijn op *private*

---

260 C. Theimer, *Mustertexte zum Zivilprozess Band I: Erkenntnisverfahren erster Instanz*, München:C.H. Beck, p. 139.

261 H.-J. Musielak, *Grundkurs ZPO*, München: C.H. Beck Verlag 2007, p. 264.

262 W. Grunsky, *Zivilprocessrecht*, München: Wolters kluwer Deutschland GmbH 2006, p. 172.

263 K. Schellhammer, *Zivilprozess, Gesetz – Praxis – Fälle*, Heidelberg: C.F. Müller Verlag, 2004, p. 267, nr. 578.

264 De regels over de bewijskracht van private akten zijn van toepassing op private elektronische Documenten die met een gekwalificeerde elektronische handtekening zijn voorzien. Private Urkunden zijn geschriften die ondertekend zijn door beide partijen die partij zijn bij de akte of

elektronische Dokumente is vooral van belang in verband met de dwingende (formele) bewijskracht die wettelijk wordt toegekend aan ondertekende *private Urkunden*.[265] Op deze dwingende bewijskracht zal ik nader ingaan in paragraaf 5.7 en 5.8.

Opmerkelijk aan § 371a *ZPO* is de plaatsing van het artikel in de *Zivilprozessordnung*. Deze is namelijk opgenomen in titel zes van boek twee onder het *beweis durch Augenschein* en niet onder titel negen van boek twee onder het *beweis durch Urkunden*. Het lijkt erop dat de wetgever hiermee heeft willen aangeven dat een *elektronisch Dokument* niet erkend wordt als *Urkunde*, waar het schriftelijkheidsvereiste geldt, maar slechts als een stuk dat door middel van rechterlijke *Augenschein* als bewijsstuk kan dienen.[266] Hiermee lijkt de Duitse wetgever de exclusiviteit van dwingende bewijskracht voor *Urkunden* te hebben doorbroken; een *elektronisch Dokument* dat als *Augenscheinsbeweis* wordt beschouwd, krijgt nu onder omstandigheden dezelfde dwingende bewijskracht als de ondertekende *Urkunde*.

Nu het *elektronisches Dokument* gekwalificeerd wordt als *Augenscheinsbeweis*, is het van belang te weten wanneer er sprake is van een *elektronisches Dokument*. Het *elektronische Dokument* kent geen wettelijke definitie en ook de rechtspraak heeft tot op heden geen uitsluitsel gegeven. Daarbij komt dat de literatuur verdeeld is over de kenmerken van het *elektronisches Dokument*.[267] Er worden drie soorten interpretaties gegeven, namelijk een enge interpretatie, een ruime interpretatie en een gemengde vorm afhankelijk van de juridische functie die het *elektronisches Dokument* vervult.

Voorstanders van het meer enge begrip verstaan op grond van § 130a *ZPO* slechts data die een geschrift bevatten (code wordt uitgesloten, alsmede data die geen reflectie is van een schriftelijk stuk zoals afbeeldingen en videomateriaal). Zij stellen dat de data slechts een elektronische vorm moet zijn van datgene wat ook in een *Urkunde* staat.[268] Dit is *'jede schriftliche Verkörperung eines Gedankens*' (zie hiervoor subparagraaf 5.5.2). Voorstanders van een ruimere begripsopvatting betrekken daarentegen juist alle mogelijke inhoud van data en code bij het *elektronisches Document*, waaronder

---

265 Zie hiervoor paragraaf 5.7.2.

266 M. Bergfelder, *Der Beweis im elektronischen Rechtsverkehr* (diss. Freiburg), Verlag Dr. Kovač, Hamburg 2006, p. 77.

267 C.B. Berger, 'Beweisführung mit elektronischen Dokumenten', *Neue juristische Wochenschrift* 2005-15, p. 1017. Zie ook: M. Bergfelder, *Der Beweis im elektronischen Rechtsverkehr* (diss Freiburg), Verlag Dr. Kovač, Hamburg 2006, p. 35 t/m 37.

268 § 130a ZPO:"(1) Soweit für vorbereitende Schriftsätze und deren Anlagen, für Anträge und Erklärungen der Parteien sowie für Auskünfte, Aussagen, Gutachten und Erklärungen Dritter die Schriftform vorgesehen ist, genügt dieser Form die Aufzeichnung als elektronisches Dokument, wenn dieses für die Bearbeitung durch das Gericht geeignet ist. (…)".

afbeeldingen, geluidsfragmenten en uitvoerbare gegevens.[269] Berger stelt dat de ruime begripsopvatting de voorkeur heeft, daar de wetgever de beperking van schriftelijke stukken bij de invoering van § 371, lid 1 , tweede zin *ZPO* opgegeven heeft.[270] Overigens doet dit niets af aan het onderscheid dat gemaakt wordt tussen geschriften die wel een verklaring bevatten en geschriften waar een verklaring ontbreekt, omdat de rechtsgevolgen betreffende dwingende rechtskracht van schriftelijke stukken met een verklaring geregeld worden in § 371a, lid 1, tweede zin *ZPO*.[271]

Een geheel eigen aanpak heeft Bergfelder die het begrip *elektronisches Dokument* eng dan wel breed hanteert al naar gelang de juridische functie. Als het begrip ziet op de verbintenisrechtelijke functie, dan hanteert hij een enge definitie (slechts data die geschriften bevatten) en als het begrip ziet op een bewijsrechtelijke functie dan hanteert hij de ruimere definitie (data en code).[272] Aangezien in de literatuur de aanhangers van de ruimere definitie in de meerderheid lijken te zijn en § 371a ZPO daartoe alle aanwijzingen geeft zal ik als definitie in dit onderzoek de ruimere definitie aanhouden welke gegeven is door Becker:"jede potentielle Fixierung von Daten auf einem Datenträger unter Einsatz elektronischer Signalverarbeitung."[273]

5.5.2 *Urkundenbeweis*

De wet kent geen definitie van het begrip *Urkunde*. In de literatuur wordt de *Urkunde* ook wel aangeduid als: "*schriftliche Äußerung mit und ohne Unterschrift*" of "*schriftliche Verkörperungen von Gedankenerklärungen durch solche Lautzeichen, die einer objectiven Deutung allein aufgrund ihrer Wahrnehmung zugänglich sind*".[274]

Het *Bundesgerichtshof* heeft echter reeds geoordeeld dat onder een *Urkunde* als bedoeld in de *ZPO* moet worden verstaan: "*jede schriftliche Verkörperung eines Gedankens*" [275] Deze definitie beschouw ik dan ook als meest

---

269 C.B. Berger, 'Beweisführung mit elektronischen Dokumenten', *Neue juristische Wochenschrift* 2005-15, p. 1017.

270 BT-Dr 14/4987, S. 23; zie ook BT-Drs. 15/4067.

271 In veel literatuur wordt nog verwezen naar § 292a ZPO (01-08-2001 t/m 31-03-2005) welke niet langer bestaat. In plaats daarvan is de ruimere opvatting van § 371a, lid 1 en 2, tweede zin ZPO van toepassing. Deze heeft niet alleen betrekking op wilsverklaringen, maar op alle verklaringen die besloten liggen in een schriftelijk stuk.

272 M. Bergfelder, *Der Beweis im elektronischen Rechtsverkehr* (diss Freiburg), Verlag Dr. Kovač, Hamburg 2006, p. 80.

273 A. Becker, *Elektronische Dokumente als Beweismittel im Zivilprozess*, Frankfurt am Main, 2004, p. 9.

274 J.W. Britz, *Urkundenbeweisrecht und Elektroniktechnologie: eine Studie zur Tauglichkeit gesetzlicher Beweisregeln für elektronische Dokumente und ihre Reproduktionen im Zivilprozeß*, München, C.H. Beck 1996, p. 99.

275 BGHZ 65, 300 = NJW 1976, 294.

gezaghebbende en zal ik daarom in dit onderzoek hanteren. Vertaald komt deze definitie neer op: iedere schriftelijke belichaming van een gedachte. Dit omvat geen opnames op cassette, platen en foto's, omdat deze schriftelijkheid ontberen[276] Deze zijn daarom niet onderwerp van de *Urkunde*, maar kunnen wel onderwerp zijn van *Augenscheinsbeweis*.

Naast het onberen van schriftelijkheid, ontbeert een elektronisches Dokument belichaming, oftewel *Verkörperung*. Het ontbreken van *Verkörperung* is de tweede reden dat *elektronische Dokumenten* geen *Urkunde* in de zin van de *ZPO* kunnen zijn.[277] Wel worden ingevolge § 371a *ZPO* elektronische documenten wat rechtsgevolg betreft gelijkgesteld met *Urkunden*.[278]

Door *elektronische Dokumenten* niet te erkennen als Urkunde, maar als Augenscheinsbeweis, lijkt de wetgever aan te willen sluiten bij de reeds langere tijd bestaande opvatting onder deskundigen dat *elektronische Dokumenten* geen *Urkunden* in de zin van de *ZPO* zijn, maar slechts als *Augenscheinsbeweis* moeten worden gekwalificeerd.[279]

Urkunden kunnen slechts in zeer grove lijnen worden vergeleken met de Nederlandse variant van het bewijs door middel van akten. Hoewel een belangrijke overeenkomst met de akte is dat de *Urkunde* een schriftelijk stuk is dat lettertekens bevat en daarmee op de akte lijkt, moet voor de vergelijking met de akte worden gewaakt. De akte en de *Urkunde* hebben in respectievelijk het Nederlandse en het Duitse recht een specifieke juridische betekenis die niet één op één met elkaar overeenstemmen. Het Duitse recht verlangt voor de *Urkunde* namelijk geen ondertekening.[280] Het zijn van een schriftelijk stuk met daarop de uiting van een gedachte is voldoende. Het Nederlandse recht kent daarentegen een expliciet ondertekeningsvereiste als vereiste voor het bestaan van een akte. Een tweede verschil is dat de het Duitse recht ook niet verlangt dat de *Urkunde* bij het ontstaan tot doel had om als bewijsmiddel te dienen.[281] Dit in tegenstelling tot het Nederlandse recht, waar de bewijsfunctie een vereiste is voor de akte.

---

276 Het Duitse strafrecht kent overigens andere vereisten, wil er sprake zijn van een *Urkunde*. Zo worden in het strafrecht opnames wel beschouwd als *Urkunde*. Zie hiervoor: R. Oberheim, *Zivilprozessrecht für Refendare*, Neuwied: Werner Verlag 2007, p. 112.

277 S. Abel, Urkundsbeweis durch digitale Dokumente *Multimedia und Recht* 1998, 944ff. Zie ook: H.-J. Musielak, *Grundkurs ZPO*, München: C.H. Beck Verlag 2007, p. 274.

278 H.-J. Musielak, *Grundkurs ZPO*, München: C.H. Beck Verlag 2007, p. 274. Zie ook: K. Schellhammer, *Zivilprozess, Gesetz – Praxis – Fälle*, Heidelberg: C.F. Müller Verlag 2004, p. 273, nr. 581. Zie ook paragraaf 5.5.1.

279 J.W. Britz, *Urkundenbeweisrecht und Elektroniktechnologie: eine Studie zur Tauglichkeit gesetzlicher Beweisregeln für elektronische Dokumente und ihre Reproduktionen im Zivilprozeß*, München: C.H. Beck 1996, p. 32 t/m 34.

280 Zie § 416 ZPO. Zie ook K. Schellhammer, *Zivilprozess, Gesetz – Praxis – Fälle*, Heidelberg: C.F. Müller Verlag 2004, p. 272, nr. 581.

281 L. Rosenberg, K.H. Schwab, P. Gottwald, *Zivilprozessrecht*, München, C.H. Beck 1993, p. 697.

De *Urkunde* is een gegevensdrager die gedachte-uitingen op schrift kan bevatten. Veel van deze uitingen, waaronder ook wilsverklaringen, worden vastgelegd om de bewijspositie van partijen te versterken.[282] De Duitse wetgever heeft dan ook bijzondere bewijskracht verleend aan de *Urkunde*. Een risico is dat de *Urkunde* wordt gewijzigd, zonder dat een van de partijen daarvan op de hoogte is. De echtheid van de *Urkunde* kan dan in twijfel getrokken worden. De wetgever heeft daarmee rekening gehouden en regels gesteld omtrent de echtheid van de *Urkunde*. Deze regels zullen in de paragraaf 5.7 nader worden besproken. Hier is van belang de opmerking dat er slechts rechtsgevolgen kunnen worden verleend aan de *Urkunde* als de echtheid van de *Urkunde* vast staat.

Het Duitse recht kent twee soorten *Urkunden*: *öffentliche Urkunden* en *private Urkunden*. De *öffentliche Urkunden* zijn Urkunden die:

"*von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer met öffentlichem Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises in der vorgeschriebene Form aufgenommen sind*."[283]

Het betreft hier *Urkunden* die door een ambtenaar binnen de grenzen van zijn ambtsbevoegdheid of door een persoon die een publieke functie bekleed binnen zijn toegewezen bevoegdheden in de voorgeschreven vorm zijn opgenomen. Alle overige *Urkunden* zijn *private Urkunden.*[284]

5.5.3 *Zeugenbeweis*

Bewijs door middel van *Zeugen*, oftewel getuigenbewijs, is een indirecte of middellijke vorm van bewijs. Een derde, de getuige, zal namelijk door middel van het afleggen van een verklaring proberen hard te maken welke feiten zich hebben voorgedaan en/of wie welke rechten heeft. De getuige kan zelf als middel ter bewijs worden opgevoerd, maar ook ondersteunend bewijs leveren door verklaringen af te leggen over een bewijsmiddel. Het zou hier dan bijvoorbeeld kunnen gaan om verklaringen over de vraag wie toegang had tot bepaalde elektronische gegevens, welke gegevens op welk moment zijn gecreëerd of om de inhoud van bepaalde gegevens nader toe te lichten.

De verklaring van een getuige is een bewijsmiddel. Het ontbeert echter de voor dit onderzoek kwalitatieve eigenschap dat deze in elektronische vorm is.

---

282 H.-J. Musielak, M. Stadler, *Grundfragen des Beweisrechts*, München, C.H. Beck'schen Buchdruckerei Nördlingen: 1984, p. 82, nr. 158.

283 § 415 *ZPO.*

284 O. Jauernig, *Zivilprozessrecht*, München: Verlag C.H. Beck, 2007, p.180.

Daarom zal ik voor dit onderzoek de rol van de getuigenverklaring enkel aan de orde laten komen, indien de rol van deze verklaring betrekking heeft op de kwaliteit van een elektronisch bewijsmiddel.

5.5.4 *Sachverständigebeweis*

Bewijsvoering door middel van een *Sachverständige* is bewijsvoering door een deskundige op een specifiek gebied, waarvan de rechter onvoldoende kennis heeft.[285] Bewijs door middel van *Sachverständige* wordt in beginsel behandeld volgens de regels van het *Zeugenbeweis*, tenzij de wet anders bepaalt.[286] De *Sachverständige* heeft een drietal taken: hij deelt ervaringskennis met de rechter en specifieke kennis uit andere wetenschapsgebieden, technieken en beroepen, hij past buitenrechtelijke regels toe op de zaak en hij onderzoekt feiten die de rechter als leek niet zelf kan vaststellen.[287] In het kader van dit onderzoek zal de rol van de *Sachverständige* verder niet aan de orde komen.

5.5.5 *Parteivernehmung*

In het Duitse recht kan de rechter onder voorwaarden ook een partij laten getuigen. Dit kan zowel de eisende partij zijn als de verdedigende partij.[288] De partij wordt onder ede gehoord en daarmee geldt ook dat als de partij niet de waarheid spreekt en dit wordt ontdekt aan de partij sancties kunnen worden opgelegd.[289] Overigens moet er een onderscheid worden gemaakt in het horen van partijen en het laten getuigen van partijen. Het horen van partijen gebeurt niet onder ede en dient om partijen hun eisen uiteen te zetten en argumenten aan te dragen. Het getuigen van partijen onder ede heeft echter waarheidsvinding als doel en heeft daarmee een andere aard dan het horen van partijen. Aangezien de *Parteivernehmung* in het kader van dit onderzoek niet van belang is, zal ik hierop verder niet dieper ingaan.

5.5.6 De toelaatbaarheid van code

Elektronische gegevens kunnen zich in verschillende vormen manifesteren. In hoofdstuk twee heb ik reeds een onderscheid gemaakt in code, computer gegenereerde data en door mensen gegenereerde data. In deze subparagraaf

---

285 K. Schellhammer, *Zivilprozess, Gesetz – Praxis – Fälle*, Heidelberg: C.F. Müller Verlag, 2004, p. 306, nr. 464.

286 § 402 ZPO.

287 BGH 37, 389; NJW 93, 1796, BVerwG NJW 86, 2268.

288 § 445 en § 447 ZPO.

289 L. Rosenberg, K.H. Schwab, P. Gottwald, *Zivilprozessrecht*, München, C.H. Beck 1993, p. 854.

ga ik nader in op de vraag of deze drie soorten elektronische gegevens worden toegelaten in het Duitse recht. Ik heb in hoofdstuk 2 gesteld dat code uit instructies bestaat die gericht zijn tot een computer of andere machine welke door middel van die code wordt aangestuurd. Code omvat in beginsel geen verklaringen van partijen. De adressant van code is een machine en niet een mens. Een computerprogramma welke bestaat uit code, kan geëxecuteerd worden door een computer of andere machine welke overweg kan met de code.

Als bewijsmiddel moet de code toegelaten worden als één van de vijf wettelijke bewijsmiddelen. Hiervoor is het *Augenscheinsbeweis* toereikend. Het is de vraag of code ook als *elektronisches Dokument* kan worden beschouwd. Als code namelijk ook kan worden gekwalificeerd als *elektronisches Dokument* dan kan de code een grotere bewijskracht krijgen, dan alleen onder het *Augenscheinsbeweis*. Afhankelijk van de definitie van het elektronisches Dokument (§ 371 ZPO) hangt het ervan af of code als dusdanig kan worden gekwalificeerd. Verschillende auteurs hebben verdedigd (zie ook paragraaf 5.5.1) dat een ruime definitie die ook code omvat, de voorkeur heeft. Daarentegen zijn er ook auteurs die verdedigen dat het begrip *elektronisches Dokument* eng opgevat moet worden en daarom niet code omvat. Aangezien de wetgever geen duidelijkheid heeft gegeven en ook de jurisprudentie hierover nog geen uitsluitsel heeft gebracht, is het tot op heden onduidelijk of code als *elektronisches Dokument* kan worden gekwalificeerd en mogelijkerwijs een hogere bewijskracht kan toekomen.

5.5.7 De toelaatbaarheid van computer gegenereerde data en door mensen gegenereerde data

Net als voor code geldt dat computergegenereerde data in ieder geval als *Augenscheinsbeweis* toegelaten kan worden. De vraag is of het ook onder de definitie van *elektronisches Dokument* valt. Zowel bij toepassing van de ruime als de enge definitie valt data die gegenereerd is door mensen te kwalificeren als *elektronisches Dokument*. Of een computergegenereerde data ook te classificeren valt als *elektronisches Dokument* is niet duidelijk. Onder de ruime definitie is dit zeker het geval, aangezien deze alle elektronische gegevens omvat. Echter bij toepassing van de enge definitie is het de vraag of computergegenereerde data wel een *Gedanken* omvat. Vooralsnog is deze vraag niet beantwoord door de wetgever of in de jurisprudentie en blijft de vraag onbeantwoord.

Een volgende vraag is of en zo ja onder welke voorwaarden computergegenereerde data als *Urkunde* kan worden beschouwd. Iedere vorm van data wordt met de plaatsing van § 371a ZPO uitgesloten van het

Urkundenbegrip. Data kan onder het huidige Duitse bewijsrecht nooit als *Urkunde* gekwalificeerd worden aangezien het zowel schriftelijkheid ontbeert als belichaming (zie paragraaf 5.5.2). Data, op welke manier ook tot stand gekomen, kan nooit als *Urkunde* gekwalificeerd worden, maar enkel als *Augenscheinsbeweis* en als *elektronisches Dokument.*

5.6 Bewijswaardering

5.6.1 Inleiding

Nadat het bewijs is toegelaten, zal de rechter zich een oordeel moeten vormen over de betrouwbaarheid van het bewijs. De bewijswaardering is een belangrijke stap om te komen tot het vaststellen van de feiten zodat een oordeel gevormd kan worden en tot een beslissing kan leiden. In het Duitse recht bestaan verschillende graden van bewijswaardering. Welke graad van overtuiging voldoende is voordat een feit als bewezen kan worden beschouwd, wordt in beginsel beoordeeld naar § 286 *ZPO*. In de volgende paragraaf zal dieper worden ingegaan op de vraag wanneer de rechter een feit als bewezen mag beschouwen. Naast de vrije bewijswaardering in § 286 *ZPO* bestaat de zogenaamde *Glaubhaftmachung*. *Glaubhaftmachung* is een vorm van plausibele bewijsvoering. Wat hieronder verstaan wordt en in welke gevallen een rechter genoegen mag nemen met *Glaubhaftmachung*, zal beschreven worden in paragraaf 5.6.3.

5.6.2 Hoofdregel: vrije bewijswaardering

Het Duitse recht kent in beginsel een vrije waardering van bewijs. Deze vrije waardering van bewijs is vastgelegd in het eerste lid van § 286 *ZPO*: "*Das Gericht hat 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. In dem Urteil sind die Gründe anzugeben, die für die richterliche Überzeugung leitend gewesen sind*." Het gerecht heeft met inachtname van de gehele inhoud van de gebeurtenissen en van de uitkomsten van een eventuele bewijsopname naar vrije overtuiging te beslissen of een feitelijke bewering als waar of als niet waar te beschouwen is. In het oordeel zijn de gronden aangegeven die voor de rechterlijke overtuiging leidend zijn gewezen.

Met § 286 I *ZPO* wordt de kern van het begrip bewijzen geraakt.[290] De rechter moet overtuigd zijn van de door de partijen gestelde feiten. Daartoe dienen de

[290] Zie hiervoor ook paragraaf 1.4.

bewijsmiddelen die de rechter aangeboden krijgt de feiten te staven. Maar welke bewijsmiddelen maken dat de rechter wordt overtuigd van de feiten en welke mate van overtuiging is toereikend om de feiten als bewezen te beschouwen?

Om met de laatst gestelde vraag te beginnen. Lange tijd is discussie geweest over de mate waarin de rechter overtuigd dient te zijn van de gestelde feiten. Vast stond en staat dat de rechter geen absolute zekerheid kan hebben, als hij niet aanwezig was op het moment dat feiten zich voordeden. Er blijft altijd een (abstracte) mogelijkheid dat feiten zich niet of anders hebben voorgedaan. De menselijke kennis is niet onbegrensd en er kan niet verwacht worden dat de rechter overtuigd is zonder onzekerheid uit te sluiten.[291]

Het feit dat er geen absolute zekerheid kan bestaan, heeft geleid tot de vraag in welke mate de rechter overtuigd moet zijn om te kunnen bepalen of een feitelijke bewering als waar of als niet waar moet worden beschouwd. Vanuit het strafrecht heeft vervolgens de waarschijnlijkheidsleer haar intrede gedaan in het civiele recht. Zo stelt de rechter vast: "*Hierfür (für die Überzeugung von der Wahrheit der zu beweisenden Tatsache) genügt ein so hoher Grad von Wahrscheinlichkeit, daß er nach der Lebenserfahrung der Gewißheit gleich zu achten ist.*"[292] In een aantal andere uitspraken heeft het *Bundesgerichtshof* zich in gelijke bewoordingen uitgelaten.[293]

De waarschijnlijkheidsleer is echter verlaten met het Anastasiaoordeel van het *Bundesgerichtshof*. Aanleiding was de eis van de feitenrechter die verlangde dat de eiseres ondanks omvangrijke bewijsvoering, zou voldoen aan onmogelijk te vervullen bewijslevering: *"Der Revision ist zuzugeben, daß ein Gericht keine 'unerfüllbaren Beweisanforderungen' stellen darf, und daß es keine unumstoßliche Gewißheit bei der Prüfung verlangen darf, ob eine Behauptung wahr und erwiesen ist."*[294]

Het *Bundesgerichtshof* gaat vervolgens verder waarbij het ingaat op de vraag welke criteria een rechter moet hanteren bij het beoordelen of een feit als bewezen mag worden verklaard of niet: *"Irrig ist jedoch der Vortrag, der Zivilprozeßrichter dürfte sich in Fällen dieser Art mit einer bloßen Wahrscheinlichkeit begnügen. Den nach § 286 ZPO muß der Richter aufgrund der Beweisaufnahme entscheiden, ob er eine Behauptung für wahr oder nicht*

---

291 E. Schneider. *Beweis und Beweiswürdigung*, München: Verlag Vahlen 1994, pag. 17.

292 BGH NJW 1951, 70/71. Voor de overtuiging van de waarheid van de te bewijzen feiten is toereikend een zo hoge graad van waarschijnlijkheid, die naar levenservaring gelijk te achten is aan zekerheid.

293 BGH, VersR 1954, 495; BGH VersR 1956, 194; BGH VersR 1956, 696.

294 BGH *NJW* 1970, 946. De herziening is op zijn plaats, want een gerecht mag geen onvervulbare eisen stellen aan bewijs en het mag geen onomstotelijke zekerheid verlangen of een bewering waar en aangetoond is.

wahr halt, er darf sich also gerade nicht mit einer bloßen Wahrscheinlichkeit beruhigen. Im übrigen stellt § 286 ZPO nur darauf ab, ob der Richter selbst die Überzeugung von der Wahrheit einer Behauptung gewonnen hat. Diese persönliche Gewißheit ist für die Entscheidung notwendig, und allein der Tatrichter hat ohne Bindung an gesetzliche Beweisregeln und nur seinem Gewissen unterworfen die Entscheidung zu treffen, ob er die an sich möglichen Zweifel überwinden und sich von einem bestimmten Sachverhalt als wahr überzeugen kann. Eine von allen Zweifeln freie Überzeugung setzt das Gesetz dabei nicht voraus. Auf diese eigene Überzeugung des entscheidenden Richters kommt es an, auch wenn andere zweifeln oder reine andere Auffassung erlangt haben würden. Der Richter darf und muß aber in tatsächlich zweifelhaften Grad von Gewißheit begnügen, der den Zweifeln schwiegen gebietet, ohne sie völlig auszuschließen."[295]

Vervolgens stelt het *Bundergerichtshof* ook welke opvatting onjuist is: *"Das wird allerdings vielfach ungenau so ausgedrückt, daß das Gericht sich mit einer an Sicherheit grenzenden Wahrscheinlichkeit begnügen dürfte; das ist falsch, falls damit von der Erlangung einer eigenen Überzeugung des Richters von der Wahrheit abgesehen werden sollte."*[296]

Het *Bundesgerichtshof* zegt in bovenstaande tekst in feite dat enkel en alleen een hoge mate van waarschijnlijkheid niet tot het oordeel mag leiden dat feiten als bewezen worden verklaard. Om vast te stellen of iets bewezen is of niet, moet de feitenrechter zelf overtuigd zijn van de waarheid van de feiten. Het komt aan op deze overtuiging; als deze ontbreekt dan kan niet tot het oordeel worden gekomen dat de feiten worden bewezenverklaard. Bovenstaande maatstaf is erg subjectief. In de recente literatuur en de rechtspraak zijn de laatste tijd stappen gezet om tot een meer objectieve beoordeling te komen, waarin de waarschijnlijkheid weer een grotere rol heeft gekregen. Het Bundesverfassungsgericht heeft namelijk bepaald dat: "*im*

[295] Verwarrend is daarentegen de opvatting dat de civiele procesrechter in dit soort gevallen genoegen zou mogen nemen met een enkele waarschijnlijkheid. Op grond van § 286 *ZPO* moet de rechter op grond van de bewijsopname beslissen of hij een bewering voor waar of voor onwaar houdt; hij mag dus niet op grond van een enkele waarschijnlijkheid berusten. Overigens stelt § 286 *ZPO* alleen dat de rechter zelf de overtuiging van de waarheid van een bewering moet hebben gekregen. Deze persoonlijke overtuiging is voor de beslissing noodzakelijk en alleen de feitenrechter moet , zonder gebonden te zijn aan wettelijke bewijsregels en enkel onderworpen aan zijn geweten, de beslissing nemen of hij zich over zijn twijfel heen kan zetten en zich van de waarheid van een bepaald feit kan overtuigen. Een overtuiging zonder enige twijfel wordt niet verlangd door de wet. Het komt aan op de eigen overtuiging van de beslissende rechter, ook als anderen twijfelen of een andere opvatting zouden verlangen. De rechter mag en moet echter genoegen nemen met een bepaalde twijfelachtige graad van zekerheid, die de twijfel het zwijgen oplegt zonder deze volledig uit te sluiten.

[296] Regelmatig wordt deze regel echter ten onrechte zo uitgedrukt dat het gerecht zich met een aan zekerheid grenzende waarschijnlijkheid tevreden moet stellen; dit is onjuist, omdat daardoor van de eigen overtuiging van de rechter van de waarheid zou moeten worden afgezien.

verfassungsbeschwedenverfahren werden gerichtliche Urteile lediglich auf verfassungsrechtliche verstöße überprüft. Ein solcher liegt unter dem Gesichtspunkt des Willkürverbots des § 3 I GG dann vor, wenn die Rechtsanwendung oder das eingeschlagene Verfahren bei verständiger Würdigung der das Grundgesetz beherrschenden Gedanken nicht mehr verständlich ist und sich daher der Schluß aufdrängt, daß die Entscheidung auf sachfremdem Erwägungen beruht." [297]

Als conclusie kan gesteld worden dat onder invloed van de jurisprudentie de huidige opvatting is dat § 286 I *ZPO* twee eisen stelt om een feit bewezen te kunnen verklaren: ten eerste subjectief de overtuiging van de feitenrechter en ten tweede objectieve waarschijnlijkheid. Zoals Schellhammer stelt: *"Wahrscheinlichkeit ohne Überzeugung genügt nicht, Überzeugung ohne Wahrscheinlichkeit ist sachfremd und reine Willkür."* Waarschijnlijkheid zonder overtuiging is niet voldoende, overtuiging zonder waarschijnlijkheid is zaaksvreemd en pure willekeur.

5.6.3 *Glaubhaftmachung*

In tegenstelling tot § 286 *ZPO* die als eis stelt dat de rechter overtuigd moet zijn van de waarheid of onwaarheid van gestelde feiten, dient bij de *Glaubhaftmachung* de rechter slechts overtuigd te zijn van de overwegende waarschijnlijkheid, "de goede mogelijkheid" van gestelde feiten.[298] Hoewel de wet geen definitie geeft van wat onder *Glaubhaftmachen* verstaan moet worden, is de literatuur eenduidig dat het gaat om het plausibel maken van de waarheid of onwaarheid van feiten, waarbij volle overtuiging door de rechter volgens § 286 *ZPO* niet noodzakelijk is.[299] De *Glaubthaftmachung* is dan wel niet in de wet gedefinieerd, toch wordt deze vorm van bewijzen genoemd in de wet. § 294 *ZPO* stelt in lid 1: *"Wer eine tatsächliche Behauptung glaubhaft zu machen hat, kann sich aller Beweismittel bedienen, auch zur Versicherung an Eides statt zugelassen werden."* Wie een bewering van de feiten geloofwaardig moet maken, kan alle bewijsmiddelen gebruiken, ook de verzekering onder belofte/eed is toegelaten. In afwijking tot de wettelijke bewijsmiddelen, zijn voor de *Glaubhaftmachung* alle bewijsmiddelen toegelaten en zelfs de

---

[297] BVerfG *NJW* 94, 847: In kwesties waarin grondwettelijke procesbezwaren spelen worden gerechtelijke oordelen alleen op grondwettelijke overtredingen getoetst. Dit soort overtredingen valt onder het gezichtspunt van het willekeurverbod van art 3 I *Grundgesetz* als de rechtstoepassing of het betreffende proces bij begrijpelijke waardering die op grond van op de grondwet heersende opvattingen niet meer begrijpelijk is en tot de conclusie moet worden gekomen dat de beslissing op buiten de zaak staande overwegingen is gebaseerd.

[298] H. Thomas, H. Putzo, *Zivilprozessordnung mit Gerichtsverfassungsgesetz, den Einführungsgesetzen und europasrechtlichen Vorschriften*, München, Verlag C.H. Beck 2007, p. 471. Zie ook O. Jauernig, *Zivilprozessrecht*, München: Verlag C.H. Beck, 2007, p. 158.

[299] O. Jauernig, *Zivilprozessrecht*, München: Verlag C.H. Beck, 2007, p.158.

verklaringen afgelegd door een partij en ook als deze verklaring ten gunste van zichzelf is.

5.6.4 *Anscheinsbeweis*

Het *Anscheinsbewijs* is een vorm van bewijs welke lijkt op de *Beweisvermutung*. Het Anscheinsbeweis komt wat bereft de gevolgen voor de bewijslast het meest overeen met de Tatsachenvermutung. Zowel het Anscheinsbeweis als de Tatsachenvermutung kennen geen bewijslastomkering. Dit in tegenstelling tot de Rechtsvermutung, waar wel sprake is van een omkering van de bewijslast.[300] Het Anscheinsbeweis verlicht enkel de bewijslast.[301] *Anscheinsbewijs*, of ook wel *beweis des ersten Anscheins*, is niet gedefinieerd in de wet, terwijl in de wet toch verschillende keren wordt gesproken over *Anscheinsbeweis*. Voor dit onderzoek is vooral § 371a *ZPO* van belang. Hierin wordt namelijk gesproken van:"*Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung (…)*" Ook met betrekking tot de bewijskracht van e-mail speelt het Anscheinsbeweis in de Duitse rechtspraak een rol. Subparagraaf 5.9.1 gaat hier nader op in.

Het *Anscheinsbeweis* is ontwikkeld in de rechtspraak, die zeer eenduidig is in de aangelegde criteria.[302] Voor de aanname van een *Anscheinsbeweis* is vereist dat *"sich unter Berücksichtigung aller unstreitigen und festgestellten Einzelumstände und besonderen Merkmale des Sachverhalts ein für die zu beweisende Tatsache nach der Lebenserfahrung typischer Geschehensablauf ergibt".*[303] De rechter toetst of met het intreden van feit X een naar levenservaring typisch gebeurtenissenverloop voordoet waarbij feit Y zich manifesteert. Daarbij neem hij alle niet-strijdige en vastgestelde omstandigheden en bijzondere kenmerken van de toedracht in acht. Verderop in dit onderzoek zal nader ingegaan worden op de vraag of het feit dat een e-mail van een bepaald e-mailadres afkomstig is, een Anscheinsbeweis oplevert voor het feit dat de e-mail ook van de houder van het e-mailadres afkomstig is.

---

300 Zie ook paragraaf 5.3.2.

301 K. Schellhammer, *Zivilprozess, Gesetz – Praxis – Fälle*, Heidelberg: C.F. Müller Verlag 2004, p. 186, nr. 404.

302 R. Oberheim, *Zivilprozessrecht für Refendare*, Neuwied: Werner Verlag 2007, p. 383, nr. 27a.

303 Bijvoorbeeld: BGH *NJW* 1996, 1828 f; BGH *NJW* 2001, 1140 (1141). Rekening houdend met alle niet strijdige en vastgestelde omstandigheden en bijzondere kenmerken van de toedracht geldt dat deze een voor de te bewijzen feiten een naar de levenservaring typische gebeurtenissenverloop tot resultaat hebben.

5.7 Dwingend bewijs: de *Urkunde*

Een uitzondering op de vrije bewijswaardering zoals vastgelegd in § 286 ZPO kan op grond van de wet gemaakt worden. Een belangrijke rechtsfiguur waarbij de rechter niet de volle vrijheid heeft om deze vrij te waarderen, is de *Urkunde*. De *ZPO* regelt de bewijskracht van *Urkunden*. Daarbij worden niet alleen *öffentliche Urkunden* en *private Urkunden* onderscheiden, maar wordt er een nadere onderverdeling gemaakt al naar gelang de bewijskracht van de verschillende *Urkunden*. Dit geeft de volgende verdeling:

1. Bewijskracht van *öffentliche Urkunden* over verklaringen (§ 415, 416a jo 371a II, 417, 418 *ZPO*);
2. Bewijskracht van *private Urkunden* (§ 416 *ZPO*);
3. Bewijskracht van *Urkunden* met gebreken (§ 419 *ZPO*);
4. Bewijskracht van een *elektronisch Dokument* (§ 371a I jo 416 *ZPO*).

Hoewel de bewijskracht in beginsel is vastgelegd in de zojuist genoemde artikelen, bestaan er nog een aantal andere regels die samenhangen met de bewijskracht zoals de (on)echtheid van *Urkunden*, het toelaten van tegenbewijs en de rechtsgevolgen daarvan. Deze regels zullen hieronder in samenhang met de reeds genoemde soorten akten nader worden beschreven. Reeds is genoemd dat de Duitse *Urkunde* en de Nederlandse akte verschillen kennen en men moet ervoor waken deze twee niet één-op-één te vergelijken. Dit geldt ook voor de bewijskracht waarbij in het Duitse recht regels gelden voor de *Urkunde* die niet één-op-één overeenstemmen met de regels die gelden voor de bewijskracht van de Nederlandse akte.

Voor de rechtgevolgen van de verschillende *Urkunden* kan er een verdeling gemaakt worden in de *öffentliche Urkunden* (§ 415, 416a jo 371 II, 417 en 418 *ZPO*), de private *Urkunden* (§ 416 *ZPO*) en de *mangelhafte Urkunden* (§ 419 *ZPO*), oftewel Urkunden met een gebrek. Deze zullen in de volgende drie subparagrafen nader behandeld worden.

5.7.1 Bewijskracht van *öffentliche Urkunden* (§ 415, 416a jo 371a II, 417 en 418 *ZPO*)

Öffentliche Urkunden kennen een weerlegbaar bewijsvermoeden van echtheid. Ingevolge § 437 I *ZPO* geldt namelijk: "*Urkunden die nach Form und Inhalt als von einer öffentlichen Behörden oder von einer mit öffentlichem Glauben versehenen Person errichtet sich darstellen, haben die Vermuting der Echtheit für sich*." *Öffentliche Urkunden* hebben een vermoeden van echtheid. Dit vermoeden is een weerlegbaar vermoeden en tegenbewijs tegen het vermoeden van echtheid staat open voor alle soorten *öffentliche Urkunden*. Ingevolge § 437 II *ZPO* heeft de rechter bij twijfel over de echtheid van de

öffentliche Urkunde de mogelijkheid om de echtheid van de *Urkunde* ambtshalve te onderzoeken door middel van een verklaring van degene die de *Urkunde* heeft opgesteld.

De *öffentliche Urkunde* kan ook in het buitenland zijn opgemaakt. In dat geval heeft de rechter de vrije bevoegdheid om de *Urkunde* naar eigen inzicht en naar de omstandigheden van het geval te waarderen, aldus § 438 I *ZPO*.

Als vaststaat dat de *öffentliche Urkunde* echt is en geen *Mangel*, oftewel gebreken, bevat, dan levert dit rechtsgevolgen op voor het bewijsrecht. Voor de verschillende *öffentliche Urkunden* zijn de volgende rechtsgevolgen te onderscheiden.

- De *öffentliche Urkunde über erklärungen* (§ 415 *ZPO*) levert vol bewijs van de gebeurtenissen die zijn opgetekend door de ambtenaar of persoon die de Urkunde heeft opgemaakt. Tegenbewijs tegen onjuist opgetekende gebeurtenissen is toegestaan, ingevolge § 415 II *ZPO*.
- De *öffentliche Urkunde über amtliche anordnung, verfügung oder entscheidung* (§ 417 ZPO) levert vol bewijs op van de inhoud van de Urkunde die door een ambtenaar is opgetekend. Tegenbewijs is niet toegelaten.
- De *öffentliche Urkunde mit anderen inhalt* (§ 418 ZPO) levert vol bewijs op van de daarin opgetekende feiten. Tegenbewijs dat feiten onjuist zijn opgetekend is toegelaten voor zoverre *landesgesetze* deze niet uitsluiten of beperken, aldus § 418 II *ZPO*.

Bij alle *öffentliche Urkunden* waarvan de echtheid vast staat, geldt formele bewijskracht. Dit betekent dat de *Urkunde* bewijs oplevert dat de tekst echt is en dat de eventuele ondertekening ook echt gedaan zijn door degene die wiens naam onder de *Urkunde* staat. Enkel in het geval van de *öffentliche Urkunde über amtliche anordnung, verfügung oder entscheidung* geldt dat ook vaststaat dat de inhoud van de *Urkunde* waar is.[304] Deze *öffentliche Urkunde* heeft dus zowel formele als materiële bewijskracht.

5.7.2 Bewijskracht van *private Urkunden* (§ 416 *ZPO*)

§ 416 *ZPO* stelt: "*PrivaturUrkunden begründen, sofern sie von den Ausstellern unterschrieben oder mittels notariell beglaubigten Handzeichens unterzeichnet sind, vollen Beweis dafür, dass die in ihnen enthaltenen Erklärungen von den*

[304] K. Schellhammer, *Zivilprozess, Gesetz – Praxis – Fälle*, Heidelberg: C.F. Müller Verlag 2004, p. 274, nr. 585.

Ausstellern abgegeben sind."[305] De *private Urkunden* kennen, in tegenstelling tot *öffenliche Urkunden* geen vermoeden van echtheid. Wanneer een partij een *Urkunde* inbrengt als bewijsmiddel, moet de tegenpartij de echtheid bevestigen: "*Über die Echtheit einer PrivatUrkunde hat sich der Gegner des Beweisführers nach der Vorschrift des § 138 zu erklären*,"[306] aldus § 439 I ZPO. "*Wird die Erklärung nicht abgegeben, so ist die Urkunde als anerkannt anzusehen, wenn nicht die Absicht, die Echtheit bestreiten zu wollen, aus den übrigen Erklärungen der Partei vorgeht*."[307]

Het begrip *Urkunde* vereist, zoals reeds in paragraaf 5.5.2 is opgemerkt, geen handtekening en ook de bewijsfunctie kan achteraf aan de *Urkunde* toegekend worden. In het geval van de *private Urkunde* wordt wel een ondertekening verlangd om aan de *Urkunde* rechtsgevolgen te verlenen. De *private Urkunde* welke is ondertekend levert dwingend bewijs op dat de verklaringen die zijn opgenomen in de *Urkunde* ook zo waren op het moment van ondertekening.[308] Het zegt echter niets over de waarheid van de inhoud van die verklaring. Deze kan bijvoorbeeld onder druk, dwang of geestesstoornis zijn gedaan. De *private Urkunde* krijgt dus alleen formele bewijskracht en ontbeert, in tegenstelling tot de Nederlandse onderhandse akte, materiële bewijskracht. De materiële bewijskracht van de *private Urkunde* wordt naar maatstaf van § 286 *ZPO* door de rechter gewaardeerd.

5.7.3 Bewijskracht van *Urkunden* met gebreken (§ 419 *ZPO*)

Zowel *private Urkunden* als *öffenliche Urkunden* kunnen een gebrek bevatten. Als gevolg daarvan ontberen deze wettelijke dwingende bewijskracht. § 419 *ZPO* stelt*:"Inwiefern Durchstreichungen, Radierungen, Einschaltungen oder sonstige äußere Mängel die Beweiskracht einer Urkunde ganz oder teilweise aufheben oder mindern, entscheidet das Gericht nach freier Überzeugung."*[309] Met deze bepaling wordt gesteld dat voor dwingend bewijs de *Urkunden* zich in ongeschonden staat dienen te bevinden. Doorhalingen, etsen,

---

[305] *Private Urkunden* bevatten, voor zover deze door de opsteller of door middel van een handtekening van een notaris ondertekend zijn, dwingend bewijs dat deze verklaringen door de opsteller zijn afgegeven.

[306] § 138 ZPO stelt een aantal regels over de verklaringen van partijen. Deze dienen volledig te zijn en op waarheid te berusten. Ook dienen zij op bewijsstukken van de tegenpartij in te gaan als dat verlangd wordt.

