Elektronische handtekening en identificatie in de virtuele wereld

Prof. dr. Rogier DE CORTE

Hoogleraar U. A., directeur Centrum Recht & Informatie,
Faculteit Rechtsgeleerdheid RUG

Inleiding

1. Het is nog steeds de vraag of de omschakeling van het type industriële maatschappij naar het type informatiemaatschappij wezenlijke verschuivingen heeft teweeg gebracht dan wel alleen "veel meer" aanbiedt dan vroeger of vooral versnelling veroorzaakt van het maatschappelijk gebeuren. Hetzelfde of toch anders? De vlotheid en de snelheid van e-mailberichten[1], de onvoorstelbare eenvoud van het oprichten van een virtuele organisatie, de quasi-kosteloosheid om te participeren en een actieve medespeler te worden in het wereldnieuws via de newsgroups, de dematerialisering van de gegevens, ... is dit "nieuw" of is dit enkel "meer van hetzelfde".[2] Is het alleen de snelheid die verbaast of is er meer aan de hand? Stelt de onvoorspelbare inzet van elektronische data de digitale burger alleen voor een kwantitatief probleem of plaatst het de mens voor fundamentele vragen?

Deze ganse ontwikkeling is zeer complex. Hierna wordt aandacht besteed aan drie aspecten die van belang zijn voor het behandelde onderwerp: [1] de argwaan-angst-agressie reactie op de snelheid waarmee alle veranderingen gebeuren en de impact op de wijze van wetgeving; [2] horizontalisering van diezelfde maatschappij, waardoor de mens zijn eigen identiteit wenst te beschermen, zodat er vragen ontstaan naar het recht op meervoudige identiteit enerzijds en anonimiteit anderzijds, en [3] de dematerialisering van vele maatschappelijke, tot en met rechtshandelingen.

A. Snelheid & verandering

2. De evolutie van een hiërarchisch gestructureerde industriële maatschappij naar een netwerk van voorzieningen gaat gepaard met of vindt zijn grondslag in twee andere verschijnselen: m.n. het teloorgaan van de sociale cohesie en het verdwijnen van vaste verbanden, dit alles in een snel veranderingstempo op elk vlak.

Het is de kweekvijver van drie andere fenomenen: **argwaan**, als gebrek aan vertrouwen in de eigen positie en het gebrek aan kennis van de nieuwe mogelijkheden[3], **angst**, omwille van het verlies van zekerheid en vat op de gebeurtenissen[4] en **agressie** omdat men de overtuiging heeft zelf te moeten instaan voor zijn eigen project. Elk van deze fenomenen krijgt een eigen impact, ook in de rechtsorde: argwaan en angst zijn bijv. duidelijk aanwezig in de wetgeving en in bepaalde rechtspraak waarbij de privacy[5] gestalte wordt gegeven. Ook agressie, het waarmaken van de individuele belangen binnen de eigen belangensfeer, ingezet via professionele lobbying[6], wordt zichtbaar in het recht. Hoe beperkter de invloed van een belangengroep is in de maatschappelijke breedte des te harder zet die groep zijn macht in.

B. Horizontalisering

3. De horizontalisering van de maatschappij heeft nog een bijkomend effect, m.n. de behoefte aan een meerduidige identiteit. In de statische agrarische maatschappij, iets

[1] Men schat dat er jaarlijks 6.000 miljard e-mails worden verstuurd tegenover 1,7 miljard brieven en pakjes.

[2] Deze vraag heeft men zich ook gesteld bij de opkomst van de boekdrukkunst in de 15de eeuw. Dit was ongetwijfeld de voornaamste informatietechnologische vinding. Deze vraag is ook gesteld bij de intrede van de telefoon (1876).

[3] Twee typische voorbeelden van de onverantwoorde angstreacties zijn art. 12*bis* WVP waarbij het principieel verboden wordt geautomatiseerde beslissingen aan mensen op te dringen en art. 4 § 1 Wet Certificatiediensten waarbij niemand kan verplicht worden rechtshandelingen op elektronische wijze te verrichten.

[4] Deze vaststelling lijkt een groot deel van de verklaring te bieden voor de malaise bij het onderwijzend personeel, dat zich als het ware op het slagveld van de informatiemaatschappij bevindt.

[5] In de multimediabijlage van *De Morgen* van 27 oktober 1999 is de inleidende titel "Technologie en het internet luiden het einde van de privacy in", eerder een misleidende dan een inleidende titel.

[6] Twee voorbeelden: het agressief gedrag van IFPI door de nieuwe mogelijkheden gecreëerd door het internet en de erbij horende MP3-technologie en meer algemeen nog het lobbyen op Europees niveau bij het totstandkomen van de richtlijnen elektronische maatschappij.

minder in de industriële maatschappij, lijkt een eenduidige identiteit een vanzelfsprekend uitgangspunt: het individu is niet zo prominent aanwezig zodat een eenduidige identiteit niet als bedreigend wordt aangevoeld. Er waren hoofdzakelijk twee terreinen waar meerduidige identiteit een maatschappelijke betekenis had: bij kunstenaars en bij kloosterlingen. Twee terreinen waarin pseudoniemen (een uiting van dubbele identiteit) gangbaar waren - weze het om totaal verschillende redenen. De horizontalisering - denk bijv. aan de communicatie via e-mail, in newsgroups en in chatboxes - brengt het individu prominent op de voorgrond. Bij een eenduidige identiteit zou een participant zich volledig en onbeperkt vrijgeven aan de buitenwereld, hoewel hij zich slechts aan een klein segment heeft geopenbaard. De meerduidige identiteit vindt trouwens een gedeeltelijke erkenning in andere delen van het rechtssysteem, zo is bijv. de verkokering van het recht er een uiting van: eenzelfde situatie wordt juridisch verschillend geregeld naar gelang de hoedanigheid van betrokkene (als consument of als handelaar bijv., terwijl diezelfde persoon tegelijkertijd consument én handelaar is).

De vraag naar het recht op anonimiteit en deze naar identificatie spelen zich in deze zone af. Zo hebben twee recente wetten[7] op een eerder sluipende wijze rechtens anoniem gedrag toegelaten, waar er voordien in de rechtsorde geen ruimte voor was.

C. Dematerialisering

4. Waar voorheen de kwetsbaarheid van de maatschappij in hoofdzaak gerelateerd werd aan de inzetbaarheid van vernietigingsmiddelen, ontstaat nu een nieuwe kwetsbaarheid omdat belangrijke maatschappelijke processen aangestuurd worden door computersystemen. De kwetsbaarheid van een computersamenleving ligt voor de hand: denk maar aan het maatschappelijk impact dat een Y2000 bug voor gevolg zou kunnen gehad hebben, de schade die door een intelligent virus kan worden aangericht, ... Maar ook maatschappelijk-culturele verschuivingen moeten correct worden ingeschat: een ambtenaar die antwoordt: “mevrouw ik kan het u niet zeggen, het zit in de computer ...”, of een loketbediende die antwoordt “dit kan het programma niet aan ...”: het is een evolutie van bureaucratie naar infocratie, waarbij de voorkeur van velen duidelijk zal uitgaan naar de bureaucraat.

Deze kwetsbaarheid doet zich voor zowel op micro-, op meso- als op macro-niveau. Deze sterke afhankelijkheid van de informatietechnologie moet een bestendige zorg uitmaken van de overheid, zonder dat deze bezorgdheid mag ingegeven zijn door angst.

5. Eén van de aspecten hierbij is de dematerialisering van elektronische gegevens: elektronische gegevens hebben als het ware een bestaan onafhankelijk van hun opslagmedium.[8] Hierdoor ontstaan voor de jurist situaties waarvoor het bestaande recht geen afdoend kader biedt. In dit verband dient bijvoorbeeld verwezen te worden naar de bedenkelijke rechtspraak m.b.t. diefstal van elektronische gegevens[9], vooraleer de wet op de computercriminaliteit was goedgekeurd.

Met zekerheid kan men stellen dat data meer en meer elektronisch zullen opgeslagen worden, zodat door de stijging van de economische waarde van “data” en door de quasi onbeperkte inzetbaarheid ervan zich nu reeds de noodzaak opdringt een fundamentele juridische regeling te ontwikkelen m.b.t. data, informatie, ...