[307] Als de wederpartij die verklaring niet afgeeft dan kan de echtheid van de *Urkunde* als bevestigd worden beschouwd als niet de indruk bestaat dat uit de overige verklaringen van de wederpartij kan worden opgemaakt dat deze de echtheid wil bestrijden.

[308] BGHZ 113, 48.

[309] In geval doorhalingen, etsen, toevoegingen/aanvullingen of overige uiterlijke gebreken de bewijskracht van een *Urkunde* geheel of gedeeltelijk opheffen of verminderen, beslist het gerecht naar vrije overtuiging (*Das Gericht* is hier vrij vertaald als 'het gerecht'. Het betreft hier de rechtssprekende instanties in civiele zaken.)

toevoegingen/aanvullingen, onvolledigheid, scheuren, vlekken, onleesbare stukken, buitengewoon uitziend schrift of formaat ontnemen allemaal het dwingende karakter van het bewijs.[310] Het is voldoende dat het gebrek de indruk van een verdachte verandering wekt.[311] Hoewel de bewijskracht niet langer dwingend is, geldt wel dat de rechter weer bevoegd is om het bewijsmiddel ingevolge § 419 jo 286 *ZPO* naar vrije overtuiging te waarderen.

5.8 Dwingend bewijs: het *elektronisches Dokument*

Hoewel het *elektronisches Dokument* geen *Urkunde* is, maar gekwalificeerd wordt als *Augenscheinsbeweis*, zijn de voorschriften met betrekking tot de bewijskracht van *private Urkunden* van toepassing als het een *privaat elektronisch Dokument* betreft welke is ondertekend met een gekwalificeerde elektronische handtekening. De eerste zin van § 371a I *ZPO* verwoordt dit als volgt:*"Auf private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, finden die Vorschriften über die Beweiskracht privater Urkunden entsprechende Anwendung."*

Met de eerste zin van § 371a I *ZPO* worden de regels die van toepassing zijn op private Urkunden tevens van toepassing verklaard op *private elektronische Dokumenten* die met een gekwalificeerde elektronische handtekening zijn ondertekend. § 371a I ZPO gaat echter verder: *"Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist*."[312]

De vraag is echter hoe de tweede zin van § 371a I *ZPO* zich verhoudt tot § 439 en § 440 *ZPO*. In § 371a I *ZPO* worden de regels van *private Urkunden* van toepassing verklaard op *private elektronische Dokumenten,* waaronder dus ook § 439 en § 440 *ZPO*. § 439 *ZPO* stelt dat de wederpartij de echtheid van de *Urkunde* of de handtekening daaronder moet worden bevestigd of dat als een verklaring met bevestiging niet wordt afgegeven deze bevestiging mag worden aangenomen als er uit de gedragingen van de wederpartij geen voornemen blijkt om de echtheid te bestrijden. De tweede zin van § 371a I *ZPO* stelt echter dat de indruk van echtheid van een in elektronische vorm beschikbaar zijnde

310 BGH NJW 80, 893.

311 BGH NJW 66, 1657; 80, 893; 86, 3086.

312 De schijn van echtheid van een in elektronische vorm beschikbaar zijnde verklaring, die op grond van toetsing voldoet aan het *Signaturgesetz*, kan slechts door feiten aangetast worden, die ernstige twijfel doen rijzen dat de verklaring door de gebruiker van de handtekeningsleutel is afgegeven.

verklaring, die op grond van toetsing voldoet aan het *Signaturgesetz*, kan slechts door feiten aangetast worden, die ernstige twijfel geven dat de verklaring door de gebruiker van de handtekeningsleutel is afgegeven. De tweede zin van § 371a *ZPO* derogeert de eerste regel van § 371a *ZPO* en daarmee op § 439 *ZPO* op basis van specialiteit.

Een vraag die zich specifiek aandient voor het *privates elektronisches Dokument* is hoe er omgegaan moet worden met het bewijzen van een gebrek, oftewel een *Mangel* aan een *privates elektronisches Dokument*. Het draait hier in feite om wat ook wel aangeduid zou kunnen worden als een integriteitschending van het document. Zoals reeds in de vorige subparagraaf is aangegeven, ontnemen doorhalingen, etsen, toevoegingen/aanvullingen of overige uiterlijke gebreken de dwingende bewijskracht van de *Urkunde* en beslist het gerecht naar vrije overtuiging.[313] Uit § 371a I eerste zin jo § 419 *ZPO* mag worden afgeleid dat een gebrek tot gevolg heeft dat ook in het geval van een *privates elektronisches Dokument* er geen sprake meer is van dwingende bewijskracht, maar slechts van vrije bewijswaardering door de rechter.

Zoals al eerder gesteld in deze paragraaf vormt de elektronische handtekening een belangrijk element in het constitueren van een *elektronisches Dokument* waaraan dezelfde rechtsgevolgen worden gegeven als de *private Urkunde*. De elektronische handtekening is, net als in de Nederlandse wetgeving, naar aanleiding van Richtlijn 1999/93/EG van het Europees Parlement en de raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen, geïmplementeerd in de Duitse wetgeving middels het *Gesetz über Rahmenbedingungen für elektronische Signaturen* oftewel het *Signaturgesetz* (verder: *SigG*). Nadere eisen zijn gesteld in de Signaturverordnung (SigV). Als gevolg van het feit dat Richtlijn 1999/93/EG zowel in de Nederlandse als in de Duitse wet zijn geïmplementeerd, zijn de functionele eisen die gesteld worden aan de verschillende begrippen in het Nederlandse en Duitse recht hetzelfde. De SigG definieert de elektronische handtekening en de begrippen zoals *Signaturschlüssel, Signaturprüfschlüssel, Zertifikate, Zertifizierungsanbieter*, enzovoorts. De SigV bevat de regels die gesteld worden in de bijlagen van Richtlijn 1999/93/EG.

Zowel de *SigG* als de *SigV* kennen geen bepalingen die de rechtsgevolgen van de elektronische handtekening regelen. De rechtsgevolgen voor het bewijsrecht en het vermogensrecht zijn te vinden in onder andere het *Bürgerliches Gesetzbuch* (*BGB*) en de *ZPO*.[314]

---

313 § 419 ZPO.

314 A. Roβnagel, 'Das neue Recht elektronischer Signaturen', *Neue Juristische Wochenschrift*, 2001-25, p. 1818.

Voor wat betreft het bewijsrecht is het gevolg reeds genoemd: § 371a I *ZPO* stelt dat op een *elektronisches Dokument* ondertekend met een gekwalificeerde elektronische handtekening dezelfde regels van toepassing zijn als voor *private Urkunden.* Hierdoor kan een *elektronisches Dokument* ondertekend met een gekwalificeerde elektronische handtekening dwingende bewijskracht krijgen.

In het *BGB* wordt het rechtsgevolg van de elektronische handtekening in het vermogensrecht duidelijk in § 126a. Indien de wet het schriftelijkheidsvereiste stelt dan kan hieraan ook worden voldaan door gebruikmaking van de elektronische vorm. In dat geval moet de opsteller van het *elektronischse Dokument* deze ondertekenen met zijn naam en deze tevens ondertekenen met een gekwalificeerde elektronische handtekening die voldoet aan het *Signaturgesetz*. Indien het een overeenkomst omvat, dienen beide partijen een gelijkluidend document met een gekwalificeerde elektronische handtekening te ondertekenen.

5.9 De vrije bewijswaardering van elektronische gegevens

5.9.1 De rechtspraak

De jurisprudentie met betrekking tot de waardering van bewijs geeft weinig aanknopingspunten. Toch is er een aantal uitspraken geweest die ingaan op de bewijswaarde van e-mail. Ook zijn er een aantal rechtszaken geweest waar wat wordt gezegd over de bewijslast en het zogenaamde *Anscheinsbeweis*.[315] Deze rechtspraak spitst zich voornamelijk toe op online veilingen, dialers en de juistheid van telefoonrekeningen. Deze zullen in deze paragraaf puntsgewijs besproken worden.

<u>Online veilingen</u>
Online veilingen bieden de mogelijkheid om zaken onder de aandacht van een groot publiek te brengen en dit publiek kan direct van achter een computer bieden op de aangeboden zaak. Een van de problemen van het internet is de mogelijkheid om je anoniem te bewegen of je voor een andere persoon uit te geven. De problematiek bij online veilingen speelt zich vooral af op het gebied van identificatie; er is een winnend bod gedaan, maar als vervolgens contact opgenomen wordt met de bieder, stelt deze zelf het bod niet te hebben gedaan. Een serie van uitspraken betreffende online veilingen laat een eenduidige lijn zien in de bewijsrechtelijke problematiek. In de eerste plaats is het de vraag of er sprake kan zijn van bewijslastomkeer op grond van billijkheid. Deze vraag wordt steevast ontkennend beantwoord. De bewijslast ligt bij de eisende partij

[315] Zie paragraaf 5.6.4.

en een daarvan afwijkende bewijslastverdeling uit billijkheidsgronden is met het oog op de risico's die ten grondslag liggen aan het sluiten van verbintenissen (in de genoemde zaken zijn dit de risico's die het internet met zich meebrengt), niet geboden.[316] Hierbij speelt het argument dat degene die besluit om gebruik te maken van de online veiling, hiervoor ook de risico's dient te dragen.[317]

De tweede vraag die zich vaak aandient is of er een *Anscheinsbeweis* aangenomen mag worden dat de persoon aan wie het password oorspronkelijk is toegekend ook degene is met wie zaken is gedaan. De heersende leer is echter dat hiervoor geen *Anscheinsbeweis* mag worden aangenomen.[318] Het

---

316 OLG Köln 6.9.2002 – 19 U 16/02 (LG Bonn): "Entgegen der Ansicht des Kl. Trägt der Bekl. Nicht allein deshlab, weil er bei G. ein E-Mailkonto mit einem bestimmten Pseudonym und Passwort unterhalten hat, das Missbrauchrisiko mit der Folge einer Beweislastumkehr nach Gefahrenkreisen. Das bloße Unterhalten einer E-mailadresse führt ebenso wenig zur Tragung der Missbrauchsgefahr wie der bloße Besitz einer Kreditkarte zu einer Haftung des Inhabers fürt im Falle der missbräuchlichen Angabe seiner (geheimen) Kreditkartennummer durch einen unbefugten Dritten z.B. im Mailorderverfahren." Het LG Bonn komt tot dezelfde conclusie zij het in andere bewoordingen (19.12.2003 – 2 O 472/03):"Die Beweislast hierfür liegt nach Auffassung des Gerichts bei dem Kl. (…) Eine davon abweichende Verteilung der Beweislast aus Billigkeitsgesichtspunkten ist auch um Hinblick auf die dem Vertragsschluss zu Grunde liegenden Gefahrenbereiche nicht geboten." en "Die Mitgliedschaft in einem Internetauktionshaus mit Mitgliedsnamen und Passwort führt nicht zur Überbürdung der Missbrauchsgefahr auf dieses Mitglied."; zie hiervoor ook: LG Bonn 7.8.2001 – 2 O 450/00 (MMR 4/2002, 255). Zie ook: LG Magdeburg 21.10.2003 – 6 O 1721/03:"Die Beweislast für das Vorliegen aller ansprichsbegründenden Umstände trägt grundsätzlich der Anspruchsteller (…) Entgegen der Ansicht des Klägers trägt der Beklagte nicht allein deshalb, weil er bei eBay ein Konto mit einem bestimmten Passwort unter Verwendung eines Pseudonyms unterhält, des Risiko des Missbrauchs seines Passwortes. Eine Beweislastumkehr nach Gefahrenkreisen kommt daher nicht in Betracht."

317 LG Bonn: Sofortkauf-Option bei eBay (19.12.2003 – 2 O 472/03: "Schließlich ist es gerade der Anbieter, der durch die Präsentation des jeweiligen Produkts auf der Website des Auktionsveranstalters gewissenmaßen der Initiator des Verkaufs ist, der die Vorteile des Internet für seine Zwecke nutzen möchte. Es liegt daher sogar näher, ihm das mit der Nutzung des Internet verbundene Risiko aufzuerlegen, dass Unbefugte unter der Verwendung fremder Passwörter an ihn herantreten". Zie ook: LG Bonn 7.8.2001 – 2 O 450/00 (MMR 4/2002, 255) Dezelfde redenering waarbij risicoverdeling als uitgangspunt voor de bewijslastverdeling geldt, is te vinden in: "OLG Köln: Beweislast für Gebote bei Internetauktion 6.9.2002 – 19 U 16/02.

318 OLG Köln 6.9.2002 – 19 U 16/02 (LG Bonn): "Auch ein Anscheinsbeweis zulasten des Bekl. Is nicht gegeben. Zu Recht und mit zutreffender Begründung hatdas LG den für die Annahme des Anscheinsbeweises typischen Geschehensablauf abgelehnt. Der Sicherheitsstandart imInternet ist, wie jedem, der zich mit dem Datenverkehr befasst, bekannt ist – derzeit nicht ausreichend, um aus de Verwendung eines geheimen Passworts auf denjednigen als Verwender zu schleißen, dem dieses Passwort ursprünglich zugeteilt worden ist. Auf die vom Kl. Dargestellten Probleme einer "Entschlüsselung" des Passworts kommt es in deisem Zusammenhang nicht an. Ein Mussbrauch setzt nämlich eine vorheriger Entschlüsselung gar nicht voraus. Vielmehr kann jemand, der mit Abläufen im Netz aureichend vertraut ist, was heute schon bei einer Vielzahl der Jegendlichen gegeben ist, ohne allzu großen Aufwand das Passwort "lesen". Von einer für einen Anscheinsbeweis ausreichenden Typizität wird man möglicherweise bei der Verwendung einer elektronischen Signatur ausgehen können, nicht aber bei einem ungeschützten Passwort." Zie ook LG Bonn (19.12.2003 – 2 O 472/03):"Ein Anscheinsbeweis für einen Gebotsabgabe durch den Bekl. Besteht ebenfalls nicht (…) Im hinblick auf den derzeitigen Sicherheitsstandard der im Internet verwendeten Passwörter als solche und auf die Art ihrer Verwendung kann nicht der Schluss gezogen werden, dass der Verwender eines Passworts nach der Lebenserfahrung auch derjenige

feit dat een password is gebruikt leidt er niet toe dat met inachtname van alle niet bestreden en vastgestelde omstandigheden en de bijzondere eigenschappen van de feiten en voor de te bewijzen feiten dat het naar levenservaring typisch is dat de conclusie mag worden getrokken dat de gebruiker tevens de persoon is aan wie het password oorspronkelijk is toegekend. Van zo'n typisch gebeurtenissenverloop is volgens de rechter namelijk geen sprake. Hiertoe wordt gesteld dat de zekerheidsstandaard van het internet op dit moment niet groot genoeg is om te mogen stellen dat als een password wordt gebruikt, het bewijsrechtelijke gevolg valt te trekken dat de gebruiker tevens de persoon is aan wie het password oorspronkelijk is toegekend. Wat de rechter hier in feite doet is bij de bewijswaardering stellen dat het systeem van eBay met gebruikersnaam en password (welke verkregen kan worden zonder enige vorm van identificatie) niet voldoende is om de identiteit van een persoon vast te stellen. Opvallend mag misschien wel genoemd worden de toevoeging die het OLG Köln doet door te stellen dat voor het *Anscheinsbeweis* typische gebeurtenissenverloop mogelijkerwijs een elektronische handtekening voldoende kan zijn.[319] Over welk soort elektronische handtekening wordt geen uitspraak gedaan.

Het OLG en de LG-en maken de door hen aangehaalde zekerheidsstandaard ook concreet door in te gaan op het password zelf, de aard van het internet en de risico's waar passwords op internet aan blootstaan:[320] "*Eine einheitliche Definition des Begriffs "Passwort" im Internet gibt es nicht, d.h. es sind keine Maßstäbe für die Verschlüsselung eines Passworts festgelegt. Vielmehr kann jeder beliebige Designer einer Website einen auf seiner Seite einzugebenden begriff Passwort bezeichnen und dann vom Benutzer bei jedem späteren Zugriff die erneute Eingabe verlangen. Auch darüber, wie (sicher) das Passwort bei dem jeweiligen Betreiber "verwaltet" wird, gibt es keine einheitlichen Standarts. Dementsprechend sind aus den Medien hinreichende Beispiele bekannt, in Denen auch als besonders sicher geltende Sicherheitssysteme von unbefugten Dritten überwunden hat, das Passwort von GMX sei "nicht knackbar", hat er diese pauschale Behauptung nicht näher begründet. Sie steht auch in*

---

ist, auf den dieses Passwort ursprünglich ausgestellt wurde." Zie ook LG Bonn 7.8.2001 – 2 O 450/00 (MMR 4/2002, 255):"Ebenso lässt sich im Volliegenden Fall kein Anscheinsbeweis zu Lasten des Bekl. Begründen. Vorrausstzung für die Annahme eines Anschinsbeweises ist, dass sich unter Berücksichtigung aller unstreitigen und festgestellten Einzelumstände und besonderen MErkmale des Sachverhältnis ein für die zu beweisende Tatsache nach de Lebenserfahrung typischer Geschenesablauf ergibt. Eine solche Typizität lässt sich hier jedoch nicht feststellen (…) Im Hinblick auf den derzeitigen Sicherheitsstandard der im Internet verwendeten Paswörter als solche und auf die Art ihrer Verwendung kann nicht der Schluss gezogen werden, dass der Verwender eines Passworts nach der Lebenserfahrung auch derjenige ist, auf den dieses Passwort orsprünglich ausgestellt wurde oder zumindest jemand, dem er die Kenntnis dieses Passworts ermöglicht hat."

319 OLG Köln 6.9.2002 – 19 U 16/02 (LG Bonn): "Von einer für einen Anscheinsbeweis ausreichenden Typizität wird man möglicherweise bei der Verwendung einer elektronischen Signatur ausgehen können, nicht aber bei einem ungeschützten Passwort."

320 LG Bonn 7.8.2001 – 2 O 450/00 (MMR 4/2002, 255).

Widerspruch zu den eigenen Angaben von GMX in deinen online abrufbaren AGB zur Frage der Datensicherheit. Darin weisst GMX ausdrücklich darauf hin, dass nach dem derzeitigen Stand der Technik ein Schutz der übertragenen Daten nicht gewahrleistet werden kann. Auch im weiteren Verlauf des Anmeldevorgangs wird bei der Eingabe der Passwortssicherheitsfrage nochmals darauf hingewiesen., dass es bei zu einfach formulierten Fragen Dritten leichter gelingt, das Passwort zu entschlüsseln. In Anbetracht dessen war dem nur pauschalen Beweisantritt des Kl. Auf Deststellung der Sicherheit des Passworts durch Sachverständigengutachten nicht nachzugeben." De rechter geeft aan dat er geen definitie bestaat van een password en dat er geen standaard bestaat voor passwords. De wachtwoorduitgevende organisatie GMX heeft daarbij zelf ook aangegeven dat de huidige stand van de techniek het niet mogelijk maakt dat data beschermd kan worden verzonden en later wordt er nogmaals op gewezen dat als de controlevragen met te eenvoudige antwoorden zijn te beantwoorden het mogelijk is het password te ontsleutelen. Hier doet de rechter een uitspraak over de zekerheid van het vaststellen van de identiteit van een persoon, welke zekerheid in het onderhavige geval niet voldoende is. De rechter maakt vervolgens een vergelijking met btx:" *Zusätzlich ist ein online verwendetes Passwort weitaus größeren Zugriffsmöglichkeiten Dritter ausgesetzt als das in den Btx-Entscheidungen behandelte "persönliche Kennwort". Letzteres dient dem Aufbau einer Verbindung i.R.d. "Wählvorgangs" und wird daher im Normalfall nur über die zwischen Nutzercomputer und Anbieter aufgebaute Telefonverbindung übermittelt. Demgegenüber wird das hier verwendete Passwort dürch ein globales Computernetz transportiert, zu dem Mio. Von Nutzern weltweit Zugang haben. In dieser Verwendung is es vielfachen Angriffsmóglichkeiten ausgesetzt, kann möglicherweise sogar von Unbefugten abgehört oder aufgezeichnet werden*." De rechter geeft aan dat internet verschilt met btx doordat het internet een open netwerk is waar miljoenen mensen op kunnen inloggen. Hierdoor staat het password bloot aan allerlei mogelijkheden van onderschepping en afluistering. Dit in tegenstelling tot btx waar een een-op-een verbinding tot stand wordt gebracht en het voor derden veel moeilijker is om gegevens te onderscheppen en af te luisteren. De vertrouwelijkheid wordt hiermee in grotere mate gewaarborgd.

E-mail

Veel mensen gebruiken dagelijks e-mail in hun communicatie. Er zijn enkele zaken bekend waarbij een e-mail als bewijsmiddel werd ingezet. De feiten die daarmee getracht werden aan te tonen, zijn van dusdanig verschillende aard, dat er (in tegenstelling tot online veilingen) geen lijn valt te ontdekken. Daarom bespreek ik puntsgewijs de verschillende conclusies uit de rechtspraak.

- Als bewijs voor het feit dat een e-mail is verstuurd door een bepaald persoon, is het voldoende om een kopie van de e-mail te overleggen,

waaruit uit het zendprotocol blijkt dat de e-mail verstuurd is.[321] Twijfel wordt geuit of deze conclusie stand zal houden in hogere instanties, aangezien het zendprotocol eenvoudig kan worden vervalst.[322] Tot op heden is hierover echter geen uitspraak gedaan in hogere instantie.

- De inhoud van een e-mail kan er onder omstandigheden toe leiden dat gestelde feiten als bewezen worden beschouwd. Komt een overeenkomst tot stand, waarbij in voorafgaande e-mails de voorwaarden worden besproken, dan kan een partij later niet terugkomen op de voorwaarden, ook als deze enkel per e-mail zijn overeengekomen.[323]
- Wie een e-mailadres onderhoudt onder een pseudoniem en met password, is niet gebonden aan verklaringen die zijn gedaan onder dit e-mailadres. De zekerheidsstandaard van het internet is niet voldoende om te kunnen stellen dat de gebruiker van het password ook de persoon is aan wie het password oorspronkelijk is toegekend.[324] Op deze uitspraak is kritiek. Critici stellen dat er goede daadwerkelijke, economische en normatieve redenen zijn om een *Anscheinsbeweis* van identiteit te verlenen aan e-mail.[325] De vraag is overigens hoe dit uitwerkt voor e-mailadressen die niet onder een pseudoniem zijn aangemaakt, maar met gebruikmaking van de eigen naam. Ook daarbij is namelijk misbruik mogelijk. Vooralsnog lijkt het erop dat het enkele gebruik van een e-mailadres onder eigen naam er niet toe kan leiden dat geconcludeerd mag worden dat degene wiens naam in het e-mailadres opgenomen is, ook gebonden is aan de verklaring in de e-mail. Daartoe zullen bijkomende omstandigheden nodig zijn (zie vorige punt).

---

321 AG Hannover (Beweis durch Kopie einer E-Mail) 20.12.1999 – 518 C 13916/99. Vergelijk met OLG München (Sendebericht >>OK<< als Anscheinsbeweis:): 8.10.1998 – 15 W 2631/98: Hoewel hier niet direct gesproken kan worden over een analogie met een faxbericht lijkt hier toch eenzelfde soort standaard gehanteerd te worden. Een Ok-opmerking is voldoende voor een Anscheinsbeweis voor het het feit dat de Fax daadwerkelijk verstuurd is naar de ontvangende partij. Zie ook: AG Rudolstadt (Sendebericht als Anscheinsbeweis für Fax-Zugang) 30.3.2004 – 2 C 694/03.

322 E-Mail/Zugangsbeweis/Kopie mit Sendeprotokoll/AG Hannover (http://www.ra-hahn.de/faq-item+M5d66e23afdc.html?&tx_simplfaq_pi1[cat]=27&tx_simplfaq_pi1[faq]=754 – laats geraadpleegd op 12-03-2009) en E-mailbewijskraft (http://www.lexexakt.de/glossar/e-mailbeweiskraft.php - laatst geraadpleegd op 12-03-2009).

323 ArbG Frankfurt/M. (Beweiskraft von E-Mail-Korrespondenz) 9.1.2002 – 7 Ca 5380/01:"Dies stehts für die erkennende Kammer fest auf Grund der zwischen den Parteien vor Formulierung und Abschluss des Aufhebungsvertrages v. 8.12.2000 gewechselten E-Mails. (…) Auf Grund der zwischen den Parteien vor Formulierung und Abschluss des Aufhebungsvertrages v. 8.12.2000 gewechselten E-Mails ist die Kammer der völligen Überzeugung, dass mit der Gehaltszahlung bis zum 28.2.2001 der Zahlung von 16.000 DM netto und der Zahlung von 200 DM bruto alls finanziellen Ansprüche der Partijen aus dem 28.2.2001 beendeten Arbeitsvertrag nach dem Willen der Parteien abgegolten sein sollen."

324 OLG Köln (Beweislast für Gebote bei Internetauktion): 6.9.2002 – 19 U 16/02. Het OLG maakt hier een vergelijking met de creditcard, waarbij het enkele bezit van een kaart niet leidt tot het gebonden zijn aan een verbintenis die door een onbevoegde is gedaan (vaak wordt dit risico afgedekt met een bewijsovereenkomst en /of aansprakelijkheidovereenkomst in combinatie met een verzekering tegen misbruik.)

325 P. Mankowski, 'Für einen Anscheinsbeweis hinsichtlich der Identität des Erklärenden bei E-Mails', *Computer und Recht* 2003-1, p. 44.

Dialerproblematiek

Meerdere zaken hebben zich afgespeeld rond heimelijk geïnstalleerde dialers, oftewel programma's die een modem een telefoonverbinding laten opzetten zonder dat de gebruiker hiervan op de hoogte is. In de meeste gevallen wordt daarbij het door de gebruiker opgeslagen inbelnummer gewijzigd voor een inbelnummer waarvan de kosten meestal hoog liggen. Het resultaat zijn torenhoge telefoonrekeningen.

Als er een meningsverschil bestaat tussen een gebruiker van een telefoonverbinding en de aanbieder van de telefoonverbinding over de rekening, dan doet zich bewijsrechtelijk het volgende voor. De lijnaanbieder heeft ingevolge de *AGB* (*Algemeine Geschäftsbedigungen*; algemene voorwaarden) in combinatie met de gedachte achter *§ 16, abs 3 TKV* (*Telekommunikations-Kundenschutzverordnung*)[326] de bewijslast om aan te tonen dat tot en met de aansluiting van de klant de verbinding technisch correct tot stand gekomen is en juist is berekend. Hoewel deze regeling van oorsprong ziet op 'normale' telefoonverbindingen, heeft het BGH reeds bepaald dat deze regeling ook van toepassing is in gevallen waarin een dialer heimelijk geïnstalleerd is. Vertoont de hiervoor genoemde technische toets gebreken die invloed kunnen hebben gehad op de beweerde vordering, dan wordt een *Anscheinsbeweis* aangenomen dat de verbindingskosten op onjuiste wijze tot stand zijn gekomen.[327] Dit *Anscheinsbeweis* kan echter weerlegd worden doordat de abonnee aantoont dat er heimelijk een dialer geïnstalleerd is op zijn computer.[328] Hierdoor is er niet langer sprake van een typisch verloop van gebeurtenissen, maar van een a-typisch verloop van gebeurtenissen, zodat het Anscheinsbeweis wordt doorbroken. Overigens moet de gebruiker van de telefoonverbinding aantonen dat er zich een dialer op de computer bevindt. Het enkel stellen dat er zich een dialer op de computer bevindt is niet voldoende.[329] Tevens stelt het BGH dat een abonnementhouder geen voorzorgen hoeft te treffen tegen dialers, zolang geen concrete aanwijzing

---

326 § 16 Abs 3: Dem Anbieter obliegt der Nachweis, die Leistung bis zu der Schnittstelle, an der der allgemeine Netzzugang dem Kunden bereitgestellt wird, technisch einwandfrei erbracht und richtig berechnet zu haben. Ergibt die technische Prüfung Mängel, die die beanstandete Entgeltermittlung beeinflußt haben könnten, wird widerleglich vermutet, daß die Verbindungsentgelte des Anbieters unrichtig ermittelt sind. Ist der Nachweis erbracht, daß der Netzzugang in vom Kunden nicht zu vertretendem Umfang genutzt wurde, oder rechtfertigen Tatsachen die Annahme, daß die Höhe der Verbindungsentgelte auf Manipulationen Dritter an öffentlichen Telekommunikationsnetzen zurückzuführen ist, ist der Anbieter nicht berechtigt, die betreffenden Verbindungsentgelte vom Kunden zu fordern.

327 In § 16, Abs 3 TKV wordt gesproken over "wird widerleglich vermutet". Daarentegen wordt in BGH, Urt. V. 4.3.2004 – III ZR 96/03 (KG) gesproken over een Anscheinsbeweis. Dit zou kunnen liggen aan het feit dat slechts de rechtsgedachte van § 16, Abs 3 TKV in acht wordt genomen.

328 BGH, Urt. V. 4.3.2004 – III ZR 96/03 (KG) Zie ook: LG Stralsund v. 22.2.2006 – 1 S 237/05, CR 2006, 616.

329 AG Karlsruhe 24.5.2005 – 5 C 35/05; AG Leer 30.5.2006 – 7d C 8/06; AG Bühl 30.9.2003 – 3 C 260/03.

bestaat dat misbruik zal optreden.[330] Met het feit dat de abonnementhouder geen voorzorgen hoeft te treffen tegen dialers, zolang er geen concrete aanwijzing bestaat dat misbruik zal optreden, zet het *Bundesgerichtshof* een streep door wat *amtsgerichten* en *landesgerichten* eerder hebben bepaald. Deze bepaalden namelijk dat de abonnementhouder er onder alle omstandigheden voor zorg dient te dragen dat er geen dialer kan worden geïnstalleerd en dat als dit toch gebeurt deze voor de daaruit voortvloeiende kosten dient op te draaien.[331]

Of het *Anscheinsbeweis* ook in het algemeen kan worden vertaald naar virussen, trojan horses en andere vormen van malware en andere vormen van schade, is maar geheel de vraag. Wat betreft virussen, trojan horses en andere vormen van malware zou te verdedigen zijn dat als deze heimelijk geïnstalleerd zouden zijn, de abonnementhouder ook niet de kosten van ongewilde verbindingen hoeft te vergoeden. Het betreft namelijk allemaal heimelijk geïnstalleerde computerprogramma's. Of dit ook opgaat voor andere vormen van schade is maar de vraag. In de rechtspraak gaat het namelijk specifiek om het totstandkomen van ongewilde verbindingen en niet om andere vormen van schade. Tevens wordt er steevast een beroep gedaan op § 16 Abs 3 TKV. In andere gevallen, bijvoorbeeld als een programma schade heeft veroorzaakt aan andermans computer, gaat het niet meer om telecomverbindingen en is § 16 Abs 3 niet van toepassing. Pas als zich een concreet geval voordoet en een rechter zich hierover buigt, zal meer duidelijk worden. Vooralsnog kan hier dan ook geen algemene regel uit worden afgeleid.

5.9.2 De bewijswaardering van code

De bewijswaardering van code in het Duitse recht is onbekend. Code wordt dan wel toegelaten als *Augenscheinsbeweis*,[332] maar hoe deze gewaardeerd dient te worden blijft onzeker. Op grond van het reeds in paragraaf 5.5.1 verdedigde standpunt dat ook code als *elektronisches Dokument* kan worden gekwalificeerd, zou gesteld kunnen worden dat code op grond van § 371a ZPO code ook dwingende bewijskracht kan toekomen, mits deze is ondertekend met een gekwalificeerde elektronische handtekening.

Is dit laatste niet het geval dan zal de code nog steeds toegelaten worden als *Augenscheinsbeweis*, maar vervolgens bij de bewijswaardering onder de vrije bewijswaardering van § 286 ZPO vallen. Mocht dit laatste het geval zijn, dan zou de rechtspraak hierover iets kunnen zeggen. Een aanknopingspunt daarbij

330 BGH, Urt. V. 4.3.2004 – III ZR 96/03 (KG).

331 AG Dillenburg, Urt. V. 13.9.2003 – 5 C 286/02, LG Nürnberg, Urt. V. 27.3.2003 – 11 S 8162/02 (AG Fürth, Urt. V. 13.6.2002 – 310 C 572/02).

332 Paragraaf 5.5.1.

zijn de zaken waarbij de dialerproblematiek een rol speelt. Daarbij wordt namelijk code geactiveerd die de computer opdrachten geeft tot het totstandbrengen van verbindingen met een andere computer.[333] In de rechtspraak betreffende de dialerproblematiek wordt gebruik gemaakt van experts die verklaren of tot en met de aansluiting van de klant de verbinding technisch correct tot stand gekomen is en juist berekend is. In de uitspraken wordt echter niet duidelijk op welke wijze zij tot deze conclusie zijn gekomen. Door het ontbreken van een antwoord op de vraag hoe aangetoond kan worden hoe een systeem technisch correct heeft gewerkt bij het totstandkomen van een verbinding en de berekening van de kosten, is niet duidelijk hoe een rechter bij gebruikmaking van zijn bevoegdheid tot het vrij waarderen van het bewijs tot de conclusie is gekomen dat code als voldoende betrouwbaar kan worden gewaardeerd.

5.9.3 De bewijswaardering van data

Zowel door mensen gegenereerde data als computer gegenereerde data wordt toegelaten als *Augenscheinsbeweis* en indien voorzien van een gekwalificeerde elektronische handtekening, zijn de regels van de *private Urkunde* met handtekening van toepassing. In dat geval krijgt de data dwingende (formele) bewijskracht.

Het overgrote deel van de data is echter niet voorzien van een gekwalificeerde elektronische handtekening. Dit doet niets af aan de toelaatbaarheid van data als *Augenscheinsbeweis*. Het heeft enkel gevolgen voor de bewijswaardering die niet dwingend is, maar op grond van § 286 ZPO vrij is. Aangezien de wet in deze gevallen geen betrouwbaarheidscriteria formuleert, zullen aanknopingspunten in de rechtspraak gezocht dienen te worden.

De rechtspraak is niet expliciet in het beoordelen van de bewijskracht van data. In het enkele geval dat er wel een expliciete uitspraak wordt gedaan over de bewijskracht van data dan gaat het om door mensen gegenereerde data waarbij verklaringen en de gebondenheid aan deze verklaringen een belangrijke rol spelen. Het volgende valt te concluderen. Voor wat betreft de identificatie van personen bestaat er geen *Anscheinsbeweis* dat de persoon van wie een e-mailadres is of die een eBay-account heeft, ook degene is die de e-mail heeft gestuurd of een bod heeft gedaan vanaf dat account. De veiligheidsstandaard is namelijk niet hoog genoeg. Echter, gevallen waarbij ook andere omstandigheden een rol spelen, zoals de kennis die partijen hebben bij het schrijven van de e-mail, de elektronische communicatie die partijen hadden en/of de communicatie ondertekend was door partijen, kunnen wel als

[333] Zie subparagraaf 5.9.1.

voldoende betrouwbaar worden geacht om er bewijskracht aan toe te kennen en gestelde feiten als bewezen te kunnen verklaren.[334] Het komt aan op verschillende omstandigheden die in hun onderlinge samenhang tot de conclusie kunnen leiden dat de data voldoende betrouwbaar is. Een enkel element lijkt vooralsnog onvoldoende gewicht te kunnen geven aan de conclusie dat data als bewijsmiddel als voldoende betrouwbaar kan worden beoordeeld.

5.10 De bewijsovereenkomst

5.10.1 Inleiding

Zoals al reeds is gesteld in paragraaf 4.15 is de bewijsovereenkomst een middel om de bewijspositie van partijen te regelen reeds voordat er een geschil ontstaat over de feiten. De bewijsmiddelen om de feiten te bewijzen zijn dan reeds via contractuele weg geregeld. Hoewel de bewijsovereenkomst niet ingrijpt op het bewijsmiddel zelf, maar op de contractuele verhoudingen tussen partijen, is het wel een middel om de bewijspositie van partijen te beïnvloeden en daarmee kan de bewijsovereenkomst wel degelijk een niet onbelangrijke rol spelen in het bewijsrecht.

Ondanks het feit dat het uitgangspunt zowel in het Nederlandse als in het Duitse recht is dat partijen vrij zijn om binnen de grenzen van de wet hun eigen contractuele verhoudingen te regelen, blijkt er toch een belangrijk verschil te bestaan voor wat betreft de bewijskrachtovereenkomst. Dit verschil is niet zozeer een gevolg van het overeenkomstenrecht, maar vloeit voort uit de grenzen van de wet en betreft de bewijskrachtovereenkomst. In paragraaf 5.10.2 zal ik hierop nader ingaan.

5.10.2 Definitie bewijsovereenkomst

De bewijsovereenkomst wordt in de Duitse wet niet nader gedefinieerd. Ook in de literatuur lijkt men geen definitie nodig te hebben om te kunnen bepalen wat een bewijsovereenkomst is. Wel wordt in de literatuur duidelijk dat de bewijsovereenkomst species van het genus procesovereenkomst is.[335]

---

334 Dit is overigens ook de lijn die in het Amerikaanse (civiele) bewijsrecht wordt aangehouden.

335 K. Schellhammer, *Zivilprozess, Gesetz – Praxis – Fälle*, Heidelberg: C.F. Müller Verlag, 2004, p. 604 en 605, nr. 1280 t/m 1283.

Het P*rozessvertrag* is ein *Vertrag über prozessuale Rechtsfolgen*[336] of wordt ook wel omschreven als *vereinbarungen zwischen (zukunftige) Parteien eines Rechtsstreits mit Auswirkungen auf den Rechtsstreit*.[337] Onder de *prozessuale Rechtsfolgen* en de *Rechtsstreit* vallen ook de rechtsgevolgen welke onder het bewijsrecht vallen, daar het bewijsrecht onderdeel uitmaakt van het civiele procesrecht.

Er zijn echter grenzen aan de toelaatbaarheid van *Prozessverträge*. Zo gelden de bepalingen in het overeenkomstenrecht onverkort.[338] Een *Prozessvertrag* is namelijk een overeenkomst en is daarmee onderhevig aan de regels die gelden in het overeenkomstenrecht. Tevens worden de grenzen aan de vrijheid tot het sluiten van *Prozessverträge* gevormd door de *ZPO* en de dispositionsvrijheid van de partijen.

In de eerste plaats worden deze grenzen gesteld door de *ZPO* zelf. De *ZPO* regelt een aantal *Prozessverträge* zoals: het *Prorogationsvertrag* (§ 38 *ZPO*), het Schiedsvertrag (§ 1032 *ZPO* en § 1042 *ZPO*), de *vertragliche Unterwerfung untern die sofortige Zwangsvollstreckung* (§ 794 I nr. 1 *ZPO*), de *Streitgegenstand* (§ 794 I nr. 5 *ZPO*) en de *Art und Höhe der Sicherheitsleistung* (§ 108 *ZPO*).

In de tweede plaats worden grenzen aan de toelaatbaarheid van het *Prozessvertrag* gesteld door het dispositionsbeginsel. Zo kunnen partijen bijvoorbeeld contracteren over het *Klageverzicht*, [339] het *Rücknahmeversprechen*, [340] *Rechtsmittelverzicht*, [341] *Versprechen Rechtsmittel zurück zu nehmen*,[342] en *Versprechen vor Rechtskraft nicht zu vollstrecken*.[343]

Nu vallen, zoals reeds gesteld, bewijsovereenkomsten onder de zojuist besproken *Prozessverträge*. Of een bewijsovereenkomst toelaatbaar is, moet worden beoordeeld naar bovenstaande grenzen die aan *Prozessverträge* gesteld worden. Als eerste zal onderzocht moeten worden of de toelaatbaarheid van het *Beweisvertrag* in de *ZPO* wordt toegestaan. De *ZPO* zwijgt echter in alle toonaarden over *Beweisverträge* en ook uit de structuur en gehanteerde bewoordingen in de *ZPO* valt niet op te maken of het *Beweisvertrag* toelaatbaar is.

---

336 BGH pp, 143.

337 R. Oberheim, *Zivilprozessrecht für Refendare*, Neuwied: Werner Verlag 2007, p. 12, nr. 24.

338 L. Rosenberg, K.H. Schwab, P. Gottwald, *Zivilprozessrecht*, München, C.H. Beck 1993, p. 421; K. Schellhammer, *Zivilprozess, Gesetz – Praxis – Fälle*, Heidelberg: C.F. Müller Verlag 2004, p. 604, nr. 1280.

339 BGH NJW 82, 2072 (Het al dan niet afzien van een proces.).

340 BGH 20, 205 (Het al dan niet terugnemen van stellingen.).

341 BGH NJW 86, 198 (Het al dan niet afzien van het gebruik van bepaalde rechtmiddelen.).

342 BGH NJW 84, 805 (Het al dan niet intrekken van bepaalde rechtsmiddelen.).

343 BGH NJW 68, 700 (Het al dan niet afdwingen van afdwingbare rechten.).

De tweede mogelijkheid voor het toelaten van *Beweisverträge* is het dispositionsbeginsel, waarbinnen *Beweisverträge* toegestaan zijn. De vrijheid van partijen om te beschikken over hun eigen proces,[344] laat het toe om ook op een aantal gebieden van het bewijsrecht overeenkomsten aan te gaan. Deze zullen hieronder nader besproken worden.

5.10.3 De inhoud van de bewijsovereenkomst

Ad 1: Bewijsmiddelenovereenkomst
De bewijsmiddelenovereenkomst is de overeenkomst waarbij partijen middels contractuele weg bewijsmiddelen kunnen toelaten of uitsluiten om het bestaan of niet bestaan van feiten aan te tonen. Het Duitse recht kent vijf wettelijke bewijsmiddelen (*Augenscheinsbeweis, Urkundenbeweis, Sachverständigenbeweis, Zeugenbeweis, Parteivernehmung*; zie paragraaf 5.5) die worden toegelaten als bewijsmiddel. De *ZPO* zwijgt over de bewijsmiddelenovereenkomst. Het dispositionsbeginsel geeft partijen echter de ruimte om te bepalen dat bewijsmiddelen door partijen worden uitgesloten.[345] Ook is het aannemelijk dat niet wettelijke bewijsmiddelen, die normaal niet worden toegelaten, toch worden toegelaten als partijen dit hebben bepaald in een bewijsovereenkomst. Er zijn namelijk geen wettelijke beperkingen en ook komt het toelaten van bewijsmiddelen niet in strijd met de wet.

Ad 2: Bewijskrachtovereenkomst
De bewijskrachtovereenkomst regelt de waardering van het bewijs door de rechter. De bewijskrachtovereenkomst schrijft de rechter dan voor hoe bepaalde bewijsmiddelen moeten worden gewaardeerd; wordt er dwingende bewijskracht toegekend aan bepaalde bewijsmiddelen of wordt de dwingende bewijskracht juist van bewijsmiddelen afgenomen.