Het B.W. regelt het statuut van de goederen: is informatie één van deze goederen (bijv. onlichamelijke goederen) of past dit begrip helemaal niet in die categorie?

6. Ook de nieuwe wetgeving i.v.m. de elektronische handtekening en de certificatiediensten toont aan dat wetgever en jurist er nog steeds niet zijn in geslaagd een naadloze overgang te creëren tussen het recht en de informatiemaatschappij.

Hoofdstuk I. Zekerheid & veiligheid

Inleiding

7. Vóór de opgang van de informatiemaatschappij kon men ervan uitgaan dat er in de meeste rechtsbetrekkingen een aanvaardbare verhouding bestond tussen maatschappelijke soepelheid en maatschappelijke zekerheid. In die fysieke wereld werden er toen ook meer dan 1 miljard geschreven boodschappen verstuurd waarbij het onmogelijk was na te gaan of de afzender wel de afzender was.

Niemand vroeg toen *meer zekerheid*, zaken werden daarenboven afgehandeld via telefoon, telex ... en het uitgangspunt was geen angst, wantrouwen of onzekerheid. In domeinen waar deze contactvormen te losjes waren had men *ad hoc* oplossingen bedacht.

Waarom wordt zekerheid in de virtuele wereld een cruciale vraag? Er zijn wel degelijk objectieve redenen aanwezig om het zekerheidsprobleem met meer aandacht te volgen dan voorheen:

- vooreerst spelen irrationele gevoelens mee: angstgevoelens omwille van de snelheid waarmee alles verandert. Gebrek aan *vertrouwd zijn met* doet wantrouwen ontstaan;

[7] Zie verder: de Wet Informaticacriminaliteit waarbij de Telecomwet werd aangevuld en de Wet Certificatiediensten.

[8] Bertel de Groote, “Het bewijs in de elektronische handel - enkele bedenkingen” *A.J.T.* 2000-2001, nr. 22

[9] Antwerpen 13 december 1984, *R.W.* 1985-86, 244

- het gebruik van elektronische communicatiemiddelen groeit exponentieel meer dan het gebruik van de fysieke communicatiemiddelen, waardoor deze communicatie, gelet op haar structuur[10], vatbaar is voor massaal misbruik[11];
- bij een ongeautoriseerde ingreep zijn wijzigingen in elektronische bestanden moeilijker zichtbaar en opspoorbaar dan in een niet-elektronische omgeving.

8. Anderzijds doet zich in de virtuele wereld ook de tegenovergestelde evolutie voor m.n. de vraag naar anonimiteit. Ook hier speelt een zeker angstgevoel mee, maar vanuit een andere invalshoek: geeft iemand, die participeert aan één of andere activiteit in de virtuele wereld, zich niet teveel "bloot"?

Deze beide aspecten enerzijds veiligheid en identificatie en anderzijds anonimiteit worden hierna toegelicht in hun technische aspecten.

Afdeling 1. Zekerheid

9. Zekerheid en veiligheid in het virtueel verkeer worden samengevat in een 5-tal beginselen: [1] identificatie, [2] authentificatie, [3] integriteit, [4] onweerlegbaarheid en [5] confidentialiteit.

Deze verschillende veiligheids- en zekerheidsaspecten moeten in beginsel worden onderzocht los van enige binding met het begrip handtekening of geschrift. Deze begrippen hebben immers een zelfstandig bestaan buiten deze toepassingen om. Pas in een later stadium kan worden onderzocht in welke mate deze begrippen van belang zijn voor een correcte vorming van een handtekening of van een werkbaar geschrift.

A. Identificatie

10. Onder "identificatie" dient te worden verstaan het geheel van activiteiten waarbij van een persoon of van een instelling de naam en het geografische adres worden vastgesteld; het gaat om de vaststelling van de primaire identificatiegegevens. Een e-mailadres of een postbusnummer beantwoordt niet aan dit vereiste van identificatie. Anderzijds volstaat het geografisch adres, zonder dat dit de wettelijke woonplaats behoeft te zijn of de plaats waar iemand is ingeschreven in het bevolkingsregister.

In de pre-virtuele wereld bestond het probleem van de identificatie eveneens, maar werd dit veelal op traditionele wijze opgelost (handtekening, het voorleggen van een uittreksel uit bevolkingsregister, ...), slechts in bepaalde gevallen leidde het tot de noodzaak om bijzondere maatregelen te nemen. Zo moest de notaris in bepaalde gevallen de identiteit van partijen controleren aan de hand van in de wet aangeduide stukken, moest de bankier tot identificatie overgaan bij het openen van een bankrekening enz.

11. In een virtuele wereld, vnl. binnen open netwerken, zijn echter geen structurele middelen meer aanwezig ter identificatie van de participanten. De elektronische handtekening wil precies die identificerende functie overnemen.

Het bijzondere is wel dat noch art. 1322 lid 2 B.W., noch art. 2, 1° Wet Certificatiediensten de identificatie als een essentieel onderdeel van de elektronische handtekening opneemt. Art. 1322 lid 2 B.W. vermeldt "tekens die aan een persoon kunnen worden toegerekend" en art. 2, 1° Wet Certificatiediensten spreekt van authentificatie.[12]

B. Authentificatie

12. Onder authentificatie verstaat men het vaststellen dat een bepaald bericht (eventueel de handtekening) afkomstig is van de persoon die als titularis is aangeduid. Is de persoon die zich identificeert ook de persoon die de handtekening heeft geplaatst?

Authentificatie wordt terecht zowel in art. 1322 lid 2 B.W. als in art. 2, 1° Wet Certificatiediensten als een essentieel onderdeel van de elektronische handtekening aangemerkt.

Problemen van authentificatie zijn in een virtuele wereld aanzienlijk omvangrijker dan in een fysieke wereld.

In de fysieke wereld wordt het probleem van de authentificatie opgelost door de eis dat een handtekening moet geplaatst worden door de fysieke persoon zelf die zich identificeert. Soms werden er bijkomende eisen gesteld zoals de bevestiging door een notaris dat een partij met hem heeft ondertekend, de controle van bepaalde documenten, enz.

In de virtuele wereld wordt hiertoe precies een beroep gedaan op de tussenkomst van certificatiediensten: dit zijn personen of instellingen die o.m. tot taak hebben te certificeren dat een bepaalde handtekening toe te rekenen is aan een persoon die zich heeft geïdentificeerd.

[10] Deze communicatie is volledig gedematerialiseerd.

[11] Indien men zich tot doel zou stellen de boodschappen, die via briefwisseling met de post worden verzonden, te manipuleren, dan zou men elke brief afzonderlijk moeten bemachtigen, openen, wijzigen, sluiten en terug in het verzendcircuit brengen. Wenst men e-mails te manipuleren, dan zou dit op een massale basis kunnen, althans indien men over de nodige kennis en middelen beschikt. De schade door één virus aangericht is soms niet te overzien, ...

[12] Volgens de Wet Certificatiediensten zou identificatie alleen een eigenschap zijn van een geavanceerde elektronische handtekening (art. 2, 2°, b Wet Certificatiediensten), wat vanzelfsprekend niet de bedoeling van de tekst kan zijn. De essentie van de handtekening is trouwens identificatie.

Authentificatie wordt onterecht zowel in art. 1322 lid 2 B.W. als in art. 2, 1° Wet Certificatiediensten als een essentieel onderdeel van de elektronische handtekening aangemerkt.

Vanzelfsprekend wil iedereen zekerheid hebben omtrent de toerekening van een handtekening aan de geïdentificeerde ondertekenaar, maar het niet voorhanden zijn van die zekerheid maakt niet de ongeldigheid uit van de handtekening. Authentificatie vormt daarentegen wel een bijkomend kenmerk van een handtekening (wanneer een notaris bevestigt dat een partij met hem heeft ondertekend, biedt deze verklaring een bepaalde meerwaarde aan de handtekening; indien de authentificatie bevestigd wordt in een certificaat, kan men spreken van een geavanceerde elektronische handtekening, ...).

C. Autorisatie

13. Het begrip "autorisatie" of "legitimatie" betekent dat van een geïdentificeerd persoon bepaalde hoedanigheden moeten worden vastgesteld: bijv. alleen een advocaat bij het Hof van Cassatie mag een memorie in civiele zaken ondertekenen; alleen bepaalde personen hebben toegang tot bepaalde bestanden, ... De controle of mevrouw X advocaat is bij het Hof van Cassatie, of een bepaald persoon toegang mag krijgen tot bepaalde bestanden, ... betreffen autorisatieproblemen. Autorisatie houdt in beginsel geen verband met identificatie[13], hoewel beide begrippen zowel in een netwerkomgeving (zie bijv. art. 550*bis* § 2 Sw.[14]) als er buiten (art. 8 § 2 Wet Certificatiediensten) nauw met elkaar verbonden zijn. Het probleem van de autorisatie blijft hier verder onbesproken.

D. Integriteit

14. De integriteit van een boodschap (handtekening, ...) betekent de zekerheid dat er geen wijzigingen zijn aangebracht op een niet-toelaatbare wijze. In die zin kon men zeggen dat papier in het verleden een zeer hoge graad van integriteit bood, vnl. in tegenstelling met elektronische bestanden. In de regel "ziet" men elke wijziging aangebracht op een papierdocument.

15. Art. 1322 lid 2 B.W. vermeldt de integriteit als een essentieel aspect van de elektronische handtekening (" ... geheel van elektronische gegevens dat ... het behoudt van de integriteit van de akte aantoont."), terwijl deze integriteitsvereiste in art. 2, 1° Wet Certificatiediensten niet wordt vermeld.[15]

E. Onweerlegbaarheid

16. Een ander veiligheidsaspect wordt de onweerlegbaarheid of non-repudiatie genoemd. Wanneer een afzender een bericht verstuurt naar de ontvanger, moet in hoofde van de ontvanger de zekerheid worden gecreëerd dat in een latere fase de afzender niet meer over de mogelijkheid beschikt om te ontkennen dat het bericht door hem werd verstuurd. Het gaat m.a.w. over de toerekening aan een geïdentificeerd persoon.

17. In de niet-virtuele wereld werd dit probleem via art. 1323 B.W. opgelost: wanneer een boodschap ondertekend werd door een persoon, wordt deze persoon geacht de auteur te zijn behalve indien hij "op stellige wijze zijn handtekening ontkent".[16] In dat geval wordt een gerechtelijk onderzoek naar de echtheid gestart. In de praktijk van elke dag schijnt deze regeling zelden voor te komen en dus zeer bevredigend te werken.

18. In de virtuele wereld leggen de certificatiediensten de band tussen de elektronische handtekening en de persoon. Deze diensten zouden het probleem van de non-repudiatie moeten oplossen. Zo vermeldde het oorspronkelijk regeringsvoorontwerp van wet Certificatiediensten[17] in art. 11 § 1 lid 2 «Elk gebruik ervan wordt, behoudens tegenbewijs, geacht de daad te zijn van diens houder.». In deze werkhypothese werd een (veilige) elektronische handtekening geacht, behoudens tegenbewijs, gesteld te zijn door de houder van het certificaat. Deze oplossing maakte de toepassing van art. 1323 overbodig en werkte derhalve een strengere regeling uit, die specifiek gold voor de virtuele wereld.

Door de nieuwe versie van art. 4 § 4 Wet Certificatiediensten is de situatie grondig gewijzigd. De assimilatieclausule stelt de geavanceerde elektronische handtekening gelijk met de gewone handtekening, onverminderd de toepassing van art. 1323 B.W.

Dit impliceert dat wanneer een geavanceerde elektronische handtekening aan een persoon wordt tegengeworpen, de ontkenning van deze handtekening volstaat om een procedure van gerechtelijk onderzoek te starten.

[13] Autorisatie is mogelijk zonder identificatie, m.n. in al die gevallen waar de autorisatieprocedure niet gekoppeld wordt aan identificatiegegevens.

[14] «§ 2. Hij die, met bedrieglijk opzet of met het oogmerk om te schaden, zijn *toegangsbevoegdheid* tot een informaticasysteem overschrijdt, wordt gestraft met gevangenisstraf van zes maanden tot twee jaar en met geldboete van zesentwintig frank tot vijfentwintigduizend frank of met een van die straffen alleen.»
Dit begrip "toegangsbevoegdheid" betreft precies een autorisatieprobleem.

[15] Integriteit is vanzelfsprekend een belangrijke zorg, maar geen essentieel onderdeel van een handtekening, zie nr. 68 en volg.

[16] Erfgenamen mogen volstaan met de bewering dat ze de handtekening van hun voorganger niet kennen.

[17] Goedgekeurd op de ministerraad van 26 maart 1999.

Hier kan men dan ernstig de vraag stellen waarom deze Wet Certificatiediensten dan wel nodig was.

F. Confidentialiteit

19. Onder de hoofding confidentialiteit van berichten worden de problemen behandeld van de toegang tot de inhoud (kennisname van de inhoud van een boodschap) door onbevoegde of niet-geautoriseerde personen.

De mogelijkheid van ongeautoriseerde toegang tot elektronische documenten is exponentieel groter en gemakkelijker te realiseren dan bij papierdocumenten.

Confidentialiteit wordt gegarandeerd door encryptie.

20. Bij de toepassing van asymmetrische encryptie[18] stelt het probleem van de confidentialiteit zich in hoofdzaak met betrekking tot de vertrouwelijkheid van de *private key*.[19] De certificatiedienstverlener staat in voor de confidentialiteit tot de samenstelling van de handtekening, na de samenstelling van de handtekening is enkel de certificaathouder aansprakelijk voor de bewaring (art. 19 § 1 Wet Certificatiediensten).

Afdeling 2. Anonimiteit

21. In omzeggens alle sites over digitale burgerrechten duikt de vraag naar het "recht" op anonimiteit op voor internetgebruik. Deze vraag sluit aan bij het gevoel van de digitale burger die participeert aan de digitale wereld en zich daardoor meer en vollediger blootstelt dan bij eender welk ander maatschappelijk gedrag. Dit fenomeen had de vraag bij anderen reeds doen rijzen naar het recht op meerdere identiteiten.

De veralgemeende verspreiding van internet speelt in de verdere ontwikkeling van het gebruik van nick-names, anoniem en naamloos optreden een doorslaggevende rol. Het verzenden van een e-mail alleen ondertekend met een naam en een e-mailadres (al dan niet waarachtig) is niet ongebruikelijk, het gebruik maken van nicknames in een chatbox is legio.

22. Met het oog op de gestelde problematiek lijkt de omschrijving van het begrip "anoniem" in Van Dale's Groot Woordenboek van de Nederlandse taal niet aangepast:

"1. zonder bekendmaking van de naam van de schrijver of spreker enz., zonder ondertekening ...".

In deze betekenis wordt anoniem niet gebruikt in de virtuele wereld: een anonieme re-mailer bijv. is een e-mailserver die zijn cliënten garandeert dat de identiteit onder geen enkel beding zal kunnen achterhaald worden.

23. Hierna wordt een onderscheid gemaakt tussen "anonimiteit" enerzijds en "naamloos optreden" anderzijds.[20] Tussen beide begrippen situeert zich soms een derde mengvorm, die wordt aangeduid als "relatieve anonimiteit".

§ 1. Anonimiteit

24. Onder *anonimiteit* kan men verstaan het optreden van een persoon in een maatschappelijke context waarbij[21]:

- hij zijn identiteit verbergt (intentioneel aspect);
- door de inzet van normale middelen geen band kan gelegd worden naar een geïndividualiseerde fysieke persoon (resultaatsaspect).

Anonimiteit wordt derhalve in een specifieke zin gebruikt, waarbij zowel de intentie (het verbergen van identiteit) als het resultaat (geen toegang tot de identiteit door inzet van gewone middelen) deel uitmaken van de omschrijving.