In tegenstelling tot het Nederlandse recht, heeft een bewijskrachtovereenkomst in het Duitse recht geen rechtskracht. Een bewijskrachtovereenkomst komt namelijk in strijd met § 286 *ZPO* die de rechter de bevoegdheid geeft om het bewijs naar vrije overtuiging te waarderen.[346] Partijen mogen wel bepalen welke feiten zij als waar aannemen en welke de rechter als waar aan moet nemen (dit valt onder het dispositiebeginsel) en hierin is de rechter lijdelijk, maar de rechter

---

344 Zie hiervoor paragraaf 5.3.1.
345 BGH WM 73, 144.
346 RG 96, 59; zie ook: L. Rosenberg, K.H. Schwab, P. Gottwald, *Zivilprozessrecht*, München, C.H. Beck 1993, p. 658. K. Schellhammer, *Zivilprozess, Gesetz – Praxis – Fälle*, Heidelberg: C.F. Müller Verlag 2004, p. 260, nr. 557.

voorschrijven hoe hij het bewijs moet waarderen, is in strijd met de wet.[347] De waardering van bewijs is echter een autonome bevoegdheid van de rechter en daarin is hij niet lijdelijk.[348]

Dat het voor partijen geen nut heeft om een bewijskrachtovereenkomst af te sluiten, omdat de rechter hier niet aan gebonden is, lijkt mij niet geheel onlogisch. Niet alleen komt zo'n overeenkomst in strijd met een wettelijke bepaling, maar doorbreekt tevens het beginsel dat alleen partijen gebonden zijn aan de overeenkomst. Met een bewijskrachtovereenkomst zouden zij namelijk niet alleen zichzelf binden, maar ook de rechter, die in feite geen partij is bij de overeenkomst. Gesteld zou kunnen worden dat dit ook het geval is bij de bewijsmiddelenovereenkomst, de bewijslastovereenkomst en overeenkomsten die op het tegenbewijs zien. Deze drie overeenkomsten grijpen echter niet in op de taak van de rechter en binden de partijen onderling. De rechter zal bij die drie overeenkomsten alleen zorg dragen voor het naleven van die overeenkomst, maar deze overeenkomsten grijpen niet in in de taken van de rechter.

Ad 3: Bewijslastovereenkomst
De bewijslastovereenkomst grijpt in in de wettelijke verdeling van de bewijslast. De bewijslastovereenkomst is in het Duitse recht toegestaan.[349] Partijen kunnen overeenkomen om van de wettelijke bewijslastverdeling af te zien en de bewijslast bij de andere partij te leggen.

Net als in het Nederlandse burgerlijke wetboek kent het *BGB* een bijzondere regeling voor algemene voorwaarden die bepalingen met betrekking tot de bewijslast bevatten. § 309 Nr. 12 BGB stelt: *"Auch soweit eine Abweichung von den gesetzlichen Vorschriften zulässig ist, ist in Allgemeinen Geschäftsbedingungen unwirksam eine Bestimmung, durch die der Verwender die Beweislast zum Nachteil des anderen Vertragsteils ändert, insbesondere indem er a) diesem die Beweislast für Umstände auferlegt, die im Verantwortungsbereich des Verwenders liegen, oder b) den anderen Vertragsteil bestimmte Tatsachen bestätigen lässt; Buchstabe b gilt nicht für Empfangsbekenntnisse, die gesondert unterschrieben oder mit einer gesonderten qualifizierten elektronischen Signatur versehen sind;"* Ook voor zover een afwijking van de wettelijke voorschriften toelaatbaar is, is een bepaling in algemene voorwaarden *unwirksam* die door de gebruiker de bewijslast in het nadeel van de wederpartij wijzigt, in het bijzonder als a) hij aan hem de bewijslast oplegt die in het verantwoordingsbereik van de

347 E. Schilken, Zivilprozessrecht, Köln/Berlin/München, Carl Heymanns Verlag GmbH 2006, p. 214, nr. 393.
348 K. Schellhammer, *Zivilprozess, Gesetz – Praxis – Fälle*, Heidelberg: C.F. Müller Verlag 2004, p. 260, nr. 557.
349 RG 96, 57 .

gebruiker liggen of b) hij de andere partij bepaalde feiten laat bevestigen. Onderdeel b geldt niet voor ontvangstbevestigingen die apart ondertekend zijn of met een afzonderlijke gekwalificeerde elektronische handtekening ondertekend zijn.

§ 309 Nr. 12 *BGB* kan van belang zijn voor het geval waarin gebruikers via elektronische weg onderhandelen en bij algemene voorwaarden hun bewijspositie proberen te regelen. In dat geval is het niet mogelijk om de bewijslast om te keren (onder a) of de wederpartij de feiten te laten bevestigen, tenzij er sprake is van een ontvangstbevestiging die apart is ondertekend (met een gekwalificeerde elektronische handtekening).

Ad 4: Tegenbewijs
Reeds in subparagraaf 4.15.3 is vastgesteld dat overeenkomsten die het tegenbewijs betreffen, slechts zien op de bewijsmiddelenovereenkomst en de bewijskrachtovereenkomst en niet de omkering van de bewijslast. Nu het Duitse recht enkel de bewijsmiddelenovereenkomst en in beperkte mate de bewijslastovereenkomst toelaatbaar acht, zal een overeenkomst die ziet op het tegenbewijs, slechts kunnen zien op het toelaten en uitsluiten van tegenbewijs en de bewijslast en niet op het regelen van de bewijskracht van bewijsmiddelen van de tegenpartij.

5.11 Samenvatting en conclusie

5.11.1 Samenvatting

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 *Dispositionsmaxime* 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), *Zeugenbeweis* (getuigenbewijs) *Sachverständigenbeweis* (deskundigenbewijs), *Urkundenbeweis* (akten) en *Parteivernehmung* (getuigenis door de procespartijen).

Als een bewijsmiddel 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. 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.

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.

5.11.2 Conclusie

Elektronische gegevens als bewijsmiddel kennen twee toetsingsmomenten. In de eerste plaats de toelatingsfase en in de tweede plaats de bewijswaarderingsfase.

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.

Eenmaal toegelaten code en data moet bewijskracht worden toegekend wil het van invloed kunnen zijn als bewijsmiddel. Hierbij kan er sprake zijn van dwingende bewijskracht of vrije bewijswaardering door de rechter. 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. In de rechtspraak blijft de bewijswaardering van code onduidelijk. 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.

6 Elektronische gegevens als bewijsmiddel in het Amerikaanse civiele recht

6.1 Inleiding

In dit hoofdstuk wordt onderzocht welke eisen het Amerikaanse recht stelt aan elektronische bewijsmiddelen. In de twee vorige hoofdstukken is gebleken dat vooral de dwingende bewijskracht van aktes en *Urkunden* en de eisen die gesteld worden aan de elektronische handtekening een grote rol spelen bij het bepalen welke criteria in het Nederlandse en Duitse recht van belang zijn voor de bewijswaarde van elektronische documenten. Het Amerikaanse recht kent een andere traditie van bewijsrecht. Er wordt op geheel eigen wijze tegen bewijsmiddelen aangekeken en dit heeft vanzelfsprekend consequenties voor de manier waarop met bewijsmiddelen wordt omgegaan. De benadering van het Amerikaanse recht is een meer kwalitatieve benadering: voordat bewijsmiddelen worden toegelaten, worden deze getoetst aan een vijftal kwalitatieve eigenschappen. Als hieraan niet wordt voldaan, wordt het bewijsmiddel niet toegelaten. Dit hoofdstuk omvat dan ook voor het grootste deel onderzoek naar deze vijf eisen die aan bewijsmiddelen gesteld worden. De focus zal daarbij uiteraard liggen op elektronische bewijsmiddelen.

In paragraaf 6.2 wordt de plaats van het Amerikaanse civiele bewijsrecht geschetst. Aangezien het Amerikaanse bewijsrecht (*common law* traditie) geheel anders is ingericht dan het Nederlandse en Duitse bewijsrecht (*civil law* traditie) zullen de belangrijkste verschillen worden belicht. Ook is aandacht voor de plaats van het civiele bewijsrecht binnen het Amerikaanse recht en de verhouding tot het strafbewijsrecht en administratieve bewijsrecht. Juryrechtspraak heeft een grote invloed gehad op de inrichting van het civiele bewijsrecht. Omdat die invloed zo bepalend is geweest op die inrichting, besteed ik in paragraaf 6.3 enige aandacht aan de rol van juryrechtspraak en de gevolgen daarvan voor de inrichting van het bewijsrecht. Paragraaf 6.4 zal de voor het Amerikaanse bewijsrecht belangrijke fase van bewijstoelating inleiden waarna in paragraaf 6.6 tot en met paragraaf 6.9 de vijf eisen worden besproken waaraan bewijsmiddelen moeten voldoen. In paragraaf 6.6 is eerst aandacht voor de *relevance rule* en de *exclusion rule*. Hoewel deze *rules* in de literatuur toch vaak afzonderlijk worden behandeld, zijn deze in dit onderzoek in één paragraaf ondergebracht. Beide kennen voor dit onderzoek namelijk een beperking: de eisen zijn relatief en daarom vallen hieruit geen harde eisen voor

de kwaliteiten van elektronische bewijsmiddelen te destilleren. Paragraaf 6.7 gaat in op de *hearsay rule*. Deze regel verbiedt in beginsel verklaringen die gedaan zijn buiten de rechtszaal toe te laten. Op deze regel bestaat een groot aantal uitzonderingen. Voor elektronische bewijsmiddelen zal onderzocht worden op welk soort verklaringen de *hearsay rule* van toepassing is en welke uitzonderingen gemaakt worden. Daarna zal in paragraaf 6.8 worden ingegaan op misschien wel de belangrijkste regel voor elektronische bewijsmiddelen, namelijk de *authentication rule*. Deze regel stelt dat bewijsmiddelen geauthentificeerd moeten worden, voordat ze als bewijs worden toegelaten. Wat dit inhoudt en volgens welke methoden bewijsmiddelen geauthentificeerd kunnen worden, zal nader worden onderzocht. Kenmerkend is dat elektronische bewijsmiddelen eigen methoden van authentificatie kennen. Deze zullen dan ook worden geïnventariseerd. Vervolgens zal in paragraaf 6.9 de *best evidence rule* worden beschouwd. Deze regel gaat uit van de opvatting dat alleen het bewijs met de beste kwaliteiten, het meest oorspronkelijke bewijs, mag worden toegelaten, tenzij er redenen zijn om duplicaten of overig bewijs toe te laten. Hoewel deze regel in het recente verleden is aangepast in verband met problemen met het toelaten van elektronische gegevens als bewijsmiddel, zou deze regel mogelijk toch nog steeds problemen kunnen geven bij het toelaten van elektronische gegevens als bewijsmiddel. Hierbij zou in het bijzonder de toelating van code problematisch zijn. Nadat de eisen voor bewijstoelating zijn besproken zal in paragraaf 6.11 kort ingegaan worden op de bewijswaardering. Ook de bewijsovereenkomst kan een rol spelen bij het verbeteren van de bewijspositie. Daarom wordt in paragraaf 6.12 enige aandacht geschonken aan de bewijsovereenkomst. Dit beperkt zich echter tot de inhoud van de bepalingen betreffende bewijsrecht; er zal niet ingegaan worden op de totstandkoming van de bewijsovereenkomst. Tenslotte bevat paragraaf 6.13 een samenvatting van dit hoofdstuk en de conclusies.

6.2 Plaats van het Amerikaanse civiele bewijsrecht

Het civiele Amerikaanse bewijsrecht kent met haar *common law* traditie een aantal specifieke kenmerken waarmee het zich onderscheidt van het Nederlandse en het Duitse bewijsrecht welke beide een *civil law* traditie hebben. Een van de kenmerken waarmee het Amerikaanse bewijsrecht zich onderscheidt, is de plaats die zij inneemt in het Amerikaanse recht. Het Amerikaanse federale bewijsrecht is geregeld in de *Federal Rules of Evidence* (*FRE*). Deze hebben zowel betrekking op het civiele recht als op het strafrecht.[350] Dit in tegenstelling tot het Nederlandse en Duitse bewijsrecht, dat voor civiele en strafrechtelijke zaken afzonderlijk geregeld is in respectievelijk het Wetboek van Burgerlijke Rechtsvordering / *die Zivilprozessordnung* en het

[350] Rule 1101(b) FRE.

Wetboek van Strafvordering / *die Strafprozessordnung*. Echter, specifieke regels binnen de *FRE* zijn slechts van toepassing op alleen civiele procedures of strafrechtelijke procedures.[351]

Een tweede kenmerk is dat het bewijsrecht in Amerika niet eenduidig is geregeld voor alle vijftig staten en het district Colombia. Als gevolg van de federale structuur van Amerika hebben de staten autonome zeggenschap over de bewijsregels die zij hanteren. Ondanks dat het bewijsrecht niet eenduidig is geregeld en niet op federaal niveau geregeld mag worden, hanteren veel staten de *Uniform Rules of Evidence* (*URE*) of een aangepaste variant daarvan. In de eerste plaats tracht men zo te komen tot een harmonisering van het bewijsrecht zodat het overeenstemt met het bewijsrecht van andere staten. In de tweede plaats tracht men zo de ongewenste situatie te voorkomen dat procedures in hoger beroep voor de zogenaamde *circuit courts* en *federal courts* op grond van andere bewijsregels worden beoordeeld dan in eerste instantie waarbij de statelijke bewijsregels van toepassing waren.[352] Hoewel de staten dus vrij zijn in het hanteren van eigen bewijsregels die van de URE of FRE afwijken, bestaat er een uniforme regeling op federaal niveau. Op dit niveau is het bewijsrecht geregeld in de reeds genoemde *Federal Rules of Evidence*.[353] In het kader van dit onderzoek zal ik mij verder beperken tot de *FRE*, omdat deze regels van toepassing zijn op de federale rechtbanken en gezien het feit dat het merendeel van de staten in Amerika de van de *FRE* afgeleide *URE* hebben geïmplementeerd in hun wetgeving.[354]

Voor dit onderzoek is enkel van belang dat de *FRE* van toepassing zijn op civiele procedures voor de federale rechtbanken (en door middel van implementatie van de *URE* in veel gevallen ook op civiele procedures voor lagere rechtbanken in de verschillende staten.

6.3 Juryrechtspraak

Het Amerikaanse rechtssysteem kent van oudsher juryrechtspraak, die zowel in het strafproces als in het civiele proces plaatsvindt. Het recht op een juryproces is voor het strafrecht en het civiele recht verschillend tot stand gekomen en geregeld. Voor het strafproces is dit geconstitueerd in art. 3 van de *United*

---

351 Bijvoorbeeld Rule 609 FRE.

352 De *Uniform Rules of Evidence* maken deel uit van een groot aantal modelwetten die zijn opgesteld om de wetgeving van de verschillende staten te uniformeren.

353 PUBLIC LAW 93-595; 88 STAT. 1926 Approved Jan. 2, 1975 [H.R. 5463] / Federal Rules of Evidence, Title 28 U.S.C.

354 Op 1 februari 2010 hanteerden 38 staten de Uniform Rules of Evidence (bron: http://www.law.cornell.edu/uniform/evidence.html).

States Constitution.[355] Het recht op een juryproces in het civiele recht bestaat minder lang dan het recht op een jury in het strafrecht en is opgenomen in het zevende amendement van de *United States Constitution*. Deze stelt: *"In Suits at Common Law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved, and no fact tried by a jury, shall be otherwise re-examined in any Court of the United States, than according to the rules of the Common Law.*" Met het zevende amendement van de *United States Constitution* lijkt het alsof ieder geschil dat een waarde van twintig dollar overstijgt middels een juryproces kan worden beslecht. Dit is echter niet het geval, omdat het amendement ook de regels van *common law* noemt. *Common law* zoals bedoeld in de *United States Constitution* staat in dit verband niet tegenover *civil law*, maar tegenover het zogenaamde *equity*. Het onderscheid tussen *common law* en *equity* is een onderscheid dat lange tijd wordt gemaakt in het Engelse en Amerikaanse recht, maar reeds in Engeland sinds 1852 en Amerika in 1938 aan betekenis grotendeels heeft ingeboet.[356] Toch is het onderscheid voor het beoordelen of er recht op juryrechtspraak bestaat nog steeds van belang.

Common law bestaat uit de jurisprudentie welke door middel van precedentwerking van reeds gedane uitspraken een stelsel van recht vormt. *Equity* kan grofweg worden beschouwd als een vorm van recht, dat wordt ingezet als toepassing van *common law* tot onrechtvaardige uitkomsten leidt.[357] Ondanks het zevende amendement van de *United States Constitution* bestaat er daarom niet altijd recht op rechtspraak door een jury.[358] Of er sprake

---

355 *Art. 3, Section 2, Clause 3 United States Constitution: "The Trial of all Crimes except in Cases of Impeachment, shall be by Jury; and such Trial shall be held in the State where the said Crimes shall have been committed; but when not committed within any State, the Trial shall be at such Place or Places as the Congress may by Law have directed." 17 september 1787.*

356 Het onderscheid verdween in Engeland fragmentarisch door invoering van *The Chancery Procedure Act (1852), The Common Law Procedure Act (1854), The Court of Probate Act (1857)* en de belangrijke *Judicature Acts (1873 – 1875)*. In 1938 verdween ook dit onderscheid in Amerika met de invoering van de *Civil Rules of Civil Procedure*.

357 D.L.A. Barker, C.F. Padfield, *Law*, Oxford: Made Simple Books 2001, p. 12 en 13.

358 Het Amerikaanse recht heeft een nauwe band met het Engelse recht. Als kolonie van Engeland viel Amerika lange tijd rechtstreeks onder jurisdictie van Engeland. Nadat dertien vertegenwoordigers in 1776 de door Thomas Jefferson opgestelde Declaration of Independence hadden aangenomen en Amerika een autonoom soeverein land werd, is het wel blijven putten uit het grote reservoir van Engelse jurisprudentie. Ook bij de inrichting van het stelsel van rechtbanken is de Engelse traditie lange tijd voortgezet en zijn veranderingen in Engeland zelfs regelmatig gevolgd. De verdeling in common law en equity die in Engeland bestond is dan ook na de onafhankelijkheid voortgezet in Amerika. In de verdeling in common law en equity is de oorsprong in de verdeling tussen juryrechtspraak en rechtersrechtspraak te vinden. Common law kende namelijk juryrechtspraak; equity daarentegen was rechtersrechtspraak. Common law en equity werden door verschillende instanties behandeld. Hieraan kwam in Engeland in 1848 een einde met de Judicature Acts waarin werd bepaald dat zowel common law als ook equity door één instantie konden worden toegepast. Dezelfde stap werd in Amerika gezet in 1938. Hoewel common law en equity tegenwoordig worden toegepast in één instantie, is het onderscheid nog steeds van belang om te bepalen of er sprake is van juryrechtspraak of rechtersrechtspraak. Zie: D.L.A. Barker, C.F. Padfield, *Law*, Oxford: Made Simple Books 2001, p. 8 t/m 20. Zie ook: J.L. Wright, M.M. Williams,

is van het recht op een jury moet volgens de *United States Supreme Court* worden beoordeeld aan de hand van het antwoord op de vraag of er onder *common law* van 1791 uit Engeland recht bestaat op een jury.[359] Dit is het geval in zaken die onder *common law* beoordeeld werden; *equity* en *admirality law* vallen hier niet onder. Gezien het feit dat *common law* geen statisch recht is, maar de rechtsnormen steeds aan veranderingen onderhevig zijn,[360] vallen hieronder ook "*to statutory clauses of action analogous to common law causes of action ordinarily decided in English law courts in the late 18th century, as opposed to those customarily heard by courts of equity or admirality*".[361]

Om te bepalen of een zaak onder *common law* of onder *equity* valt, zal altijd de materiële inhoud van de zaak onderzocht moeten worden. De rechter zal daarom per zaak moeten kijken naar de feiten, de rechtsnormen onder *common law* en de rechtsnormen onder *equity* en op grond daarvan moeten overwegen of er wel of geen recht bestaat op beoordeling van de feiten door een jury.

Het feit dat het systeem juryrechtspraak kent, neemt niet weg dat er altijd een rechter aanwezig is in de rechtszaal en deze houdt een belangrijke rol in het proces. De rechter en de jury hebben ieder hun eigen taken en bevoegdheden. Grofweg is de verdeling tussen de jury en de rechter als volgt: de jury oordeelt over de feiten en de rechter past het recht toe.[362] Hierbij moet worden aangetekend dat deze verdeling geen harde verdeling is. De rechter heeft in een aantal gevallen toch zeker een oordeel te vormen over de feiten. Dit is namelijk het geval als de rechter een oordeel moet geven over de verschillende toelatingseisen van bewijsmiddelen.[363] Hoewel overigens de regels van bewijstoelating hun oorsprong vinden in het systeem van juryrechtspraak, gelden de regels van bewijstoelating onverkort voor rechtszaken die alleen door de rechter worden behandeld.[364]

De taakverdeling van de jury en de rechter, heeft sterk haar sporen nagelaten in de fase van bewijstoelating. De jury is misschien wel de aangewezen entiteit

---

'Remember the Alamo: the seventh Amendment of the United States Constitution, the doctrine of incorporation, and state caps of jury Awards', *South Texas Law Review* 2004-449, p. 45.

359 U.S. v. Stein, 452 F.Supp.2nd 276; Dimick v. Schiedt, 293 U.S. 474, 476, 55 S.Ct. 296, 79 L.Ed. 603 (1935).

360 D.L.A. Barker, C.F. Padfield, *Law*, Oxford: Made Simple Books 2001, p. 8 t/m 20. Zie ook: J.L. Wright, M.M. Williams, 'Remember the Alamo: the seventh Amendment of the United States Constitution, the doctrine of incorporation, and state caps of jury Awards', *South Texas Law Review* 2004-449, 45, p. 28.

361 Zie ook: City of Monterey v. Del Monte Dunes at Monterey, LTD, 119 S.Ct. 1624. De rechter hanteert daar precies dezelfde maarstaf.

362 D.P. Leonhard, *The New Wigmore, A Treatise on Evidence, Selected Rules of Limited Admissibility*, Gaithersburg / New York: Aspen Law & Business, p. 1:5.

363 Zie paragraaf 6.5 en verder.

364 K.S. Broun, *McCormick on Evidence*, St. Paul, Thomson West 2006, p. 113.

om te oordelen over de feiten, maar zij is niet opgeleid in het recht en zij is niet altijd bekend met regels van procesrecht. Daarbij komt dat de leden van de jury veelal geen experts zijn in het inschatten van de gevaren waaraan bewijs kan blootstaan en niet de kennis heeft om de betrouwbaarheid van bewijsmiddelen in te schatten. Daarom heeft de rechter een belangrijke rol gekregen die in het bewijsrecht duidelijk blijkt uit in de uitgebreide fase van bewijstoelating. De rechter toetst hier de bewijsmiddelen op betrouwbaarheid voordat de jury de bewijsmiddelen onder ogen krijgt. Pas als de rechter een oordeel heeft gegeven over de kwaliteit van de bewijsmiddelen zal de jury de bewijsmiddelen mogen gebruiken om haar oordeel op te baseren in de fase van bewijswaardering.

6.4 De rolverdeling tussen partijen en *juror*

Het Amerikaanse recht kent een specifieke rolverdeling tussen de *juror* (de rechter of de jury) en de partijen die een geschil hebben. Deze rolverdeling in *common law* onderscheidt zich op een aantal specifieke punten van de rolverdeling tussen de rechter en partijen in landen met *een civil law* traditie. Op het eerste gezicht lijkt de rol van de rechter in het Amerikaanse recht gelijk aan de rol van de rechter in het Nederlandse en Duitse recht. De verschillen worden echter zichtbaar als de rol van de Amerikaanse rechter wordt vergeleken met de rechter in Nederland/Duitsland.

Het Amerikaanse recht gaat uit van een *adversary* systeem, waarbij in het Nederlandse en Duitse recht wordt uitgegaan van een *inquisitorial* systeem. Voordat ik inga op de twee systemen moet opgemerkt worden dat beide systemen niet volledig en in volle omvang doorgevoerd zijn in respectievelijk het Amerikaanse en het Nederlandse en Duitse recht. Het gaat om een grove indeling waar nuanceverschillen bestaan.

In een *adversary* systeem heeft de rechter een duidelijk gescheiden rol van partijen. Hierbij leidt de rechter het proces en velt de jury uiteindelijk een oordeel over de feiten. Het presenteren van de feiten en het aandragen van bewijs, ligt net als in het Nederlandse recht geheel bij de partijen. Partijen ondervragen de getuige en de rechter houdt zich zo veel mogelijk afzijdig bij het ondervragen van getuigen. Als deze taken worden afgezet tegen de taken van de Nederlandse en Duitse rechter, dan valt op dat de Nederlandse en Duitse rechters veel meer onderzoeksrechters zijn. Deze leiden het proces en vellen een oordeel, maar houden zich daarbij ook veel meer bezig met het zoeken naar de feiten en de bewijsgaring. Zo worden getuigen in Nederland en Duitsland in eerste instantie door de rechter gehoord en partijen kunnen pas in de tweede plaats vragen stellen. Ook op het gebied van bewijsmiddelen is er verschil. De rechter kan in het Nederlandse en Duitse recht een bewijsopdracht

geven. In het Amerikaanse recht ligt de bewijsvoering geheel bij de partijen.

In het Nederlandse en Duitse recht is de rechter derhalve veel meer een onderzoeksrechter die op zoek gaat naar de materiële waarheid. In het Amerikaanse recht is de rechter eerder een "scheidsrechter" en staat de zoektocht naar de waarheid meer in het teken van het zoeken naar een zo eerlijk mogelijke oplossing van het geschil. Door de taakverdeling staat de rechter verder af van partijen en is zijn lijdelijkheid zelfs groter dan in het Nederlandse en Duitse recht. Dit heeft als gevolg dat de partijen zelf veel meer in zouden moeten gaan op het antwoord op de vraag waarom bewijsmiddelen betrouwbaar zijn.

6.5 Toelaatbaarheid van bewijsmiddelen (*admissibility*)

Het Amerikaanse bewijsrecht heeft een sterk ontwikkeld stelsel van regels dat de toelating van bewijsmiddelen regelt.[365] Stelt het Nederlandse recht dat in beginsel alle bewijsmiddelen zijn toegelaten en het Duitse recht dat een bewijsmiddel gekwalificeerd moet worden als wettelijk bewijsmiddel,[366] het Amerikaanse bewijsrecht stelt eisen aan de kwaliteit van de bewijsmiddelen om deze toelaatbaar te achten als bewijs. Het Amerikaanse recht stelt voor de toelating eisen waaraan alle bewijsmiddelen moeten voldoen, ongeacht hun identiteit. Deze eisen zijn kwalitatief van aard, wat wil zeggen dat ieder bewijsmiddel moet voldoen een aantal criteria die de betrouwbaarheid van het bewijsmiddel aantonen voordat deze worden toegelaten in een rechtszaak. De kwalitatieve criteria die in de *FRE* worden genoemd zijn:

- *relevancy (Rule 401 FRE)*
- *exclusion (Rule 402 FRE)*
- *hearsay (Rule 801 FRE)*
- *authentication (Rule 901 FRE)*
- *best evidence (Rule 1001 FRE)*.

In de volgende paragrafen zullen deze eisen worden besproken.

---

365 Dit is een gruwel in het oog van J. Bentham, die stelt: *"To find infallible rules for evidence, rules which insure a just decision, is, from the nature of things, absolutely impossible; but the human mind is too at to establish rules which only increase the probabilities of a bad decision. All the service that an impartial investigator of the truth can perform in this respect is to put legislators and judges on their guard against such hasty rules."* J. Bentham, *A Treatise of Judicial Evidence*, London: Messrs. Baldwin, Cradock, Joy 1825, p 180. Zie ook: P. Murphy, Evidence, *Proof, and Facts: A Book of Sources*, Oxford: Oxford University Press.

366 Hiermee bedoel ik dat het Duitse recht limitatief opsomt welke bewijsmiddelen toegelaten worden als bewijsmiddel en stelt per soort bewijsmiddel verschillende eisen. Zie ook de paragrafen 5.4 en 5.5.

Alle bewijsmiddelen moeten voldoen aan de hierboven opgesomde criteria. Een complicerende factor is dat is dat twee van bovenstaande kwaliteiten relatief van aard zijn, namelijk *relevancy* en *exclusion*. Met een kwaliteit van relatieve aard bedoel ik dat de kwaliteit niet in alle omstandigheden gelijk is. Afhankelijk van een bepaald feitencomplex kunnen bepaalde eigenschappen bijdragen aan de toelaatbaarheid dan wel de niet toelaatbaarheid van het betreffende bewijsmiddel. In de komende subparagrafen zal aan de orde komen in hoeverre dit een probleem oplevert voor het intrinsieke kwaliteiten van het bewijsmiddel en in het bijzonder elektronische bewijsmiddelen.

De kwalitatieve eigenschappen waaraan bewijsmiddelen moeten voldoen zijn slechts een eerste betrouwbaarheidstoets, maar wel de enige betrouwbaarheidtoets die expliciet wordt gemaakt in de rechtszaak. De regels voor toelating van bewijsmiddelen dienen om te zorgen dat de jury slechts bewijsmiddelen krijgt voorgelegd die aan een minimale standaard van betrouwbaarheid voldoen. Dit laat onverlet dat de jury bij het waarderen van het bewijs alsnog bewijsmiddelen onvoldoende betrouwbaar kan achten. Dit kan dan overigens alleen worden afgeleid uit de uitspraak van de jury dat feiten bewezen zijn of niet. De jury gaat verder niet inhoudelijk in op de waarde van de bewijsmiddelen. Zij geeft slechts een eindoordeel over de feiten.[367]

6.6 *Relevancy* en *exclusion*

6.6.1 *Relevancy*

De eerste toelatingseis in het Amerikaanse bewijsrecht is de eis dat bewijs relevant dient te zijn. Deze eis is vervat in *Rule 402 FRE* welke stelt: *"All relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other rules prescribed by the Supreme Court pursuant to statutory authority"* In beginsel is al het relevante bewijs toelaatbaar. Slechts indien anders bepaald door de constitutie van de Verenigde Staten van Amerika, door een wet van het Amerikaanse *Congress*, door de *Federal Rules of Evidence* of door regels van het *Supreme Court* ingevolge statutaire bevoegdheid, kan afgeweken worden van de regels dat bewijs dat relevant is, toegelaten wordt als bewijsmateriaal. Uitdrukkelijk wordt in *Rule 402 FRE* vervolgens ook gesteld dat bewijs dat niet relevant is, niet toelaatbaar is: *"Evidence which is not relevant is not admissible."*

[367] C.B. Mueller, L.C. Kirkpartick, *Modern Evidence, Doctrine and Practise*, Boston, New York, Toronto, London: Little, Brown and Company 1999, p. 59, 60 en 104.

Nu gesteld is dat in beginsel relevant bewijs toelaatbaar bewijs is en niet relevant bewijs geen toelaatbaar bewijs is, volgt de vraag wanneer bewijs als relevant gekwalificeerd kan worden. *Rule 401 FRE* geeft aan wanneer bewijs als relevant beschouwd kan worden, namelijk: *"'Relevant evidence' means evidence having 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."* Relevant bewijs heeft de strekking om het bestaan van enig feit dat van invloed is op de uitkomst van de gerechtelijke actie meer waarschijnlijk of minder waarschijnlijk te maken dan zonder het bewijs. *Rule 401 FRE* legt een verband tussen het bewijsmiddel en de waarschijnlijkheid dat bepaalde feiten bestaan.[368] Pas op het moment dat de inbreng van een bewijsmiddel een verandering in de waarschijnlijkheid van het bestaan van een bepaald feit tot gevolg heeft en deze verandering in waarschijnlijkheid van het bestaan van dat feit tot gevolg heeft dat de uitkomst van de gerechtelijke actie wordt beïnvloed, zal het bewijs worden gekwalificeerd als relevant bewijs.

In de vorige paragraaf is reeds aangegeven dat relevantie een relatief criterium is. Dit valt in de eerste plaats op te maken uit het verband dat wordt gelegd tussen de relevantie van het bewijsmiddel en de waarschijnlijkheid van het bestaan van een bepaald feit en in de tweede plaats uit het verband dat het bestaan van dat feit mogelijkerwijs ook van invloed moet zijn op de uitkomst van de rechtszaak. Een grote rol is weggelegd voor de feiten en niet voor het bewijsmiddel zelf. Dit wordt ook onderkend door de Advisory Committee on Proposed Rules die stelt: "*Relevancy is not an inherent characteristic of any item of evidence but exists only as a relation between an item of evidence and a matter properly provable in the case.*"[369] Relevantie is niet zozeer een juridische aangelegenheid, maar eerder een van feitelijke aard, waarbij levenservaring, logica en gezond verstand leiden tot een antwoord.[370]

Hoe groot moet de verschuiving in waarschijnlijkheid van het bestaan van een bepaald feit nu zijn? *Rule 402 FRE* stelt niet dat het bestaan van een feit onomstotelijk moet worden aangetoond. Iedere mogelijke kleine wijziging van de waarschijnlijkheid in het bestaan van een bepaald feit moet worden aangetoond.[371] Ook bewijs welke op het eerste gezicht weinig bewijswaarde lijkt te hebben, voldoet aan de relevantieregel als het bestaan van een bepaald feit waarschijnlijker of onwaarschijnlijker wordt.[372] In andere woorden: als het bewijsmiddel ook maar enige mogelijke bewijswaarde kan hebben, hoe klein

368 Notes of Advisory Committee on Proposed Rules (Pub. L. 93-595, § 1, Jan. 2, 1975, 88 Stat. 1931.)
369 Notes of Advisory Committee on Proposed Rules (Pub. L. 93-595, § 1, Jan. 2, 1975, 88 Stat. 1931.)
370 G. Weissenberger, J.J. Duane, *Federal Evidence*, Cincinnati: Anderson Publishing Co. 2001, p. 74.
371 K.S. Broun, *McCormick on Evidence*, St. Paul, Thomson West 2006, p. 776.
372 G. Weissenberger, J.J. Duane, *Federal Evidence*, Cincinnati: Anderson Publishing Co. 2001, p. 76.

ook, is het bewijsmiddel relevant.[373]

Elektronische bewijsmiddelen moeten voldoen aan de eis van relevantie. Daarbij is het probleem dat relevantie afhankelijk is van het feitencomplex in een specifiek geval en specifieke omstandigheden. Relevantie is niet een intrinsieke kwaliteit van een bewijsmiddel, maar een eigenschap die afhankelijk is van de feiten die mogelijkerwijs kunnen worden aangetoond met het bewijsmiddel. Het is daarom niet mogelijk om eisen te stellen die verband houden met de relevantie van elektronische bewijsmiddelen.

6.6.2 Exclusion

Als bewijs als relevant gekwalificeerd is, is het de vraag of er geen gronden zijn die het bewijsmiddel uitsluiten. *Rule 403 FRE* en verder stellen regels voor de uitsluiting van bewijsmiddelen, ondanks het feit dat deze de toets van relevantie hebben doorstaan. Rule 403 FRE biedt de basis om bewijsmiddelen uit te sluiten als bewijsmiddel op basis van een aantal omschreven gronden. Rule 403 FRE stelt: *"Although relevant, evidence may be excluded 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."* Ook al is bewijs relevant, het mag worden uitgesloten als de bewijswaarde substantieel wordt overtroffen door het risico van partijdige vooringenomenheid, verwarring van de geschilpunten, of misleiding van de jury, of door overwegingen van onbehoorlijke vertraging, verspilling van tijd, of onnodige inbreng van cumulatief bewijs.

Met regel 403 FRE wordt een uitzondering gemaakt op de regel dat het ontbreken van relevantie de enige grond is om bewijs uit te sluiten in een rechtszaak. Uitsluiting mag alleen plaatsvinden als de bewijswaarde "*substantially outweighed*" is door oneerlijke vooroordelen, verwarring van de feiten en misleiding van de jury of overwegingen van grote vertraging, tijdsverspilling en onnodige inbreng van cumulatief bewijs. De rechter krijgt grote discretie bij het toepassen van deze regel en appèlrechtbanken laten het standpunt van de feitenrechter meestal intact.[374] Wel wordt er verwacht dat de rechter uitermate terughoudend is met het toepassen van deze regel.[375]

---

373 D.A. Sklansky, *Evidence: cases, commentary, and problems*, New York: Aspen Publishers, Inc 2003, p. 16.

374 G.C. Lilly, *Principles of Evidence*, St. Paul: Thomson West 2006. p. 42. Zie ook: K.S. Broun, *McCormick on Evidence*, St. Paul, Thomson West 2006, p. 647.

375 M.H. Graham, *Federal Rules of Evidence in a Nutshell*, St. Paul: Thomson West 2007, p. 111.

De *exclusion rule* vind haar oorsprong in *case law*, waar erkend wordt dat bewijs dat relevant is, niet altijd zou mogen dienen als bewijs op grond van bepaalde omstandigheden en eigenschappen. Hiervoor zijn drie gronden welke ik kort zal bespreken:

1. Unfair prejudice

Van *unfair prejudice* is sprake als de kans buitensporig groot is dat de beslissing van de jury wordt beïnvloed op onrechtvaardige gronden. Daarbij gaat het vaak om het oproepen van emoties als sympathie, haat, minachting of afschuw bij de jury. De rechter moet ervoor waken dat de bewijswaarde opweegt tegen de vooroordelen die het kan oproepen bij de jury. Dat feiten een gevoel, bijvoorbeeld van walging of sympathie kunnen oproepen, is dus niet voldoende om een bewijsmiddel uit te sluiten.[376] Het gaat erom dat de bewijswaarde opweegt tegen de vooroordelen van de jury.

2. Confusion of the issues or misleading the jury

Verwarring van de feiten en misleiding van de jury kunnen een grond zijn voor uitsluiting van bewijs. Onduidelijk is het onderscheid in verwarring van de feiten en misleiding van de jury.[377] Hoewel kan worden gesteld dat verwarring van de feiten een jury kan misleiden, gaat het er vooral om dat de jury zich te snel laat verleiden bewijsmiddelen als te betrouwbaar aan te merken.[378] Hierbij moet gedacht worden aan het feit dat de uitslag van een leugendetector zonder uitvoerige uitleg van de werking en de significantie van de resultaten, vaak als waar wordt aangenomen. Als het elektronisch bewijs betreft zou naar mijn mening het risico kunnen bestaan dat conclusies die automatisch gegenereerd zijn door een computer te snel als waar worden aangenomen. Conclusies zijn namelijk een uitkomst van een gegevensverwerkend proces. Om waarde te kunnen hechten aan automatisch gegenereerde conclusies moet naar mijn mening duidelijk zijn welke redenering een proces heeft gemaakt. Niet zou mogen worden volstaan met slechts de eindconclusie, omdat inzicht in de beredenering dan ontbreekt.

3. Consideration of undue delay, waste of time and the needles presentation of cumulative evidence

Als reeds in behoorlijke mate is vast komen te staan dat feiten bewezen zijn, kan bewijs dat dezelfde feiten aantoont worden uitgesloten omdat het bewijs slechts cumulatief is. Ook als bewijs onnodige vertraging van het proces oplevert of slechts tijd vergt zonder dat dit van invloed is op de bewijswaarde, kan bewijs worden uitgesloten.

---

376 J.WM. Moore, *Moore's Federal Rules Pamplet 2007 – Part 2: Federal Rules of Evidence*, Newark/San Francisco: LexisNexis 2006, p. 172 en 173.

377 M.H. Graham, *Federal Rules of Evidence in a Nutshell*, St. Paul: Thomson West 2007, p. 113.

378 J.H. Wigmore, P. Tillers (revision), *Wigmore on Evidence, Evidence in Trials at Common Law*, Boston, Toronto, Little, Brown and Company 1983, p. 528 en 529.

Voor elektronische bewijsmiddelen geldt voor deze exclusionregel hetzelfde probleem als voor *relevancy*: bij de bepaling of deze regel van toepassing is op een concreet geval, moeten ook de feiten in acht worden genomen. De *exclusion rule* legt een verband tussen het bewijsmiddel en de feiten. Aangezien het feitencomplex van zaak tot zaak verschilt en daarmee ook bewijsmiddelen steeds in een andere verhouding tot de feiten komen te staan, kan er niet een eenduidige uitspraak worden gedaan wat dit betekent voor een specifiek bewijsmiddel in het algemeen.

6.7 *Hearsay*

6.7.1 Inleiding

Zoals blijkt uit Rule 802 *FRE* zijn varklaringen die *hearsay* bevatten in beginsel niet toegestaan als bewijs. Het antwoord op de vraag of bepaalde uitingen geclassificeerd kunnen worden als *hearsay*, is onder andere van belang in het geval dat elektronische bewijsmiddelen ingezet worden als bewijs in een rechtszaak. Hierbij moet onderscheid gemaakt worden tussen code, door mensen gegenereerde informatie en door de computer gegenereerde informatie. Makers van code (computerprogramma's) die feitelijk kunnen handelen, bijvoorbeeld door informatie te selecteren en verzamelen, zullen misschien wel rekening moeten houden met het feit dat deze informatie nog wel eens noodzakelijk kan zijn om bepaalde feiten aan te tonen. Een ander punt is dat computers naast gegevensverwerkende eenheden ook observerende eenheden kunnen zijn. Hierbij valt te denken aan het puur waarnemen en registreren van feiten als temperatuur, luchtvochtigheid, maar ook het lezen van bijvoorbeeld barcodes en RFID chips. Bij zowel het verzamelen van informatie als het observeren en registreren moet voorkomen worden dat deze informatie zo kan worden geclassificeerd dat deze onder het verbod van de *hearsay rule* valt. Indien de *hearsay rule* wel van toepassing is kan het anders zijn dat deze informatie niet toegelaten wordt.

In het Amerikaanse bewijsrecht is de *hearsay rule*, oftewel het verbod op *an out of court statement*, een reden om bewijs niet toe te laten. Het verbod op *hearsay* kent een lange traditie in het Angelsaksische recht en heeft vele uitzonderingen die gaandeweg in de jurisprudentie zijn gevormd.[379] In deze paragraaf zal onderzocht worden welke rol *hearsay* speelt in het geval dat elektronische bewijsmiddelen gebruikt worden om bepaalde feiten aan te

[379] Zie voor een uitgebreidde verhandeling over de historie van hearsay: J.H. Wigmore, *Wigmore On Evidence, Treatise on the Anglo-American System of Evidence in Trials at Common Law, Volume 5*, Boston: Little Brown and Company 1940, p. 9 t/m 27. Zie ook: C.B. Mueller, L.C. Kirkpartick, *Modern Evidence, Doctrine and Practise*, Boston, New York, Toronto, London: Little, Brown and Company 1999, p. 1046.

tonen. Hoewel in paragraaf 6.7.3 wordt ingegaan op de wettelijke definitie, zal ik met onderstaand voorbeeld proberen te verduidelijken in welk soort situaties er sprake is van hearsay. Hierbij wordt gebruik gemaakt van de casus in hoofdstuk 1.

In de eerste subparagraaf zal kort worden ingegaan op het wettelijke verbod op *hearsay* en wat de gevolgen van deze rechtsregel zijn; het is tenslotte het verbod op *hearsay* dat toelating van bewijsmiddelen beperkt en juist dit toelatingsverbod van als *hearsay* gekwalificeerde bewijsmiddelen raakt de kern van dit onderzoek. Vervolgens zal, voordat dieper wordt ingegaan op de wettelijke definitie van *hearsay*, worden onderzocht wat de ratio is van het verbod op *hearsay*. Het begrijpen van de reden waarom *hearsay* niet toegestaan is levert, naast de nodige achtergrondinformatie, relevante informatie om de juridische betekenis van *hearsay* te begrijpen. Daarna zal worden ingegaan op de wettelijke definitie van *hearsay* en de vereisten van *hearsay*. De wettelijke uitzonderingen, waarvan er een groot aantal bestaat, zullen worden onderzocht voor zover deze van toepassing kunnen zijn op het al dan niet toelaten van elektronische bewijsmiddelen als code, door mensen gegenereerde data en door computer gegenereerde data.

Voor het lezen van subparagraaf 6.7.2 acht ik het voldoende om *hearsay* voorlopig te definiëren als een verklaring welke buiten de rechtbank en niet onder ede is afgelegd om bepaalde feiten aan te tonen in een rechtszaak. Het gaat hier overwegend om uitspraken waarbij verklaard wordt wat iemand buiten de rechtszaal heeft verklaard.[380] Voor de wettelijke definitie verwijs ik naar subparagraaf 6.7.3.