25. In deze betekenis wordt anoniem gebruikt in de wet van 8 december 1992 WVP, waar het begrip "persoonsgegeven" wordt omschreven (art. 1 § 2): deze wet is niet van toepassing op persoonsgegevens die anoniem zijn gemaakt, het zijn dan immers geen persoonsgegevens meer.[22]

De Raad van State heeft in het arrest nr. 45.218 van 10 december 1993[23] terecht verwezen naar de realiteit: gegevens zijn slechts anoniem indien uit het geheel van de voorhanden zijnde elementen (bijv. de gemeente, de leeftijd, de kliniek, de opnameperiode) in redelijkheid geen identificatie mogelijk is.

26. Zijn, in de betekenis van deze wet, evenmin anoniem de zgn. "gecodeerde gegevens". Gecodeerde gegevens zijn data waarbij een scheiding is gemaakt tussen de inhoud van de data (die van een code voorzien zijn) en de identificatiegegevens (de identiteit, eveneens voorzien van die code). Deze techniek wordt veelal gebruikt bij

[18] Zie nr. 87 en volg.

[19] In art. 2, 6° Wet Certificatiediensten aangeduid als «gegevens voor het aanmaken van een handtekening».

[20] Ph. Traest, *Het bewijs in strafzaken*, Mys & Breesch, 1992, nr. 741 maakt deze onderscheiden niet omdat ze in de door hem onderzochte materie van geen belang zijn.

[21] G. Luc Ballon, "Ik gaf mijzelf (g)een naam, over anoniem en pseudoniem optreden in de openbaarheid", *T.P.R.* 1981, 557-592, nr. 18. Deze auteur gaat uit van een ander concept in hoofdzaak omdat de problematiek werd onderzocht vanuit het standpunt van de kunstenaar en het daarbij horende vaderschap.

[22] Een persoonsgegeven wordt als identificeerbaar omschreven wanneer het direct of indirect kan geïdentificeerd worden.

[23] R.v.St. nr. 45.218, 10 december 1993, *Vl. T. Gez.* 1993-94, 281.

wetenschappelijke enquêtes om de privacy-gegevens bij de behandeling en de verwerking van de enquête zoveel mogelijk te beschermen. De identificatie wordt in een afzonderlijk bestand, meestal ook op een afzonderlijke plaats bewaard met het oog op een eventuele opvolgingsenquête enkele jaren later. Dergelijke gecodeerde gegevens zijn geen anonieme gegevens.

27. Het verzamelen van statistisch materiaal en enquêtes uitgezonderd, heeft anonimiteit meestal een a-sociale connotatie: een anoniem telefoontje, een anonieme brief met verbijsterende onthullingen, ... worden nog steeds als maatschappelijk storend ervaren, daar het zich onttrekken aan de door de rechtsorde opgelegde verplichtingen centraal staat. In deze zin is anonimiteit geen beschermingswaardig goed.

§ 2. Naamloos optreden

28. *Naamloos optreden* is het optreden van mensen waarbij de identiteit niet wordt naar voor gebracht omdat er geen behoefte bestaat zich te identificeren. Het naamloos optreden verbergt geen identiteit, maar gebruikt ze evenmin, daar het maatschappelijk niet verwacht wordt. Wanneer men winkelt in de Nieuwstraat te Brussel is de identiteit van die persoon geen onderdeel van die activiteit, maar die persoon verbergt ze evenmin. Wanneer je tijdens die wandeling een pakje sigaretten aankoopt, identificeer je je niet. Niemand heeft er ook behoefte aan. Mocht iemand je staande houden en vragen "wie zijt gij?" zou je daar vermoedelijk niet op antwoorden, niet omdat je je identiteit wenst te verbergen, maar omdat je identiteit in die maatschappelijke context niet relevant is. Je identiteit kan wel relevant worden bijv. voor een politiepatrouille of voor een winkelier waar je een diamant van ettelijke miljoenen hebt gekocht en je betaalt met een kredietkaart.

In bredere betekenis is naamloos optreden het optreden zonder identiteitsaanduiding: in deze betekenis treedt een faillissementscurator bijv. naamloos op, hij duidt niet aan voor welke schuldeisers hij optreedt, terwijl een mandataris in rechte niet naamloos kan optreden.

29. Aan het naamloos optreden kan een identificatieplicht gekoppeld zijn.[24] Deze is o.m. voorzien in de wet op het Politieambt.[25] Een identificatieplicht wordt in verschillende Europese landen sterk verschillend aangevoeld. Zo hangt er bijv. in de Amsterdamse trams volgend bericht: "zwartrijders moeten een boete betalen van x gulden, betalen ze de boete niet dan moeten ze zich identificeren". Identificatie is er als een sanctie aangemerkt.

§ 3. Relatieve anonimiteit

30. Naast anonimiteit en naamloosheid is er nog een derde vorm, aan te duiden als *relatieve anonimiteit*. Dit optreden dekt het gedrag waarbij men bijv. voor een krant of voor de televisie een verklaring wenst af te leggen zonder dat de lezer of de kijker je kan identificeren. De desbetreffende journalisten weten precies wie je bent, ze hebben je doopceel gelicht. Je bent slechts anoniem, je verbergt je identiteit voor een bepaalde groep uit de bevolking: bijv. het gebruik van pseudoniemen bij kunstenaars en kloosterlingen, een anonieme getuige voor de opsporingsambtenaar of voor de rechtbank.[26]

Relatieve anonimiteit vertoont zowel aspecten van anonimiteit als aspecten van naamloosheid.[27]

Het is verwant met anonimiteit omdat de betrokkene bewust zijn identiteit verbergt (intentie), langs de andere kant heeft het gemeen met naamloosheid dat een bepaalde belanghebbende[28] onmiddellijk in bezit gesteld wordt van de identiteit (afwezigheid van resultaat).

De redenen van "relatief anoniem"[29] optreden kunnen zeer divers zijn:

- men wil zich indekken tegen bepaalde maatschappelijke gevolgen die verband kunnen houden met de gedane bekendmaking: een persoon die informatie aan de media verstrekt, maar reactie van overheid, werkgever of omgeving vreest;
- bewuste keuze om persoonlijk uit de actualiteit te blijven;
- gevolgen van bekendheid vermijden;

In de regel is het zich "relatief anoniem" opstellen niet ongeoorloofd.

[24] Het bekendmaken van de naam van een getuige wiens verklaring anoniem is opgenomen is geen verplichting voor de opsporingsambtenaar (Ph. Traest, *Bewijs in strafzaken,* nr. 746).

[25] Zie arrest Filip Reyntjens Cass.27 februari 1990, *Arr. Cass*. 1989-90, 848 dat vóór de invoering van de wet op het Politieambt de identiteitscontrole door politie en rijkswacht conform het bestaande recht bevond. Thans is deze aangelegenheid geregeld in art. 34 §1, lid 1 Wet Politieambt 5 augustus 1992.

[26] Ph. Traest, *Het bewijs in strafzaken,* nr. 740 en volg.

[27] *In cognito* wordt meestal gebruikt voor een feitelijk optreden van bekende personen, waarbij zij hun hoedanigheid van "bekende" persoon zoveel mogelijk verbergen.

[28] Met de verwachting dat de identiteit naar buiten toe afgeschermd wordt.

[29] De eerste toepassing is het zich identificeren via een postbus, …

Conclusie

31. De vraag naar de bescherming van het naamloos optreden in een virtuele omgeving kan als een terechte vraag worden aangezien, niet de aanspraak op anonimiteit. Twee wettelijke bepalingen hebben nochtans een andere toon gezet zonder dit op een uitdrukkelijke wijze te motiveren of toe te lichten:

- de verstrekkers van telecommunicatiediensten moeten telecommunicatie-, oproep- en identificatiegegevens gedurende 12 maanden bijhouden enkel met het oog op het opsporen van misdrijven (art. 109*ter*E § 2 Telecomwet van 21 maart 1991, zoals gewijzigd door de Wet Informaticacriminaliteit van 28 november 2000);
- in art. 5 § 2 Wet Certificatiediensten moet de certificatiehouder enkel de identiteit mededelen van de houder van een pseudoniem in de gevallen van art. 90*ter–decies* Sv.