6.7.2 Verbod op *hearsay*

Het Amerikaanse recht kent een expliciet verbod op *hearsay*, ruwweg te vertalen als een verbod op van-horen-zeggen of ook wel als een verbod op informatie uit tweede (of derde, vierde, vijfde, etc) hand.[381] Het *hearsay* verbod is neergelegd in Rule 802 *FRE* welke stelt: *"Hearsay is not admissible except as provided by these rules or by other rules prescribed by the Suprese Court persuant to statutory authority or by Act of Congress."* Deze regel stelt dat *hearsay* in beginsel niet toegelaten wordt als bewijs, tenzij de *Federal Rules of Evidence* of andere regels welke worden gesteld door de *Supreme Court* op grond van haar statutaire bevoegdheid of door een wet van het *Congress*. Vooral de *FRE* kennen een aantal uitzonderingen op het verbod op *hearsay*.[382]

---

380 A.S. Lipton, *Is It Admissible?*, Costa Mesa: James Publishing 1999, p. 5-2.

381 C.B. Mueller, L.C. Kirkpartrick, *Modern Evidence, Doctrine and Practise*, Boston, New York, Toronto, London: Little, Brown and Company 1999, p.1047.

382 Zie Rule 803 en 804 FRE. Zie ook paragraaf 6.7.4.

Hearsay is een van de meest complexe regelingen die het *common law* kent. Hoewel de regeling uitermate complex is,[383] is de aard van de regel eenvoudig: verklaringen dienen ten overstaande van de rechter en/of jury en onder ede worden afgelegd en er is in beginsel geen plaats voor wat mensen buiten de rechtbank zeggen.[384]

De ratio van het *hearsay* verbod is gelegen in de aanname dat beweringen onbetrouwbaar zijn.[385] Hierbij moet worden uitgegaan van het feit dat beweringen worden gedaan door mensen. Als een persoon een verklaring aflegt waarin beweringen worden gedaan, bestaat er een aantal risico's die de verklaringen onbetrouwbaar kunnen maken.[386] Deze risico's worden in de literatuur ook wel de *hearsay risks* genoemd.[387] Dit zijn een viertal risico's welke op enigerlei wijze ongewenste invloed kunnen hebben op de beweringen die gedaan worden. De vier onderkende *hearsay* risico's zijn:[388]

1. Het risico van misperceptie

Uitgangspunt is dat zintuiglijke waarnemingen niet altijd even betrouwbaar zijn. Onder invloed van allerlei omstandigheden kan een waarneming een situatie anders doen lijken dan deze daadwerkelijk is. Zo kan bijvoorbeeld reflectie van zonlicht een vertekening geven van bepaalde kleuren.

2. Het risico van onjuiste herinneringen

Als mensen informatie opslaan in hun geheugen wordt deze informatie niet alleen vastgelegd, maar bestaat de kans dat mensen, bewust of onbewust, elementen gaan toevoegen, wijzigen of verwijderen waardoor herinneringen vervormen en anders kunnen zijn dan de waarneming.

3. Het risico van onjuiste verklaringen

Als herinneringen worden weergegeven door middel van een verklaring, dan kan het zijn dat mensen bewoordingen gebruiken die voor meerdere uitleg vatbaar zijn of er kunnen woorden gebruikt worden die niet altijd de juiste lading weergeven.

---

383 P. Murphy, D. Barnard, *Evidence and Advocacy, Blackstone:* Blackstone Pr 2002, p. 22; zie ook: R.D. Friedman, *The Elements of Evidence*, St. Paul: Thomson West 2004, p. 192.

384 D.A. Sklansky, *Evidence: cases, commentary, and problems*, New York: Aspen Publishers, Inc, 2003, p. 41. Zie ook: R.D. Friedman, *The Elements of Evidence*, St. Paul: Thomson West 2004, p. 192.

385 E.J. Imwinkelried, *Evidentiary Foundations*, Newark/San Francisco/Charlottesville: LexisNexis 2005, p. 401.

386 C.B. Mueller, L.C. Kirkpartick, *Modern Evidence, Doctrine and Practise*, Boston, New York, Toronto, London: Little, Brown and Company 1999, p. 1047.

387 M.H. Graham, *Federal Rules of Evidence in a Nutshell*, St. Paul: Thomson West 2007, p. 385.

388 C.B. Mueller, L.C. Kirkpartick, *Modern Evidence, Doctrine and Practise*, Boston, New York, Toronto, London: Little, Brown and Company 1999, p. 1048 t/m 1051.

4. Het risico van ruis en valse verklaringen

Buiten de genoemde risico's van misperceptie, onjuiste herinneringen en verklaringen, zijn er andere risico's die samengevat kunnen worden als ruis en het risico van valse verklaringen. Hierbij valt respectievelijk te denken aan allerlei omstandigheden van buitenaf die op enigerlei wijze invloed kunnen hebben op de verklaring, zodat deze verklaring niet meer de feiten beschrijft zoals deze daadwerkelijk zijn en simpelweg bedrog door degene die de verklaring aflegt.

Om de waarheid te achterhalen en de risico's die het gevolg zijn van de *hearsay risks* te beperken, dienen verklaringen (*statements)* waarin beweringen (*assertions)* gedaan worden en non-verbale gedragingen die bedoeld zijn als een bewering, onder ede plaats te vinden zodat een rechter (of jury) de verklaring kan beoordelen met als doel de waarheid vast te stellen. Om de waarheid zo betrouwbaar mogelijk vast te stellen zijn er een drietal uitgangspunten waaraan verklaringen die bedoeld zijn als een bewering te dienen, moeten voldoen.[389] Deze uitgangspunten zijn:[390]

1. De verklaring dient te geschieden onder ede of onder belofte. Verklaringen onder ede of onder belofte zouden meer druk leggen op een getuige om de volledige waarheid te spreken, omdat deze zich daartoe verbindt. Een valse verklaring onder ede gedaan, levert dan ook een strafbaar feit op.[391]

2. De verklaring wordt persoonlijk door de getuige gedaan zodat de rechter en/of de jury het gedrag van de getuige kunnen/kan observeren. De gedachte achter deze regel is dat een getuige die niet de hele waarheid spreekt eerder geneigd is om nerveus gedrag te vertonen en al helemaal in het bijzijn van de wederpartij.[392]

3. De getuige kan en mag door de tegenpartij ondervraagd worden. De tegenpartij heeft haar eigen belangen en zou mogelijk eerder door bepaalde gedragingen van een getuige kunnen prikken. Zo zou de volledige waarheid eerder achterhaald kunnen worden.[393]

---

389 D.A. Sklansky, *Evidence: cases, commentary, and problems*, New York: Aspen Publishers, Inc, 2003, p. 45 en 46. Zie ook: E.J. Imwinkelried, *Evidentiary Foundations*, Newark / San Francisco / Charlottesville: LexisNexis 2005, p. 401.

390 J.H. Wigmore, *Wigmore On Evidence, Treatise on the Anglo-American System of Evidence in Trials at Common Law, Volume 5*, Boston: Little, Brown and Company 1940, p. 33; G. Weissenberger, J.J. Duane, *Federal Evidence*, Cincinnati: Anderson Publishing Co. 2001, p. 407.

391 Title 18 U.S.C. § 1621.

392 M.H. Graham, *Federal Rules of Evidence in a Nutshell*, St. Paul: Thomson West 2007, p. 379.

393 M.H. Graham, *Federal Rules of Evidence in a Nutshell*, St. Paul: Thomson West 2007, p. 380; K.S. Broun, *McCormick on Evidence*, St. Paul, Thomson West 2006, p. 422 en 423.

6.7.3 Wettelijke definitie van *hearsay*

Voordat ik toekom aan het verbod op hearsay en de uitzonderingen daarop, zal ik eerst ingaan op de vraag hoe *hearsay* gedefinieerd wordt in het positieve recht.

Het Nederlandse of Duitse recht kent een soortgelijke regel als de *hearsay rule*, of een variant daarop niet en dus ook geen verbod op *hearsay*. De vraag wat *hearsay* is, zal daarom enkel naar Amerikaanse recht gedefinieerd kunnen worden. Als definitie van hearsay geeft Rule 801(c) *FRE*: *"…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."* Bij *hearsay* betreft het dus (a) *a statement* (verklaring), (b) die gemaakt is door *the declarant* (de verklarende), (c) en deze verklaring is niet gedaan tijdens een zitting of verhoor en (d) en die als bewijs is aangeboden om de waarheid van een *assertion* (bewering) te bewijzen. Deze definitie blinkt naar mijn mening niet uit in overzichtelijkheid. In de eerste plaats hanteert de definitie een negatieve uitsluiting (namelijk "*other than one made by the declarant*"). Een tweede complicerende factor is dat binnen de definitie twee andere nader gedefinieerde begrippen worden gehanteerd, namelijk: *statement* en *declarant*, waarvan binnen het begrip *declarant* ook weer het begrip *statement* gehanteerd wordt.

Het begrip *hearsay* is zowel wat betreft inhoud als omschrijving geen eenvoudig te begrijpen begrip. Als de definities van *statement* en *declarant* uitgeschreven worden in het begrip *hearsay* dan ontstaat al een iets overzichtelijker beeld:"*Hearsay is a oral or written assertion or nonverbal conduct, if it is intended by the person as an assertion, other than one made by the person who makes a oral or written assertion or nonverbal conduct, if it is intended by the person as an assertion while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted*."

Voordat ik nader in ga op wat ook wel begrepen wordt als de kern van het begrip *hearsay,* zal ik eerst de begrippen *statement* en *declarant* nader bespreken aan de hand van de wettelijke definities. Vervolgens zal ik ingaan op de overige twee eisen die wel de kern van *hearsay* vormen, namelijk: dat de verklaring niet gedaan is tijdens de zitting (*out of court statement*) en welke als bewijs is aangeboden om de waarheid van een *assertion* te bewijzen (*to prove the truth of the matter asserted*).

A) Statement

Rule 801(a) *FRE* geeft als definitie van *statement: "…(1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by the person as an assertion."* Een *statement* is een verklaring welke volgens de wetstekst

zowel mondeling als schriftelijk kan worden geuit. Het Adv*isory Committee on Rules* geeft in haar *Notes* aan dat het belang van een definitie van *statement* gelegen is in het feit dat een *statement* bedoeld moet zijn als *assertion* en dat beweringen die niet bedoeld zijn als *assertion* ook geen statement zijn.[394] Niets is een *assertion* tenzij het bedoeld is een *assertion* te zijn.[395] Voor verbale *assertions* geldt dus dat deze wel gedaan moeten worden met de bedoeling dat deze een *assertion* is. Ook voor non-verbale gedragingen geldt dat de persoon die deze gedraging doet de bedoeling moet hebben met deze gedraging een *assertion* te doen. Bij gedragingen zijnde een *assertion* kan gedacht worden aan het bevestigend knikken of ontkennend schudden met het hoofd.

B) Declarant

Rule 801(b) FRE stelt dat een *declarant* is:*"…a person who makes a statement."* Hoewel het in eerste instantie lijkt alsof declarant slechts de persoon is die een verbale *assertion* doet, wordt hieronder (door intersectie van Rule 801(a) FRE en Rule 801(b) FRE ook verstaan de persoon die een nonverbale uiting, oftewel een gedraging doet die bedoeld is als een *assertion*.[396]

C) Out of court statement

Binnen de *hearsay rule* worden twee statements onderscheiden: namelijk het *statement* niet onder ede voor de rechter en het *statement* wel onder ede voor de rechter. Met de bewoordingen "*other than one made by*" wordt het *statement* welke wel onder ede voor de rechter wordt gedaan, uitgesloten van de *hearsay rule*. Alleen een *statement* welke niet onder ede is gedaan voor de rechter valt in beginsel (er bestaan namelijk meerdere uitzonderingen, welke in subparagraaf 6.7.4 aan de orde komen) onder de *hearsay rule* en dan alleen als deze is "*offered in evidence to prove the truth of the matter asserted*"

D) To prove the truth of the matter asserted

Een laatste, en reeds genoemd criterium, is dat het statement moet zijn aangeboden als bewijs om de waarheid van datgene dat beweerd wordt, te bewijzen. Andere statements vallen niet onder de hearsay rule. Dit zijn bijvoorbeeld statements die niet zijn aangeboden of statements die wel zijn aangeboden maar niet als bewijs om de waarheid van datgene dat wordt beweerd te bewijzen. Rule 801(d) FRE noemt een aantal specifieke gevallen waarbij geen sprake is van hearsay, terwijl er meestal wel voldaan is aan alle eisen van de wettelijke definitie van hearsay. Deze uitzonderingen zien op getuigenverklaringen (Rule 801(d)(1 A, B en C FRE)) en specifieke feiten (Rule

---

394 Notes of Advisory Committee on Proposed Rules, Rule 801(a) FRE (Pub. L. 93-595, § 1, Jan. 2, 1975, 88 Stat. 1931.

395 S.A. Saltzburg, K.R. Redden, *Federal Rules of Evidence Manual*, Charlottesville: The Michie Company Law Publishers 1986, p. 717.

396 S.A. Saltzburg, K.R. Redden, *Federal Rules of Evidence Manual*, Charlottesville: The Michie Company Law Publishers 1986, p. 717.

801(d)(2 A t/m E FRE)). Aangezien dit onderzoek gaat over elektronische bewijsmiddelen, zijn deze specifieke gevallen niet relevant voor dit onderzoek en zullen daarom buiten beschouwing worden gelaten.

Bij *hearsay* gaat het vaak om verklaringen die door mensen zijn gedaan of opgetekend. Ook als elektronische gegevens worden gebruikt om verklaringen in vast te leggen geldt de hearsay rule. Een voorbeeld is e-mail. E-mail is een communicatiemiddel waarvan veel gebruik wordt gemaakt en waarin verklaringen worden gedaan door mensen. Ook voor communicatie via e-mail kan er sprake zijn dat de e-mail verklaringen bevat die als *hearsay* aangemerkt kunnen worden. Dit is bijvoorbeeld het geval in *State v. Microsoft*,[397] waarin de rechter e-mailbewijs aanmerkt als *hearsay*: *"The Court First rejects the assertion that the contents of Plaintiffs' Exhibit 1237 (de e-mail) are not offered for the truth of the matter asserted therein. As is apparent from Mr. Richards' testimony and his description of the letter, Mr. Richards is relying on the letter to establish that Microsoft, through its representative, behaved as recounted by Mr. Glaser in the e-mail. In this regard , Mr. Richards uses the letter to lend credence to his testimony regarding the treatment of Realnetworks by Microsoft. Based upon this use, it does not appear that Mr. Glasers "motive, intent, knowledge, or notice" is at issue in this portion of his testimony. Accordingly, the Court rejects Plaintiffs' contention that they have offered the Glaser e-mail to establish such facts"*

Vervolgens stelt de rechter dat dit bewijs in casu niet onder een van de uitzonderingen valt als genoemd in *Rule 803(1)* en *803(6) FRE*.[398] Wat de rechter in feite doet is eerst toetsen of de verklaring een verklaring is die valt aan te merken als *hearsay* om vervolgens te toetsen of de verklaring ook onder de *hearsay rule* valt en of er uitzonderingen van toepassing zijn. Uit bovenstaand voorbeeld blijkt ook dat verklaringen die op elektronische wijze zijn gedaan, worden getoetst aan *hearsay* en de *hearsay rule*.

6.7.4 Uitzonderingen op de hearsay rule

Op de *hearsay* rule wordt in 803 en 804 *FRE* een groot aantal uitzonderingen gemaakt. Een uitzondering op *hearsay* houdt in dat er wel sprake is van *hearsay*, maar dat het bewijsmiddel toch wordt toegelaten, omdat de omstandigheden voldoende aanknopingspunten bieden dat het bewijs voldoende betrouwbaar is om het ontbreken van een eed, confrontatie met de jury of ondervraging door de wederpartij te kunnen overkomen.[399] Slecht een aantal van deze

397 2002 WL 649951 (D.D.C. April 2002).
398 Voor de uitzonderingen op de hearsay rule, zie ook subparagraaf 6.7.4.
399 P.R. Rice, *Electronic Evidence, Law and Practice*, Chicago: ABA Publishing 2005, p. 281.

uitzonderingen is mogelijk van toepassing op elektronisch bewijs. Deze uitzonderingen zullen in deze paragraaf nader besproken worden.

De eerste uitzondering op de *hearsay* rule is de situatie waarin een verklaring een gebeurtenis beschrijft of uitlegt direct nadat deze heeft plaatsgevonden. *Rule 803(1) FRE*: "*A statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter.*" Het risico van *hearsay* wordt niet groot geacht als tijdens of direct volgend op de gebeurtenis die beschreven wordt, een verklaring wordt gedaan of opgetekend, die de gebeurtenis beschrijft.[400] Een voorbeeld van elektronisch bewijs dat toegelaten werd is een e-mail met de optekening van een telefoongesprek en waarbij deze optekening direct na het gesprek werd gedaan.[401]

De tweede uitzondering betreft *Rule 803(3) FRE*:"*A statement of the declarant's ten existing state of mind, emotion, sensation, or physical condition (such as intent, plan, motive, design, mental feeling, pain, and bodily health), but not including a statement of memory or belief to prove the fact remembered or believed unless it relates to the execution, revocation, identification or terms of declarant's will.*"[402] Ook hiervoor geldt dat verklaringen over de geestelijke staat, emotie, waarneming of fysieke conditie van de declarant zijn toegelaten als bewijs, ook als deze in elektronische vorm zijn gedaan.[403]

De derde uitzondering betreft *Rule 803(5) FRE*:" *A memorandum or record concerning a matter about which a witness once had knowledge but now has insufficient recollection to enable the witness to testify fully and accurately, shown to have been made or adopted by the witness when the matter was fresh in the witness' memory and to reflect that knowledge correctly. If*

---

400 See *United States v. Blakey,* 607 F.2d 779, 785 (7th Cir.1979): statements gedaan binnen 23 minuten na de gebeurtenis zijn toegelaten op grond van Rule 803(1); *Miller v. Crown Amusements, Inc.,* 821 F.Supp. 703, 706-07 (S.D.Ga.1993): statements gedaan binnen 10 minuten na de gebeurtenis zijn toegelaten op grond van Rule 803(1).

401 United States v. Ferber, 966 F.Supp. 90, 98-99 (D. Mass. 1997).

402 Een verklaring van de op dat moment bestaande geestelijke gesteldheid, emotie, waarneming of fysieke conditie (zoals intentie, plannen, motieven, ontwerp, geestelijke gesteldheid, pijn en lichamelijke gezondheid) van de declarant, maar niet inhoudende een verklaring van geheugen of overtuiging om het onthouden of geloofde feit te bewijzen, tenzij het gerelateerd is aan de uitvoering, herroeping, identificatie of voorwaarden van de wil van de declarant.

403 Mota v. University of Texas Houston Health Ctr., 261 F.3d 512, 527 (5th Cri. 2001): Dr. Mota eist schadevergoeding van zijn werkgever, nadat deze het in een langslepend conflict opneemt voor Prof. Caffesse die Mota ongewenst sexueel heeft benaderd en Mota het leven op het werk zuur maakt. Daar Prof. Caffesse als een der wereld's beste periodontisten bekend stond, zocht Low (directeur van de universiteit) vergelding op Mota. Nadat de jury uitspraak had gedaan en aan Mota een schadevergoeding was toegewezen, stuurde Low een e-mail naar 8000 werknemers van de universiteit, waarin Mota het verder moest ontgelden. Weer zocht Mota recht. Daarbij werd de betreffende e-mail toegelaten als bewijsmiddel op grond van het feit dat de verklaring in de e-mail bewijs was van de geestelijke staat van Low.

admitted, the memorandum or record may be read into evidence but may not itself be received as an exhibit unless offered by an adverse party."[404] Deze uitzondering geldt evenzeer voor notities die in elektronische vorm zijn opgetekend.[405]

De vierde uitzondering voor computer gerelateerde hearsay, is de business records exception in *Rule 803(6) FRE*.[406] *"A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Rule 902(11), Rule 902(12), or a statute permitting certification, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit."* In de zakelijke wereld worden veel computersystemen gebruikt bij het bedrijven van commerciële activiteiten, waarbij vaak nauwkeurig gewerkt wordt en er grote belangen aan deze nauwkeurigheid gehecht worden, wordt het toelaatbaar geacht om een uitzondering te maken op het verbod op *hearsay* in het geval van zogenaamde *business records*.[407] Om te voldoen aan de *business record exception* zijn er drie eisen: (1) de records moeten zijn gemaakt in de uitvoering van de gangbare bedrijfsactiviteiten (*regularity*), (2) deze moeten ingevoerd worden tijdens of omstreeks de tijd dat de evenementen plaatsvonden (*timeliness*) en (3) er moet kunnen worden vertrouwd op de uitvoering van het bedrijf tijdens het creëren en onderhouden van de records (*reliance*).[408] In het geval van zogenaamde *records of regularly conducted activity* worden de aantekeningen, rapportages, opnames of data-compilaties toegelaten als bewijsmiddel als deze in het kader

---

404 Een notitie of opname van een gebeurtenis waar een getuige kennis van had, maar zich daar nu onvoldoende van kan herinneren om volledig en accuraat te getuigen en waarbij de notitie of opname gemaakt is toen de gebeurtenis nog vers in het geheugen van de getuige was en dat de kennis juist is. Indien toegelaten mag de optekening of opname als bewijs worden gebruikt, maar mag niet worden gebruikt om nader te worden onderzocht.

405 De Bolt v. Outboard Marine Corp., 2001 WL 311300, at *2 (W.D. Mich. Jan. 16, 2001): De Bolt werd door haar werkgever Everett ongewenst sexueel benaderd. Hiervan heeft zij aantekeningen bijgehouden en vervolgens opgetekend in een elektronisch bestand. Tijdens de rechtszaak kon zij zich niet alle details herinneren. Omdat het haar ontbrak aan accurate herinneringen en de optekening is gedaan toen haar geheugen vers was en de notities accuraat waren, werd dit opgetekende bewijs toegelaten als uitzondering op de hearsay rule.

406 D. Bender, *Computer Law, A Guide to Cyberlaw and Data Privacy Law*, Newark, New Jersey: LexisNexis / Matthew Bender 2008, p. 6-4.

407 D. Bender, *Computer Law, A Guide to Cyberlaw and Data Privacy Law*, Newark, New Jersey: LexisNexis / Matthew Bender 2008, p. 6-6.

408 D. Bender, *Computer Law, A Guide to Cyberlaw and Data Privacy Law*, Newark, New Jersey: LexisNexis / Matthew Bender 2008, p. 6-4.

van en tijdens de gebruikelijke bedrijfsactiviteiten worden opgemaakt en als de optekeningen nauwkeurig worden vastgelegd en onderhouden.[409]

De vijfde uitzondering bestaat uit public records en reports. Deze uitzondering wordt gemaakt in *Rule 803(8) FRE*: *"Records, reports, statements, or data compilations, in any form, of public offices or agencies, setting forth (A) the activities of the office or agency, or (B) matters observed pursuant to duty imposed by law as to which matters there was a duty to report, excluding, however, in criminal cases matters observed by police officers and other law enforcement personnel, or (C) in civil actions and proceedings and against the Government in criminal cases, factual findings resulting from an investigation made pursuant to authority granted by law, unless the sources of information or other circumstances indicate lack of trustworthiness."*[410] De ratio achter deze bepaling is dat ambtenaren hun werkzaamheden uitvoeren zonder dat zij direct persoonlijke belangen hebben bij een zaak en daarom niet geneigd zijn de stukken te vervalsen.[411] Ook als de gegevens zijn opgemaakt in elektronische vorm zijn deze toelaatbaar als bewijsmiddel.[412]

In Rule 803(17) FRE wordt een zesde uitzondering gemaakt voor *market reports* en *commercial publications*: "*Market quotations, tabulations, lists, directories, or other published compilations, generally used and relied upon by the public or by persons in particular occupations."* Een uitzondering op de hearsay rule geldt voor prijsopgaven, tabellen, lijsten, gegevensbestanden of andere gepubliceerde verzamelingen die in het algemeen gebruikt worden en waarop vertrouwd wordt door het publiek of door personen in specifieke beroepen. De ratio achter deze bepaling is dat grote gegevensverzamelingen waar het publiek op mag vertrouwen, voldoende betrouwbaar zijn om een uitzondering op de *hearsay rule* te kunnen billijken. In een rechtszaak waarin een meningsverschil was over welke rentetarieven gebruikt hadden moet worden bij het berekenen van de rente werden overzichten van rentes welke waren gepubliceerd op een website van de *Federal Reserve Board* toegelaten als bewijsmiddel:" *(…) Furthermore, many of the rates used by Finnerty were obtained from the Federal Reserve Board website or from Bloomberg and are*

---

409 D. Bender, *Computer Law, A Guide to Cyberlaw and Data Privacy Law*, Newark, New Jersey: LexisNexis / Matthew Bender 2008, p. 6-6.

410 Uitgezonderd van de *hearsay rule* zijn opnames, rapportages, verklaringen of data verzamelingen, in iedere vorm, van publieke kantoren/loketten of agentschappen, die (A) de activiteiten van het kantoor of agentschap uiteenzetten, of (B) geobserveerde zaken die uitgevoerd zijn ter uitvoering van de wet welke een uitvoeringsrapportage verlangt, maar in strafrechtelijke zaken exclusief zaken die geobserveerd zijn door politieagenten en ander personeel dat de wet uitvoert, of (C) in civiele acties en procedures en tegen de overheid in strafrechtelijke zaken, feitelijke bevindingen welke het resultaat zijn van een onderzoek welk uitgevoerd zijn door aan de wet toegekende autoriteiten, tenzij de informatiebronnen of andere omstandigheden een gebrek aan betrouwbaarheid vertonen.

411 M.H. Graham, *Federal Rules of Evidence in a Nutshell*, St. Paul: Thomson West 2007, p. 481.

412 United States v. Griffin, 191 F.3d 453, 453-54 (6th Cir. 1999).

admissible under Fed.R.Evid. 803(17). (…)"[413]

6.7.5 Elektronisch bewijs en de *hearsay rule*

De *hearsay rule* is ontwikkeld in een tijd waarin alleen mensen verklaringen aflegden. Deze verklaringen kunnen zowel in mondelinge als in schriftelijke vorm gedaan worden. De vraag is of de *hearsay rule* ook van toepassing is op menselijke verklaringen in elektronische vorm en verklaringen die met behulp van machines tot stand komen. In deze subparagraaf zal ik dan ook nader ingaan op de vraag of verklaringen van machines onder de *hearsay rule* vallen.

6.7.5.1 De *hearsay rule* en code

Code is door mensen geschreven zodat een machine door middel van het executeren van deze code bepaalde handelingen kan verrichten. De vraag is of code uitgesloten kan worden als bewijsmiddel op grond van het feit dat er sprake is van *hearsay*. Onderzocht dient dus te worden of ten eerste code als *hearsay* gekwalificeerd kan worden en ten tweede of code onder het verbod op *hearsay* valt en als dat het geval is of er uitzonderingen van toepassing (kunnen) zijn.

Rule 801(a) FRE stelt dat het hier gaat om een verklaring (*statement)* oftewel *an oral or written assertion or a non-verbal conduct*. Het gaat hier dus om een verklaring waarin een bewering besloten ligt. Code is wel een uiting van een persoon die de code schrijft, maar in de code zelf ligt geen verklaring besloten. Code bestaat enkel uit instructies die een machine aansturen. Code kan door zijn aard geen verklaringen bevatten en daarom zal code nooit onder de definitie van *hearsay* kunnen vallen. Als gevolg hiervan is de *hearsay rule* ook niet van toepassing op code en kan gesteld worden dat de *hearsay* rule geen beletsel oplevert om code als bewijsmiddel toe te laten.

Code ontstaat niet vanzelf, maar is door mensen geschreven. Het is echter niet uitgesloten dat in de toekomst code wel door computers gegenereerd kan worden. Of de door de computer gegenereerde code dan wel als *hearsay* gekwalificeerd kan worden, is de vraag. Code bevat namelijk geen verklaringen. Het maakt daarom niet uit door wie de code gegenereerd wordt voor het antwoord op de vraag of code als *hearsay* gekwalificeerd kan worden. Het antwoord blijft namelijk nee.

[413] Elliott Accociates., L.P. v. Banco de la Nacion, 194 F.R.D. 116, 121 (S.D.N.Y. 2000).

6.7.5.2 De *hearsay rule* en door mensen gegeneerde data

Veel data, zoals e-mails, chatgesprekken, (postings op) websites, vastleggingen van observaties, enzovoort is vastgelegd door mensen. Deze hebben hun observaties opgetekend in verklaringen. De *hearsay rule* is toegespitst op verklaringen van mensen. Zoals in subparagraaf 6.7.3 is beschreven kunnen deze verklaringen object zijn van het verbod op *hearsay* als deze een verklaring bevatten welke buiten de rechtszaal is gedaan en als deze is bedoeld om de waarheid te bevestigen. Het maakt niet uit of de vorm van deze verklaring ligt in een mondelinge verklaring of dat deze verklaring op papier is vastgelegd. Tevens maakt het geen onderscheid of de verklaring is vastgelegd op elektronische wijze.[414]

Op het moment dat een verklaring in elektronische vorm is gedaan en deze bedoeld is om de waarheid te verklaren, zal deze verklaring in beginsel onderwerp zijn van het verbod op *hearsay*. Dit geldt ook voor verklaringen die zijn overgenomen door zoekmachines. Deze veranderen niets aan de verklaring zelf en ontdoen de verklaring ook niet van de risico's die ten grondslag liggen aan de *hearsay rule*. Zoekmachines creëren zelf dan wel geen extra *hearsay*,[415] omdat zij geen verklaring tot stand brengen, maar de gevonden data die verklaringen bevat, kan onderwerp zijn van het verbod op *hearsay* als er geen sprake is van door *Rule 803* of *804 FRE* uitgezonderde *hearsay*.
Aan elektronische bewijsmiddelen met verklaringen kan echter niet eenduidig vooraf een eis worden gesteld om te voorkomen dat een bewijsmiddel wordt uigesloten op grond van de *hearsay rule*. Dit is namelijk afhankelijk van de verklaring en het feit of in de verklaring een bewering ligt besloten welke gedaan is met de intentie om de waarheid aan te tonen.

6.7.5.3 *Hearsay* en door computers gegenereerde data

Naast het feit dat mensen data genereren is het mogelijk dat computers data genereren.[416] Computers hebben de mogelijk om met behulp van sensoren hun omgeving te observeren. De observaties van computers worden in het systeem vastgelegd; aan de observering wordt een bepaalde waarde meegegeven die vervolgens opgeslagen wordt. Hoewel de computer variabelen waarneemt, registreert en vervolgens presenteert (bv door middel van een print of op een beeldscherm), bestaat er geen risico dat een van de *hearsay risks* zich voordoet. De computer legt objectief meetbare gegevens vast en de computer heeft geen ruimte om een eigen interpretatie te geven aan gedane waarnemingen, ook tijdens de opslag blijven de gegevens hetzelfde; een risico zoals dat bij het

414 In re Vee Vinhnee, 336 B.R. 437, r.o. 13.
415 P.R. Rice, *Electronic Evidence, Law and Practice*, Chicago: ABA Publishing 2005, p. 277.
416 De door mensen gedane verklaringen die worden vastgelegd in elektronische gegevens (computer stored data) kunnen onder omstandigheden wel worden aangemerkt als hearsay. Zie hiervoor: U.S. v. Ruffin, 575 F.2d 346.

menselijke geheugen bestaat, waar waarnemingen flexibel zijn en aan veranderingen onderhevig, bestaat niet.

Is er dan geheel geen sprake van *hearsay*? De gegevens kunnen namelijk een verklaring bevatten. Als deze gegevens dan in een rechtszaak ingezet worden om de waarheid te bevestigen, zou er gesteld kunnen worden dat er sprake is van *hearsay*. Het is echter ook van belang om te onderzoeken of er bij het verklaren sprake is van een bedoeling om de waarheid te verklaren. Nu met de huidige stand van technische ontwikkeling computers geen intentie ofwel doelgerichtheid kunnen hebben om de waarheid te verklaren, is maar geheel de vraag of er voldaan is aan het criterium:"*to prove the truth of the matter asserted*". Pas als computers wel een intentie of doelgerichtheid kunnen hebben om de waarheid te verklaren, dan zou er sprake kunnen zijn van *hearsay*. Is er dan sprake van verboden *hearsay* of hebben we hier dan te maken met toegestane *hearsay*? Zoals in paragraaf 6.7.2 reeds is aangegeven, is het belangrijk om bij het bepalen of een verklaring onder het *hearsay*-verbod valt, te bepalen of de *hearsay*- risico's een risico vormen. Nu dat niet het geval is, zou dat leiden tot de uitkomst dat er wel sprake kan zijn van *hearsay*, maar dat er geen sprake is van het verbod op *hearsay*.

In de rechtspraak heeft bovenstaande redenering ook weerklank gevonden. In *State v. Armstead* overweegt de rechter dat verklaringen die gegenereerd zijn door een computer zich onderscheiden van door mensen gemaakte verklaringen. Hij noemt tevens een aantal voorbeelden van andere soortgelijke verklaringen die door de computer gegenereerd worden:[417]

"*The computer generated data by recording the source of various telephone connections as it was making them. Therefore, the evidence in this case was generated solely by the electrical and mechanical operations of the computer and telephone equipment, and was not dependant upon the observations and reporting of a human declarant. We therefore view the printout offered as evidence in this case differently from printouts of human statements fed into the computer. Since the computer was programmed to record its activities when it made the telephone connections, the printout simply represents as self-generated record of its operations, much like a seismograph can produce a record of geological occurrences, a flight recorder can produce a record of physical conditions onboard an aircraft, and an electron microscope can produce a micrograph, which is a photograph of things too small to be viewed by the human eye."*

De rechter gaat vervolgens verder door te bepalen of er sprake is van *hearsay*: *"The printout of results of the computer's internal operations is not hearsay*

[417] *State v. Armstead*, 432 So.2d 837:

evidence. It does not represent the output of statements placed into the computer by out of court declarants. Nor can we say that this printout itself is a "statement" constituting hearsay evidence. The underlying rationale of the hearsay rule is that such statements are made without an oath and their truth cannot be tested by cross-examination. Of concern is the possibility that a witness may consciously or unconsciously mispresent what the declarant told him or that the declarant may consciously or unconsciously mispresent a fact or occurrence. With a machine, however, there is no possibility of a conscious mispresentation, and the possibility of inaccurate or misleading data only materializes if the machine is not functioning properly. For this reason, apparently, most definitions of hearsay are limited to out of court statements by a person made out of court and thus not under oath, an not subject of cross-examination or confrontation." Volgens de rechter zijn de interne verwerkingen van gegevens geen *hearsay*. Deze representeren namelijk geen *statements* die door de een declarant in een computer zijn ingevoerd. Tevens kan niet gesteld worden dat de printout een *statement* is die *hearsay* constitueert. De risico's van *hearsay* kunnen zich dan ook niet voordoen bij computers die gegevens verwerken.

6.8 *Authentication*

6.8.1 Inleiding

Als bewijs wordt ingebracht in een rechtszaak, moet er een toets plaatsvinden welke voldoende zekerheid geeft dat het bewijsmiddel echt is. Deze echtheidstoets wordt ook wel *authentication* of *identification* genoemd. Aangetoond moet worden dat het bewijsmiddel inderdaad dát bewijsmiddel is wat gesteld wordt dat het is. In de volgende subparagrafen zal ik achtereenvolgens ingaan op de juridische grond waarop *authentication* en *identification* is gebaseerd, wat *authentication* en *identification* is, welke bewijsdrempel genomen moet worden voordat een bewijsmiddel en in het bijzonder een elektronisch bewijsmiddel wordt toegelaten, welke methoden van *authentication* en *identification* bestaan en welke daarvan van toepassing zijn op elektronische documenten.

6.8.2 *Authentication* als toelatingseis

In de voorgaande paragrafen over *relevancy* en *exclusion*, *hearsay* en in de nog komende paragraaf over *best evidence* wordt aangevangen met het betreffende wetsartikel dat uitdrukkelijk de toelaatbaarheid op grond van *relevancy* en *exclusion*, *hearsay* en *best evidence* aan de orde stelt. De reden dat in deze paragraaf niet begonnen wordt met de regel welke de

toelaatbaarheid regelt, is omdat een wetsartikel dat toelaatbaarheid van ongeauthenticeerd of ongeïdentificeerd bewijs regelt, slechts indirect te vinden is.

Toch kan ongeauthentificeerd of ongeïdentificeerd bewijs niet zomaar worden toegelaten. De vraag is hoe het toelaten van bewijsmiddelen die voldoen aan de eisen van *authentication* en *identification* dan tot stand wordt gebracht? Het antwoord kan gevonden worden in Rule 104(b) FRE. *Authentication* en *identification* worden namelijk beschouwd als een bijzondere variant op *relevancy*, namelijk zogenaamde *conditional relevancy*.[418] *Conditional relevancy* is geregeld in Rule 104(b) FRE welke stelt:

"When the relevancy of evidence depends upon the fulfillment of a condition of fact, the court shall admit it upon, or subject to, the introduction of evidence sufficient to support a finding of the fulfillment of the condition."

Als de relevantie van bewijs afhankelijk is van de vervulling van een voorwaarde, dan zal het bewijs pas worden toegelaten als deze voorwaarde ook daadwerkelijk is vervuld; zolang de voorwaarde niet vervuld is, wordt het bewijs ook niet toegelaten. De eis dat bewijs relevant moet zijn om toegelaten te worden tot de rechtszaak omvat,[419] door middel van Rule 104(b) FRE, ook dat indien eventuele voorwaarden die van belang zijn of bewijs als relevant beschouwd kan worden of niet, aangetoond dienen te worden. Twee van deze voorwaarden voor relevantie welke expliciet in de FRE worden genoemd, zijn *authentication* en *identification*. *Authentication* en *identification* representeren daarmee een bijzondere vorm van *relevancy*,[420] welke vastgesteld moeten worden voordat er überhaupt sprake kan zijn van *relevancy*.[421]

6.8.3 Definitie van *authenication*

Authentication en *identification* houden in dat aangetoond moet worden dat het bewijsmiddel datgene is wat gesteld wordt dat het is (door de aanbieder van het bewijs).[422] De eis van *authentication* en *identification* wordt gesteld in

---

418 S.A. Saltzburg, K.R. Redden, *Federal Rules of Evidence Manual*, Charlottesville: The Michie Company Law Publishers 1986, p. 1005.

419 Relevant bewijs: "*having 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.* Zie paragraaf 6.6.1.

420 D.A. Schlueter, S.A. Saltzburg, *Emerging Problems Under The Federal Rules of Evidence*, Charlottesville: Lexis Law Publishing 1998, p. 377; G. Weissenberger, J.J. Duane, *Federal Evidence*, Cincinnati: Anderson Publishing Co. 2001, p. 631.

421 S.A. Saltzburg, K.R. Redden, *Federal Rules of Evidence Manual*, Charlottesville: The Michie Company Law Publishers 1986, p. 1005.

422 S.A. Saltzburg, K.R. Redden, *Federal Rules of Evidence Manual*, Charlottesville: The Michie Company Law Publishers 1986, p. 1005.

Rule 901(a) FRE: *"The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what it proponent claims."*

Aan het vereiste van *authentication* of *identification* als kenmerk voorafgaand aan toelating wordt voldaan door middel van bewijs welke een feit ondersteunt dat het bewijsmiddel datgene is wat het stelt te zijn.

Als voorbeeld verwijzen de *Notes of Advisory Committee* naar een telefoongesprek.[423] Als men met het telefoongesprek wil aantonen dat persoon X op locatie Y was, dan moet voldoende aangetoond worden dat persoon X ook de spreker aan de andere kant van de lijn was (bijvoorbeeld door middel van getuigenverklaringen). Als de spreker niet geïdentificeerd is, kan het middel ook niet gebruikt worden als bewijs om aan te tonen dat spreker X ook daadwerkelijk persoon X was. Aan de eis van authentication of identification is dan niet voldaan. Hetzelfde geldt mijn inziens in de elektronische wereld voor een gesprek via een chatkanaal of voor messengers, aangezien daar dezelfde vraag speelt, namelijk is de persoon waarmee wordt gechat, wel daadwerkelijk de persoon voor wie deze zich uitgeeft. Een ander voorbeeld is een e-mail. Als iemand claimt een e-mail te hebben ontvangen van persoon Y en de e-mail wordt ingezet als bewijsmiddel, dan moet aangetoond worden dat de e-mail door persoon Y is geschreven.[424]

Authentication kan naar mijn mening gezien worden als een betrouwbaarheidstoets van de intrinsieke kwaliteit van het bewijs (wat is het bewijs?) en de afkomst van het bewijsmiddel (van wie komt het bewijs?) Als authentificatie-eis wordt in Rule 901(a) FRE gesteld: *"…to support a finding that the matter in question is what its proponent claims."* Deze woorden spreken echter niet voor zichzelf. Verschillende begrippen, zoals *reliability*, *accuracy* en *integrity*, worden namelijk gebruikt in verband met het begrip *authentication*. Ter illustratie:

"The authentication requirements of Rule 901 are designed to set up a threshold preliminary standard to test the reliability of evidence (…)"[425]

"(…) consider the accuracy and reliability of computerized evidence."[426]

---

423 Notes of Advisory Committee on Proposed Rules Rule 901 FRE (Pub. L. 93-595, § 1, Jan. 2, 1975, 88 Stat. 1931.

424 D.A. Schlueter, S.A. Saltzburg (editors), *Emerging Problems Under The Federal Rules of Evidence*, Charlottesville: Lexis Law Publishing 1998, p. 377.

425 Lorraine v. Markel American Insurrance Company, 2007 WL 1300739 (DMd May 4, 2007).

426 Manual for Complex Litigation (Fourth) § 11.446 (2004).

Tevens wordt *authentication* door Rice in verband gebracht met integriteit, waarbij integriteit beschouwd wordt als een subset van *authentication*.[427] Bij het onderzoeken of een bewijsmiddel wel aan de eisen van *authentication* voldoet, moet niet alleen gekeken worden waar het bewijsmiddel vandaan komt, maar tevens naar de betrouwbaarheid van het bewijsmiddel, de mate waarin het bewijsmiddel accuraat is en of er geen onregelmatige wijzigingen zijn doorgevoerd waardoor het bewijsmiddel niet meer in de oorspronkelijke staat verkeert. Rice vat bovenstaande samen door te omschrijven wat aangetoond dient te worden om de authenticiteit vast te stellen en dus te voldoen aan Rule 901 FRE. In de eerste plaats dient men aan te tonen dat het bewijsmiddel compleet is en geen veranderingen heeft ondergaan. Ten tweede dient aangetoond te worden wat de origine is van het bewijsmiddel en, in het geval van een verklaring, van wie het bewijsmiddel afkomstig is (oftewel: wie gaat er achter de boodschap schuil). Ten derde dient, in het geval van documenten, aangetoond te worden dat degene voor wie het document is opgemaakt, gebonden wil zijn aan de inhoud van het document.

6.8.4 De bewijsdrempel van *Rule 901 FRE*

Rule 901 FRE stelt dat de *authentication* of *identification* van een bewijsmiddel voldoende (*sufficient*) moet worden aangetoond. Het bewijzen dat iets datgene is wat beweerd wordt dat het is, kent geen hoge bewijsdrempel bij het toelaten van bewijsmiddelen.[428] In de literatuur wordt gesteld dat onder *sufficient* zoals bedoeld in Rule 901 FRE wordt verstaan "*a bare showing, bleached of any analysis by the trial judge of the proffer's credibility or trustworthyness*."[429] In de rechtspraak wordt gesteld in *United States v. Safavian*:

"The threshold for the Court's determination of authenticity is not high. (…) The question for the Court under Rule 901 is whether the proponent of the evidence has "offered a foundation from which the jury could reasonably find that the evidence is what the proponent says it is" (…) The Court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so"[430]

De drempel voor de rechtbank om de authenticiteit te bepalen is niet hoog.[431] De vraag voor de rechtbank onder Rule 901 is of de aanbieder van het bewijs

---

427 P.R. Rice, *Electronic Evidence, Law and Practice*, Chicago: ABA Publishing 2008, p. 335.

428 U.S. v. Safavian, 435 F. Supp. 2d 36.

429 D.A. Schlueter, S.A. Saltzburg (editors), *Emerging Problems Under The Federal Rules of Evidence*, Charlottesville: Lexis Law Publishing 1998, p. 377.