Deze beide bepalingen leiden ertoe dat de wetgever zelf elke burger het recht geeft zich in de virtuele wereld onrechtmatig te gedragen en op foutieve wijze schade aan een derde te veroorzaken (voor zover er geen misdrijven worden gepleegd). Immers de identiteit van de persoon die schade heeft veroorzaakt of zich onrechtmatig gedroeg mag niet aan het slachtoffer worden bekend gemaakt.

Hoofdstuk II. Juridische componenten rechtshandeling, akte en handtekening

Inleiding

32. Eén van de belangrijke problemen door de informatiemaatschappij aan de juristen voorgeschoteld, betreft het werken met elektronische documenten, d.w.z. gedematerialiseerde stukken. Vroeger was het eenvoudig: geschriften waren vrijwel steeds de basis van het juridisch handelen. Door het aanbrengen van een handgeschreven handtekening op een document ontstond het origineel en daar waar nodig konden meer originelen worden gemaakt, door een handtekening te plaatsen op elk van de exemplaren. De verschillende originelen konden desgewenst met elkaar worden vergeleken. Een relatief bevredigende oplossing.

Elektronische documenten zijn gedematerialiseerd en het plaatsen van een handgeschreven handtekening is vanzelfsprekend onmogelijk, terwijl anderzijds elke elektronische kopie van een elektronisch bestand even origineel is als het origineel. Daarenboven kan elk elektronisch bestand in beginsel worden gewijzigd, zonder dat een dergelijke wijziging zichtbaar is. Vergelijking van documenten met elkaar heeft in deze context geen zin. Waar in een virtuele wereld geen fysieke handtekening in de hierboven vermelde vorm kan geplaatst worden, kan de informatica wel op haar eigen wijze een hoge graad van zekerheid bieden door identificatie, authentificatie, integriteitsgarantie, non-repudiatie en confidentialiteit.

33. Drie wettelijke normenstelsels zijn hiervoor gecreëerd:

a. de Europese richtlijn nr. 1999/93 van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen;
b. de wet 20 oktober 2000 tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en de buitengerechtelijke procedure, waarbij art. 1322 B.W. wordt aangevuld met een tweede lid;
c. Wet 9 juli 2001 houdende vaststelling van bepaalde regels i.v.m. het juridisch kader voor elektronische handtekeningen en certificatiediensten (Wet Certificatiediensten), *B.S.* 29 september 2001.

34. Hoewel het bewijsrecht vatbaar is voor conventionele regeling drong een wettelijke regeling zich op vnl. naar aanleiding van het gebruik van open netwerken. In gesloten netwerken regelen de partijen meestal hun rechten en verplichtingen op voorhand (*Interchange Agreement*). Wanneer iemand tankt met een kaart aan een benzinestation zijn een aantal bewijsaspecten geregeld door de algemene voorwaarden van de bank. Wanneer handel gedreven wordt op internet, wanneer een burger elektronisch contact kan opnemen met zijn overheid, ... kennen de partijen elkaar op voorhand niet en dient de wetgever een afdoende regeling te bieden.

35. De door de wetgever geboden oplossingen hebben tot doel de problemen te regelen die zich voordoen in het elektronisch verkeer. Om de zwakke en sterke punten van de bestaande situatie goed te kunnen inschatten alsmede de wetswijzigingen te kunnen duiden worden vooraf de basisbeginselen van de bestaande toestand in herinnering gebracht en pas daarna wordt gepoogd een schets te bieden van de nieuwe evolutie.

36. Zowel bij de totstandkoming van de wet van 20 oktober 2000 tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en de buitengerechtelijke procedure[30], als bij de wet 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten is op soms pijnlijke wijze gebleken hoe onzorgvuldig met bepaalde basisbegrippen wordt omgesprongen. De snelle wijziging

[30] Dit is de wet waarbij art. 1322 B.W. werd gewijzigd en art. 2281 B.W. werd ingevoerd.

van opeenvolgende voorontwerpen van wet zonder een samenhangende evolutie, onderstreept eveneens het gebrek aan "meesterschap" in de materie. De lezing van het verslag van de Senaatscommissie n.a.v. de aanvaarding of verwerping van amendementen[31] op de eerder door de Kamer vastgestelde tekst over de certificatiediensten[32], kan als een schoolvoorbeeld van spraakverwarring aangewezen worden.

Deze verwarring is in een zekere mate begrijpelijk omdat bepaalde basisbegrippen die gebruikelijk door juristen worden gehanteerd pas gedefinieerd worden nadat ze hetzij door maatschappelijke evolutie, hetzij door nieuwe technologieën in vraag worden gesteld. Zo is bekend dat de juristen de criteria voor geslachtsbepaling van de mens pas formuleerden nadat het probleem van de geslachtsverandering zich had aangediend. Pas vanaf dat ogenblik formuleert men immers de criteria die men onbewust in het verleden heeft gehanteerd.

37. Het elektronisch sluiten van contracten, de elektronische handtekening, certificatie, ... hebben een aantal latente basisvragen aan de oppervlakte gebracht: wat is een "geschrift", wat is de essentie van een handtekening, wat is het verschil tussen een bewijsmiddel, de toelaatbaarheid ervan en de bewijswaarde? Bij nader inzien is de complexiteit van deze materie groter dan men aanvankelijk heeft ingeschat.[33] Bij dit alles mag men echter een andere basisregel niet uit het oog verliezen: de confrontatie van het recht met de informatietechnologie mag geen aanleiding geven tot het creëren van problemen die eigenlijk reeds opgelost waren of slechts een variante zijn van bestaande problemen en die aan de hand van de bestaande juridische instrumenten kunnen worden opgelost. Het uitgangspunt "on line is off line" moet volledig worden geëerbiedigd: indien een probleem, gesteld door de informatietechnologie, perfect kan opgelost worden aan de hand van de bestaande oplossingsmodellen, moet niet naar nieuwe oplossingsmodellen gezocht worden.

38. Hierna worden de drie polen waarrond de elektronische handtekening zich afspeelt samengevat: [1] de rechtshandeling, [2] het bewijs van een rechtshandeling - de schriftelijke akte en [3] de handtekening. Elk van deze drie juridische concepten heeft een eigen functie, die niet steeds duidelijk af te lijnen is. Zo is immers het plaatsen van een handtekening op een schriftelijke akte op zichzelf reeds een rechtshandeling. Voor elk van deze drie begrippen zal gepoogd worden de impact van de informatietechnologie te schetsen, pas dan kan men inschatten of de door de wetgever aangeboden oplossing adequaat is. Omwille van de duidelijkheid zal verder enkel aandacht besteed worden aan rechtshandelingen en hun bewijs, met uitsluiting van rechtsfeiten. Bewijsaspecten m.b.t. rechtsfeiten zijn niet onbelangrijk maar bieden geen relevante perspectieven voor het bewijsprobleem van rechtshandelingen.

Afdeling 1. Rechtshandeling

39. Het begrip "rechtshandeling" op zichzelf is een voldoende vertrouwd concept: het is een eenzijdige of meerzijdige wilsuiting gericht op het produceren van rechtsgevolgen. Zo zijn huurcontracten, het verrichten van een BTW-aangifte en het toestaan van een hypotheekbelofte, ... rechtshandelingen.

Met het oog op de toepassing van de informatietechnologie dient aandacht besteed te worden aan zowel aspecten van geldigheid van een rechtshandeling als aan aspecten van tegenwerpelijkheid aan derden van het bestaan van rechtshandelingen.

A. Rechtsgeldigheid

40. In de regel wordt de rechtsgeldigheid van rechtshandelingen beoordeeld los van het bestaan van een geschrift, waarin de rechtshandeling vervat kan zijn en los van de andere vormvereisten waarmee de wilsuiting kan worden omringd.