430 In bijna gelijke bewoordingen laat de rechter zich uit in United States v. Tank, 200 F.3d 627: "*The government made a prima facie showing of authenticity because it presented evidence sufficient to allow a reasonable juror to find that the chat room log printouts were authenticated.*"

431 Het betreft de toelating. Voor de bewijswaardering zie paragraaf 6.10.

voldoende basis heeft gelegd op grond waarvan de jury in redelijkheid kan bepalen dat het bewijs datgene is wat gesteld wordt dat het is door de aanbieder. De rechtbank hoeft niet te bepalen dat het bewijs ontegenzeggelijk is wat de aanbieder stelt dat het is, maar enkel dat er voldoende bewijs is dat de jury dat uiteindelijk kan doen. De eis dat bewijsmiddelen *authentication* of *identification* behoeven, is net als de meeste regels in het Amerikaanse bewijsrecht, reeds ontstaan voordat er sprake was van elektronische gegevens. Toch lijkt het erop dat rechters geen principiële bezwaren zien om de eis van *authentication* ook van toepassing te verklaren op elektronisch opgeslagen informatie. In *In re Vee Vinhnee* verwoordt de rechter dit als volgt:[432]

"Authenticating a paperless electronic record, in principle, poses the same issues as for a paper record, the only difference being the format in which the record is maintained: one must demonstrate that the record that has been retrieved from the file, be it paper or electronic,[433] is the same as the record that was originally placed into the file." (…) "The paperless electronic record involves a difference in the format of the record that presents more complicated variations on the authentication problem than for paper records. Ultimately, however, it all boils down on the same question of assurance that the record is what is purports to be".[434]

Hoewel, zoals eerder werd gesteld, de bewijsdrempel voor *authentication* of *identification* klaarblijkelijk niet als hoog wordt beschouwd door de rechtbanken. Deze hebben blijkbaar weinig moeite om de regels van *authentication* of *identification* ook van toepassing te verklaren op informatie in elektronische vorm. Toch wordt er niet altijd aan de eisen van *authentication* of *identification* voldaan, in het bijzonder als het elektronisch opgeslagen informatie betreft. De rechter stelt in een onderzoek naar de admissibility van elektronisch opgeslagen informatie (ESI)[435] dan ook in *Lorraine v. Markel* (waar ik later in deze paragraaf verder op in zal gaan):[436]

"Ironically, however, counsel often fail to meet even this minimal showing when attempting to introduce ESI, which underscores the need to pay careful attention to this requirement. Indeed, the inability to get evidence admitted because of a failure to authenticate it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation."

---

432 In re Vee Vinhnee, 336 B.R. 437, r.o. [13].

433 Zie ook: P.R. Rice, *Electronic Evidence, Law and Practice*, Chicago: ABA Publishing 2008, p. 335.

434 Dezelfde overtuiging is de rechter toegedaan in In re F.P. 878 A.2d 91 stelt de rechter nadat appellant heeft aangegeven dat zijn e-mails en instant messages niet voldoen aan de eis van authentificatie*:"Essentioally, appellant would have us create a whole new body of law just to deal with e-mails or instant messages. (…) We believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework."*

435 ESI = electronically stored information.

436 Lorraine v. Markel American Insurance Company, 2007 WL 1300739 (DMd May 4, 2007).

Ondanks de lage bewijsdrempel, slaagt de partij die elektronisch bewijs heeft aangeboden er toch volgens de rechter vaak niet in om te voldoen aan de minimale eis van authentificatie. De rechter gaat echter nog een stuk verder door in de tweede zin van het citaat op bijna verwijtende toon de partij die faalt in het aantonen van de authenticiteit, terecht te wijzen. Hij stelt dat het niet voldoen aan de eis van authenticiteit een vorm van *self inflicted injury* is. Hoewel de rechter het niet letterlijk zegt, lijkt de boodschap op: eigen schuld, dikke bult. De vraag is of uit deze bewoordingen opgemaakt moet worden dat het niet heel ingewikkeld dan wel moeilijk is om in het geval van ESI te voldoen aan de eisen van *authentication* of *identification*?

In de volgende paragrafen zal ik deze vraag beantwoorden door onderzoek te doen naar de methoden van *authentication* en *identification* die genoemd worden in *Rule 901 F*RE en in het bijzonder de methoden van *authentication* van elektronische documenten.

6.8.5 Methoden van *authentication* of *identification*

Met de komst van digitale technologieën is het vaak eenvoudiger om documenten te vervalsen. Dezelfde technologieën bieden daarentegen ook mogelijkheden die authentificatie mogelijk maken. In deze paragraaf zal ik nader ingaan op de verschillende methoden die kunnen dienen ter authentificatie.

Terecht wordt er in *Lorraine v. Markel* door de rechter op gewezen dat *authentication* als vereiste gesteld wordt aan bewijsmiddelen, maar dat *Rule 901(a) FRE* verder niet aangeeft op welke wijze voldaan kan worden aan de eis van *authentication*:[437] *"Although Rule 901(a) addresses the requirement to authenticate electronically generated or electronically stored evidence, it is silent regarding how to do so. Rule 901(b), however, provides examples of how authentication may be accomplished (…)"*

In *Rule 901(b) FRE* wordt echter een tiental voorbeelden genoemd van *authentication* en *identification*: *"Illustrations. – By way of illustrations only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule."*

De voorbeelden die genoemd worden zijn niet uitputtend, maar dienen slechts als voorbeelden van *authentication* of *identification* ingevolge de vereisten van *Rule 901 FRE*. Dit betekent dat buiten de genoemde voorbeelden ook situaties kunnen bestaan, waarbij ook voldaan is aan de eisen van *authentication* of

[437] Lorraine v. Markel American Insurance Company, 2007 WL 1300739 (DMd May 4, 2007).

identification. Ik zal hieronder alleen ingaan op de voorbeelden van Ru*le 901(b) FRE* als die van toepassing zijn op elektronisch opgeslagen informatie; dit 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), public records or reports (Rule 901(b)(7) FRE), process or system (Rule 901(b)(9) FRE)*. Hieronder zullen eerst kort bovenstaande wettelijke voorbeelden van authentificatie worden besproken. Daarna zal in de volgende paragraaf (6.8.6) ingegaan worden op de verschillende vormen van elektronisch bewijs, omdat (zoals terecht in *Lorraine v. Markel* wordt gesteld) er niet één middel voor authentificatie is dat voor ieder bewijsmiddel geldt.[438] Er wordt een verdeling gemaakt naar soort elektronisch bewijsmiddel te weten: e-mail, internet website postings, text messages en chat room content, computer stored records en data, computer animation en computer simulations en tot slotte digital photographs. Ongeveer eenzelfde verdeling wordt overigens ook gemaakt door Rice en deze zal ik hierna ook aanhouden.[439] Aan de hand van jurisprudentie zal worden bekeken welke eisen gesteld worden om aan de authentificatie van de verschillende vormen van elektronische bewijs te voldoen.

Het eerste voorbeeld van authentificatie bestaat uit getuigenissen van experts. *Rule 901(b)(1) FRE* stelt dat een "*testimony that a matter is what it is claimed to be*" kan dienen ter authentificatie. Een voorbeeld in de rechtspraak zijn business records die werden geauthentificeerd door een getuige.[440] Indien het websites betreft dient er een verklaring of bevestiging van iemand met kennis van de website te zijn; een webmaster of iemand anders met persoonlijke kennis van de website is daartoe toereikend.[441]

Ten tweede kan gedacht worden aan *comparison by trier or expert witnesses*. *Rule 901(b)(3) FRE* geeft aan dat authentificatie mogelijk is door middel van "*comparison by the trier of fact or by expert witnesses with specimens which have been authenticated*".

Als derde voorbeeld van authentificatie voor elektronische documenten noemt Rule 901(b)(4) FRE: *"appearance, contents, substance, internal patterns, or other distinctive characters, taken in conjunctions with circumstances"*. Hierbij kan gedacht worden aan (extra) elektronische gegevens die zijn aangebracht aan of in een document (bijvoorbeeld meta informatie),[442] e-mailadressen, het

---

438 Lorraine v. Markel American Insurance Company, 2007 WL 1300739 (DMd May 4, 2007).

439 P.R. Rice, *Electronic Evidence, Law and Practice*, Chicago: ABA Publishing 2008, p. 357 t/m 400.

440 Hardison v. Balboa Ins, 4. Fed. Appx. 663, 2001 WL 135677 (A.C. 10 (Okla.).

441 St. Lukes's Cataract and Laser Institute, P.A. v. Sanderson, 2006 WL 1320242 *M.D. Fla. May 12, 2006). Zie ook: Sun Protection Factory, Inc v. Tender Corp., 2005 WL 2484710 en *In re Homestore.com, Inc. Sec. Litig.,* 347 F.Supp.2d 769, 782 (C.D.Cal.2004).

442 Sinotes-Cruz v. Gonzales, 468 F.3d 1190 : "Here, the two INS (Naturalization Service) stamps at the end of the records clearly indicate that the documents were received by an INS official on the

replyadres en namen van betrokken partijen.[443]

Als vierde methode van *authentication* worden *public records or reports* in *Rule 901(b)(7) FRE* als voorbeeld gegeven. Als public records of public reports worden gemaakt en bijgehouden, dan kunnen deze vanwege hun publieke aard en de aanname dat de ambtenaar geen belang heeft bij het vervalsen van publieke documenten,[444] worden gebruikt als middel ter *authentication*.

Een proces of systeem is het laatste voorbeeld van de methode van *authentication* in *Rule 901(b)(9) FRE.* Hierbij gaat het om bewijs dat een proces of systeem beschrijft om aan te tonen dat het proces of systeem een accurate uitkomst oplevert. Zo kunnen video-opnamen worden geauthentificeerd door de getuigenis van een videomonteur dat de videorecorder of de opnameapparatuur correct heeft gewerkt.[445]

6.8.6 *Authentication* van verschillende elektronische toepassingen

In de rechtspraak wordt in veel gevallen de authentificatie van enkel het bewijsmiddel dat in de zaak een rol speelt, beoordeeld. Als gevolg van het common law systeem, worden algemene vereisten voor authentificatie vaak niet gegeven. Er wordt ook uitdrukkelijk onderkend dat ieder bewijsmiddel zijn eigen authentificatiemethoden kent.[446] Daarom zal ik verder gaan met het bespreken van authentificatiemethoden van elektronische bewijsmiddelen waaraan in de rechtspraak aandacht is besteed. De typerende eigenschappen van deze bewijsmiddelen zijn reeds in hoofdstuk twee aan de orde geweest.

E-mail

E-mailberichten kunnen door middel van verschillende karakteristieken geauthentificeerd worden. Dit kan op basis van onderscheidende karakteristieken zoals de inhoud, interne patronen (als terugkerende reeksen met tekens), of andere onderscheidende karakteristieken die in onderlinge samenhang beoordeeld moeten worden. In *State v. Siddiqui* wordt nader beoordeeld wanneer een e-mail op grond van *Rule 901(b)(4) FRE* voldoende geauthentificeerd is, namelijk als de e-mail het e-mailadres de naam van de appalant bevat, het replyadres de naam van de appellant bevat, de feitelijke

---

dates specified, and the records on their face give every indication of being official Arizona court record. Further the dates given in the upside-down FAX notations on the bottom of the pages indicate that the documents were FAXed on the same day they were stamped as received by the INS, and the term "LEGALRECORDS" in the same notations strongly suggest that the records were FAXed from an Arizona legal records depository."

443 United States v. Siddiqui, 235 F.3d 1318.

444 Wat in mijn ogen toch een naïeve aanname is.

445 In re Welfare of L.J.L.. 2006 WL 3719652 (Minn App. Dec. 19, 2006)

446 Lorraine v. Markel American Insurance Company, 2007 WL 1300739 (DMd May 4, 2007).

gegevens van de e-mail waren de appellant bekend, deze gegevens bevatten de nickname van de appellant én de e-mail werd opgevolgd door telefoongesprekken die dezelfde informatie bevatten.[447] In *Massimo v. State* was het voldoende dat het slachtoffer appellants e-mailadres herkende, de e-mail informatie bevatte die alleen het slachtoffer, de appellant en enkele andere personen wisten, de e-mails waren geschreven op een manier zoals ook de appellant schreef én een getuige had gezien dat appellant ook al eerder aan het slachtoffer bedreigingen uitte via e-mail.[448] Hoewel in eerste instantie verschillende omstandigheden in onderlinge samenhang eerst tot de conclusie leiden dat er aan de eis van authentificatie is voldaan, neemt de rechter ook genoegen met minder. In *Swanton v. Brideois-Ashton* was het voldoende om aan de authentificatie-eis te voldoen door een getuigenverklaring van de ontvangende partij dat zij de e-mail had ontvangen van de verzendende partij in combinatie met het feit dat de inhoud van de e-mail verwijst naar gedane betalingen.[449] De vraag is echter waar de grens ligt tussen wel of niet

---

447 United States v. Siddiqui, 235 F.3d 1318: "In this case, a number of factors support the authenticity of the e-mail. The e-mail sent to Yamada and von Gunten each bore Siddiqui's e-mail address "msiddiquo@jajuar1.usouthal.edu" at the University of South Alabama. This address was the same as the e-mail sent to Siddiqui from Yamada as introduced by Siddiqui's counsel in his deposition cross-examination of Yamada. Von Gunten testified that when he replied to the e-mail apparently sent by Siddiqui, the "reply-function" on von Gunten's e-mail system automatically dialed Siddiqui's e-mail address as the sender. The context of the e-mail sent to Yamada and von Gunten shows the author of the e-mail to have been someone who would have known the very details of Siddiqui's conduct with respect to the Waterman Award and the NSF's subsequent investigation. In addition, in one e-mail sent to von Gunten, the author makes apologies for cutting short his visit to EAWAG, the Swiss Federal Institute for Environmental Science and Technology. In his deposition, von Gunten testified that in 1994 Siddiqui had gone to Switzerland to begin a collaboration with EAWAG for three or four months, but had left after only three weeks to take a teaching job. Moreover, the e-mail sent to Yamada and von Gunten referred to the author as "Mo." Both Yamada and von Gunten recognized this as Siddiqui's nickname. Finally, both Yamada and von Gunten testified that they spoke by phone with Siddiqui soon after the receipt of the e-mail, and that Siddiqui made the same requests that had been made in the e-mail. Considering these circumstances, the district court did not abuse its discretion in ruling that the documents were adequately authenticated."

448 Massimo v. State 144 S.W.3d 210:" Likewise, the characteristic evidence concerning State's Exhibit 6, purported e-mails sent from Massimo to Sparby, yields the following: (1) the e-mails were signed "Amanda," Massimo's given name, and were sent from an e-mail address Taylor recognized as belonging to Massimo, babycol20@yahoo.com; (2) the e-mails exchanged between Massimo and Sparby are consistent with Sparby's testimony that Massimo was not responding to her efforts to talk to her and was uncooperative; (3) the author of the e-mails knew the subject of the investigation, harassing e-mails, before Sparby revealed that to her; and (4) the November 16 e-mail threatened to report Sparby for harassment, and was sent the same day that Massimo appeared at the police station in person to file harassment charges against Sparby. While Massimo asserted defensively that someone was impersonating her and sending the e-mails on her behalf, she introduced no evidence to support this assertion, and Taylor specifically denied such action. Again, in reviewing the admission of evidence under Texas Rules of Evidence 901, and under the abuse of discretion standard, we cannot say that the trial court abused its discretion in admitting State's Exhibit 6 over a lack-of-authentication objection." Zie voor een soortgelijke zaak met toepassing van gelijke criteria: Texas v. Shea, 167 S.W.3d 98.

449 Swanton v. Brideois-Ashton, 134 Wash.App. 1067, 2006 WL 2664497:" In her supporting declaration, Swanton identified the e-mails as those that she had received on her computer from

voldoende bewijs voor authentificatie. Die grens ligt in ieder geval voorbij het enkel kunnen aantonen van welk e-mailadres de e-mail afkomstig is;[450] er dienen altijd bijkomende elementen te zijn die aantonen dat de e-mail daadwerkelijk van een bepaalde persoon komt. Deze bijkomende elementen dienen qua kwaliteit dan wel kwantiteit groter te zijn als door de aangewezen schrijver wordt ontkend dat deze de e-mail heeft geschreven.[451]

Text messages en chat room content

Tekstberichten en *chat room content* kunnen gebruikt worden als bewijs in een rechtszaak. Daartoe moet volgens Salzburg cumulatief vastgesteld worden dat (1) de persoon die schuil gaat achter de chatnaam ook de persoon is die deelnam aan het chatgesprek, (2) als er een afspraak wordt gemaakt met deze persoon, ook die persoon verschijnt, (3) deze persoon zich ook identificeert als de persoon achter de chatnaam, (4) deze persoon over informatie beschikt die hij heeft verkregen tijdens de chat en (5) bewijs van de harddisk van de computer (zoals de chat naam).[452] Naar mijn mening komen de punten 1 t/m 5 erop neer dat aangetoond dient te worden dat de persoon waarvan gesteld wordt dat hij de chat heeft gevoerd, ook daadwerkelijk de persoon is die de chat heeft gevoerd. Daarnaast moet aangetoond worden dat de prints van de chat authentiek zijn.

Beide stappen ((1) authentificatie van de print en (2) authentificatie van de persoon achter het gesprek) worden ook gemaakt in *United States v. Tank*.[453]

Ashton. The record before the trial court also included corroborating evidence documenting the payments that Ashton referred to in the July 20, 2003, e-mail. These circumstances, which were uncontroverted, were sufficient to establish the authenticity of the e-mails."

450 Morgenstern v. Entpro, Cal. Rptr.3d, 2007 WL 475481:" The only evidence was when Morgenstern's counsel received the documents and Morgenstern's statements describing the documents, none of which he authored. Counsel's statement that he received the documents is not proper authentication. Morgenstern's description of the writings, none of which he authored, do not authenticate them."

451 Hood-O'hara v. Wills, 873 A.2d 757, 2005 PA Super 145:"Additionally, as pointed out by the trial judge, there were authentication problems with regards to the e-mails. Although testimony revealed that the e-mail address grannyprix@aol.com did in fact belong to O'Hara's mother, Mrs. Hood, it was denied by Mrs. Hood that she was the author of the e-mails. (…) We find that the e-mails were properly excluded" Zie ook: CCP Limited Partnership v. First Source Financial Inc., 856 N.E.2d 492.

452 S.A. Saltzburg, *Federal Rules of Evidence Manual, Part 4*, Newark / San Francisco: LexisNexis 2002, p. 20.

453 United States v. Tank, 200 F.3d 627: "In testimony at the evidentiary hearing and at trial, Riva explained how he created the logs with his computer and stated that the printouts, which did not contain the deleted material, appeared to be an accurate representation of the chat room conversations among members of the Orchid Club. (…) The government also established a connection between Tank and the chat room log printouts. There is no question that the chat room log printouts were relevant to prove the conspiracy charge in the indictment and Tank's participation in the conspiracy. Tank admitted that he used the screen name "Cessna" when he participated in one of the conversations recorded in the chat room log printouts. Additionally, several co-conspirators testified that Tank used the chat room screen name "Cessna" that appeared throughout the printouts. They further testified that when they arranged a meeting with

Voor authentificatie van de print van de chat is voldoende dat de persoon die de prints heeft uitgedraaid, verklaart dat hij de prints heeft gemaakt, dat deze niet gewijzigd zijn en dat deze de volledige en accurate inhoud weergeven van de chat. Voor authentificatie van de persoon achter de chat is voldoende dat persoon X heeft aangegeven dat deze een bepaalde chatnaam gebruikte, dat ook andere chatters getuigden dat deze persoon X deze chatnaam gebruikte en dat toen zij een afspraak hadden met persoon X die de chatnaam gebruikte, ook persoon X kwam opdagen.

In *United States v. Simpson* komt slechts de authentificatie van de persoon aan de orde. De combinatie van inhoud van de uitdraaien van de chatgesprekken, waaronder het e-mailadres van de verdachte, het correcte huisadres, en de aantekeningen inhoudende het adres, e-mail en telefoonnummers van de undercover agent die gevonden werden naast de computer van de verdachte, leveren voldoende bewijs op om de persoon achter de chat te authentificeren.[454]

In Hammontree v. State wordt nader ingegaan op instant messages.[455] Voor instant messages geldt dat deze geauthentificeerd kunnen worden door middel van de inhoud van de berichten waarin de verzender zichzelf identificeert. Ondanks het feit dat het bericht werd verstuurd vanaf een account toebehorend aan een ander gezinslid (namelijk de zoon) was een getuigenverklaring van die zoon dat hij het bericht niet had geschreven in combinatie met het feit dat de account niet beveiligd was met een wachtwoord, waardoor iedereen die toegang had tot de computer het bericht had kunnen schrijven.

In United States v. Jackson wordt bewijs echter niet toegelaten. Het betreft chats waarvan enkel kopieën van de chat die door middel van knippen-en-plakken in Word bewaard zijn gebleven.[456] Het blijkt dat verschillende regels halverwege zijn afgebroken. Daarnaast zijn er aantekeningen gemaakt in het

---

the person who used the screen name "Cessna," it was Tank who showed up. On the record before us, it is clear that the government made an adequate foundational showing of the relevance and the authenticity of the chat room log printouts. Thus, we cannot say that the district court abused its discretion by admitting the printouts into evidence and allowing the jury to decide what weight to give that evidence."

454 U.S. v. Simpson, 152 F.3d 1241, 49 Fed. R. Evid. Serv. 1631, 98 CJ C.A.R. 4348.

455 Hammontree v. State 642 S.E.2d 412: "Although the instant message was sent from the account of Hammontree's son, there was evidence from which the jury could infer the sender of the message was Hammontree. The sender of the message identified himself as "Jeff", "spider man," and "daddy." Hammontree's son, who testified at trial, denied being the sender of the message or participating in the conversation. And the victim testified that anybody who had access to the computer in the Hammontree home could send an instant message from Hammontree's son's account, which was not password protected. Under these circumstances, the trial court did not abuse its discretion by admitting the challenged evidence."

456 U.S. v. Gerald Jackson, 488 F. Supp. 2d 866.

Word document. Hierdoor is het Word document niet langer voldoende betrouwbaar als bewijsmiddel en is het niet toegelaten op grond van Rule 901 FRE.[457]

Internet website postings

Informatie op websites kan relevant zijn als bewijsmiddel. Rechters hanteren bij de authentificatie van de informatie op websites niet altijd een eenduidige aanpak. Zo stelt de rechter in *St. Clair v. Johnny's Oyster and Shrimp, Inc.* dat informatie op websites niet zomaar toegelaten kan worden gezien het feit dat iedereen die informatie op een website kan hebben geplaatst. De rechter beschouwt websites dan ook een katalysator voor roddel, insinuaties en onjuiste informatie.[458] Aan het einde van zijn overweging stelt de rechter nog dat ieder bewijs verkregen van het internet voldoende adequaat is voor bijna niets. Dezelfde opvattingen hebben het *Court of Appeals* in *Basada v. Mukasey* en *het Court of Federal Claims* in *Campbell v. Sectretary of Health and Human Services.*[459] In beide zaken heeft een lagere instantie (respectievelijk een rechter en een arbiter) zich gebaseerd op informatie gevonden op Wikipedia en in beide gevallen wordt deze informatie niet voldoende betrouwbaar geacht om een beslissing op te baseren.[460] Diametraal met deze opvatting lijkt de rechter in *Perfect 10, Inc. v. Cybernet Ventures, Inc* staan.[461] Daar oordeelt de rechter dat printouts van website postings voldoende geauthentificeerd zijn als deze aan de criteria voldoen die in *United States v. Tank* voor chat room content aangelegd zijn.[462] Toch gaat de rechter vervolgens alleen in op de authentificatie van de print van de website posting. Daarbij oordeelt de rechter

---

457 Overigens speelt hier ook het probleem van best evidence. Ook op grond van Rule 1001 t/m 1004 FRE wordt het bewijs niet toegelaten. Zie ook paragraaf 6.10.

458 St. Clair v. Johnnoy's Oyster and Shrimp, Inc., 76 F.Supp.2d 773, 2000 A.M.C. 769, 53 Fed. R. Evd. Serv. 1.:" Plaintiff's electronic "evidence" is totally insufficient to withstand Defendant's Motion to Dismiss. While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation. So as to not mince words, the Court reiterates that this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon in his Response to Defendant's Motion. There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No web-site is monitored for accuracy and *nothing* contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on *any* web-site from *any* location at *any* time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules found in FED.R.CIV.P. 807."

459 Basada v. Mukasey, 540 F.3d 909 en Campbell v. Sectretary of Health and Human Services, 69 Fed.Cl. 775.

460 Zie ook het commentaar: R. Jason Richards, Courting Wikipedia, 44 Trial 62 9Apr. 2008) "Since when did a Web site that any Internet surfer can edit become an authoritative source by which law students could write passing papers, experts could provide credible testimony, lawyers could craft legal arguments, and judges could issue precedents?"

461 Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F.Supp.2d 1146. Hetzelfde is het geval in Premier Nutrition Inc. v. Organic Food Bar Inc., F. Supp. 2d, 2008 WL 1913163 (C.D. Cal.).

462 United States v. Tank, 200 F.3d 627.

dat de website postings echte en correcte kopieën van pagina's die geprint zijn van het internet omdat de persoon die ze heeft uitgedraaid dit heeft verklaard. Hierbij gaat de rechter niet zozeer in op de waarheid van de informatie op de kopieën, maar authentificeert hij enkel of de informatie op de kopieën dezelfde is als op de website.

Computer stored records en data

Voor bestanden en data die op elektronische wijze zijn opgeslagen bestaat niet één strikte eis die gesteld wordt aan de authentificatie. Rechters gaan op een strikte of juist veel minder strikte wijze om met data die op elektronische wijze is opgeslagen. Het contrast wordt het beste duidelijk aan de hand van *United States v. Meienberg* en *In re Vee Vinhnee*. In de eerste zaak wordt gesteld dat de rechter voor authentificatie geen genoegen mag nemen met een verklaring van degene die een print heeft gemaakt van de data, maar dat ook aangetoond moet worden dat de data accuraat is. Daarop oordeelt de rechter dat accuraatheid niet wordt beoordeeld bij de beoordeling van de authentificatie, maar dat accuraatheid wordt beoordeeld in de fase van bewijswaardering.[463] Deze lijn vindt echter weinig aanhang bij andere rechters. Een veel zwaardere authentificatietoets wordt aangehouden in *In re Vee Vinhnee*.[464] Volgens de rechter komt het niet zozeer aan op de omstandigheden waaronder de records zijn gecreëerd, maar eerder op de omstandigheden waaronder de record bewaard werd om ervan zeker te kunnen zijn dat het document hetzelfde document is als dat oorspronkelijk is gecreëerd. Om te beoordelen of de integriteit niet is aangetast moet niet alleen gekeken worden naar de identificatie van de gebruikte computers en progamma's, maar evenzo naar de policies en de procedures die zijn gehanteerd bij het gebruik van de computers en programma's. Hoe wordt de toegang tot de database beheerd en hoe wordt de toegang tot de programma's beheerd? Hoe worden veranderingen in de database bijgehouden? Tevens moet onderzocht worden hoe de structuur en implementatie van back up systemen en audits bijdragen aan het bewaren van de integriteit van de database.[465] In *Lorraine v. Markel* wordt ingegaan op het feit dat rechters zich in twee kampen lijken te bevinden, waarbij de ene rechter veel striktere eisen stelt aan de eis van authentificatie dan de andere rechter.

---

463 United States v. Meienberg, 263 F.3d 1177: "Any question as to the accuracy of the printouts, whether resulting from incorrect data entry or the operation of the computer program, as with inaccuracies in any other type of business records, would have affected only the weight of the printouts, not their admissibility."

464 Zie ook noot 114.

465 In re Vee Vinhnee, 336 B.R. 437:" The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the question of whether records have been changed since their creation."

"*Lawyers can expect to encounter judges in both camps, and in the absence of controlling precedent in the court where an action pending setting forth the foundational requirements for computer records, there is uncertainty about which approach will be required. Further although "it may be better to be lucky than good," as the saying goes, counsel would be wise not to test their luck unnecessarily. If it is critical to the success of your case to admit into evidence computer stored records, it would be prudent to plan to authenticate the record by the most rigorous standard that may be applied. If less is required, then luck was with you*."

6.9 *Best evidence*

6.9.1 Inleiding

De *best evidence rule* is een regel die stelt dat in beginsel alleen het originele bewijs is toegestaan als bewijsmiddel en dat secundair bewijs is toegelaten als aan specifieke voorwaarden voldaan is. De *best evidence rule* is gecodificeerd in *Rule 1002 FRE* en stamt af van *case law* waarin werd bepaald dat geen bewijs was toegelaten, tenzij het het beste bewijs was dat gezien de aard van de zaak mogelijk was.[466] Deze regel kent haar ratio in het feit dat het in de achttiende eeuw gebruikelijk was dat kopieën werden gemaakt door de klerk. Het idee is gestoeld op de aanname dat als er geen origineel document kon worden getoond er wel met de kopie moest zijn geknoeid. *Best evidence* is een regel die voortkomt uit het bestaan van fraude.[467] Met de komst van elektronische methodes van reproductie en het grote gebruik van elektronische reproducties in het zakelijk verkeer, is het de vraag in hoeverre de *best evidence rule* beperkingen oplevert voor het toelaten van elektronische bewijsmiddelen. Deze bewijsmiddelen in elektronische vorm dienen om door mensen bekeken te kunnen worden, worden afgedrukt of op een beeldscherm zichtbaar te worden gemaakt. Is er dan echter nog sprake van een origineel exemplaar en is er nog wel sprake van *best evidence*. Ook hebben deze bewijsmiddelen als eigenschap dat deze regelmatig gekopieerd worden, waarna het originele exemplaar gewist wordt of verloren gaat. De vraag is hoe het Amerikaanse bewijsrecht hiermee omgaat.

---

466 Omychund v. Barker (1745) 1 Atk, 21, 49; 26 ER 15, 33; Zie ook: B.A. Garner a.o. Black's Law Dictionary, Thomson West: St. Paul 2004 (best evidence):"Evidence of the highest quality available, as measured by the nature of the case rather than the thing being offered as evidence."

467 J.W. Cotchett, *Federal Courtroom Evidence*, Newark / San Francisco: LexisNexis / Matthew Bender 2002, p. 25-2. Zie ook: P.R. Rice, *Electronic Evidence, Law and Practice*, Chicago: ABA Publishing 2008, p. 298.

6.9.2 Grondslag voor *best evidence* en *secundary evidence* als toelatingseis

In *Rule 1002 FRE* wordt het beginsel van *best evidence* verwoord: *"To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or Act of Congress."*

Om de inhoud van een geschrift, opname of afbeelding te bewijzen is volgens *Rule 1002 FRE* in beginsel vereist dat het originele exemplaar overlegd wordt. Het beginsel van best evidence kan echter doorbroken worden in het geval dat de FRE of een wet van het *Congress* anders bepalen. Onder de *best evidence rule* wordt in beginsel alleen het meest originele (primaire) bewijsmiddel toegelaten in een rechtszaak. Op deze regel bestaat een tweetal uitzonderingen. Het bewijs dat onder deze uitzonderingen wordt toegelaten in de rechtszaak wordt ook wel secundair bewijs genoemd. Secundair bewijs bestaat uit *duplicates* en uit ander bewijs.

In de eerste plaats zijn er de duplicaten. De rechtsgrond voor het toelaten van een *duplicate* wordt gegeven in *Rule 1003 FRE*, welke stelt:*"A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original."*

Rule 1003 FRE opent de mogelijkheid om in plaats van het origineel, een *duplicate* toe te staan als rechtsgeldig bewijsmiddel. In het geval dat een *duplicate* wordt overlegd en de methode waarmee het *duplicate* is gemaakt is voldoende accuraat en precies, zou het *duplicate* zonder problemen gebruikt kunnen worden als bewijsmiddel. *Rule 1003 FRE* kent echter twee gronden waarop een *duplicate* niet wordt toegestaan. In de eerste plaats kan de authenticiteit van het *original* oprecht in twijfel worden getrokken (bijvoorbeeld als er het vermoeden bestaat dat er geknoeid is met het *original*) met het gevolg dat het bewijs niet wordt toegelaten. Een enkele speculatie of suppositie betreffende de authenticiteit van het bewijsmiddel is niet voldoende om oprechte twijfel te zaaien.[468] De tweede reden dat bewijs niet zou kunnen worden toegelaten is dat het onrechtvaardig is om het *duplicate* toe te laten ter vervanging van het *original*. Naar mijn mening zou hiervan sprake kunnen zijn als de partij die een *duplicate* in het geding brengt het *original* met opzet doet verdwijnen en de rechter geen andere keus te laten dan het *duplicate* te accepteren. Het enkel verdwijnen zonder dat het aannemelijk is dat er sprake is van opzet maakt niet dat een bewijsmiddel niet meer toegelaten wordt; ook

[468] People v. Huehn, 53 P.3d 733, 738 (Colo.Ct.App.2002): "Mere speculation or supposition that an original document may have contained information that the duplicate did not, or vice versa, does not amount to a showing that it would be unfair to admit the duplicate and thus does not preclude admission of the duplicate under CRE 1003."

niet in het geval van elektronische bewijsmiddelen.[469]

In de tweede plaats zijn er andere bewijsmiddelen dan het *original*. In een aantal in de *FRE* omschreven gevallen wordt ander bewijs dan het *original* toegelaten. Hier wordt niet zozeer gedoeld op *duplicates* daar die als op grond van *Rule 1003 FRE* worden toegelaten, maar het betreft ander bewijs. *Rule 1004 FRE* stelt:

"The original is not required, and other evidence of the contents of a writing, recording, or photograph is admissible if-
(1) (…) All originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith; or
(2) (…) Original not obtainable. No original can be obtained by any available judicial process or procedure; or
(3) (…) At a time when an original was under the control of the party against whom offered, that was put on notice, by the pleadings or otherwise, that the contents would be a subject of proof at the hearing, and that party does not pruduce the original at the hearing, or
(4) (…) The writing, recording, or photograph is not closely related to a controlling issue."

Rule 1004 FRE stelt dat een origineel niet noodzakelijk is en ander bewijs van de inhoud van een *writing, recording* of *photograph* toegestaan is als er aan een van de in leden 1 tot en met 4 van datzelfde artikel is voldaan. *Rule 1004 FRE* kent geen gradaties van secundair bewijs, wat in de praktijk wil zeggen dat er geen voorkeur bestaat van toepassing van één van deze leden, als meer dan één van de vier genoemde situaties van toepassing is. Verder worden er geen eisen gesteld aan secundair bewijs; het is aan de rechter om bij de waardering te komen tot een beoordeling van de bewijswaarde van het bewijsmiddel. Secundair bewijs is ingevolge lid 1 van *Rule 1004 FRE* toegestaan als alle *originals* zijn verdwenen of vernietigd, tenzij de wederpartij deze te kwader trouw heeft laten verdwijnen of vernietigd. Deze regel is naar mijn mening een logische en rechtvaardige tegemoetkoming aan de eisende partij als deze wordt dwarsgezeten door een tegenpartij die bewijs te kwader trouw laat verdwijnen of vernietigt.

Twee begrippen die in *Rule 1002 FRE* en *Rule 1003 FRE* worden genoemd, spelen een sleutelrol en worden nader uitgewerkt in *Rule 1001 FRE*. Dit zijn

[469] People v. Huehn, 53 P.3d 733, 738 (Colo.Ct.App.2002): "Admission of the duplicate was not an abuse of discretion. The foundation witness testified that the location of the original tape was unknown, and there was nothing to indicate that the original had been lost or destroyed in bad faith. For the reasons set forth in Part I, above, there is no genuine question as to the authenticity of the original tape. Finally, defendant has not shown that it was unfair to admit the duplicate in lieu of the original."

writings, recordings en photographs en het *original*. Als er geen sprake is van een *writing, recording of photograph*, dan is de *best evidence rule* ook niet van toepassing.[470] De volgende twee paragrafen zullen nader ingaan op de begrippen *writings, recordings* en *photographs* en de begrippen *original* en *duplicate.*

6.9.3 Subject van *best evidence*: *writings, recordings* en *photographs*

De *best evidence rule* wordt voorafgegaan door *Rule 1001(1) FRE* welke de definities geeft van de begrippen *writings*, *recordings*, *photographs*, *originals* en *duplicates*: *"Writings and recordings consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation."*

Voordat er getoetst kan worden of er sprake is van *best evidence*, moet worden onderzocht of de *beste evidence rule* wel van toepassing is. Met andere woorden: er moet sprake zijn van een *writing* of *recording*. In sommige gevallen kan er worden gediscussieerd of iets een *writing* of *recording* is. Het is namelijk de vraag of bijvoorbeeld een serienummer als *writing* aangemerkt moet worden of slechts een reeks nummers die een produkt identificeren. De rechter heeft grote discretionaire bevoegdheid bij het beoordelen of er sprake is van een *writing* of slechts van leestekens.[471] In de rechtspraak is vast komen te staan dat alleen *writings* en niet leestekens onderwerp zijn van de *best evidence rule*.[472] Daarbij moet tevens in acht worden genomen dat *writings* en *recordings* alleen onder de *best evidence rule* vallen als deze aangeboden worden "*to prove its contents*".[473]

Toen in de twintigste eeuw steeds meer *writings* en *records* werden opgemaakt in elektronische vorm, is het toepassingsbereik van de *best evidence rule* uitgebreid met equivalenten van *writings* en *recordings*. *Rule 1001(1) FRE* gaat namelijk verder met:"*or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation."* In principe is de reikwijdte zo breed geworden, dat iedere vorm van elektronisch opgeslagen informatie kan vallen onder het bereik van *electronic recording* of iedere andere vorm van *data compilation*.

---

470 S.A. Saltzburg, M.M. Martin, D.J. Capra, Fe*deral Rules of Evidence Manual, A complete guide to the Federal Rules of Evidence, volume 5*, Newark / San Francisco: LexisNexis 2002, p. 1001-3.

471 G.C. Lilly, *Principles of Evidence*, St. Paul: Thomson West 2006. p. 42.

472 United States v. Duffy, 454 F.2d 809 (5th Cir. 1972).

473 Rule 1002 FRE.

Rule 1001(2) FRE definieert niet zozeer het begrip *photographs* zelf, maar geeft een aantal juridische gelijkstellingen die onder het begrip *photographs* worden geschaard: "*photographs include still photographs, X-ray films, video tapes, and motion pictures*." Niet alleen stilstaande beelden, maar ook bewegende beelden en andere afbeeldingen moeten hieronder verstaan worden. Hoewel in tegenstelling tot *Rule 1001(1) FRE*, *Rule 1001(2) FRE* zwijgt over een gelijkstelling van de elektronische variant van *photographs*, valt er wel een gelijkstelling met het origineel te vinden in de derde zin van *Rule 1001(3) FRE* voor de foto of film die op elektronische wijze is vastgelegde. Deze regel zegt: *"An 'original' of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original'."* Een negatief van een foto of film wordt niet gelijkgesteld met een foto of film, maar kan wel beschouwd worden als origineel daarvan. In dat geval bestaan er meerdere *originals* naast elkaar. Voor data die photos en/of films bevat en die op elektronische wijze is opgeslagen wordt de visualisatie of output middels print of op een scherm beschouwd als een *original* als aangetoond kan worden dat de data accuraat weergegeven wordt.

6.9.4 Het *original* en het *duplicate*

Rule 1001(3) FRE geeft de definitie wat verstaan moet worden onder een *original* van een *writing* of *recording*, namelijk: *"An 'original' of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An 'original' of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original'."*

De eerste zin van deze tekst spreek naar mijn mening niet voor zich. Een *original* kan de *writing* of de *recording* zelf zijn, maar ook ieder equivalent dat tot doel heeft hetzelfde effect te hebben bij de gebruiker die het tot stand brengt of gebruik van maakt. Bij dit equivalent moet gekeken worden naar de bedoeling van de partijen die dit equivalent uitgeven.[474] Ook als de *originals* niet hetzelfde uiterlijk hebben, maar wel dezelfde inhoud hebben en partijen de bedoeling hebben dat de documenten als *originals* worden beschouwd, dan behandelt het recht deze als *originals*.[475] Dit kan ook een *duplicate* zijn, welke door de bedoeling juridisch beschouwd kan worden als *original*.[476] Hierbij kan in een niet elektronische variant gedacht worden aan een carbon copy van een

[474] S.A. Salzburg, M.M. Martin, D.J. Capra, *Federal Rules of Evidence Manual, A complete guide to the Federal Rules of Evidence, volume 5*, Newark / San Francisco: LexisNexis 2002, p. 1001-3.
[475] P.R. Rice, *Electronic Evidence, Law and Practice*, Chicago: ABA Publishing 2008, p. 300.
[476] G.C. Lilly, *An Introduction to the Law of Evidence*, St. Paul: West Publishing Co. 1978, p. 435.

reçu,[477] welke door de uitgever daarvan beschouwd mag worden hetzelfde effect te hebben als het origineel (namelijk als bewijsstuk). In de elektronische wereld zou gedacht kunnen worden aan de print van een foto in elektronische vorm of de afdruk van een elektronisch document.[478] In het bijzonder in het geval van elektronische documenten kunnen er meerdere uitdraaien bestaan. In dat geval bestaan er meerdere *originals* met gelijke bewijskracht.[479]

Interessant is in dit geval ook de bepaling van het origineel van het telegram naar analogie van de regels betreffende transmissierisico in het verbintenissenrecht. Bepaalt de verzender de transmissiemethode dan wordt het exemplaar dat de ontvanger ontvangt, beschouwd als een origineel. Bepaalt de ontvanger de transmissiemethode, dan wordt het stuk dat door de verzender is verstuurd, beschouwd als het origineel.[480] Hoewel in de literatuur geopperd wordt dat deze regel naar analogie toepasbaar is op e-mail en andere elektronische berichten,[481] zijn hier geen voorbeelden van te vinden in de rechtspraak dat deze regel inderdaad opgaat voor e-mail en andere vormen van elektronisch berichtenverkeer. De oorzaak zou kunnen liggen in het feit dat het niet nodig was deze stelling te verdedigen, omdat het bewijs ook als duplicaat zou kunnen zijn toegelaten.

De tweede zin van *Rule 1001(3) FRE* is vooral voor informatie in elektronische vorm van belang:"*An 'original' of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original'."* Aan deze regel is reeds aandacht besteedt in de voorgaande paragraaf.

Naast het *original* kan een *duplicate* onder omstandigheden worden toegelaten in een rechtszaak. Wat verstaan moet worden onder *duplicate* wordt nader omschreven in *Rule 1001(4) FRE*:

"A 'duplicate' is a couterpart produced by the same impression as the original, or from the same matrix, or by means of photograpy, including enlargements and miniatures, or by mechanical or electronic re-recoring, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original."

---

477 United States v. Rangel, 585 F.2d 344 8th Cir. 1978.

478 G.C. Lilly, *An Introduction to the Law of Evidence*, St. Paul: West Publishing Co. 1978, p. 435.

479 G.C. Lilly, *An Introduction to the Law of Evidence*, St. Paul: West Publishing Co. 1978, p. 435.

480 M.H. Graham, *Federal Rules of Evidence in a Nutshell*, St. Paul: Thomson West 2007, p. 595.

481 Notes of Advisory Committee on Proposed Rules Rule 1001(3) FRE (Pub. L. 93-595, § 1, Jan. 2, 1975, 88 Stat. 1931.); M.H. Graham, *Federal Rules of Evidence in a Nutshell*, St. Paul: Thomson West 2007, p. 595.