Rechtshandelingen zijn in beginsel vormvrij d.w.z. dat ze rechtsgeldig tot stand zijn gekomen op het ogenblik dat de wil geldig werd geuit, ongeacht de vorm. Een belangrijke afwijking van de regel van het consensualisme zijn de zgn. vormelijke rechtshandelingen. Dit zijn de rechtshandelingen die slechts rechtsgevolgen teweeg brengen indien tegelijkertijd aan twee voorwaarden werd voldaan: [1] rechtsgeldige wilsuiting en [2] de naleving van de door de wet gestelde vormvereisten. Het klassieke voorbeeld van een vormelijke rechtshandeling is het huwelijk. De rechtsgevolgen treden slechts in wanneer én [1] de toestemming van de partijen is gegeven én wanneer [2] al de wettelijke vormen zijn nageleefd (het verstrekken van de toestemming in elkaars aanwezigheid voor de ambtenaar van de burgerlijke stand, het opstellen van een huwelijksakte, ...).

Bij de verdere uiteenzetting wordt geen aandacht besteed aan deze zgn. vormelijke rechtshandelingen: de wet

[31] *Parl St*., Senaat, zitting 2000-2001, nr. 2-662/4 van 8 mei 2001.

[32] *Parl. St*., Kamer, 15 februari 2001, nr. 50-0322/005.

[33] Een aandachtige lezing van de bijdrage van Matthias E. Storme toont dit overigens duidelijk aan: M.E. Storme, "De invoering van de elektronische handtekening in ons bewijsrecht — Een inkadering van en commentaar bij de nieuwe wetsbepalingen", *R.W.* 2000-2001, 1505-1525. Zie in dit verband ook: J. Dumortier en P. Van Eecke, "De Europese ontwerprichtlijn over de digitale handtekening: waarom is het misgelopen?", *Computerr*. 1999, 3-10.

regelt ze immers meestal op bindende wijze, zodat deze wettelijke voorwaarden moeten nageleefd worden, zonder dat er ruimte is voor nieuwe inzichten of technieken[34]: de regel *forma dat esse rei* geeft de vorm voorrang boven de inhoud.

41. Op het gebied van de geldigheidsvereisten zelf van rechtshandelingen heeft de informatietechnologie de aandacht gefocust op twee aspecten met een specifiek karakter[35]: [1] het totstandbrengen van rechtshandelingen wanneer de wil niet door mensen wordt geuit maar door systemen (relatief nieuw probleem) en [2] het tot standbrengen van rechtshandelingen op afstand (relatief vertrouwd probleem).

42. Het eerste probleem is bekend aan bedrijven en diensten die met EDI[36]-toepassingen werken: rechtsbetrekkingen worden in deze omgeving gecreëerd door computersystemen die hiertoe geprogrammeerd zijn, zonder tussenkomst van een fysiek persoon. Wanneer een programma, waarbij de magazijnvoorraad wordt gecontroleerd, vaststelt dat de voorraad van één product beneden een bepaald peil is gedaald, kan meteen door het computersysteem een bestelling worden geplaatst bij een contractant, die deze bestelling ontvangt en verwerkt via zijn computersysteem. Het geheel van deze verrichtingen is gebaseerd op communicatie van systeem tot systeem. Vooralsnog wordt deze werkwijze juridisch onderbouwd door uitgebreide voorafgaande overeenkomsten tussen partijen (*Interchange Agreement)*. Zonder dergelijke overeenkomsten moet men een beroep doen op "juridische spitstechnologie".

Een aangepaste en geëigende regeling lijkt dan ook op zijn plaats. Na de invoering van de elektronische handtekening zou deze regeling voor een gedeelte ondersteund worden door het plaatsen van een elektronische handtekening, die uiteraard geldig is, zonder dat een fysiek persoon behoeft tussen te komen. Een globale regeling lijkt nochtans aangewezen te zijn.

43. Het tweede probleem betreft het creëren van rechtshandelingen op afstand.[37] Dit probleem is niet nieuw en zeker niet specifiek voor het omgaan met de informatietechnologie. Zoals dikwijls het geval is duiken er ingevolge de informatietechnologie aspecten op die voorheen niet werden opgemerkt. Deze aspecten werden deels geregeld door de wet van 25 mei 1999 waarbij de art. 77 en volg. WHP werden aan gepast.[38] Deze aanpassing is dermate overtrokken dat een aantal van de gestelde regelen in de praktijk van elke dag niet kunnen worden nageleefd (zo wordt bijv. de verzakingstermijn van 7 dagen naar drie maand gebracht indien aan de informatieverplichting niet wordt voldaan, art. 80 § 2 WHP).

B. Tegenwerpelijkheid aan derden

44. Hoewel rechtshandelingen in de regel slechts rechtsgevolgen teweegbrengen hetzij tussen de partijen die een overeenkomst sloten (gelding *inter partes*), hetzij binnen de rechtsverhouding die tot stand kwam (relatieve werking van bijv. een erkenning van een kind), wordt algemeen aangenomen dat een rechtshandeling als feit tegen een derde kan worden tegengeworpen: waar niets relatiever werkt dan rechtsgevolgen, werkt er niets absoluter dan feiten. Wetgever en rechtspraak hebben doorheen de jaren op dit domein sterk ingegrepen. Vooreerst heeft de wetgever ingegrepen in het beperken van de inroepbaarheid van het bestaan van een rechtshandeling tegen een derde. In een aantal gevallen heeft de wetgever beslist dat het bestaan van een rechtsverhouding als feit tegenover derden afhankelijk wordt van het naleven van een bijzondere vorm van publiciteit (zo bijv. bepaalt art. 1 Hyp. W. de publiciteit op het hypotheekkantoor voor de overdracht van zakelijke onroerende rechten onder levenden). Anderzijds heeft de rechtspraak derden in beperkte mate bepaalde gevolgen doen ondergaan van bestaande rechtsverhoudingen (boswachter arrest, derde-medeplichtige aan contractbreuk, ...).

45. Voor zover thans kan overzien worden, komen deze beginselen niet onder druk door de toepassing van de informatietechnologie. De fysionomie van de verhouding en kan wijzigen, de inhoud van de rechtsverhoudingen zelf blijft overeind.

Afdeling 2. Schriftelijke akte

46. Rechtshandelingen kunnen vastgelegd worden in een schriftelijke akte, dienstig als bewijsmiddel. De akte wordt aangeduid met de Latijnse benaming *instrumentum*,

[34] Zijn niet als vormelijke rechtshandelingen te omschrijven, de rechtshandelingen waarvoor de wetgever op straffe van nietigheid de naleving van vormen vereist ter bescherming bijv. van de consument, zoals bijv. in art. 17 Consumentenkredietwet.

[35] Benoît De Nayer en Jacques Laffineur, "Le consentement électronique: le cadre législatief belge" in X. *Le consentement électronique*, Collections droit et consommation, Bruylant 2000, 55- 76.

[36] *Electronic Data Interchange.*

[37] Marc Fallon, "Le concept de distance dans l'échange de consentement électronique" in X. *Le consentement électronique*, Collections droit et consommation, Bruylant 2000, 247-274.

[38] Door de wet van 25 mei 1999 werd de omzetting gerealiseerd van de Richtlijn nr. 97/7 van het Europees Parlement en de Raad van 20 mei 1997 betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten en van Richtlijn nr. 97/ ☞

in tegenstelling tot de rechtshandeling, *negotium*.

M.b.t. het *instrumentum* dienen zich de volgende vragen aan [1] de rechtsgeldigheid van de akte zelf, [2] de toelaatbaarheid van een bewijsmiddel en [3] de bewijswaarde van een bewijsmiddel. Het geschrift wordt soms met de handtekening gelijkgesteld, wat volkomen incorrect is.

De informatietechnologie heeft juist op dit domein een diepgaande invloed gehad.