Deze regel opent de weg om zo goed als iedere reproductie die er precies hetzelfde uitziet als het origineel (*by the same impression as the original*) of volgens dezelfde matrix wordt geproduceerd en welke het origineel accuraat reproduceert, te beschouwen als een *duplicate* in de zin van Rule 1001(4) *FRE*. Het is dan ook deze regel die ervoor zorgt dat de meeste bezwaren die worden ingebracht voor het gebruik van *duplicates* niet langer kunnen worden gebruikt.

Deze regel gaat nog een stap verder. Niet alleen als data accuraat wordt weergegeven wordt deze weergave beschouwd als een origineel, maar ook als deze met behulp van digitale technieken *enhanced* is, waarbij wel duidelijk moet zijn wat er verbeterd is.[482]

6.9.5 *Best evidence rule* en elektronische bewijsmiddelen

6.9.5.1 *Best evidence* en code

Het is de vraag of code moet voldoen aan de eis van *best evidence*. Is dit namelijk het geval dan kan dit aanzienlijke gevolgen hebben voor de technische eisen die gesteld moeten worden aan een code. Van belang is te weten of een code gekwalificeerd kan worden als een *writing, recording* of *photograph* welke tevens als *original* beschouwd kan worden, want als dat het geval is dient te worden voldaan aan de eis van *best evidence* om (de inhoud van) de code te kunnen gebruiken als bewijs.

Eerst moet worden bepaald of code kan worden gekwalificeerd als *writing, recording* of *photograph* als bedoeld in *Rule 1001(1) FRE*. In paragraaf 2.2 heb ik beschreven dat elektronische gegevens, waaronder code, in de vorm van bits worden opgeslagen op een gegevensdrager. Code bestaat uit instructies met als adressant de computer. Het bevat geen boodschap die aan mensen gericht is. Toch kan verdedigd worden dat hogere vormen van code, zoals source code, maar misschien zelfs machine code aangemerkt worden als letters en cijfers en daarmee als writing in de zin van Rule 1001(1) FRE worden gekwalificeerd.

Uitgaande dat code inderdaad als *writing* kan worden gekwalificeerd, dan zou deze subject kunnen zijn van de best *evidence rule*. Bij de beoordeling of een writing valt onder het bereik van de *best evidence rule* als beschreven in *Rule 1002 FRE* moet er sprake zijn van "*to prove the content of a writing*". Deze content (van code) bestaat uit instructies voor een machine. Als een partij nu juist wil bewijzen hoe een machine heeft gefunctioneerd en welke acties een machine heeft uitgevoerd, dan lijkt mij ook voldaan aan het vereiste "*to prove the content of a writing*"; de inhoud van de code representeert dan namelijk de werking van de machine. Hiermee sluit ik niet uit dat de *best evidence rule* ook

[482] United States v. Seifert, 351 F. Supp.2d 926, 66.

van toepassing kan zijn op code.

Een volgende vraag die zich aandient is hoe omgegaan moet worden met code die zichzelf verplaatst over een netwerk? Het technisch procedé dat daarvoor gebruikt wordt, bestaat uit het kopiëren van de code van locatie A naar locatie B, om vervolgens de code te verwijderen van locatie A. Is er dan nog wel sprake van *best evidence*? Moet de kopie op locatie B beschouwd worden als *original*, aangezien op locatie A zich geen code meer bevindt en alleen de code nog bestaat op locatie B? In paragraaf 6.10.4 is onderzocht waar een *original* aan moet voldoen. Daarbij is gebleken dat er meerdere originelen kunnen bestaan van dezelfde *writing, recording* of *photograph* op grond van de bedoeling die partijen hadden bij het produceren van deze *originals*. Nadat de code zich heeft verplaatst bestaan er kort twee exemplaren, waarna het eerste exemplaar wordt verwijderd. Dit procedé kan zich vervolgens herhalen. Op het moment dat er twee exemplaren van dezelfde code bestaan, is er naar mijn mening sprake van twee *originals*; beide codes zijn *originals*. Een print van een elektronisch document moet opgevat worden als een *original* en als er meerdere prints gemaakt worden is er sprake van meerdere *originals*.[483] Voor het geval van code welke zich verplaatst over een netwerk is de kopie in feite niet meer dan een exacte kloon van het *original*.

Indien de gekopieerde code niet als *original* beschouwd mag worden, is de *best evidence rule* dan een beletsel om code toch toe te laten? Eventueel kan code namelijk ook als secundair bewijs worden toegelaten. Op grond van R*ule 1003 FRE* is een *duplicate* ook toegelaten, behalve als er oprechte twijfel is over de authenticiteit van het origineel of het onder de gegeven omstandigheden onrechtvaardig is om het duplicaat in plaats van het origineel toe te laten. Deze twee laatste eisen zien niet op het bewijsmiddel zelf en daarom kunnen deze eisen niet betrokken worden in de eisen die gesteld worden aan elektronische bewijsmiddelen.

6.9.5.2 Best evidence en data

Data is een vorm waarin informatie kan worden opgeslagen. Deze informatie bestaat vaak uit teksten, informatie, beeldmateriaal en in sommige gevallen ook geluidsopnames. De vraag is of data in elektronische vorm ook onderwerp van de eis van *best evidence* is. Daarvoor moet eerst gekeken worden of data onder toepassingsbereik van *writing, recording* of *photog,* valt. Voor *writings* is een gelijkstelling met data te vinden in *Rule 1001(1) FRE*. *Writings* kunnen ook in elektronische vorm opgemaakt zijn. Voor beeldmateriaal (foto's, film) is *Rule 1001(3) FRE* van toepassing, welke data niet gelijk stelt met foto's en film, maar waarbij de print of output op een scherm beschouwd wordt als een *original* van die foto/film. Voor wat betreft de elektronische vorm van data zie ik geen

[483] G.C. Lilly, *An Introduction to the Law of Evidence*, St. Paul: West Publishing Co. 1978, p. 435.

probleem voor toepassing van de *best evidence rule.*

De vraag is of er bij data wel sprake is van een *original* een *duplicate* of geen van beide? Data voor zoverre die *writings* bevatten, vallen op grond van *Rule 1001(1) FRE* al onder het begrip van *writings*. Op grond van *Rule 1001(2) FRE* is daarmee de data zelf al een *original*. Voor foto's en films geldt dat *Rule 1001(3) FRE* de prints en visualisaties op een beeldscherm als origineel beschouwd. Niet de data zelf is daarmee een *original*, maar slechts de visualisatie.

Verschillende schrijvers hebben reeds opmerkingen gemaakt over de toepasselijkheid van de *best evidence rule*. Zo stelt Rice dat de *best evidence rule* in het internet tijdperk zijn beste tijd gehad heeft en eigenlijk een relikwie is uit het verleden.[484] Problemen met de *best evidence rule* ontstaan nauwelijks bij elektronisch opgeslagen informatie,[485] sinds de b*est evidence rules* zijn aangepast aan de moderne tijd waar dit soort informatie veelvuldig gebruikt wordt. Skupsky heeft een artikel gewijd aan het feit dat de *best evidence rule* geen betekenis meer heeft in de moderne rechtspraktijk. Volgens hem komt het erop neer dat men bewijst dat het bewijsmiddel voldoende wordt geauthentificeerd.[486]

6.10 Bewijswaardering

De verdeling van taken tussen de rechter en de jury heeft specifieke sporen nagelaten op het gebied van de bewijswaardering. Zoals al in paragraaf 6.4 is uiteengezet heeft de rechter als taak zich bezig te houden met het recht en heeft de jury als taak zich bezig te houden met de feiten. De jury heeft de opdracht om zich op grond van de toegelaten bewijsmiddelen uit te spreken over het bestaan van gestelde feiten en te komen tot een oordeel. Dit doet zij door de aangeboden bewijsmiddelen te waarderen op hun betrouwbaarheid. De bewijswaardering is een taak voor de jury. De jury heeft namelijk te oordelen over de feiten en dit doet zij op basis van de toegelaten bewijsstukken. Ook al is bewijs reeds toegelaten, dan nog mag de jury zelf oordelen over de betrouwbaarheid en geloofwaardigheid van bewijs. Hierover stelt Rule 104(e):*"This rule does not limit the right of a party to introduce before the jury evidence relevant to weight or credibility."*

In tegenstelling tot wat in landen met een civil law traditie gebruikelijk is, zijn er in het Amerikaanse recht geen regels over de bewijswaarde van

---

484 P.R. Rice, *Electronic Evidence, Law and Practice*, Chicago: ABA Publishing 2008, p. 305.

485 P.R. Rice, *Electronic Evidence, Law and Practice*, Chicago: ABA Publishing 2008, p. 298.

486 D.S. Skupsky, 'The Best Evidence Rule is Dead…Except in the Mind of the Law!', *Records Management Quarterly;* July 1992, Vol. 26 Issue 3, p. 32.

bewijsmiddelen.[487] Het ontbreekt in het Amerikaanse recht geheel aan wettelijk opgelegde bewijswaarde, zoals het Nederlandse recht kent voor aktes en het Duitse recht voor *Urkunden*. Eenmaal toegelaten bewijs is niet onderworpen aan enige regel van bewijswaardering.[488] Wigmore stelt dat voor zoverre logica en psychologie ons kunnen ondersteunen, het niet goed mogelijk is om een algemene bewering te doen waarbij groter gewicht wordt toegekend aan een bepaald soort bewijsmiddel dan aan een ander soort bewijsmiddel. De bewijskracht van verschillende bewijsmiddelen is afhankelijk van afwegingen die te complex zijn. Wetenschap kan enkel wijzen op bepaalde risico's en bepaalde voordelen die kleven aan verschillende soorten bewijsmiddelen.[489] Toch heeft het rechtssysteem geen onbeperkt vertrouwen in de jury; iets wat naar mijn mening geheel terecht is. De jury is misschien wel de aangewezen entiteit om te oordelen over de feiten, maar zij is niet opgeleid in het recht en zij is niet altijd bekend met regels van procesrecht. Daarom heeft de rechter een belangrijke rol gekregen die zich in het bewijsrecht uit in de uitgebreide fase van bewijstoelating. De rechter toetst hier de bewijsmiddelen op betrouwbaarheid voordat de jury de bewijsmiddelen onder ogen krijgt.

6.11 De bewijsovereenkomst

Van bewijsovereenkomsten (of clausules die bewijsaspecten regelen) kan gebruik worden gemaakt om de bewijsmiddelen, bewijskracht en bewijslast te regelen. Zoals blijkt uit de paragrafen 4.15 en 5.10 is de bewijsovereenkomst in veel gevallen een toegestaan middel in het Nederlandse recht en in het Duitse recht (met uitzondering van de bewijskrachtovereenkomst).

Het Amerikaanse recht kent geen bewijsovereenkomsten. In dit onderzoek ben ik op zoek gegaan naar het bestaan van bewijsovereenkomsten in het Amerikaanse recht. Daarbij kwam ik niet alleen tot de conclusie dat bewijsovereenkomsten niet bestaan in het Amerikaanse recht, maar dat ook de constatering dat bewijsovereenkomsten in het Amerikaanse recht niet bestaan, geheel niet wordt gedaan. Hoewel ik dit niet kan hardmaken, vermoed ik dat bewijsovereenkomsten in strijd zijn met de regels van bewijsrecht en/of met de bevoegdheden van de rechter. De FRE laten nergens expliciet toe om af te wijken van de FRE. Hiermee zou het kunnen zijn dat de FRE dwingend recht zijn voor alle partijen. Ook zou het kunnen zijn dat een bewijsovereenkomst ingrijpt in de exclusief aan de rechter toegewezen bevoegdheden. Een overeenkomst

---

487 T. Anderson, D. Schum, W. Twining, *Analysis of Evidence*, New York: Cambridge University Press 2005, p. 226.

488 J.H. Wigmore, P. Tillers (revision), *Wigmore on Evidence, Evidence in Trials at Common Law*, Boston, Toronto, Little, Brown and Company 1983, p. 958.

489 J.H. Wigmore, P. Tillers (revision), *Wigmore on Evidence, Evidence in Trials at Common Law*, Boston, Toronto, Little, Brown and Company 1983, p. 958.

tussen partijen zou dan nooit de rechter en/of jury kunnen binden, omdat deze geen partij is bij die overeenkomst.

6.12 Samenvatting en conclusie

6.12.1 Samenvatting

Het Amerikaanse civiele bewijsrecht is in tegenstelling tot het Duitse en Amerikaanse recht 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 rechtsstelsel 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 existance of any fact that is of consequence tot he 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 outweighted 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 F*RE 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.

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*". Aangetoond moet worden dat een bewijsmiddel daadwerkelijk is wat gesteld wordt dat het is en dat aangetoond wordt van wie het afkomstig is. Authentificatie 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 authentificatie voldoen.

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.

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.

6.12.2 Conclusies

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.

Hearsay
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* .[490] 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)[491]
- 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 (Rule 803(3) FRE) 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.
- 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(8) FRE).
- De verklaring aan te merken is als een market report of een commercial publication waarop het publiek mag vertrouwen. ((Rule 803(17) FRE).

---

490 Enkel moet aangetoond worden dat de computer correct werkte.

491 *United States v. Blakey,* 607 F.2d 779, 785 (7th Cir.1979): statements gedaan binnen 23 minuten na de gebeurtenis zijn toegelaten op grond van Rule 803(1); *Miller v. Crown Amusements, Inc.,* 821 F.Supp. 703, 706-07 (S.D.Ga.1993): statements gedaan binnen 10 minuten na de gebeurtenis zijn toegelaten op grond van Rule 803(1).

Authentication
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 geauthentificeerd. 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 authentication 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
In beginsel dient het meest originele *writing, recording* of *photograph* ingebracht te worden als bewijsmiddel. *Duplicates* worden pas toegelaten als daarvoor in de *FRE* omgeschreven 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*.

7 Conclusies

7.1 Inleiding

Elektronische gegevens zijn niet meer weg te denken uit de hedendaagse samenleving. Of het nu gaat om elektronisch berichtenverkeer, digitale foto's en films, digitale muziek, enzovoorts. In een aantal decennia is er een snelle verandering geweest van een analoge naar digitale samenleving. De impact van de digitalisering van de samenleving lijkt echter in schril contrast te staan met de juridische werkelijkheid als het aankomt op elektronische gegevens als bewijsmiddel. De Nederlandse en de Duitse wetgever hebben dan wel de elektronische handtekening geïmplementeerd, maar daarbij hebben zij zich gericht op functionele criteria die niet altijd rechtszekerheid bieden en die tevens niet altijd even eenvoudig hanteerbaar zijn. Ook in de rechtspraak is het vaak niet duidelijk wanneer elektronische gegevens voldoende betrouwbaar zijn als bewijsmiddel. Elektronische gegevens worden wel ingezet als bewijsmiddel in rechtszaken, maar het is vaak helemaal niet duidelijk hoe de rechter tot een betrouwbaarheids oordeel van deze gegevens komt.

In dit afsluitende hoofdstuk behandel ik vier onderwerpen. Ten eerste ga ik in de tweede paragraaf in een samenvatting in op de algemene regels en beginselen die ten grondslag liggen aan het bewijsrecht in Nederland, Duitsland en Amerika. Er wordt een vergelijking gemaakt tussen de beginselen (autonomie van partijen, rechterlijke lijdelijkheid, bewijstoelating, bewijswaardering, dwingend bewijs en de bewijsovereenkomst) van de drie verschillende stelsels. In de derde paragraaf presenteer ik mijn onderzoeksresultaten. In de eerste plaats geef ik antwoord op de vraag welke concrete criteria worden gesteld aan de betrouwbaarheid van elektronische gegevens als bewijsmiddel. Ten tweede geef ik antwoord op de vraag welke abstracte criteria worden gesteld aan elektronische gegevens als bewijsmiddel. Ten derde vind ik geen ondersteuning voor de veelgemaakte aanname in de juridische literatuur dat het belangrijk is om bewijsmiddelen van het zwaarste juridische en technische geschut te voorzien om hun bewijskracht te garanderen. Ten vierde ga ik in op de in hoofdstuk 1 gemaakte aanname dat er in Nederland, Duitsland en Amerika een gemeenschappelijk idee bestaat wanneer elektronische gegevens betrouwbaar dan wel onbetrouwbaar zijn als bewijsmiddel. Deze wordt in mijn onderzoek ten minste deels bevestigd. In de

vierde paragraaf bespreek ik een aantal punten ter discussie. In de vijfde paragraaf ga ik tenslotte nog kort in op vragen voor vervolgonderzoek.

7.2 Samenvatting

Invloed van de beginselen van civiel procesrecht op bewijsmiddelen
Bewijsmiddelen staan niet op zichzelf, maar staan in verband met zowel procesrechtelijke als materieelrechtelijke regels. Bewijsmiddelen vallen binnen een bewijsrechtelijk stelsel dat op zijn beurt weer binnen een procesrechtelijk stelsel valt. Zoals in de vorige hoofdstukken is beschreven, geldt in het burgerlijk procesrecht het uitgangspunt dat het gelijk en ongelijk dat partijen krijgen in een overgroot deel van de gevallen slechts een gelijk is dat alleen tussen partijen geldt.[492] De rechter heeft in beginsel een lijdelijke rol.[493] De lijdelijke rol van de rechter houdt in dat enkel partijen bepalen of zij een proces starten en enkel partijen feiten stellen en bewijs aanbieden. De lijdelijkheid van de rechter in het civiele proces brengt binnen het bewijsrecht met zich dat feiten die gesteld zijn en niet worden betwist als vaststaand worden beschouwd. Pas als partijen het niet eens zijn over de feiten, met andere woorden, als de gestelde feiten worden betwist, zal de rechter bewijsmiddelen verlangen om die feiten te onderbouwen. Bewijsmiddelen komen dus pas aan de orde als de gestelde feiten met elkaar in conflict zijn. In het Amerikaanse recht gaat deze lijdelijkheid verder dan in landen met een *civil law traditie*. Zo is de rechter in Amerika eerder een scheidsrechter dan een onderzoeksrechter.

De kern van het toelaten en waarderen van bewijsmiddelen is om bewijsmiddelen te selecteren en om een betrouwbaarheidsoordeel van de bewijsmiddelen te geven. Dit betrouwbaarheidoordeel ligt besloten in de wet in de fase van bewijstoelating en bewijswaardering.[494] De rechter dient te onderzoeken of het bewijsmiddel daadwerkelijk betrouwbaar genoeg is om de gestelde feiten aan te tonen. In dit onderzoek ligt de focus op de betrouwbaarheid van elektronische gegevens als bewijsmiddel. Deze hebben een aantal kenmerken dat hen onderscheidt van niet-elektronische bewijsmiddelen. Deze in hoofdstuk één omschreven kenmerken omvatten ten eerste het risico dat bewijsmiddelen gemodificeerd zijn zonder dat achteraf valt te zien dàt dit het geval is en ten tweede dat het minder eenvoudig is om aan te tonen dat bepaalde elektronische gegevens, zoals een e-mail, een chatgesprek, websitepostings, enzovoorts, daadwerkelijk van een bepaalde

[492] Uitzonderingen zijn te vinden in familierechtelijke zaken en zaken waarbij rechten van derden in het geding zijn.
[493] Echter, onder invloed van recente ontwikkelingen is een begin gemaakt met het inperken van de rechterlijke lijdelijkheid.
[494] In Nederland in het Wetboek van Burgerlijke Rechtsvordering, in Duitsland in de Zivilprozessordnung en in Amerika in de Federal Rules of Evidence.

persoon afkomstig zijn. Als een rechter, of in Amerika een jury, geconfronteerd wordt met elektronische gegevens als bewijsmiddel zal hij, evengoed als bij 'normale' bewijsmiddelen, een betrouwbaarheidsoordeel moeten geven. De rechter dient zich af te vragen of het bewijsmiddel betrouwbaar genoeg is om te concluderen dat de gestelde feiten inderdaad als vaststaand kunnen worden beschouwd.

Twee vragen zijn van belang bij het oordelen over de betrouwbaarheid van elektronische gegevens als bewijsmiddel. Ten eerste: is het bewijsmiddel op zichzelf betrouwbaar genoeg? Daarbij wordt onderzocht of de intrinsieke kwaliteit wel voldoende is om het bewijsmiddel als voldoende betrouwbaar te kunnen kwalificeren. Hierbij zijn de aan te tonen feiten niet van invloed op de kwaliteit van het bewijsmiddel. Oplossingen die de intrinsieke kwaliteit van bewijsmiddelen garanderen zijn bijvoorbeeld het gebruikmaken van encryptie en versleuteling. Het is vooral de wetgever en in mindere mate de rechter die zich richt op deze intrinsieke kwaliteit.[495] De tweede vraag is of het bewijsmiddel wel voldoende betrouwbaar is om de gestelde feiten aan te kunnen tonen. Bij deze vraag draait het niet om de intrinsieke waarde van het bewijsmiddel, maar is het betrouwbaarheidsoordeel tevens afhankelijk van de feiten waarvan geprobeerd wordt om deze met de bewijsmiddelen aan te tonen. In dit geval is het juist de rechter die de bewijskracht van het bewijsmiddel onderzoekt. Dit onderzoek tracht op beide bovenstaande vragen een antwoord te vinden.

Bewijstoelating van elektronische gegevens in Nederland, Duitsland en Amerika

De bewijstoelating in Nederland, Duitsland en Amerika is in ieder land op eigen wijze geregeld. Nederland heeft onder invloed van de gedachte dat het binnen het formele civiele proces van belang is recht te doen aan de materiële waarheid gekozen voor een zoveel mogelijk open karakter van toelating van bewijsmiddelen. Alle bewijsmiddelen zijn in beginsel toegelaten, tenzij de wet anders bepaalt. Aangezien de wet maar in een beperkt aantal gevallen anders bepaalt, kunnen voor het aantonen van bijna alle feiten, alle bewijsmiddelen worden toegelaten. Voor elektronische gegevens geldt hetzelfde: elektronische gegevens worden toegelaten als bewijsmiddel, tenzij er sprake is van een wettelijke uitzondering of als deze middels een bewijsmiddelenovereenkomst zijn uitgesloten.[496]

Duitsland kent een gesloten stelsel voor het toelaten van bewijsmiddelen. De wet noemt vijf soorten bewijsmiddelen (*Augenscheinsbeweis, Zeugenbeweis, Sachverständigenbeweis, Urkundenbeweis* en *Parteivernehmung*) en een

[495] Bijvoorbeeld met wetgeving die de elektronische handtekening regelt (art 3:15a BW)
[496] Zie hoofdstuk 4 en 5.

bewijsmiddel moet kunnen worden gekwalificeerd als een van deze bewijsmiddelen om toegelaten te worden. Voor elektronische gegevens was tot midden jaren negentig weinig erkenning. Pas vanaf dat moment werden aan *elektronische Dokumenten* dezelfde rechtsgevolgen verleend als aan *Urkunden*. Deze *Dokumenten* blijven echter gekwalificeerd als *Augenscheinsbeweis*.

Het Amerikaanse recht kent een open kwalitatief stelsel van bewijsmiddelen. De aard van het bewijsmiddel is niet van belang als toelatingseis. Daarentegen moet wel elk bewijsmiddel voldoen aan een aantal kwalitatieve kenmerken om te worden toegelaten tot een rechtszaak (namelijk de eis van *relevancy, non-exclusion, non-hearsay, authentication* en *best evidence*). Deze criteria die soms al eeuwen geleden tot ontwikkeling zijn gekomen in de rechtspraak gelden onverkort voor elektronische gegevens als toelatingseis.[497] In het Amerikaanse recht worden bewijsmiddelen door middel van toetsing aan deze criteria beoordeeld op betrouwbaarheid.

Bewijswaardering van elektronische gegevens in Nederland, Duitsland en Amerika

De Nederlandse rechter heeft een discretionaire bevoegdheid gekregen van de wetgever om bewijsmiddelen in beginsel vrij te waarderen. Dit doet de rechter ook. In alle door mij onderzochte zaken ontbreekt het echter aan een expliciete bewijsmotivering. Ik heb hiervoor twee mogelijke oorzaken gevonden. In de eerste plaats zou de beperkte motiveringsplicht die de rechter heeft als het op bewijswaardering aankomt, daarvan de oorzaak kunnen zijn. In de tweede plaats zou de processuele rol die de rechter heeft een oorzaak kunnen zijn. Dit kan ertoe leiden dat:

- dat elektronische gegevens eenvoudigweg niet worden ingebracht als bewijs;
- dat ingebrachte middelen niet of onvoldoende worden betwist door partijen;
- dat de rechter een impliciete waardering maakt van de bewijsmiddelen;
- dat de rechter zijn oordeel reeds baseert op ander bewijs of;
- dat betreffende rechters misschien niet voldoende op de hoogte zijn van de manipulatiemogelijkheden van ogenschijnlijk betrouwbare ingebrachte elektronische middelen.

Mijn conclusie ten aanzien van de Nederlandse jurisprudentie is dat deze slechts in een enkel geval houvast biedt in het geven van een betrouwbaarheidsoordeel van elektronische bewijsmiddelen.

[497] In re Vinhnee, 336 B.R. 437, r.o. [13]

In het Duitse recht is ook sprake van een discretionaire bevoegdheid van de rechter in het waarderen van het bewijs. Ook hier is de rechtspraak beperkt, doch zijn er enige aanknopingspunten voor de bewijskracht van elektronische gegevens te vinden. Deze zijn in hoofdstuk 5 aan de orde gekomen en zijn opgenomen in de tabel in de volgende paragraaf.

Zowel in het Nederlandse als in het Duitse recht kunnen bewijsmiddelen dwingende bewijskracht hebben. Het betreft dan voor Nederland akten en strafvonnissen (deze laatste laat ik buiten beschouwing in dit onderzoek) en voor Duitsland *Urkunden*. In de jaren negentig heeft de discussie gespeeld of elektronische gegevens ook waren te kwalificeren als akte dan wel *Urkunde*. Als dit bevestigend kon worden beantwoord, dan konden namelijk ook elektronische documenten de status van akte, dan wel *Urkunde* krijgen en daarmee kon aan elektronische gegevens dwingende bewijskracht toekomen. In Nederland werd het antwoord op de vraag of elektronische gegevens beschouwd konden worden als akte niet eenduidig beantwoord. Pas met invoering van de Richtlijn Elektronische Handtekeningen werd ten aanzien van elektronische gegevens geconcludeerd dat deze onder omstandigheden als akte konden worden gekwalificeerd. In Duitsland werd geconcludeerd dat elektronische gegevens niet konden worden gekwalificeerd als *Urkunde*, omdat deze schriftelijkheid ontbeerden, dan wel niet ondertekend waren met een geldige handtekening. Na een aantal wetswijzigingen is het naar hedendaags recht mogelijk om in Nederland onderhandse aktes en in Duitsland *elektronische Dokumenten* waarop de regels van *private Urkunden* van toepassing zijn via elektronische weg tot stand te laten komen. Met behulp van een (gekwalificeerde) elektronische handtekening en een verklaring in elektronische vorm kan er onder omstandigheden een elektronische onderhandse akte of een *elektronisches Dokument* met dwingende bewijskracht tot stand komen. De Nederlandse elektronische onderhandse akte en het Duitse *elektronisches Dokument* hebben dan wel beide dwingende bewijskracht, toch wil dit niet zeggen dat deze dwingende bewijskracht hetzelfde is. De elektronische onderhandse akte heeft namelijk materiële bewijskracht, wat betekent dat ervan uitgegaan wordt dat de inhoud van de akte waar is. Zij ontbeert echter formele bewijskracht, wat betekent dat het niet zo is dat er dwingend van uitgegaan moet worden dat de tekst die in de akte staat ook echt is. Daarentegen is het omgekeerde het geval bij het Duitse *elektronisches Dokument*: deze ontbeert materiële bewijskracht, maar deze heeft wel formele bewijskracht. Om een elektronische onderhandse akte of een *privates elektronisches Dokument* te constitueren, is een (gekwalificeerde) elektronische handtekening een vereiste.

In het Nederlandse recht dient de methode van authentificatie van de elektronische handtekening voldoende betrouwbaar te zijn. De betrouwbaarheidscriteria zijn uitgewerkt in lid 2 en 3 van art 3:15 BW. Als de

elektronische handtekening (1) op unieke wijze aan de ondertekenaar verbonden is, (2) de ondertekenaar kan identificeren, (3) deze de handtekening onder zijn uitsluitende controle kan houden, (4) de integriteit van de gegevens waarmee deze verbonden is kan garanderen, (5) deze gebaseerd is op een gekwalificeerd certificaat en (6) is gegenereerd door een veilig middel, dan wordt vermoed dat de elektronische handtekening voldoende betrouwbaar is. Het enkele feit dat een elektronische handtekening niet is gebaseerd op een gekwalificeerd certificaat, op een door een certificaatdienstverlener afgegeven certificaat of een veilig middel, maakt de handtekening niet onbetrouwbaar. Het is dan aan de rechter om op grond van bijkomende omstandigheden te oordelen of van deze vorm van de elektronische handtekening de methode van authentificatie voldoende betrouwbaar is. In het Duitse recht worden alleen aan de gekwalificeerde elektronische handtekening wettelijke rechtsgevolgen verleend. Voor het bewijsrecht betreft dit het al eerder genoemde *elektronisches Dokument.* Deze krijgt dwingende rechtskracht als het ondertekend is met een gekwalificeerde elektronische handtekening.

In tegenstelling tot het Nederlandse en Duitse recht is de bewijswaardering in Amerika altijd vrij. De jury heeft een vrije bevoegdheid om bewijsmiddelen te waarderen. Hierbij hoeft de jury dan ook geen motivering te geven.[498] In de fase van bewijswaardering zijn dan ook geen kwalitatieve criteria te vinden voor elektronische gegevens als bewijsmiddel. Deze kwalitatieve criteria worden echter reeds in de toelatingsfase van de bewijsmiddelen expliciet gemaakt waardoor een expliciet oordeel wordt gegeven over de betrouwbaarheid van bewijsmiddelen.

Tenslotte kan in bepaalde landen gebruik worden gemaakt van een bewijsovereenkomst om de bewijspositie van partijen te regelen. Er zijn drie soorten bewijsovereenkomsten, namelijk de bewijsmiddelenovereenkomst, de bewijskrachtovereenkomst, de bewijslastovereenkomst en de overeenkomst die tegenbewijs regelt. Een probleem hierbij is dat het fenomeen bewijsovereenkomst niet bestaat. Het is dan ook niet duidelijk of een bewijsovereenkomst onder Amerikaans recht geaccepteerd wordt. In Duitsland is het niet mogelijk een bewijskrachtovereenkomst aan te gaan. Deze komt in strijd met de in § 286 ZPO aan de rechter opgedragen bevoegdheid om bewijsmiddelen vrij te waarderen. De overige soorten bewijsovereenkomsten (de bewijsmiddelenovereenkomst en de bewijslastovereenkomst) zijn wel toegestaan. In Nederland kunnen alle soorten bewijsovereenkomsten gesloten worden tenzij het recht gevolgen verbindt aan feiten die niet ter vrije bepaling van partijen staat en tenzij er gronden zijn waarop zij krachtens het Burgerlijk Wetboek buiten beschouwing dienen te blijven.

[498] Er wordt alleen een uitspraak gedaan of de feiten bewezen zijn of niet.

7.3 Onderzoeksresultaten

In de inleiding van dit onderzoek heb ik een tweeledige onderzoeksvraag geformuleerd, namelijk: *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 en gebruikers 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?* Op bovenstaande tweeledige vraag zal ik in deze paragraaf nader ingaan (in 7.3.1 en 7.3.2). Daarnaast ga ik in op twee andere resultaten die tijdens mijn onderzoek zijn verkregen, namelijk de relativering van de veelgemaakte aanname in de juridische literatuur dat het belangrijk is om bewijsmiddelen van het zwaarste juridische en technische geschut te voorzien om hun bewijskracht te garanderen (7.3.3) en de aanname die ik in hoofdstuk 1 heb gedaan betreffende het gemeenschappelijk idee van de betrouwbaarheid van bewijsmiddelen (7.3.4).

7.3.1 Concrete betrouwbaarheidscriteria in wetgeving en rechtspraak

Bewijsmiddelen staan in nauw verband met de feiten en beide kunnen niet van elkaar worden losgekoppeld. De betrouwbaarheid van bewijsmiddelen is daarom niet alleen afhankelijk van alleen de intrinsieke waarde, maar tevens van de verhouding tot de feiten die ze moeten aantonen. Een inhoudelijke en kwalitatieve beoordeling ligt dan ten grondslag aan de beoordeling van het bewijsmiddel. Bij het kwalitatief beoordelen van de betrouwbaarheid van bewijsmiddelen zijn in de loop van de tijd verschillende beoordelingscriteria ontwikkeld, voornamelijk in wetgeving. In deze wetgeving zijn deze criteria meestal slechts op functioneel niveau beschreven. In de jurisprudentie, is het aannemelijk er criteria worden gehanteerd door rechters (hoe komen rechters anders tot het oordeel dat feiten kunnen worden aangetroond met elektronische gegevens)[499], maar zijn deze criteria vaak niet expliciet gemaakt en blijft het meestal onduidelijk welke criteria een rechter heeft gehanteerd bij het beoordelen van elektronisch bewijs. De vraag is welke beoordelingscriteria worden gesteld aan specifiek elektronische gegevens zodat deze voldoende betrouwbaar zijn om als bewijs te kunnen dienen.

De criteria voor het beoordelen van de betrouwbaarheid van elektronische gegevens als bewijsmiddel worden gevonden in de fase van bewijstoelating en

[499] Zie ook paragraaf 4.8.

bewijswaardering. Hiervoor put ik in dit onderzoek uit het Nederlandse, Duitse en Amerikaanse bewijsrecht. De Nederlandse wetgever heeft de rechter veel vrijheid gegeven om bewijsmiddelen inhoudelijk kwalitatief te beoordelen. Het open stelsel van toelating van bewijsmiddelen en de vrije bewijswaardering die in de wet verankerd zijn, zijn daarvan het bewijs. Daarbij lijkt het er sterk op dat de rechter zijn bewijsoordeel niet hoeft te motiveren en dit doet hij dan ook nauwelijks, waardoor het moeilijk is om inzicht te krijgen in welke criteria er bij rechters toe leiden dat ze een bewijsmiddel betrouwbaar genoeg achten om feiten als bewezen aan te nemen.

Enig houvast voor de betrouwbaarheid van elektronische gegevens als bewijsmiddel kan worden gevonden bij de middelen die bij wet dwingende bewijskracht toegekend hebben gekregen, zoals aktes en de elektronische handtekening. Aktes dienen aan bepaalde vormvereisten te voldoen en krijgen dan materiële dwingende rechtskracht. Dit geldt evenzeer voor de elektronische onderhandse akte. Verder heeft de wetgever voorzien in een weerlegbaar bewijsvermoeden voor de betrouwbaarheid van de methode van authentificatie voor de elektronische handtekening. Ook de Duitse rechter heeft net als de Nederlandse rechter veel ruimte gekregen om bewijsmiddelen inhoudelijke kwalitatief te beoordelen. Elektronische gegevens zijn expliciet ondergebracht bij het *Augenscheinsbeweis*, dat valt onder de vrije bewijswaardering van de rechter. Als de gegevens echter worden voorzien van een gekwalificeerde elektronische handtekening, dan zijn de regels van de *private Urkunde* van toepassing en krijgen de gegevens dwingende (formele) bewijskracht. De Amerikaanse rechter hanteert vijf criteria die in de rechtspraak zijn ontwikkeld en die nu zijn gecodificeerd in de *Federal Rules of Evidence*. De rechter moet alle aangeboden bewijsmiddelen met behulp van deze criteria toetsen op inhoudelijke kwaliteiten. Hiermee moet worden voorkomen dat juryleden te snel de betrouwbaarheid van een bewijsmiddel aannemen. Een vorm van dwingende bewijskracht kent het Amerikaanse recht niet.

Elektronische gegevens die worden gebruikt als middel ter bewijs, worden zowel onder het Nederlandse, Duitse en Amerikaanse recht toegelaten. Daarbij ondergaan deze bij de toelating alleen in het Amerikaanse recht een kwalitatieve toets. Deze kwalitatieve toets vindt in het Nederlandse en Duitse recht niet plaats in de toelatingsfase, maar in de bewijswaarderingsfase. Bij de bewijswaardering kunnen de bewijsmiddelen in het Nederlandse en Duitse recht binnen het bereik van de dwingende bewijskracht vallen, mits aan een aantal (naar mijn mening zware) criteria is voldaan. Is niet aan deze criteria voldaan of is er sprake van Amerikaans recht, dan vallen deze gegevens onder de vrije bewijswaardering. De rechter of jury is dan vrij in het beoordelen van het bewijs.

In dit onderzoek is naast wetgeving ook jurisprudentie behandeld die ingaat op de criteria die aangelegd worden bij de beoordeling van de betrouwbaarheid van elektronische gegevens als bewijsmiddel. Hierbij heb ik jurisprudentie gevonden waarin geconcludeerd wordt dat elektronische gegevens als bewijs niet als voldoende betrouwbaar kunnen worden aangemerkt, maar ook jurisprudentie die tot de conclusie komt dat elektronische gegevens wel voldoende betrouwbaar zijn om als bewijs te dienen. De vraag is welke beoordelingscriteria de rechters nu aanleggen voor de beoordeling van deze betrouwbaarheid. Vervolgens heb ik regelgeving onderzocht waarbij aan elektronische gegevens dwingende bewijskracht kan worden toegekend. Deze wetgeving en jurisprudentie heb ik in een tabel ondergebracht onder de aanname dat er in Nederland, Duitsland en Amerika een gemeenschappelijk idee van betrouwbaarheid / onbetrouwbaarheid bestaat.[500] Zoals ik in paragraaf 7.3.4 zal concluderen, bevestigen de gelijke uitkomsten van gelijksoortige zaken deze aanname.

In de onderstaande tabel onderscheid ik vier niveaus van betrouwbaarheid, gebaseerd op wetgeving en jurisprudentie. In de eerste plaats de criteria waarbij een bewijsmiddel niet als voldoende betrouwbaar wordt beschouwd. Daarna volgt het niveau waarbij het onduidelijk is of het enkel voldoen aan bepaalde criteria voldoende is om de betrouwbaarheid van elektronische gegevens als bewijsmiddel aan te mogen nemen. Vervolgens komt het niveau waarbij elektronische gegevens aan de criteria voldoen waarbij deze elektronische gegevens wel als voldoende betrouwbaar worden gekwalificeerd. Tenslotte volgt het niveau waarbij elektronische gegevens zo betrouwbaar worden geacht, dat deze dwingende bewijskracht krijgen toegekend.

Betrouwbaarheid bewijs onvoldoende
Betrouwbaarheid bewijs onduidelijk of niet eenduidig
Betrouwbaarheid bewijs voldoende
Betrouwbaarheid bewijs hoog of dwingende bewijskracht

Vereisten:	Land	J/W	Beoordeling op grond van	Rechtsgevolg:	Bron:
Identiteit	Dsl	J	Omstandigheden: - Persoon die een e-mailadres aanhoudt onder een pseudoniem en met een password (welke online is medegedeeld).	E-mail vanaf dit e-mailadres kan niet tegen de vermoedelijke verstuurder worden gebruikt als bewijs,	OLG Köln 6.9.2002 – 19 U 16/02

[500] Zie paragraaf 1.2

Identiteit	Dsl	J	Gebruik van een eBay account door op een aangeboden artikel te bieden. Account bij eBay onder een pseudoniem is niet voldoende betrouwbaar, omdat het account anoniem aangemaakt kan worden en er geen controle is op de persoon die het account onderhoud. Kans op misbruik is te groot	Geen bewijs en geen omkering van de bewijslast	LG Bonn 19.12.2003 – 2 O 472/03
Identiteit	Dsl	J	Gebruik van een eBay account door op een aangeboden artikel te bieden. Account bij eBay onder een pseudoniem is niet voldoende betrouwbaar, omdat het account anoniem aangemaakt kan worden en er geen controle is op de persoon die het account onderhoud. Kans op misbruik is te groot	Geen bewijs en geen omkering van de bewijslast	LG Magdeburg 21.10.2003 – 6 O 1721/03
Identiteit	Dsl	J	Omstandigheden: - Op een online veilig kan een bod dat gedaan is niet worden toegerekend aan een deze persoon die het profiel heeft aangemaakt. De zekerheidsstandaard van het internet is niet voldoende.	Geen vol bewijs Geen *Anscheinsbeweis*	LG Bonn 7.8.2001 – 2 O 450/00
Identiteit	VS	J	Omstandigheden: - Enkel kunnen aantonen van welke e-mailadres een e-mail afkomstig is	Bewijsmiddel wordt niet toegelaten: voldoet niet aan eis van authentificatie (meer specifiek: identificatie)	Morgenstern v. Entpro, Cal. Rptr.3d, 2007 WL 475481
Identiteit	VS	J	Omstandigheden: - Enkel kunnen aantonen van welk e-mailadres een e-mail afkomstig is. - Aangewezen verzender ontkent dat de e-mail van hem afkomstig is	E-mails zijn niet voldoende betrouwbaar om de identiteit aan te tonen van de schrijver	Hood-O'hara v. Wills, 873 A.2d 757, 2005 PA Super 145
Identiteit	VS	J	Omstandigheden: - Een e-mail die ondertekend is met een naam, maar verder geen enkele andere vorm van bevestiging dat de e-mail daadwerkelijk was verstuurd door de betreffende ondertekenaar. - De aangewezen verzender ontkent dat de e-mails van hem afkomstig zijn.	E-mails zijn niet voldoende betrouwbaar om de identiteit aan te tonen van de schrijver	CCP Limited Partnership v. First Source Financial Inc., 856 N.E.2d 492

Integriteit	VS	J	Omstandigheden: - Slechts alleen een kopie gemaakt door middel van knippen-en-plakken van de originele chat is bewaard gebleven.	Chat-kopie in Word wordt niet toegelaten als bewijsmiddel.	U.S. v. Gerald Jackson, 488 F. Supp. 2d 866
Integriteit	VS	J	Voor toelating van websites op grond van Rule 901 FRE dienen bijkomende omstandigheden te zijn zoals een getuigenis van iemand met kennis dat de website inderdaad de website is waarvan geclaimd wordt dat deze het is.	Zonder bijkomende omstandigheden worden websites niet toegelaten op grond van Rule 901 FRE.	St. Lukes's Cataract and Laser Institute, P.A. v. Sanderson, 2006 WL 1320242 *M.D. Fla. May 12, 2006)
Integriteit	VS	J	Bijkomende omstandigheden moeten aangetoond worden om websites op grond van Rule 901 FRE toe te laten.	Zonder bijkomende omstandigheden worden websites niet toegelaten op grond van Rule 901 FRE.	Sun Protection Factory, Inc v. Tender Corp., 2005 WL 2484710
Integriteit	VS	J	Bijkomende omstandigheden moeten aangetoond worden om websites op grond van Rule 901 FRE toe te laten.	Zonder bijkomende omstandigheden worden websites niet toegelaten op grond van Rule 901 FRE.	*In re Homestore.com, Inc. Sec. Litig.,* 347 F.Supp.2d 769, 782 (C.D.Cal.2004)
Integriteit	VS	J	Informatie gevonden op Wikipedia	Informatie gevonden op Wikipedia kan niet worden geauthentificeerd en is onbetrouwbaar als bewijsmiddel.	Basada v. Mukasey, 540 F.3d 909.
Integriteit	VS	J	Informatie gevonden op Wikipedia	Informatie gevonden op Wikipedia is onbetrouwbaar als bewijsmiddel.	Campbell v. Sectretary of Health and Human Services, 69 Fed.Cl. 775

Integriteit / Identiteit	Nl	W	Methode van authentificatie van een gewone elektronische handtekening is voldoende betrouwbaar gelet op het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval. (De rechter krijgt zoveel vrijheid om de methode van authentificatie te waarderen, dat het mede door het ontbreken van jurisprudentie niet duidelijk is wanneer een uitspraak voldoende betrouwbaar is.	Rechtsgevolgen van elektronische handtekening worden gelijkgesteld met de rechtgevolgen welke aan een "gewone" handtekening worden verleend.	Art. 3:15a, lid 1 BW
Identiteit	Dsl	J	Het gebruikt van een elektronische handtekening (onduidelijk blijft welke) kan een *Anscheinsbeweis* opleveren voor het feit dat een bod via een account bij een online veiling ook van de persoon is die het account heeft aangemaakt	Kan een *Anscheinsbeweis* opleveren	OLG Köln 6.9.2002 – 19 U 16/02
Integriteit	VS	J	Omstandigheden: - Informatie op websites met verklaringen/informatie (over de opvatting of informatie op websites voldoende betrouwbaar is verschillen de meningen. Deze uitspraak lijkt in tegenspraak met andere uitspraken (zie hieronder Tank / Perfect 10)	Alleen deze informatie is nooit voldoende om te voldoen aan de eis van authentificatie	St. Clair v. Johnny's Oyster and Shrimp, Inc., 76 F.Supp.2d 773
Integriteit	VS	J	Omstandigheden: - Identificatie bij toegang tot software en hardware moet op orde zijn. - policies en procedures die gebruikt zijn bij de toegang op de computers moeten in orde zijn	Als de genoemde omstandigheden in orde zijn dan is de integriteit van het bewijsmiddel voldoende gewaarborgd.	In re Vee Vinhee, 336 B.R. 437
-	NL	J	Omstandigheden: - verzender heeft e-mail ontvangen die verzonden is vanaf hetzelfde e-mailadres als waar zij eerder e-mails heeft gezonden. - verzender heeft een e-mail ontvangen met dezelfde referentie als de e-mail die zij verzonden heeft. - verzender heeft een e-mail ontvangen met inhoud die moeilijk anders te begrijpen dan een reactie op de door haar gezonden e-mail.	Nu er is voldaan aan aan genoemde omstandigheden is het in redelijke mate aannemelijk dat ontvanger de e-mail van verzender ontvangen heeft.	*LJN* BC6016

-	NL	J	Feiten zijn in redelijke mate aannemelijk gemaakt. Echter de gronden waarop ontbreken.	De gestelde feiten zijn in redelijke mate aannemelijk of vol bewezen.	*LJN* BF5982 *LJN* BJ7622 *LJN* BA6212 *LJN* BC8136 *LJN* BC8079 *LJN* BG 5275 *LJN* BG9737 *LJN* BJ2001 *LJN* BI0345
-	Dsl	J	Omstandigheden: - Feit dat zendprotocol data bevat waaruit blijkt dat een e-mail is verstuurd. (!!! experts plaatsen vraagtekens bij de houdbaarheid van deze uitspraak)	Levert vol bewijs voor het feit dat de e-mail is verstuurd.	AG Hannover 20.12.1999 – 518 C 13916/99
Integriteit / identiteit	Dsl	J	Omstandigheden: - Correspondentie via e-mail tussen personen die met elkaar bekend zijn - De e-mails volgen elkaar op wat betreft de inhoud. - In een later getekende overeenkomst wordt gebruik gemaakt van gegevens die voorkomen in de e-mails.	Leveren vol bewijs op voor het feit dat de voorwaarden zijn overeengekomen. Partijen zijn aan de voorwaarden gebonden.	ArbG Frankfurt 9.1.2002 – 7 Ca 5380/01
Identiteit	VS	J	Omstandigheden: - E-mailadres en replyadres bevatten naam van afzender - Feitelijke inhoud was afzender bekend - De nickname van afzender is in deze gegevens genoemd - E-mail werd opgevolgd door telefoongesprekken met dezelfde soort verzoeken als in de e-mail.	Authenticiteit van de persoon die de e-mail verstuurde staat in voldoende mate vast.	United States v. Siddiqui, 235 F.3d 1318
Identiteit	VS	J	Omstandigheden: - ontvanger e-mail herkent e-mailadres - Feitelijke inhoud was alleen afzender en ontvanger bekend - Schrijfstijl e-mail was kenmerkend voor verzender - Getuige had gezien dat verzender eerder soortgelijke e-mails verzond aan ontvanger	Bewijs is voldoende om aan te tonen dat Amanda Massimo e-mails had verstuurd van babycol20@ yahoo.com	Massimo v. State 144 S.W.3d 210

Identiteit	VS	J	Omstandigheden: - Na het versturen van enkele e-mails, verstuurt verzender op verzoek van ontvanger de volgende e-mails naar een ander e-mailadres. - Inhoud van de e-mail verwijst naar specifieke informatie (in casu het kluisnummer van ontvanger en het beroep van verzender) - Getuigenis van ontvanger dat de e-mails hetzelfde onderwerp hadden als gesprekken over de telefoon. - De verzender gebruikte een afkorting van zijn naam als ondertekening.	Bewezen is dat Shea de schrijver van het bericht is.	Texas v. Shea, 167 S.W.3d 98
Identiteit	VS	J	Omstandigheden: - Verklaring ontvanger dát de e-mail ontvangen is - Feitelijke inhoud verwijst naar eerdere gebeurtenis	Bewijst dat de aangewezen schrijver van de e-mail, ook daadwerkelijk de schrijver is van de e-mail.	Swanton v. Brideois-Ashton, 134 Wash.App. 1067, 2006 WL 2664497
Identiteit	VS	J	Omstandigheden: - Verklaring door de persoon die print dat de print niet gewijzigd is en de volledige en accurate inhoud wordt weergegeven. - Afzender bevestigt dat hij de naam gebruikte die in de chat genoemd werd - Getuigen geven aan dat de afzender de betreffende chatnaam gebruikte.	Bewezen is dat Tank de schrijver van het bericht is.	United States v. Tank
Identiteit	VS	J	Omstandigheden: - Feitelijke inhoud chatgesprekken: e-mailadres afzender, correcte huisadres. - Aantekeningen gevonden naast de computer met daarin informatie (adres, e-mail en telefoonnummers) die waren uitgewisseld in de chat.	Bewezen dat Simpson als aangewezen chatter ook daadwerkelijk degene was die de chat gevoerd heeft.	U.S. v. Simpson, 152 F.3d 1241, 49 Fed. R. Evid. Serv. 1631, 98 CJ C.A.R. 4348
Identiteit	VS	J	Omstandigheden: - Schrijver niet zijnde houder van het account waarvan het bericht is verstuurd, identificeert zichzelf (in casu als: “Jeff”, “spiderman” en als “Daddy”) - De rechtmatige houder van het account getuigt ter zitting dat hij de verzender was van de berichten en dat een ander in het huis gebruik kon maken van het computer en het account welke niet voorzien was van een password.	Voldoende staat vast dat Hammontree de schrijver van het bericht was.	Hammon-tree v. State 642 S.E.2nd 412

Identiteit	VS	J	Omstandigheden: (Tank criteria worden toegepast: zie) - Verklaring door de persoon die print dat de print niet gewijzigd is en de volledige en accurate inhoud wordt weergegeven. - Afzender bevestigt dat hij de naam gebruikte die in de chat genoemd werd - Getuigen geven aan dat de afzender de betreffende chatnaam gebruikte.	Bewezen is dat gestelde schrijver ook daadwerkelijk de schrijver van het bericht is.	Perfect 10, Inc., v. Cybernet Ventures, Inc
Integriteit	VS	J	Omstandigheden - Verklaring dat printouts echt zijn en correct weergegeven kopien zijn van op Lexis gevonden artikelen na de zoekterm “organice food bar” en “organice food bars”. - Printout bevat de web adressen en de data van de print	Bewezen isdat de pints en de informatie op de prints echt is.	Premier Nutrition Inc. v. Organic Food Bar Inc., F. Supp. 2d, 2008 WL 1913163 (C.D. Cal.)
Integriteit en identiteit	VS	j	Omstandigheden: - Inhoud van de e-mail - onderscheidende eigenschappen - Vergelijking met reeds geauthentificeerde stukken	Bewezen dat de e-mails niet gewijzigd zijn en van de persoon afkomstig van wie gesteld wordt dat deze afkomstig zijn.	U.S. v. Safavian, 435 F. Supp. 2d 36
Integriteit	VS	J	Getuigenis onder ede onder Rule 901(b)(1) FRE dat de records zijn gegenereerd tijdens de gebruikelijke gang van zaken in het bedrijf.	Door computer gegenereerde records die gemaakt zijn tijdens de gebruikelijke gang van zaken in het bedrijf worden toegelaten als bewijsmiddel	Hardison v. Balboa Ins, 4. Fed. Appx. 663, 2001 WL 135677 (A.C. 10 (Okla.))
Authenticiteit	VS	J	Omstandigheden: - Datumstempels van ambtenaren wanneer de stukken zijn ingekomen. - Faxdata zijn gelijk aan de datumstempels. - De term ‘LEGALRECORDS’ geeft sterke aanwijzingen dat de stukken van een officiële instantie afkomstig zijn.	Stukken worden toegelaten als bewijsmiddel	Sinotes-Cruz v. Gonzales, 468 F.3d 1190
Integriteit	VS	J	Getuigenis van videomonteur is voldoende om te authentificeren dat de videorecorder of opnameapparatuur correct heeft gewerkt.	Correcte werking videoapparatuur kan worden aangetoond door middel van een getuigenverklaring van een expert.	In re Welfare of L.J.L. 2006 WL 3719652 (Minn App. Dec. 19, 2006)

Hearsay	VS	J	Data die door een computer gegenereerd is, wordt niet geclassificeerd als hearsay	Computer gegenereerde data is geen hearsay en daarom toegelaten als bewijs	*State v. Armstead*, 432 So.2d 837
Integriteit / identiteit	Nl	W	Methode van authentificatie is voldoende betrouwbaar., zodat sprake is van een geavanceerd elektronische handtekening met gekwalificeerd certificaat.	Rechtsgevolgen van elektronische handtekening worden gelijkgesteld met de rechtgevolgen welke aan een "gewone" handtekening worden verleend.	Art. 3:15A BW
Integriteit / identiteit	Nl	W	Overeenkomsten tot stand gekomen langs elektronische weg en ondertekend met een geavanceerde elektronische handtekening met gekwalificeerd certificaat	Dwingend bewijs van de waarheid van hetgeen in de verklaring staat (alleen materiële rechtskracht)	Art 3:15A BW jo art. 6:227a BW en art. 157 Rv
Integriteit / identiteit	Dsl	W	*Private elektronische Dokumente* (met iedere vorm van elektronische gegevens (dus code en data)) voorzien van een gekwalificeerde elektronische handtekening.	De regels die van toepassing zijn op *Urkunden* zijn ook van toepassing op het *elektronisches Dokument*. Hieronder valt de dwingende bewijskracht (alleen formele rechtskracht).	§ 371a (1) ZPO

<u>Betrouwbaarheid bewijs onvoldoende</u>

In de eerste categorie zijn uitspraken opgenomen waarbij elektronische gegevens niet voldoende betrouwbaar zijn gekwalificeerd om als bewijsmiddel te dienen. De bewijsmiddelen betreffen 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. Deze gegevens zijn niet zonder meer voldoende betrouwbaar om als bewijsmiddel te dienen. In een aantal gevallen betreft het de website Wikipedia. Rechters maken korte metten met het gebruik van

Wikipedia als bewijsmiddel aangezien iedereen informatie kan toevoegen en verwijderen. Er kan in de eerste plaats niet voldoende controle worden uitgeoefend op wie de informatie bewerkt. Op de tweede plaats is er geen garantie dat de informatie op Wikipedia juist is.

Betrouwbaarheid bewijs onduidelijk of niet eenduidig

In een klein aantal gevallen blijft het onduidelijk wat de bewijskracht is of kan zijn van elektronische gegevens, omdat bijvoorbeeld wetgeving ruimte voor interpretatie laat, experts ruimte laat om vraagtekens plaatsen bij de houdbaarheid van de uitspraak, de jurisprudentie niet eenduidig is en een hoogste rechter nog geen uitspraak heeft gedaan. In Nederlandse en Duitse wetgeving is nog niet duidelijk wat de bewijskracht van een gewone elektronische handtekening en een geavanceerde elektronische handtekening is. In het Nederlandse recht geeft art 3:15 BW de rechter heel veel ruimte om de gewone elektronische handtekening vrij te waarderen. In Duitsland heeft een rechter uitgesproken dat het gebruik van een elektronische handtekening zou kunnen leiden tot de aanname van een *Anscheinsbeweis*. De rechter gaat echter niet in op de vraag welk soort elektronische handtekening daarvoor voldoende betrouwbaar zou kunnen zijn.

Betrouwbaarheid bewijs voldoende

Een groot aantal uitspraken waarbij de betrouwbaarheid van bewijsmiddelen wordt beoordeeld, is afkomstig uit Amerikaanse rechtspraak. Een enkele uitspraak komt van de Duitse rechter. De meeste jurisprudentie gaat in op de authentificatie van personen. De vraag is dan of het bewijs voldoende betrouwbaar is om vast te kunnen stellen dat de persoon waarvan gesteld wordt dat deze de elektronische gegevens heeft opgesteld, dan wel verstuurd, ook daadwerkelijk de persoon is die de elektronische gegevens heeft opgesteld, dan wel verstuurd. Eerder bleek dat het enkele feit dat de gegevens vanaf een bepaald account verstuurd zijn, niet tot de conclusie kan leiden dat de persoon van wie het account is, ook de persoon is die de gegevens heeft verstuurd. Als rechtspraak wordt bekeken waarbij de betrouwbaarheid voldoende wordt geacht, dan valt op dat een cumulatie van meerdere omstandigheden ertoe kan leiden dat een bewijsmiddel wel als voldoende betrouwbaar kan worden aangemerkt. Dit gaat op voor verschillende soorten van communicatie via verschillende accounts, zoals e-mails, chats en websitepostings. Het gaat dan om gegevens waaruit de identiteit van de persoon blijkt of valt af te leiden. Gegevens waaruit de identiteit van de persoon blijkt en die in de rechtspraak zijn genoemd zijn bijvoorbeeld:

- 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. Op grond van de jurisprudentie is mijn indruk dat verschillende omstandigheden waaruit de identiteit van een persoon blijkt of afgeleid kan worden, tot de conclusie kunnen leiden dat het bewijs voldoende betrouwbaar is dat een aangewezen persoon de gegevens heeft gecreëerd en verzonden. Een enkel feit lijkt echter niet toereikend te zijn om tot dezelfde conclusie te komen. 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. Het feit dat niet één, maar meerdere omstandigheden nodig zijn om een persoon te authentificeren, lijkt ook in overeenstemming met het principe van *two factor* identification zoals deze te vinden is in computer security.[501] Daarbij wordt gesteld dat authentificatie van een persoon pas voldoende betrouwbaar is als van twee authentificatiemethoden gebruik wordt gemaakt. Overigens dient te worden opgemerkt dat er soms gebruik wordt gemaakt van andere bewijsmiddelen (zoals getuigeverklaringen). Deze hebben als functie de elektronische gegevens extra kracht bij te zetten in hun functie als bewijsmiddel.

De authenticiteit dan wel integriteit van elektronische gegevens laat een ander beeld zien dan de authenticiteit van de persoon. In de rechtspraak is namelijk maar weinig aandacht voor de integriteit van gegevens. In enkele zaken wordt aandacht besteed aan de integriteit van elektronische gegevens, bijvoorbeeld:

- de correctheid van de inhoud van de gegevens blijkt uit een telefoongesprek dat later plaatsvond;
- echtheid blijkt uit andere reeds geauthentificeerde stukken;
- echtheid blijkt uit een getuigenverklaring.

In twee onderzochte zaken komt de integriteit aan de orde waar het de betrouwbaarheid van informatie op Wikipedia betreft. Hierbij gaat het echter niet om de integriteit van data, maar om de integriteit van informatie. De informatie op Wikipedia is niet voldoende betrouwbaar omdat niet duidelijk is

[501] Zie paragraaf 3.3.

of de informatie inhoudelijk juist is. Iedereen kan informatie op Wikipedia plaatsen en deze kan onjuist zijn. De hierboven opgesomde criteria komen uit Amerikaanse rechtspraak. In Nederland en Duitsland is het echter de wetgever die integriteit expliciet maakt in wetgeving betreffende de geavanceerde en gekwalificeerde elektronische handtekening. Van een geavanceerde / gekwalificeerde elektronische handtekening is pas sprake als ook aan de eis is voldaan dat de integriteit waar de handtekening 'onder' is geplaatst, is gewaarborgd. Deze integriteit zou bijvoorbeeld kunnen worden gewaarborgd met een aantal in hoofdstuk 3 besproken technieken, zoals hashing of het gebruik van (dubbele) asymmetrische versleuteling. Of deze technieken ook daadwerkelijk voldoende juridische zekerheid bieden, valt niet uit de rechtspraak af te leiden, ook al is het wel aannemelijk aangezien de kans groot is dat integriteitschendingen kunnen worden gedetecteerd.

Betrouwbaarheid bewijs hoog / dwingende bewijskracht

De hoogste bewijskracht is de dwingende bewijskracht in het Nederlandse en Duitse recht. Ondanks dat in Nederland sprake is van materiële rechtskracht en in Duitsland van formele rechtskracht, gaat het in beide gevallen om een door de wet geformuleerde bewijskracht welke een beperking van de vrije bewijswaardering betekent. De bewijskracht is dwingend als aan een aantal in de wet omschreven eisen is voldaan. Dit geldt ook 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.

Een opmerking moet gemaakt worden bij de *hearsay rule*. Dit is een typisch Angelsaksisch leerstuk en kent geen tegenhanger in het Nederlandse en Duitse recht. De hearsay rule ziet ook enkel op de betrouwbaarheid van verklaringen, ongeacht de vorm waarin deze verklaringen liggen. Een vergelijking maken en de conclusies doortrekken om gevolgen voor het Nederlandse en Duitse bewijsrecht te trekken doe ik dan in het kader van dit onderzoek dan ook niet.

Voor wat betreft de *best evidence rule* kan gesteld worden dat met de recente aanpassingen van de FRE ook deze regel in beginsel geen problemen meer oplevert voor de betrouwbaarheid van bewijsmiddel. De *best evidence rule* zag namelijk op de originaliteit van bewijsmiddelen. Echter bij elektronische bewijsmiddelen is het maar geheel de vraag wat onder *original* moet worden verstaan, aangezien elektronische gegevens vaak worden gekopieerd.

7.3.2 Abstracte betrouwbaarheidscriteria

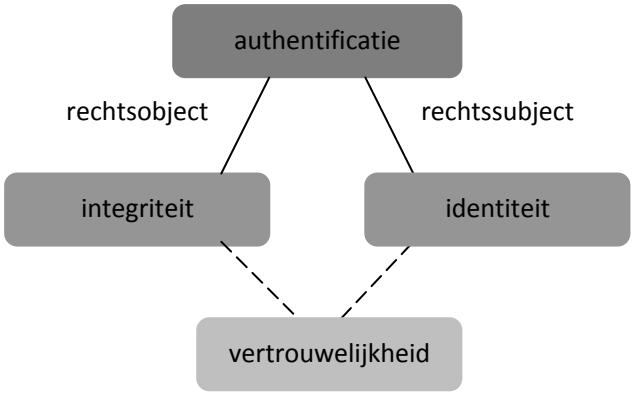
In de voorgaande hoofdstukken zijn verschillende criteria onderzocht die in de wetgeving en jurisprudentie zijn gesteld om de betrouwbaarheid van elektronische bewijsmiddelen te vergroten of zelfs te garanderen. Hierbij valt op dat er één criterium is dat expliciet in alle drie de bewijsstelsels terugkomt en dit criterium is zo ruim dat het meteen een aantal andere criteria omvat. Dit is authentificatie. Hoewel in het Nederlandse en Duitse recht het criterium authentificatie alleen expliciet genoemd wordt bij de regelgeving betreffende de elektronische handtekening, vermoed ik dat de rechter bij het beoordelen van de betrouwbaarheid van een bewijsmiddel impliciet de vraag stelt of het bewijsmiddel wel voldoende geauthentificeerd is.

Nu moet worden opgemerkt dat authentificatie verschillende betekenissen kan hebben al naar gelang het object waar het betrekking op heeft. Heeft het criterium betrekking op personen (rechtssubjecten) of verklaringen van personen dan wordt met authentificatie gedoeld op de vraag of degene die zich uitgeeft voor persoon X ook daadwerkelijk persoon X is. Hiervan is sprake bij de elektronische handtekening in het Nederlandse en Duitse recht. Het criterium authentificatie of *authentication* in het Amerikaanse recht heeft in beginsel betrekking op een bewijsmiddel (rechtsobject), dan gaat het over de vraag of het bewijsmiddel wel echt het bewijsmiddel is dat gesteld wordt dat het is. Meer concreet: is het gepresenteerde bewijsmiddel X wel echt bewijsmiddel X? Hierbij spelen weer twee vragen een rol. Ten eerste de vraag of het betreffende object *hetzelfde* object is als gesteld wordt dat het is (originaliteit) en ten tweede dat het object *geen wijzigingen* heeft ondergaan (integriteit). In hoofdstuk 3 heb ik verdedigd dat bij authentificatie van rechtsobjecten binnen de informatica meestal het woord integriteit gebruikt wordt.[502]

Het criterium authentificatie is ten gevolge van de verschillende betekenissen een paraplucriterium. Het is afhankelijk van de vraag of authentificatie betrekking heeft op een rechtssubject of rechtsobject. Authentificatie omvat namelijk zowel de het criterium integriteit als het criterium identiteit. De verhoudingen tussen deze criteria zijn weergegeven in afbeelding 7.1 In deze afbeelding is de scheiding zichtbaar gemaakt in authentificatie van rechtsobjecten en rechtssubjecten. Heeft authentificatie betrekking op rechtsobjecten dan gaat het om de vraag of de integriteit vaststaat, oftewel of het bewijsmiddel niet (onrechtmatig) is gemodificeerd en of het wel het originele bewijsmiddel betreft. Heeft authentificatie betrekking op rechtssubjecten dan gaat het om de vraag of degene die zich heeft geïdentificeerd wel daadwerkelijk degene is die hij claimt te zijn. Heeft de authenticiteit betrekking op gegevens met daarin verklaring of verwijzingen

[502] Hoewel dit niet altijd het geval is. Zie hiervoor paragraaf 3.2.

naar personen, dan moet zowel de integriteit van de gegevens vast komen te staan als ook de correctheid van de identiteit van de genoemde persoon of de data die afkomstig is van deze persoon. Als laatste speelt ook het criterium vertrouwelijkheid een rol, hoewel slechts indirect.



Afbeelding 7.2

De vertrouwelijkheid heeft een andere relatie met authentificatie. Vertrouwelijkheid houdt in dat bepaalde gegevens die alleen bekend horen te zijn bij daartoe aangewezen personen, ook bekend worden bij andere personen. Hier gaat het bijvoorbeeld om wachtwoorden en inlognamen. Als de vertrouwelijkheid van bepaalde vertrouwelijke elektronische gegevens is aangetast en derden de informatie kunnen inkijken, is het mogelijk dat deze derden van deze informatie gebruik maken door data te wijzigen (integriteit aan te tasten) of door zich voor te doen als een andere persoon (identiteit).

7.3.3 De relativering van de veelgemaakte aanname in de juridische literatuur dat het belangrijk is om bewijsmiddelen van de zwaarste juridische en technische middelen te voorzien om hun bewijskracht te garanderen.

In de vorige paragraaf bleek dat als het om het beoordelen van de betrouwbaarheid van bewijsmiddelen gaat, het bewijsmiddel niet volledig kan worden losgekoppeld van het bewijsrecht en van een aantal beginselen dat ten grondslag ligt aan het procesrecht. Omdat dit onderzoek zich specifiek richt op elektronische bewijsmiddelen gelden deze conclusies in beginsel voor dit soort bewijsmiddelen. Bewijsmiddelen worden in de huidige rechtspraak nooit geïsoleerd om vervolgens slechts de intrinsieke waarde van het bewijsmiddel te

onderzoeken en waarderen. Zelfs elektronische bewijsmiddelen waarvoor juist specifieke encryptie- en versleutelingtechnieken bestaan die de integriteit, identiteit en vertrouwelijkheid kunnen waarborgen en daarmee een belangrijke bijdrage leveren om de intrinsieke waarde te kunnen garanderen, moeten in samenhang met de feiten worden onderzocht op hun bewijskracht. Als in de civiele rechtspraak gezocht wordt naar uitspraken waarbij deze encryptie- en versleutelingstechnieken een rol spelen bij het waarderen van bewijsmiddelen, dan is het resultaat nihil. Er is mij geen jurisprudentie bekend waarbij geoordeeld wordt over de betrouwbaarheid van de elektronische gegevens als bewijsmiddel die voorzien zijn van encryptie en versleuteling of waarbij gebruik is gemaakt van een geavanceerde/gekwalificeerde elektronische handtekening. Hieruit mag overigens niet de conclusie worden getrokken dat deze technieken niet worden gebruikt. Dit onderzoek omvat namelijk niet het daadwerkelijke gebruik van deze technieken. Het is mogelijk dat de technieken inderdaad weinig gebruikt worden. Evengoed zouden deze technieken echter juist een dusdanig hoge graad van betrouwbaarheid van het bewijsmiddel kunnen opleveren, dat het voor partijen evident is welke feiten zich hebben voorgedaan, welke rechtsposities de partijen hebben en dat partijen tot de conclusie komen dat een rechtszaak overbodig is.

Hoewel de juridische literatuur focust op technische middelen om de betrouwbaarheid van bewijsmiddelen te garanderen, wordt de betrouwbaarheid van bewijsmiddelen in de praktijk op geheel andere wijze beoordeeld. Rechters beoordelen de bewijsmiddelen op een aantal juridisch functionele criteria (deze criteria zijn reeds aan de orde geweest in de twee voorgaande paragrafen) door de bewijsmiddelen in samenhang met de feiten te beschouwen. In plaats van dat de rechter het bewijsmiddel puur op zijn intrinsieke waarde beoordeelt, bekijkt de rechter welke feiten aangetoond moeten worden en hoe het bewijsmiddel eraan bijdraagt deze feiten op betrouwbare wijze te bewijzen. Dat de rechter dit op grond van alle omstandigheden doet is overigens niet verrassend, omdat in de rechtszaken die ik in het kader van dit onderzoek heb gevonden en onderzocht geen gebruik werd gemaakt van technische middelen om de betrouwbaarheid te garanderen.

7.3.4 Vermoeden van bevestiging van de aanname dat er in Nederland, Duitsland en Amerika een gemeenschappelijk idee bestaat wanneer elektronische gegevens betrouwbaar dan wel onbetrouwbaar zijn als bewijsmiddel.

In hoofdstuk 1 heb ik de aanname gedaan dat in Nederland, Duitsland en Amerika een gemeenschappelijk idee bestaat wanneer een elektronisch bewijsmiddel voldoende betrouwbaar is om er het gevolg aan te geven dat een

feit dat daardoor ondersteund wordt als bewezen kan worden beschouwd. Op grond van de jurisprudentie lijken er enige aanwijzingen te bestaan, die deze aanname ondersteunen voor het Duitse en Amerikaanse recht. In het Nederlandse recht ontbreekt het aan jurisprudentie. Opvallend is de maatstaf dat elektronische gegevens waarbij geen waarborg is dat de authentificatie van een persoon gegarandeerd is, tot de conclusie leidt dat de gegevens niet voldoende betrouwbaar zijn als bewijsmiddel.[503] Een tweede aanknopingspunt is slechts op de enige voor dit onderwerp beschikbare Duitse rechtszaak gebaseerd. Deze komt wat betreft het aanleggen van criteria voor de betrouwbaarheid van het bewijsmiddel overeen met criteria die ook in de Amerikaanse rechtspraak zijn aangelegd.[504] Hoewel de jurisprudentie gering is, lijkt het erop dat mijn aanname tenminste deels bevestigd kan worden.

7.4 Discussie

Elektronische gegevens moeten voldoende betrouwbaar zijn om als bewijs te kunnen dienen. Dit zeer ruime en algemene criterium zal ook gelden voor elektronische gegevens in de toekomst. Het is echter de vraag op welke wijze die betrouwbaarheid kan worden gewaarborgd. Als duidelijk is welke criteria aangelegd worden om de betrouwbaarheid te beoordelen, dan kan bij het ontwikkelen van nieuwe technologieën reeds in een vroeg stadium rekening worden gehouden met deze criteria. Het blijft natuurlijk echter een niet te beantwoorden vraag hoe de technologie zich in de toekomst ontwikkelt en waarmee rekening moet worden gehouden om die betrouwbaarheid ook in de toekomst te garanderen. In dit onderzoek is gebleken dat in de praktijk tot nu toe de focus ligt op authentificatie van een bewijsmiddel. Dit is een algemeen functioneel criterium, waarmee ontwikkelaars in de toekomst rekening kunnen houden bij het ontwikkelen van nieuwe technologieën door bijvoorbeeld te kiezen voor het implementeren van bepaalde functionaliteiten, het meegeven van specifieke kenmerken, enzovoorts.

Een tweede criterium is de waarborging van de authenticiteit van elektronische gegevens. Dit is een criterium waarop vooral de Nederlandse en de Duitse wetgever zich richten in de wetgeving betreffende de geavanceerde en gekwalificeerde elektronische handtekening. Echter in de rechtspraak lijkt er nauwelijks aandacht te bestaan voor de authenticiteit van elektronische gegevens. Deze richt zich namelijk zo goed als volledig op de authenticiteit met betrekking tot personen. Het gaat hier om de herleidbaarheid van gegevens

503 Zie OLG Köln 6.9.2002 – 19 U 16/02, LG Bonn 19.12.2003 – 2 O 472/03, LG Magdeburg 21.10.2003 – 6 O 1721/03, Morgenstern v. Entpro, Cal. Rptr.3d, 2007 WL 475481, Hood-O'hara v. Wills, 873 A.2d 757, 2005 PA Super 145, CCP Limited Partnership v. First Source Financial Inc., 856 N.E.2d 492

504 ArbG Frankfurt 9.1.2002 – 7 Ca 5380/01. Vergelijk met o.a.United States v. Siddiqui, 235 F.3d 1318, Massimo v. State 144 S.W.3d 210, Texas v. Shea, 167 S.W.3d 98.

naar een bepaalde persoon van wie de gegevens afkomstig zijn. Ik vind het opmerkelijk dat de authenticiteit van objecten of gegevens weinig aandacht krijgt in de rechtspraak, juist omdat deze ook vaak zo eenvoudig te vervalsen zijn. Speelt de authenticiteit van gegevens geheel geen rol in de jurisprudentie of lijkt dit maar zo? Ik vermoed dat het laatste het geval is. Het kan zijn dat als partijen niet noemen dat de gegevens wel eens gemodificeerd (vervalst, gewijzigd) zouden kunnen zijn, de rechter zich hier ook niet op richt.

Een ander punt is de gehanteerde methode van onderzoek. Hierdoor heb ik bij mijn onderzoek naar Amerikaanse rechtspraak alleen die rechtspraak onderzocht die is beoordeeld door de federale gerechten. Deze hanteren namelijk allemaal de *Federal Rules of Evidence*. Hiermee worden de zaken die alleen in eerste instantie (in een lagere rechtbank) zijn behandeld, niet meegenomen. Deze rechtbanken hanteren namelijk eigen bewijsregels die kunnen afwijken van de *FRE*. Als gevolg van deze keuze zijn de zaken waarbij is ingegaan op de integriteit van elektronische gegevens en waarbij partijen niet in beroep zijn gegaan, niet meegenomen in dit onderzoek.

Een laatste punt dat beperkingen heeft kunnen opleveren is het feit dat in Nederland en Duitsland niet alle jurisprudentie gepubliceerd wordt. Er wordt slechts een selectie gemaakt van jurisprudentie. In Nederland is hierbij het oordeel van de rechtbank of bepaalde uitspraken voldoende interessant zijn voor publicatie van doorslaggevende betekenis. Hierdoor is het mogelijk dat relevante jurisprudentie niet bekend wordt en daardoor niet is meegenomen in dit onderzoek.

7.5 Aanbevelingen voor vervolgonderzoek

Tijdens de uitvoering van dit onderzoek is het mij opgevallen dat als de rechter de bewijsmiddelen inhoudelijk kwalitatief beoordeelt, de Duitse rechter vooral tot de conclusie komt dat bewijsmiddelen niet kwalitatief voldoende betrouwbaar zijn en dat de Amerikaanse rechter vooral tot de conclusie komt dat de bewijsmiddelen wel kwalitatief voldoende betrouwbaar zijn. Hoewel ik het niet hard kan maken en het buiten het bestek van dit onderzoek valt, vermoed ik dat de oorzaak is dat de Duitse rechter een negatieve opdracht heeft tot onderzoek van de bewijsmiddelen en de Amerikaanse rechter een positieve opdracht. Hiermee bedoel ik dat de Duitse rechter de bewijsmiddelen wel inhoudelijk kwalitatief onderzoekt, maar zijn oordeel slechts uitspreekt in de gevallen waarbij het bewijsmiddel niet voldoet aan de eisen waarvan de rechter van oordeel is dat deze het bewijsmiddel voldoende betrouwbaar maken. Hierdoor is dus het gevolg dat een rechter vaak alleen toekomt aan het expliciet afwijzen van bewijsmiddelen. De Amerikaanse rechter daarentegen heeft onder invloed van de juryrechtspraak een taak om alle bewijsmiddelen

eerst op betrouwbaarheid te beoordelen en dient hierbij zijn oordeel expliciet uit te spreken. Daarbij geeft de rechter dan ook een expliciet oordeel over de kwaliteit van elektronische bewijsmiddelen. Vervolgonderzoek zou mogelijk kunnen uitwijzen of er inderdaad een verschil bestaat op welke wijze rechters in verschillende landen tot hun oordeel komen.

8 Enkele maatregelen ter vergroting van de betrouwbaarheid van elektronische gegevens als bewijsmiddel

In dit hoofdstuk wordt ingegaan op de maatregelen die getroffen kunnen worden om de bewijswaarde van elektronische gegevens te waarborgen en te vergroten. In de hoofdstukken 4, 5 en 6 heb ik onderzocht welke voorwaarden de Nederlandse, Duitse en Amerikaanse wet stellen om elektronische bewijsmiddelen als bewijsmiddel toe te laten en welke waardering er gegeven wordt aan elektronische gegevens als bewijsmiddel. Op grond van de uitkomsten in deze drie hoofdstukken zal ik hier nader beschrijven welke maatregelen voldoende of waarschijnlijk voldoende zijn om aan de criteria te voldoen die de wet en de rechtspraak stellen om elektronische gegevens als voldoende betrouwbaar te kwalificeren om als bewijsmiddel te dienen. Daarvoor noem ik in dit hoofdstuk enige aanknopingspunten waar gebruikers van elektronische gegevens rekening mee kunnen houden om hun bewijspositie te beïnvloeden.

Er zijn verschillende mogelijkheden om de betrouwbaarheid van elektronische gegevens te waarborgen door gebruik te maken van verschillende technische middelen. Het betreft hier zowel middelen waaraan de wet rechtsgevolgen heeft verbonden (bijvoorbeeld de verschillende elektronische handtekeningen) als middelen waar de jurisprudentie in specifieke gevallen rechtsgevolgen aan heeft verbonden. In deze paragraaf zal ik een aantal oplossingen noemen die ertoe (kunnen) bijdragen dat de betrouwbaarheid van elektronische gegevens gewaarborgd worden.

Opgemerkt moet worden dat het vooral een combinatie is van verschillende factoren die ertoe kunnen bijdragen dat de betrouwbaarheid van de gegevens toeneemt.

Geavanceerde elektronische handtekening met gekwalificeerd certificaat

Het toepassen van de geavanceerde elektronische handtekening met een gekwalificeerd certificaat levert ten aanzien van de bewijsfunctie van elektronische gegevens de meeste garanties. Niet alleen worden technisch beschouwd de gegevens beschermd tegen modificatie door derden, zodat de authenticiteit van de gegevens voldoende vaststaat, maar tevens is de authentificatie van personen gewaarborgd. Naast de feitelijke bescherming

door de combinatie van versleuteling van gegevens en authentificerende technieken, heeft de wet juridische consequenties verbonden aan het gebruik van een elektronische handtekening met een gekwalificeerd certificaat. Art. 3:15a BW bevat namelijk een bewijsvermoeden van betrouwbaarheid van de methode van authentificatie van de elektronische handtekening. Hierdoor worden de rechtsgevolgen van de elektronische handtekening met een gekwalificeerd certificaat gelijkgesteld aan die van een gewone handtekening.

Bij het gebruik van een elektronische handtekening met een gekwalificeerd certificaat moet een afweging gemaakt worden tussen de noodzaak om de betrouwbaarheid van gegevens te waarborgen en de kosten en moeite die daarmee gemoeid zijn.

Geavanceerde elektronische handtekening

Het in art. 3:15a BW genoemde bewijsvermoeden geldt in beginsel ook voor de geavanceerde elektronische handtekening. Daarbij is niet voldaan aan alle eisen die gelden voor de geavanceerde elektronische handtekening met een gekwalificeerd certificaat. Echter als er slechts aan één van deze eisen niet voldaan is dan doet dit niets af aan het bewijsvermoeden. Pas als er aan meerdere eisen niet voldaan is of er aan één van deze eisen niet voldaan is in combinatie met andere omstandigheden, geldt er geen bewijsvermoeden van de methode van authentificatie meer.

Gewone elektronische handtekening

De gewone elektronische handtekening krijgt niet automatisch een bewijsvermoeden. Het is aan de rechter te oordelen of de methode van authentificatie voldoende betrouwbaar is om te kunnen concluderen dat de elektronische handtekening gelijkgesteld wordt met de handgeschreven handtekening. De bewijskracht van enkel de gewone elektronische handtekening is niet groot. Het enkel ondertekenen van een bericht met een naam, is namelijk al voldoende voor de kwalificatie als elektronische handtekening. Het is maar de vraag of een rechter deze dezelfde rechtsgevolgen zal geven als de handgeschreven handtekening.

Cryptografische *hash* functies

Door gebruik te maken van cryptografische *hash* functies kan een "vingerafdruk" van deze gegevens worden gecreëerd. Hoewel technische maatregelen (zoals het gebruik van cryptografische *hash* functies) ter voorkoming van de aantasting van de authenticiteit van elektronische gegevens (integriteit) nergens in de jurisprudentie ter sprake komen, kunnen deze naar mijn mening wel de betrouwbaarheid van elektronische gegevens vergroten. Door een *hash* waarde te creëren en deze mee te sturen met de gegevens, of beter nog afzonderlijk van de gegeven naar de wederpartij te sturen, kan

gecontroleerd worden of het oorspronkelijke bericht in ongewijzigde staat is aangekomen.

Het gebruiken van de naam van de ondertekenaar

Het gebruiken van een naam, initialen, afkortingen van namen en/of een aan een bepaalde persoon gekoppelde nickname is een methode om iemand te authentificeren. Echter, het is niet uitgesloten dat iemand een naam vervalst. Zeker in het geval van niet versleutelde gegevens of versleutelde gegevens die eenvoudig zijn te kraken, is het denkbaar dat de naam van de ondertekenaar niet de naam is van degene wiens naam verbonden is met de andere elektronische gegevens. Daarentegen in combinatie met andere authentificerende gegevens kan de naam een aanknopingspunt zijn om de betrouwbaarheid van de gegevens te waarborgen.

Het is zaak zoveel mogelijk de naam te laten opnemen in e-mailberichten, omdat deze specifiek naar een persoon verwijzen. Daarbij moet opgemerkt worden dat niet enkel de naam voldoende bewijs oplevert, maar het in combinatie met andere gegevens een aanknopingspunt kan bieden om een persoon te authentificeren.

Het gebruikte (e-mail)adres

E-mailadressen en chatnamen hebben tot op zekere hoogte een authentificerende functie. In de rechtspraak in Amerika is het vooral de combinatie van verschillende gegevens in combinatie met het e-mailadres die authentificerend kan werken. Temeer geldt dit als het e-mailadres de naam bevat van degene van wie het bericht afkomstig is. Duitse rechtspraak is echter heel eenduidig in gevallen waarbij enkel een e-mailadres wordt gebruikt en waarbij de naam van degene aan wie het e-mailadres toebehoort niet in het e-mailadres staat. De authentificatie is dan onvoldoende en de e-mail die verstuurd is van zo'n adres, is niet voldoende betrouwbaar als bewijsmiddel.

Voor de bewijspositie van partijen is het toch van belang zoveel mogelijk via betrouwbare e-mailadressen te communiceren. E-mailadressen die tot een specifiek domein behoren, kunnen betrouwbaarder zijn dan e-mailadressen van andere specifieke domeinen. Zo is een e-mailadres dat tot het domein van een bepaalde organisatie behoort en alleen door bepaalde daartoe bevoegde personen kan worden aangemaakt betrouwbaarder dan e-mailadressen van domeinen waar iedereen anoniem een e-mailadres kan aanmaken, zoals hotmail.com e-mailadressen (bijvoorbeeld m.vanstekelenburg@hotmail.com). Het kost iemand die onrechtmatig het e-mailadres m.vanstekelenburg@rechten.vu.nl wil aanmaken, veel meer moeite om dit e-mailadres te creëren, dan om m.vanstekelenburg@hotmail.com te creëren.

De inhoud van een elektronisch bericht

Een veelgebruikte methode om de betrouwbaarheid te waarderen is door te kijken naar de inhoud van elektronische berichten. Het betreft dan de inhoud in verschillende velden, zoals het tekstveld, maar ook de onderwerpregel. Daarbij kan verwezen worden naar informatie die alleen bekend was bij specifieke personen. Ook de reacties over en weer en de opvolging van een informatie kan een rol spelen bij de waardering van de betrouwbaarheid van elektronische gegevens.

Om de bewijspositie te versterken zou een gebruiker beter gebruik kunnen maken van een mogelijkheid om de reeds ontvangen informatie ook weer mee te sturen in de reactie of deze informatie op andere wijze te herhalen of ernaar te verwijzen. Voor e-mailverkeer is het enkele gebruik van de beantwoordfunctie (reply-functie of “replyen”) al een mogelijkheid om de gegevens eenvoudigweg weer te kopiëren en mee te sturen. Ook is het raadzaam om de wederpartij te verzoeken op jouw bericht te reageren. Dit kan met het zenden van een ontvangstbevestiging, maar beter is een reactie die verwijst naar de specifieke situatie en gebruikmaking van een ondertekening met de naam.

Ontvangstbevestiging

In verband met de bewijslast is het raadzaam om na verzending van een elektronisch bericht een bewijs van ontvangst te ontvangen. Indien de ontvangende partij namelijk ontkent elektronische gegevens te hebben ontvangen, rust op de verzendende partij de bewijslast dat de ontvangende partij de gegevens ontvangen heeft.

Het is in verband hiermee aan te raden gebruik te maken van een functie die automatisch vraagt om een ontvangstbevestiging. Als deze functie niet ingebouwd is in de gebruikte programmatuur, is het raadzaam de ontvangende partij te verzoeken een ontvangstbevestiging te sturen.

Het (automatisch) aanmaken van logs

Logs of logboeken van wat zich heeft afgespeeld (welke berichten zijn ontvangen, verstuurd, door wie, van wie, enzovoorts) kunnen bijdragen aan het reconstrueren van welke feiten zich hebben voorgedaan.

Als een computerprogramma een log-functie heeft is het raadzaam deze aan te schakelen en aan te laten staan. Hiermee verzamel je vooraf actief gegevens die achteraf mogelijk kunnen dienen als bewijsmiddel.

Het maken van één of meerdere back ups

Elektronische gegevens liggen enkel vast als elektrisch geladen deeltjes op/in een gegevensdrager of als 'putjes' op een lichtgevoelige gegevensdrager. Deze zijn media die veelal gevoelig zijn voor invloeden van buitenaf. Niet alleen kan het medium fysiek beschadigd worden, ook kunnen de gegevens gewist of overschreven worden. In het laatste geval bestaat de gegevensdrager nog wel, maar bestaan de gegevens niet meer. Juist als deze gegevens tot bewijs (kunnen) dienen, is het van belang zorgvuldig met de gegevens om te gaan.