A. Rechtsgeldigheid van een schriftelijke akte

47. De rechtsgeldigheid van een rechtshandeling dient beoordeeld te worden los van de rechtsgeldigheid van de schriftelijke akte, waarvan ze tot bewijs strekt.[39]

Zes variaties zijn derhalve mogelijk:

rechtshandeling	akte	voorbeeld
geldig	geldig	geldige verkoop, met geldige akte
	ongeldig	geldige verkoop, akte niet ondertekend
	geen	geldige verkoop, geen geschrift
ongeldig	geldig	verkoop door non-eigenaar, akte geldig opgesteld
	ongeldig	verkoop door non-eigenaar, akte niet ondertekend
	geen	verkoop door non-eigenaar, geen geschrift

48. Indien een schriftelijke akte enkel tot functie heeft als bewijs te dienen voor het bestaan en de inhoud van een rechtshandeling, zonder dat de geldigheid van de schriftelijke akte deze van de rechtshandeling beïnvloedt, zou het logische gevolg zijn dat de partijen slechts in die mate de ongeldigheid van het bewijsmiddel mogen opwerpen, als er een betwisting is van de rechtshandeling zelf. Vanuit functioneel standpunt is het inderdaad niet aanvaardbaar dat een partij de nietigheid van een schriftelijk bewijsstuk opwerpt (bijv. de afwezigheid van een dubbel origineel bij een wederzijdse verbintenis), wanneer het bestaan of de geldigheid van de verbintenis zelf niet betwist wordt.

De rechtspraak stelt deze functionele beperking helaas niet.

49. De geldigheid van een akte (bewijsmiddel) wordt door de wetgever op twee wijzen geregeld: op algemene wijze voor alle schriftelijke akten in het algemeen en op bijzondere wijze, hetzij bij bepaalde situaties (aantal originelen bij wederkerige overeenkomsten, "goed voor"-bepaling voor onderhandse biljetten) hetzij voor bepaalde geschriften in het bijzonder (bijv. een notariële akte[40], de verwerping van een nalatenschap, ...). Hierna wordt alleen ingegaan op de algemene vereisten die voor alle akten gelden.

50. Er zijn 3 algemene geldigheidsvereisten voor alle schriftelijke akten: als bewijsmiddel is een schriftelijke akte geldig indien [1] de akte vervat is in een geschrift, [2] opgesteld werd met het doel als bewijs te dienen en [3] de handtekening bevat van de partij die de rechtsgevolgen aanvaardt.

In de regel zijn er geen andere vereisten, zoals het aanbrengen van een datum op een schriftelijke akte, de taal van het document of de gelijktijdige aanwezigheid van partijen, ...

Het is duidelijk dat deze regelen ontworpen zijn ten tijde van de hoogconjunctuur van "het geschrift" en als zodanig sterk onder druk staan van de informatietechnologie, waar het schrijven vervangen is door de elektronische representatie van tekens.

§ 1. Geschrift

51. Zonder met zoveel woorden in het B.W. vermeld te zijn, gaat de wetgever ervan uit dat een schriftelijke akte als bewijsmiddel moet vervat zijn in een geschrift. In de huidige terminologie zou men spreken van: "op een grafische drager vastgelegd", ongeacht de grafische drager (papier, karton, steen, ...), ongeacht het schrijfprocédé (met de hand, tikmachine, ...), ongeacht de taal (Engels, dialect, ...) en ongeacht de schrijfwijze (bijna onleesbaar, kaligrafisch, ...). Het volstaat dat het om een geschreven stuk gaat. Het zou derhalve onjuist zijn te stellen dat een geschrift behoort samen te vallen met een boodschap op papier, hoewel dit meestal wel het geval zal zijn. Een met krijt op een bord geschreven boodschap of met griffel op een lei, is dit eveneens.

René Dekkers[41] omschrijft het als volgt:

Een ... akte bevat natuurlijk een tekst. Wat die betreft, schrijft de wet hoegenaamd niets voor:

- de tekst mag dus met de hand geschreven zijn, of getypt, of gedrukt, of gestencild, of gefotografeerd, enz.;
- hij mag met inkt geschreven zijn, of met potlood, of met krijt, in 't zwart, in 't wit, met kleuren, enz.;
- hij mag op papier geschreven zijn, of op karton, of op hout, of op een lei, enz.;

55 van het Europees Parlement en de Raad van 6 oktober 1997 tot wijziging van Richtlijn nr. 84/450 inzake misleidende reclame teneinde ook vergelijkende reclame te regelen.

[39] Dit uitgangspunt geldt niet bij vormelijke overeenkomsten. Deze soort rechtshandelingen worden buiten beschouwing gelaten.

[40] Jean-Luc Snyers, "De elektronische authentieke akte en de notariële elektronische archivering", *Limb. Rechtsl*. 2000, 283-305.

[41] René Dekkers, *Handboek burgerlijk recht Deel II*, Bruylant Brussel 1971, nr. 656.

- de geldsommen mogen zowel met cijfers als met letters geschreven worden;
- de toevoegsels en de doorhalingen zijn aan geen bepaalde voorschriften onderworpen: ze moeten nl. niet in de rand ondertekend of geparafeerd worden;
- de tekst mag door een derde opgesteld of geschreven zijn;
- de tekst mag in een vreemde taal opgesteld zijn, ook al kent één der partijen die taal niet; enz.

52. Een akte is een in lettertekens geschreven document op een grafische drager, met uitsluiting van boodschappen vastgelegd via audio- of beeldsignalen. Een videoopname of een geluidsband waarop partijen hun rechtshandeling vastleggen, kan niet als een geschrift worden aanvaard.

Als reden hiervoor kan men niet aanvoeren dat video- of audiosignalen fraudegevoeliger zouden zijn dan geschreven lettertekens. Immers zelfs indien men de authenticiteit van een audio- of videoboodschap kan garanderen, komt het voor dat dit niet onder het begrip geschrift valt.

Het doorslaggevend argument om uit te maken of de verpakking van een boodschap al dan niet als geschrift kon worden beschouwd, was de vraag of kennis kon worden genomen van de inhoud van de boodschap zonder daarbij noodzakelijkerwijze een beroep te moeten doen op apparatuur en instrumenten om de boodschap te kunnen lezen.[42] Dit is niet het geval voor audio- en videoboodschappen waarvoor men noodzakelijk een leestoestel nodig heeft om de audio- en videosignalen om te zetten naar voor de mens begrijpelijke tekens.

53. Door de intrede van de informatietechnologie rees de vraag of een elektronisch bestand als een geschrift kon worden beschouwd. Rekening houdend met de hierboven vermelde benadering is de beslissing snel genomen: voor het omzetten van een elektronische gegevensverzameling naar voor de mens begrijpelijke tekens is tussenapparatuur volstrekt noodzakelijk: een elektronisch bestand is derhalve geen geschrift. De aarzeling om deze beslissing te nemen is nochtans veel groter dan voor audio- of videosignalen. Niet alleen ziet het ernaar uit dat de elektronische representatie de "schriftelijke" representatie in grote mate zal verdringen, daarenboven is de elektronische representatie ook meteen geschikt voor een schriftelijke uitdrukking.[43] De representatie zelf is elektronisch, maar elke kennisname van een elektronisch bestand impliceert de visualisering ervan en dit kan zowel in geschrift, in beeld, in klank, ... naar keuze.

54. Op dit domein behoort de wetgever derhalve tussen te komen. De wetgever is nochtans de weg niet opgegaan om expliciet elektronische bestanden en geschriften als bewijs toe te laten, ondanks het feit dat in een eerdere regeringsnota dit het uitgangspunt was:

> "Op de tweede plaats zou in het Burgerlijk Wetboek een functionele en technologie-onafhankelijke definitie van [het] begrip[..] "geschrift" ... opgenomen moeten worden, zodat als geschrift niet enkel een papieren document ... kan beschouwd worden. ...."
> (Nota aan de Ministerraad, Naar een juridische regeling van de digitale handtekening van Stefaan De Clerck, Minister van Justitie, en Elio Di Rupo, Vice-Premier en Minister van Economie en Telecommunicatie.)

De door de wetgever geboden oplossing is een oplossing op een onrechtstreekse wijze. De wetgever had inderdaad een elektronische verzameling van tekens kunnen gelijkstellen met een geschrift, hij deed het niet. Hetzelfde resultaat wordt bereikt door het creëren van een elektronische handtekening waardoor onrechtstreeks een elektronisch bestand als geschrift wordt erkend. Immers een elektronische handtekening kan enkel op een elektronisch bestand worden aangebracht.

De elektronische handtekening en het elektronisch bestand worden als één geheel beschouwd, wat technisch gezien in bepaalde gevallen juist kan zijn, doch conceptueel volkomen onjuist is.