Raadzaam is om regelmatig een back-up te maken van de gegevens. Dat klinkt eenvoudig en voor de hand liggend en dat is het ook. Toch zijn er veel mensen die niet regelmatig een back-up maken van hun gegevens. Er hoeft dan maar iets te gebeuren en alle gegevens zijn weg. Zeker als het mogelijk is om automatisch een back up te laten maken naar een andere gegevensdrager, is het raadzaam dit te doen. Met welke regelmaat dat moet zijn, zal onder andere afhangen van de aard van de gegevens, het belang dat met de gegevens gemoeid is en de gegevensdrager zelf.

Inschakelen van derden

Derde partijen, zoals TTP's (Trusted Third Parties) kunnen een rol spelen bij het verzamelen van elektronische gegevens. De rol van een derde partij kan heel groot zijn (bijvoorbeeld het uitgeven van gekwalificeerde certificaten) tot het enkel ontvangen en bewaren van elektronische gegevens.

Derde partijen kunnen ingeschakeld worden om kopieën van elektronische gegevens te bewaren zodat in een later stadium een beroep kan worden gedaan op deze gegevens. Aangetoond kan dan bijvoorbeeld worden dat bepaalde gegevens op een bepaald moment bestonden of bepaalde informatie bevatten. Ook kunnen derde partijen certificaten uitgeven waaruit de identiteit van de gebruiker van het certificaat blijkt. Het is ook weer afhankelijk van de verschillende omstandigheden, zoals de aard van de gegevens, de belangen die met het gebruik van de gegevens gemoeid zijn, en dergelijke, om te kunnen bepalen welke diensten van derden kunnen bijdragen aan het bewaren en vergaren van bewijs.

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 aan zien 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 soorgelijke zaken tot soortgelijke uitkomsten hebben geleidt 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 geautomatieerd 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 aansturingsregels 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. Authentificatie en integriteit staan echter in de computerwetenschap en de rechtswetenschap in een andere verhouding tot elkaar. In de computerwetenschap heeft authentificatie betrekking op mensen en integriteit op gegevens. In de rechtswetenschap kan authentificatie 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 authentificatie 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 authentificatie 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 schriftelijkheideis 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 authentificatie moet voldoen om voldoende betrouwbaar te zijn. Is eenmaal vastgesteld dat de methode van authentificatie 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 ambthalve de methode van authentificatie 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 *Dispositionsmaxime* 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), *Zeugenbeweis* (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 rechtsstelsel 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 existance 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 outweighted 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 F*RE 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*". Aangetoond moet worden dat een bewijsmiddel daadwerkelijk is wat gesteld wordt dat het is en dat aangetoond wordt van wie het afkomstig is. Authentificatie 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 authentificatie 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 geauthentificeerd. 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 authentication 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* omgeschreven 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 authentificatie 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 gebruikt 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 belangrijkst criterium, welke een rode draad vormt in dit onderzoek, is authentificatie. 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.

Summary

The better byte in the battle to be right

The reliability of electronic data as evidence under Dutch, German and American civil law of evidence

Chapter 1
This thesis researches the probative value of electronic data as evidence in Dutch, German and American civil law of evidence. With the introduction of electronic means in the economic and social course of business, electronic data has entered the courtroom as a form of evidence. This causes courts to value and weigh this evidence on its quality and its trustworthiness, despite their lack of knowledge as to the precise risks of electronic evidence a reliable source of the truth.

The main research question in this thesis is: which concrete criteria in Dutch, German and American civil law of evidence are set to electronic data with regard to safeguarding the trustworthiness of these data to prove the facts provided by parties; and which abstract criteria do developers need to take into account when developing new technologies in order to provide for the reliability of the processed and executed electronic data so it can be used as evidence. This research question is twofold. First, I research the concrete criteria which are set by law and precedent to assess electronic data as evidence. Second, by using the answer of the first question as input, I research the more abstract criteria which can be derived from the concrete criteria.

The main concept in this thesis is *to prove*. As a complicating factor Dutch, German and American law have different legal definitions of *to prove*. This does not have to be a difficulty. The assessment of the reliability of evidence is of a factual nature. In this thesis I make an assumption: there is a common understanding on the question when evidence is trustworthy or not and that the courts in the Netherlands, Germany and America are aware of the same risks when weighing the evidence. Indications hereto can be found in the fact that the same kind of legal cases lead to the same kind of outcomes based on the same kind of findings in mainly German and American jurisprudence. Under Dutch law the court need to have become a reasonable extent of certainty (*redelijke mate van zekerheid*). Under German law § 286 ZPO is applicable. The

judge has to make a decision if a fact is true or not true based on due regard of the whole content of the treatise and the conclusions of observation of evidence based on the judge's discretionary conviction. Under American law the preponderance standard of evidence is applicable. The court needs to find that the existence of a fact is more probable than its nonexistence.

Chapter 2

In chapter two the object of research, electronic data, is specified and put into context. Electronic data are facts, concepts or instructions which are stored electronically and which are suitable for communication, interpretation, processing or execution by humans or by automatic means. The smallest building blocks of electronic data are signs. These are symbols, (alphanumeric) characters and other shapes by which data can be represented and processed. Both signs and data are objective. Data can form information when it is interpreted and meaning has been given to it. The human factor of giving meaning to the data makes information subjective.

Electronic data can consist of code and data (in strict sense). Code consists of instructions recorded electronically and which are suitable for initiating, maintaining and ending a process by an automatic means. Data in strict sense consists of facts and concepts (not the instructions though) which are stored electronically and which are usable for communication, interpretation, processing or execution by humans or by automatic means. The justification for the distinction is the difference in function. Code consists of execution rules for a machine which are the instructions for a machine's behaviour. Data on the other hand contains information only. Another argument which justifies the distinction into code and data is the qualification of *geschriften*, *elektronische Dokumenten* and writings. On the other hand the distinction of code and data is not always very clear. Sometimes code is part of data (for instance source code, although without compilation or interpretation this code is not executable) or data is part of code (for instance in print commands)

Chapter 3

Chapter three is on the security of electronic data. The main right to be protected is the right "to prove", the authenticity and the integrity need to be safeguarded. Authentification and integrity relate differently in computer science and legal science. In computer science authentification relates to people (legal subjects) and integrity relates to data (legal objects). Safeguarding authenticity is possible by proving the identity of a person. Computer science distinguishes three classic means to authenticate a person, namely: something a person knows (password, login code), something a person possesses (ID-card, RFID-chip) and something a person is (DNA, fingerprint, voice). Safeguarding the integrity of data is possible by using cryptographic hash functions,

symmetric encryption, a-symmetric encryption, double a-symmetric encryption or a combination of several kinds of encryption.

Chapter 4

Chapter four researches the reliability of electronic data under Dutch civil law of evidence. The probative value cannot be researched without researching the procedural mechanism of the court. Main principle is the passiveness of the court and the autonomy of the parties. The parties decide the scope of the dispute and the court is not competent to complete the legal facts; only the legal grounds can be completed by the court. The autonomy of the parties is limited by legal presumptions. The law or an agreement sets rules with regard to the probative value of legal facts. In this research the legal presumption of the method of authentication of the electronic signature is of importance. A second important principle is the theory of freedom of evidence. This theory holds two mean ideas. First, the open system of the admission of evidence, which entails that all evidence is admissible unless the law stipulates differently. Second, the freedom of the court to weigh the evidence in its official capacity. If jurisprudence is researched for grounds why evidence is trustworthy or not, there are hardly any grounds to find. Though electronic data has been accepted as evidence to prove facts, the reasons why are hardly made explicit in legal decisions. The reasons could be found in the limited obligation to motivate evidentiary decisions or the procedural mechanism of the court. This makes it harder to retrieve the criteria the court based its decisions on to weigh probative value of the evidence. The little jurisprudence available concentrates on the question who needs to prove what and by what means whether an e-mail has been received. The courts are clear and speak with one voice: when a party denies he has received the e-mail, the sending party has to prove that the receiving party has actually received the e-mail. Only in one case the court explicitly motivates why it is convinced the e-mail has been received:

- the sender has received an e-mail which was sent from the same e-mail address as where it has sent an e-mail before.
- the sender has received an e-mail with the same reference as the e-mail it sent before.
- the sender has received an e-mail with content which can only be understood as a response to the e-mail it sent before.

Both the open system of the admission and the freedom of court to weigh the evidence have exceptions. An important exception is the electronic version of the deed. This can be constituted by signing an agreement in electronic form (art. 6:227a BW) in combination with an electronic signature (art. 3:15a BW). De equivalence set in art. 6:227a BW opens the possibility to meet the legal criteria of writing by a document in electronic form. Art. 3:15 BW treats the electronic signature equal as the handwritten signature if the method of authentication is reliable enough. This reliability is determined by the purpose the electronic signature was used for and all other circumstances of the case.

Nevertheless the method of authentication is reliable when it meets six criteria. In that case the law prescribes the legal presumption of the reliability of the method of authentification and as a consequence the electronic signature will be treated equal as the handwritten signature. A problem which arises is that the court can, on its own initiative, weigh the probative value of the criteria of 3:15 BW. If the court finds these criteria not trustworthy or rightfully implemented, is can decide the method of authentication is not reliable enough. As a consequence the electronic signature will not be treated equally as the handwritten signature. The electronic deed therefore offers a false certainty.

Another way to influence the evidentiary position of the parties is a contract of evidence. By using this contract parties can regulate the admission of evidence, the weighing of evidence, the burden of evidence for both parties.

Chapter 5

Chapter five researches the German civil law of evidence. This is part of civil procedural law and is codified in the *Zivilprozessordnung* (*ZPO*). Main principles are the passiveness of the court and the autonomy of the parties. Both have found their way into the so called *Maximen* theories. Under current law the focus is on the *Dispositionsmaxime* and the *Beibringungsmaxime*. Exceptions can be found in the law and several legal presumptions. The German law of evidence has a closed system of admission of evidence, called *Strengbeweis*, meaning it only allows certain types of evidence. Only when determining facts which parties agree on and which are not the essence of the case, other evidence is allowed as well. This is called *Freibeweis*. Under *Strengbeweis* five types of evidence are admissible: observation by the court (*Augenscheinsbeweis*), evidence by witness (*Zeugenbeweis*), evidence by expert (*Sachverständigenbeweis*), evidence by deed (*Urkundenbeweis*) and evidence by the parties themselves (*Parteivernehmung*).

After evidence has been admitted the court has to weigh the evidence on its reliability. Based on § 286 *ZPO* the court is free to weigh the evidence. The court needs to be personally convinced of the truth or untruth of the facts. High probability only is not enough. New jurisprudence tends towards a symbiosis of both subjective and objective elements by requiring personal convincement of the juror and objective probability. No jurisprudence on code can be found. Nevertheless there is jurisprudence on probative value of data and especially on the identity of persons. When a person has an account (e-mail/eBay) which does not have any security mechanisms, then it cannot be used to prove the person who is said to have used the account, really is the person who used it. The security standard is not high enough. In cases where more element scan lead to the conclusion who sent a certain statement, really is the person who made the statement, then the court can qualify the data as

having enough probative value. Under these circumstances are: a combination of content, facts which are mentioned outside the electronic correspondence, names under the statement and the knowledge parties have. The probative value does not depend on one element, but increases when more elements in their mutual relationship lead to the conclusion that evidence is reliable enough and has enough probative value to support the stated facts.
A legal exception to the free weighing of evidence is the *Urkunde*. A distinction is made between *öffentliche Urkunden* and *private signed Urkunden*. Before probative value can be admitted, the court has to make sure that there are no defects to the *Urkunde* and a check to make sure the *Urkunde* is real. Another legal exception to the free weighing of evidence is the *elektronisches Dokument*. As evidence this *Dokument* is admitted as evidence by observation by the court. When the probative value has to be determined, and the *elektronisches Dokument* is signed with an electronic signature, then the *Dokument* gets obligatory force. If the *elektronisches Dokument* is not signed with an electronic signature, then the court is free to weigh the *Dokument* on its merits on the ground of § 286 *ZPO*. When code or data is signed with a qualified electronic signature then the rules of the private Urkunde are applicable to the elektronic Dokument. Its formal binding force is then a fact. In case code and date have not been signed with a qualified electronic signature the Judge is free to weigh them on their reliability.

As under Dutch law, also under German law the evidentiary position of the parties can be arranged by a contract of evidence. Contrary to Dutch law, under German law a contract on the probative value (weighing the evidence) is invalid. § 286 *ZPO* prescribes it is the judge's authority to weigh the evidence. Therefore parties cannot interfere by contract. Parties can only regulate the admission of evidence and the burden of evidence.

Chapter 6
In chapter 6 American law of evidence is researched. In contrast to Dutch and German law of evidence, American law of evidence is not just part of civil procedural law, but it has its own place in law. It is applicable to civil, administrative and criminal law. The American law of evidence originated from English law. Over the last centuries it has developed on its own. Still many rules originating from English law of evidence can be found in modern American law of evidence. In 1971 the prevailing rules have been codified and brought together in the Federal Rules of Evidence (FRE).

Trial by jury was and still is of great influence on American law of evidence. This caused a system in which the judge can investigate whether evidence meets certain legal requirements. First after this qualitative investigation, in the phase of admission, the jury can weigh the evidence.

The American law has an open system of admissibility. This means that all presented evidence will be investigated on five qualitative grounds, namely: relevancy, exclusion, hearsay, authentication and best evidence.

Relevancy means that evidence can only be admitted if it has any tendency to make the existence of any fact that is of consequence to the termination of the action more probable or less probable than it would be without the evidence. As it is strongly depending on the facts, this rule does not provide rules what requirements evidence needs to meet under all circumstances.

Exclusion means that under specific circumstances evidence which is relevant can be excluded. The FRE state the exclusivity grounds, namely: if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues or misleading by the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence". Only on these grounds evidence can be excluded. As with relevancy, it is very dependant on the facts to give criteria which need to be met by electronic evidence.

Hearsay means that no evidence can be admitted when there is no statement other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matted asserted. De ratio of this rule is that statements done out of court are not reliable by definition. Statements need to be made under oath, in front of the juror and with the possibility to be questioned by the other party. The FRE lists the exceptions to this rule. No problems arise to admit code and computer generated data, because hearsay cannot occur. Data which is generated by humans can be subject to hearsay. In the following situations there is no hearsay:

- the statement has been made immediately after the event occurred and reflects the memory of the witness' knowledge correctly. What must be understood by immediately is not clear. I can imagine this is dependant on the circumstances. In one of the cases 23 minutes after the occurrence of an event was immediately enough to have Rule 803(1) FRE applicable.
- the statement of the then existing state of mind, emotion, sensation, or physical condition (such as intent, plan, motive, design, mental feeling, pain, and bodily health), but not including a statement of memory or belief to prove the fact remembered or believed unless it relates to the execution, revocation, identification, or terms of declarant's will (Rule 803(3) FRE).
- statements which are recorded by a witness and who has insufficient recollection to testify accurately (Rule 803 (5) FRE).
- statements which the business exception applies to: a memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation, all as

shown by the testimony of the custodian or other qualified witness (Rule 803 (6) FRE).
- statements containing market quotations, tabulations, lists, directories, or other published compilations, generally used and relied upon by the public or by persons in particular occupations (Rule 803 (17) FRE).

The authentication rule means that evidence needs to be sufficient to support a finding that the matter in question is what it proponent claims. It needs to be proven that the evidence is what the proponent claims it to be and that it can be proven whom it comes from. There are many ways to authenticate evidence. Rule 901(b) FRE lists examples without being limitative. There are many ways to authenticate evidence and it is depending on the kind of evidence which method of authentication is most suitable. As code and data have different functions these can be authenticated differently. Methods of authentication listed under Rule 901(b) FRE and applicable to code and date are: the *testimony of witness with knowledge (Rule 901(b)(1) FRE), the 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)*. For data the *public records or reports (Rule 901(b)(7) FRE* are of importance. In jurisprudence several methods of authentication have been developed. Most noticeable is the fact that authentication is considered by several characteristics in their mutual relation. Chapter six analyses these characteristics.

Best evidence (Rule 1001 FRE) is a rule which decides that in principle only the originals of writings, recordings and photographs can be admitted. Duplicated and secondary evidence is only allowed to be admitted in case the original can't be submitted and only under the conditions set in the FRE. When it comes to code and data, the best evidence rule does not seem to apply very well, because it is not always clear if code and data can be considered an original, a copy or secondary evidence. Therefore electronic evidence is assessed by the authentication rule rather than the best evidence rule.

The weighing of evidence and the admission of evidence are strictly separated under American law of evidence, because the first is the exclusive domain of the judge and the latter is the domain of the jury. There are no rules applicable to the weighing of evidence. The weighing of evidence is to the jury who is the fact finder (or in some cases this is the judge). Restrictions like legal presumptions as under Dutch and German law of evidence do not exist under American law of evidence.

Contracts of evidence are non-existent under American law of evidence. Although it is not certain, it is possible these contracts are void based on the fact that a juror cannot be bound by a contract between parties.

Chapter 7

In chapter seven the conclusions of this research are drawn. Jurisprudence and legislation make clear that when it comes to weighing electronic data as evidence most attention goes to the authentication of persons. Electronic data is reliable enough when several characteristics are considered. For instance: the name of the signatory, the name of the sender in the (reliable) e-mail address, the name of the sender in the reply address, the usage of a nickname by a person who is known for using that nickname, abbreviations of the name of the sender, specific characteristics of the text a person has written, the content of a message, the actions/behaviour following to a message which is received by a person, a statement data has been received, witness statement of a person who saw the indicated sender actually is the real sender. To prove certain electronic data was sent by a person, one of these characteristics is not sufficient. The exact amount of characteristics is not clear in detail, but in most cases three of these characteristics seem to be sufficient. This seems to be in line with the principle of two factor identification as known in computer security.

Under Dutch and German law evidence can have binding force. Under Dutch law this binding force is material; under German law this binding force is formal. The binding force is applicable to electronic documents signed with a qualified electronic signature. Under Dutch law these documents can be signed with a normal or advanced electronic signature as well.

Evidence can be unreliable. This is the case with electronic data sent from accounts which are don't provide enough certainty what person the data has come from, but also from accounts the user is know, but when it is not certain enough that person has sent the data itself. The other category consists of the reliability of data found on websites.

In some cases it remains unknown what the probative value of electronic data is. Under Dutch and German law it is not clear what the probative value of the normal electronic signature and the advanced electronic signature is.

The most important criterium in this research is authentication. It can be applicable to legal subjects; then it means to prove the identification of a person. If it is applicable to legal objects, then it means to prove the object has not been modified.

In literature is has been defended that it is important to use the most advanced technical mechanisms to avoid legal problems. However in practice judges seem to have no trouble to weigh electronic data as evidence on its reliability and to consider facts proven.

Chapter 8

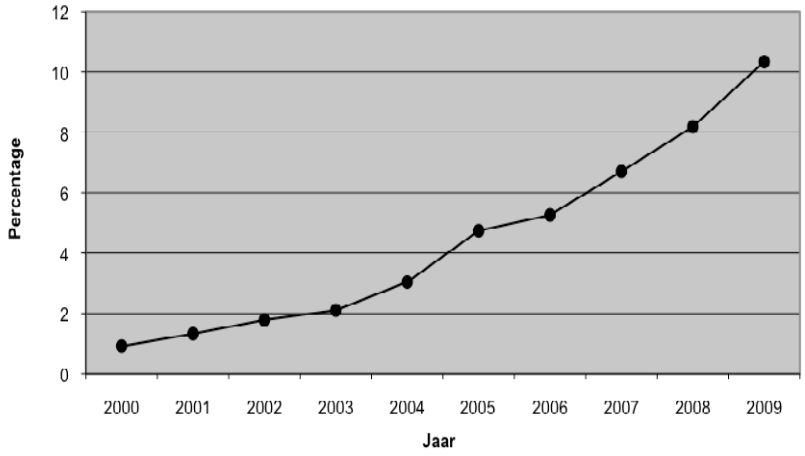
Chapter eight lists some recommendations to increase the reliability of electronic data as evidence. These are:

- the usage of a qualified electronic signature;
- the usage of an advanced electronic signature;
- the usage of a normal electronic signature;
- the usage of cryptographic hash functions;
- the usage of the name of the sender;
- the used e-mail address;
- the content of an electronic message;
- the usage of confirmation of receipt;
- to work with (automatic) logs;
- the usage of (automatic) back ups;
- the usage of (trusted) third parties.

Bijlage

Percentage civiele zaken waarin e-mail een rol speelt t.o.v. alle civiele zaken in www.rechtspraak.nl.

Jaar	zaken met e-mail in rechtspraak.nl	totaal aantal zaken in rechtspraak.nl	ratio
2000	8	870	0,91954023
2001	14	1053	1,329534663
2002	27	1513	1,784534038
2003	40	1902	2,103049422
2004	72	2370	3,037974684
2005	137	2890	4,740484429
2006	214	4070	5,257985258
2007	329	4911	6,699246589
2008	475	5804	8,184011027
2009	602	5825	10,33476395



Jurisprudentie

Nederland

Rb. Amsterdam 6 maart 2006, *LJN* AV3919.
Rb. Rotterdam 16 mei 2007, *LJN* BA6212
Rb. Amsterdam 21 november 2007, *LJN* BC0337
Rb. Haarlem 27 februari 2008, *LJN* BC8136
Rb. Leeuwarden 12 maart 2008, *LJN* BC8079
Rb. Roermond 23 april 2008, *LJN* BD2165.
Rb. Middelburg 24 september 2008, *LJN* BG5275
Rb. Roermond 13 januari 2009, *LJN* BG9737
Rb. Middelburg 21 januari 2009, *LJN* BJ3831
Rb. Middelburg 10 maart 2009, *LJN* BJ2001
Rb. Middelburg 10 maart 2009, *LJN* BI0345
Rb. Middelburg 24 juni 2009, *LJN* BK8790

Hof Amsterdam 4 maart 2008, *LJN* BF5982
Hof Amsterdam 6 maart 2008, *LJN* BC 6016.
Hof Leeuwarden 8 november 2009, *LJN* BJ7622

HR 17 december 1885, *Weekblad van het recht* 1886-5251
HR 21 januari 1898, *Weekblad van het recht* 7078
HR 6 mei 1910, *Weekblad van het recht* 1910-9025
HR 7 december 1934, *NJ* 1935
HR 23 december 1943, *NJ* 1944, 130
HR 30 november 1945, *NJ* 1946, 88
HR 31 oktober 1986, *NJ* 1987, 207
HR 13 september 1988, *NJ* 1989, 12
HR 6 maart 1992, *NJ* 1992, 373 (Micherna Beheer / Kamerbeek)
HR 4 juni 1993, *NJ* 1993, 659
HR 19 november 1993, *NJ* 1994, 622 (COVA/Internationale Bank)
HR 7 april 1995, *NJ* 1997, 21
HR 16 oktober 1998, *NJ* 1999, 7 (Finkenburgh / van Mansum)
HR 2 maart 2001, *LJN*: AB0377
HR 29 juni 2001, *NJ* 2001, 495
HR 23 november 2001, *LJN* AD4006
HR 18 februari 2005, *LJN*: AR7438

Duitsland

ArbG Frankfurt/M. 9.1.2002 – 7 Ca 5380/01

AG Hannover 20.12.1999 – 518 C 13916/99
AG Fürth, Urt. V. 13.6.2002 – 310 C 572/02
AG Dillenburg, Urt. V. 13.9.2003 – 5 C 286/02
AG Bühl 30.9.2003 – 3 C 260/03
AG Rudolstadt 30.3.2004 – 2 C 694/03
AG Karlsruhe 24.5.2005 – 5 C 35/05
AG Leer 30.5.2006 – 7d C 8/06

LG Bonn 7.8.2001 – 2 O 450/00
LG Nürnberg 27.3.2003 – 11 S 8162/02
LG Magdeburg 21.10.2003 – 6 O 1721/03
LG Bonn 19.12.2003 – 2 O 472/03
LG Stralsund 22.2.2006 – 1 S 237/05, CR 2006, 616

OLG Köln 6.9.2002 – 19 U 16/02
OLG München 8.10.1998 – 15 W 2631/98

BGH *NJW* 1920, 205
BGH *NJW* 1951, 70/71
BGH *NJW* 1951, 442
BGH *NJW* 1951, 517
BGH VersR 1954, 495
BGH VersR 1956, 194
BGH VersR 1956, 696
BGH *NJW* 1966, 1657
BGH *NJW* 1968, 700
BGH *NJW* 1970, 946
BGH *WM* 1973, 144
BGH *NJW* 1980, 893
BGH *NJW* 1982, 2072
BGH *NJW* 1984, 805
BGH *NJW* 1986, 198
BGH *NJW* 1986, 3086
BGH *NJW* 1993, 1796
BGH *NJW* 1996, 1828
BGH *NJW* 2001, 1140
BGH Urt. V. 4.3.2004 – III ZR 96/03 (KG)

BGHZ *NJW* 1998, 487
BGHZ *NJW* 1976, 294

BVerwG NJW 86, 2268.

BVerfG *NJW* 94, 847

Verenigde Staten van Amerika

Basada v. Mukasey, 540 F.3d 909
Campbell v. Sectretary of Health and Human Services, 69 Fed.Cl. 775
CCP Limited Partnership v. First Source Financial Inc., 856 N.E.2d 492.
City of Monterey v. Del Monte Dunes at Monterey, LTD, 119 S.Ct. 1624
De Bolt v. Outboard Marine Corp., 2001 (alleen gepubliceerd in: WL 311300)
Dimick v. Schiedt, 293 U.S. 474, 476, 55 S.Ct. 296, 79 L.Ed. 603 (1935)
Elliott Accociates., L.P. v. Banco de la Nacion, 194 F.R.D. 116, 121
Hammontree v. State, 642 S.E.2d 412
Hardison v. Balboa Ins., 4. Fed. Appx. 663, 2001
Hood-O'hara v. Wills, 873 A.2d 757, 2005 PA Super 145
In re F.P., 878 A.2d 91
In re Homestore.com, Inc. Sec. Litig., 347 F.Supp.2d 769, 782
In re Vee Vinhnee, 336 B.R. 437
In re Vee Vinhnee, 336 B.R. 437
In re Vee Vinhnee, 336 B.R. 437
In re Welfare of L.J.L., 2006 WL 3719652
Lorraine v. Markel American Insurrance Company, 2007 WL 1300739
Massimo v. State, 144 S.W.3d 210
Miller v. Crown Amusements, Inc., 821 F.Supp. 703, 706-07
Miller v. Crown Amusements, Inc., 821 F.Supp. 703, 706-07
Morgenstern v. Entpro, Cal. Rptr.3d, 2007
Mota v. University of Texas Houston Health Ctr., 261 F.3d 512, 527
Omychund v. Barker, 1 Atk, 21, 49; 26 ER 15, 33
People v. Huehn, 53 P.3d 733, 738
Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F.Supp.2d 1146
Premier Nutrition Inc. v. Organic Food Bar Inc., F. Supp. 2d
R. Jason Richards, Courting Wikipedia, 44 Trial 62 9Apr. 2008
Sinotes-Cruz v. Gonzales, 468 F.3d 1190
St. Clair v. Johnnoy's Oyster and Shrimp, Inc., 76 F.Supp.2d 773
St. Lukes's Cataract and Laser Institute, P.A. v. Sanderson, 2006
State v. Armstead, 432 So.2d 837
Sun Protection Factory, Inc v. Tender Corp., 2005 (alleen gepubliceerd in: WL 2484710)
Swanton v. Brideois-Ashton, 134 Wash.App. 1067, 2006
Texas v. Shea, 167 S.W.3d 98.
U.S. v. Gerald Jackson, 488 F. Supp. 2d 866.
U.S. v. Ruffin, 575 F.2d 346

U.S. v. Safavian, 435 F. Supp. 2d 36.
U.S. v. Simpson, 152 F.3d 1241, 49 Fed. R. Evid. Serv. 1631, 98 CJ C.A.R. 4348.
U.S. v. Stein, 452 F.Supp.2d 276
United States v. Blakey, 607 F.2d 779, 785
United States v. Blakey, 607 F.2d 779, 785
United States v. Duffy, 454 F.2d 809
United States v. Ferber, 966 F.Supp. 90, 98-99
United States v. Griffin, 191 F.3d 453, 453-54
United States v. Meienberg, 263 F.3d 1177
United States v. Rangel, 585 F.2d 344 8th Cir. 1978
United States v. Seifert, 351 F. Supp.2d 926, 66
United States v. Siddiqui, 235 F.3d 1318
United States v. Tank, 200 F.3d 627
United States v. Tank, 200 F.3d 627

Literatuurlijst

S. Abel, Urkundsbeweis durch digitale Dokumente *Multimedia und Recht* 1998, 944ff.

Advisory Committee, *Notes of Advisory Committee on Proposed* Rules (Pub. L. 93-595, § 1, Jan. 2, 1975, 88 Stat. 1931.)

R. Anderson, Security Engineering, *A Guide to Building Dependable Distributable Distributed Systems*, New York: Wiley Compter Publishing

T. Anderson, D Schum, W. Twining, *Analysis of Evidence*, New York: Cambridge University Press 2005

M. Apistola, *Advocaat & Kennismanagement* (diss. Amsterdam VU), 2007

C. Asser, A. Anema, P.J. Verdam, *Handleiding tot de beoefening van het Nederlands Burgerlijk Recht, Vijfde deel – van Bewijs*, Zwolle: W.E.J. Tjeenk Willink 1953

W.D.H. Asser, *Monografieën Nieuw BW, Bewijslastverdeling*, Deventer: Kluwer 1992

W.D.H. Asser, H.A. Groen, J.B.M. Vranken, I.N. Tzankova, *Een nieuwe Balans: Interim-rapport Fundamentele herbezinning Nederlands Burgerlijk Procesrecht*, Den Haag 2003

S. Baase, *A Gift of Fire, Social, Legal, and Ethical Issues for Computing and the Internet*, New Jersey: Pearson, Prentice Hall, 2009

D.L.A. Barker, C.F. Padfield, *Law*, Oxford: Made Simple Books 2001

T.H. Barr, *Invitation to Cryptology*, New Jersey: Prentice Hall, 2002

A. Becker, *Elektronische Dokumente als Beweismittel im Zivilprozess*, Frankfurt am Main, 2004

D. Bender, *Computer Law, A Guide to Cyberlaw and Data Privacy Law*, Newark, New Jersey: LexisNexis / Matthew Bender 2008

J. Bentham, *A Treatise of Judicial Evidence*, London: Messrs. Baldwin, Cradock, Joy 1825

C.B. Berger, 'Beweisführung mit elektronischen Dokumenten', *Neue juristische Wochenschrift* 2005-15

M. Bergfelder, *Der Beweis im elektronischen Rechtsverkehr* (diss. Freiburg), Verlag Dr. Kovač, Hamburg 2006

S.K.Th Boersma, *Management van kennis. Een creatieve onderneming*, Assen: Koninklijke Van Gorcum 2002

J.E. Bosch-Boesjes, *Lijdelijkheid in geding* (diss. Groningen), Kluwer, Deventer: 1991

A.F.M. Brenninkmeijer, 'De plaats van de rechter in onze constitutionele rechtsorde', in: R.H.M. Jansen, J. Godrie (red.), *De rechter als dictator?*, Lochem: J.B. van den Brink & Co. 1987

J.W. Britz, *Urkundenbeweisrecht und Elektroniktechnologie: eine Studie zur Tauglichkeit gesetzlicher Beweisregeln für elektronische Dokumente und ihre Reproduktionen im Zivilprozeß*, München, C.H. Beck 1996

K.S. Brown (red.), *McCormick ON EVIDENCE*, St Paul: Thomson West 2006

J.M.J. Chorus, *De lijdelijkheid van de rechter. Historie van een begrip* (oratie Leiden), Deventer: Kluwer 1987

J.W. Cotchett, *Federal Courtroom Evidence*, Newark / San Francisco: LexisNexis / Matthew Bender 2002

T. Daler, R. Gulbrandsen, B. Melgård, T. Sjølstad, *Security of Information and Data*, Chichester: Ellis Horwood Ltd.

D.E.R. Denning, *Cryptography and Data Security*, Reading: Addison-Wesley Publishing Company

Devitt, Blackmar, Wolff, *Federal Jury Practise and Instructions* ff 72.01, 4h edition, 1987

ECP.nl (M. Durinck, I. Aarts (red.)), Bewaren en bewijzen, Efficiënta Offsetdrukkerij bv

R. van Esch, *Electronic data interchange (EDI) en het vermogensrecht*, (diss. Nijmegen), Deventer: W.E.J. Tjeenk Willink 1999

R.E. van Esch, 'De betrekkelijke waarde van de Wet elektronische handtekeningen voor de elektronische handel', *Computerrecht* 2003

Europese Commissie, Europees jusititieel netwerk, *Verkrijging van bewijs en bewijsvoering – Duitsland*

R. Florijn, M. van Gurchom & M. van der Meulen, *Kennis leren managen. De theorie an praktijk van kennismanagement*, Den Haag: Ten Hagen & Stam 2000

P. Förschler. *Der Zivilprozess, Ein Lehrbuch für die Praxis mit Aktenfall*, Stuttgart: Kohlhammer 2004

H. Franken, H.W.K. Kaspersen, A.H. de Wild (red.), *Recht en computer* (Recht en Praktijk), Deventer: Kluwer 2004

R.D. Friedman, *The Elements of Evidence*, St. Paul: Thomson West 2004

B.A. Garner a.o. Black's Law Dictionary, Thomson West: St. Paul 2004
I. Giesen, "De bewijswaardering in civiele zaken: vage noties of scherpe normen?", Ars Aequi 1999

D. Gollman, *Computer Security*, Chichester: John Wiley & Sons, Ltd. 2006

M.H. Graham, *Federal Rules of Evidence in a Nutshell*, St. Paul: Thomson West 2007

R.A. Grimes, *Malicious Mobile Code*, Sebastopol: O'Reilly & Associates, Inc, 2001

W. Grunsky, *Zivilprocessrecht*, München: Wolters kluwer Deutschland GmbH 2006

J.H.M. ter Haar, E.D.C. Neppelenbroek, 'Het elektronisch ondertekend document: wel, niet of zoiets als een akte', *Weekblad voor Privaatrecht, Notariaat en Registratie* 2006

A.S. Hartkamp, *Compendium van het vermogensrecht volgens het nieuwe Burgerlijk Wetboek*, Deventer: Kluwer 1999

M.L Hendrikse, A.W. Jongbloed (red.), *De Toekomst van het Nederlands burgerlijk procesrecht*, Deventer: Kluwer 2004

T.R. Hidma, G.R. Rutgers, *Bewijs*, Deventer: Kluwer, 2004

E.J. Imwinkelried, *Evidentiary Foundations*, Newark/San Francisco/Charlottesville: LexisNexis 2005

P. Ingelse (red.), *Commentaren op fundamentele herbezinning*, Nijmegen: Ars Aequi Libri 2004

O. Jauernig, *Zivilprozessrecht*, München: Verlag C.H. Beck 2007

M.L. Kan, *Bewijslast en bewijswaardering*, Amsterdam: N.V. Johannes Müller 1921

H.W.K. Kaspersen, *Strafbaarstelling van computermisbruik* (diss. Amsterdam VU), Deventer: Kluwer 1990

A.M.Ch. Kemna, 'De vraagstukken van bewijs en bewaring in een elektronische omgeving', in: H. Franken, H.W.K. Kaspersen, A.H. de Wild (red.), *Recht en computer* (Recht en Praktijk), Deventer: Kluwer 2004

W. Kilian, 'EDI Forschungsprojekt 'ELTRADO' – Juristische Aspekte', in: Alt, Rainer; Schmid, Beat F.; Zbornik, Stefan, *EM - Electronic Markets*, Vol. 4 , No. 1, April. 1994.

W. Kilian, 'Zweck und Inhalt des deutschen EDI-Rahmenvertrages', *Computer und Recht* 1994

J. Koëter, A.M.Ch. Kemna, C. Stuurman, 'E-mail: bewijzen, bewaren, vormvoorschriften en contracteren', in: H.W.K. Kaspersen en C. Stuurman, *Juridische aspecten van e-mail*, Deventer: Kluwer 2001

E. Korthals Altes, 'Het motiveringsvereiste in burgerlijke zaken als toetsingsgrond in cassatie', in: P.A. Wackie Eysten (e.a. (red.), *Gemotiveerd gehuldigd*, Zwolle: W.E.J. Tjeenk Willink 1993

C.A. Kraan, *De authentieke akte* (diss. UvA), Arnhem: Goude Quint BV
E.C. Kraan-Beekman, 'Leerstukken – Elektronisch contracteren, maar toch de pen (moeten) hanteren?', *Contracteren* 2009-3

D.P. Leonhard, The New Wigmore, *A Treatise on Evidence, Selected Rules of Limited Admissibility*, Gaithersburg / New York: Aspen Law & Business

G.C. Lilly, *An Introduction to the Law of Evidence*, St. Paul: West Publishing Co. 1978

G.C. Lilly, *Principles of Evidence*, St. Paul: Thomson West 2006

A.S. Lipton, *Is It Admissible?*, Costa Mesa: James Publishing 1999

A.R. Lodder, J. Dumortier, S.H. Bol, *Het recht rond elektronische handtekeningen, Richtlijn 1999/93/EG en de omzetting in België en Nederland*, Deventer, Kluwer: 2005

P. Mankowski, 'Für einen Anscheinsbeweis hinsichtlich der Identität des Erklärenden bei E-Mails', *Computer und Recht* 2003-1

H.P.A.J. Martius, *Elektronisch Handelsrecht* (diss. Heerlen), Zutphen: Paris 2008

A. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, Boca Raton: CRC Press 1997

C.L. Montesquieu, *Over de geest van de wetten*, Amsterdam: Boom 2006

J.WM. Moore, *Moore's Federal Rules Pamplet 2007 – Part 2: Federal Rules of Evidence*, Newark/San Francisco: LexisNexis 2006

C.B. Mueller, L.C. Kirkpatrick, *Modern Evidence, Doctrine and Practise*, Boston, New York, Toronto, London: Little, Brown and Company 1999

P. Murphy, Evidence, *Proof, and Facts: A Book of Sources*, Oxford: Oxford University Press.

P. Murphy, D. Barnard, *Evidence and Advocacy, Blackstone:* Blackstone Pr 2002

H.-J. Musielak, M. Stadler, *Grundfragen des Beweisrechts*, München: C.H. Beck'schen Buchdruckerei Nördlingen 1984

H.-J. Musielak, *Grundkurs ZPO*, München: C.H. Beck Verlag 2007

R. Oberheim, *Zivilprozessrecht für Refendare*, Neuwied: Werner Verlag 2007

A. Oskamp, A.R. Lodder, *Informatietechnologie voor Juristen*, Deventer: Kluwer 2002

D. Pei, *Authentication Codes and Combinatorial Designs*, Boca Raton: Chapman & Hall/CRC 2006

M.E.M.G. Peletier, *Rechterlijke vrijheid en partij-autonomie* (diss. Amsterdam VU), Den Haag: Boom Juridische Uitgevers 1999

C.P. Pfleeger, *Security in Computing*, New Jersey: Prentice Hall International, Inc. 1997

Pitlo, Hidma, T.R., Rutgers, G.R., *Het Nederlands burgerlijk recht: Bewijs, deel 7*, Deventer: Kluwer 2004

P.R. Rice, *Electronic Evidence, Law and Practice*, Chicago: ABA Publishing 2008

L. Rosenberg, K.H. Schwab, P. Gottwald, *Zivilprozessrecht*, München, C.H. Beck 1993

A. Roβnagel, 'Das neue Recht elektronischer Signaturen', *Neue Juristische Wochenschrift*, 2001-25

G.R. Rutgers (red.), *Parlementaire geschiedenis van het bewijsrecht in civiele zaken*, Deventer: Kluwer 1988

S.A. Saltzburg, K.R. Redden, *Federal Rules of Evidence Manual*, Charlottesville: The Michie Company Law Publishers 1986

S.A. Saltzburg, M.M. Martin, D.J. Capra, Fe*deral Rules of Evidence Manual, A complete guide to the Federal Rules of Evidence, volume 5*, Newark / San Francisco: LexisNexis 2002

K. Schellhammer, *Zivilprozess, Gesetz – Praxis – Fälle*, Heidelberg: C.F. Müller Verlag, 2004

F.G. Scheltema, H.J. Scheltema, *Nederlandsch burgerlijk bewijsrecht*, Zwolle: W.E.J. Tjeenk Willink 1940

E. Schilken, Zivilprozessrecht, Köln/Berlin/München, Carl Heymanns Verlag GmbH 2006, p. 214

D.A. Schlueter, S.A. Saltzburg, *Emerging Problems Under The Federal Rules of Evidence*, Charlottesville: Lexis Law Publishing 1998

Schneider. *Beweis und Beweiswürdigung*, Verlag Vahlen, 5. Auflage

B. Schneier, *Secrets & Lies, Digital Security in a Networked World*, New York: John Wiley & Sons, Inc. 2000

D.A. Sklansky, *Evidence: cases, commentary, and problems*, New York: Aspen Publishers, Inc 2003

D.S. Skupsky, 'The Best Evidence Rule is Dead…Except in the Mind of the Law!', *Records Management Quarterly;* Jul 92, Vol. 26 Issue 3

H.J. Snijders, C.J.M. Klaassen, G.J. Meijer, *Nederlands burgerlijk procesrecht, Deventer*: Kluwer 2007

C.W. Star Busmann, L.E.H. Rutten, *Hoofdstukken van burgerlijke rechtsvordering*, De Erven F. Bohn N.V.: Haarlem 1972

P.A. Stein, A.S. Rueb, Burgerlijk Procesrecht, Deventer: Kluwer 2003

D.R. Stinson, Cryptography, Theory and Practise, Boca Raton: CRC Press 1995

F. Stajano, *Security for Ubiquitous Computing*, Chichester: John Wiley & Sons, Ltd 2002

C. Theimer, *Mustertexte zum Zivilprozess Band I: Erkenntnisverfahren erster Instanz*, München: C.H. Beck

H. Thomas, H. Putzo, *Zivilprozessordnung mit Gerichtsverfassungsgesetz, den Einführungsgesetzen und europasrechtlichen Vorschriften*, München, Verlag C.H. Beck 2007

D.J. Veegens, E. Korthals Altes, H.A. Groen, *Cassatie in burgerlijke zaken*, Deventer: Kluwer 2005

G. Weissenberger, J.J. Duane, *Federal Evidence*, Cincinnati: Anderson Publishing Co. 2001

M. Weggeman, *Kennismanagement - Inrichting en besturing van kennisintensieve organisaties*, Schiedam: Scriptum Management 1997

R.J.J. Westerdijk, *Produktenaansprakelijkheid voor software* (diss. Amsterdam VU), 1995

G.J. Wiarda, *Drie typen van rechtsvinding*, Deventer: Kluwer 1999

B.T.M. van der Wiel, "De bewijsovereenkomst", *Weekblad voor Privaatrecht, Notariaat en Registratie 2002-2*

H.L.G. Wieten, *Bewijs, Studiereeks burgerlijk procesrecht*, Kluwer: Deventer 2004

J.H. Wigmore, *Wigmore On Evidence, Treatise on the Anglo-American System of Evidence in Trials at Common Law, Volume 5*, Boston: Little Brown and Company 1940

J.H. Wigmore, P. Tillers (revision), *Wigmore on Evidence, Evidence in Trials at Common Law*, Boston, Toronto, Little, Brown and Company 1983

H.D. van Wijk, W. Konijnenbelt, *Hoofdstukken van bestuursrecht*, Den Haag: Elsevier Juridisch 2008

J.L. Wright, M.M. Williams, 'Remember the Alamo: the seventh Amendment of the United States Constitution, the doctrine of incorporation, and state caps of jury Awards', *South Texas Law Review* 2004-449

Trefwoordenregister