55. Deze benadering van de wetgever kan misschien de eenvoudigste zijn, de beste is het zeker niet. Dat het probleem van het elektronisch bestand niet opgelost is, blijkt o.m. uit de tekst van het nieuw ingevoerde art. 2281 B.W., waar verwezen wordt naar een boodschap via telecommunicatietechnieken die kan resulteren in een schriftelijk stuk aan de zijde van de geadresseerde, zonder dat deze communicatie noodzakelijk moet resulteren in een schriftelijk stuk.

Een dergelijke omschrijving kan niets anders betekenen dan de erkenning dat een elektronisch bestand gelijkstaat met een geschrift minstens wat een kennisgeving betreft.

Het ware nochtans beter geweest dit ook meteen zo in de wet op te nemen.

§ 2. Opgemaakt tot bewijs

56. Een geschrift kan slechts dan als een schriftelijk bewijs gekwalificeerd worden indien het door partijen op-

[42] Anders Reinhard Steennot, "Juridische problemen in het kader van de elektronische handel", *T.B.H.* 1999, 664-676, nr. 39.

[43] De vermelding bij een regeringsamendement dat elektronische teksten leesbaar zijn, raakt kant noch wal (*Parl. St.* Kamer, 50-0038/6).

gesteld is met het oog op het vormen van een bewijsstuk. Immers het opstellen van een schriftelijk bewijs kan op zichzelf beschouwd worden als het verrichten van een rechtshandeling, zodat de intentie als een geldigheidsvereiste kan worden aangemerkt.

De bewijsrechtelijke functie is tweeërlei: preventief (door het op voorhand uitschrijven beogen partijen rechtszekerheid te creëren en derhalve onderling conflicten te vermijden) en repressief (in geval van betwisting voor de rechter, biedt het geschrift de zekerheid dat de rechter door de inhoud ervan gebonden is).

Dit uitgangspunt komt niet onder druk door de informatietechnologie.

§ 3. Handtekening

57. Een geschrift opgesteld als bewijs kan tenslotte enkel gelding hebben indien het geschrift werd ondertekend. Door het plaatsen van deze handtekening onderaan een akte identificeert men zich en geeft men zijn wil te kennen de tekst te aanvaarden. De aspecten eigen aan de handtekening worden hierna (nrs. 68 en volg.) afzonderlijk onderzocht.

§ 4. Betrouwbaarheid

58. Soms wordt staande gehouden dat een voldoende "betrouwbaarheid" van de akte of een geringe kans op frauduleuze wijzigingen tot het wezen van de akte behoort.[44] In sommige literatuur worden als essentiële kenmerken van een geschrift aangehaald: de onveranderlijkheid, de leesbaarheid[45] en de stabiliteit. Stuk voor stuk zijn dit waardevolle aspecten van een geschrift, zonder dat ze daarvan een essentieel onderdeel zouden zijn.

De rechtsgeldigheid van een bewijsmiddel wordt niet beïnvloed door de aard of de betrouwbaarheid van het bewijsstuk of bewijsmiddel, dit aspect vertoont wel belang voor de bewijswaarde die door de wetgever of door de rechter aan dat bewijsmiddel wordt vastgeknoopt.[46] Zo heeft een geschrift een grotere bewijswaarde dan een getuigenverklaring, een authentiek geschrift een hogere bewijswaarde dan een onderhands geschrift, ...

Wat de elektronische handtekening betreft schijnt de wetgever van dit uitgangspunt te zijn afgeweken en wordt het veiligheidsaspect geïncorporeerd in het begrip van de handtekening zelf (art. 1322 lid 2 B.W.: «... en het behoud van de integriteit van de inhoud van de akte aantoont.»)

B. Toelaatbaarheid van een bewijsmiddel

59. De toelaatbaarheid betreft de vraag of de rechter een bepaald bewijsmiddel mag toelaten met het oog op het leveren van het bewijs van een rechtshandeling. De vraag rijst in hoofdzaak ten aanzien van het bewijs van rechtshandelingen in civiele zaken ingevolge art. 1374 B.W. waarin gesteld wordt dat een rechtshandeling waarvan de waarde hoger is dan 375,-€ dient bewezen te worden aan de hand van hetzij een authentieke akte, hetzij een onderhandse akte, behoudens in zaken van koophandel (art. 25 W. Kh.).

Het niet-opstellen van een op voorhand aangemaakt bewijsmiddel (geschrift) verhoogt enkel het bewijsrisico, maar beïnvloedt niet noodzakelijk de geldigheid van de rechtshandeling of de gevolgen ervan.

60. Door het feit dat er verschillende bewijsmiddelen bestaan en dat in bepaalde gevallen slechts bepaalde bewijsmiddelen zijn toegelaten, kan het voorkomen dat een aangeboden bewijsmiddel dient gekwalificeerd te worden. Pas na de kwalificatie kan de toelaatbaarheid worden bepaald. Wanneer een persoon in een door hem ondertekend geschrift bepaalt dat hij aanwezig was en heeft vastgesteld dat twee andere personen een bepaalde overeenkomst met een bepaalde inhoud hebben gesloten, kan een dergelijk stuk niet gekwalificeerd worden als een onderhandse akte (de akte gaat niet uit van de partij op wie de rechtsgevolgen slaan) maar als een getuigenverklaring.

61. Ten aanzien van de toelaatbaarheid van de elektronische handtekening als bewijsmiddel is art. 5.2 van de Richtl. nr 1999/93 van 13 december 1999 betreffende het gemeenschappelijk kader voor de elektronische handtekening doorslaggevend. In dit artikel wordt bepaald dat elke lidstaat er in zijn wetgeving zorg moet voor dragen dat een bewijsmiddel niet ontoelaatbaar wordt verklaard enkel en alleen omdat het een elektronische handtekening bevat. Deze bepaling is thans opgenomen in art. 4 § 5 van de Wet Certificatiediensten.

Een rechter kan derhalve een elektronisch bestand, voorzien van een elektronische handtekening (zowel de fraudegevoelige als de fraudeongevoelige), niet als schriftelijk bewijs ontoelaatbaar verklaren enkel en alleen omdat de handtekening elektronisch is.

Nochtans is het niet zo dat alle vormen van elektronische handtekeningen daarom gelijk zijn gesteld met de handgeschreven handtekeningen.

[44] Etienne Davio, "Questions de certifications, signature en cryptographie", In X. *Internet face au droit*, Crid 1997: III. 3 La sécurité comme condition de validité des contracts, p. 76 en volg.

[45] Dominique Mougenot, "Droit de la preuve et technologies nouvelles: synthèse et perspectives", in X., *Droit de la preuve*, CUP 1997, nr. 28.

[46] Rogier de Corte, "Opnemen eigen telefoongesprekken verdeelt rechters", *Juristenkrant* 5 december 2000, afl. 19, 5.

C. Bewijswaarde van een bewijsmiddel

62. Het schriftelijk bewijs, zowel de onderhandse als de authentieke akte, geeft tussen partijen een afdoend bewijs (art. 1322 B.W.): de onderhandse en de authentieke akte hebben op dit punt dezelfde bewijswaarde.

De voorwaarde hiervoor is de erkenning van de handtekening. Enkel ter zake van de erkenning van de handtekening bestaat er een verschil tussen onderhandse en authentieke akten. Voor authentieke akten is de erkenning van de handtekening rechtens, voor onderhandse akten moet men in de regel erkennen of ontkennen (art. 1332 B.W.).

De bewijswaarde heeft hierop betrekking dat een rechter de inhoud van een geschrift moet aanvaarden, terwijl dit bijv. niet het geval is met de verklaring van een getuige, waar de rechter over een grotere vrijheid in beoordeling beschikt.

D. Kennisgevingen en bewijsrecht

63. De hierboven geschetste regels zijn in hoofdzaak ontworpen voor initiële of zelfstandige rechtshandelingen, zoals het sluiten van een contract of het stellen van een rechtshandeling als zelfstandige juridische gebeurtenis, zoals bijv. de erkenning van een kind. Er zijn nochtans tal van andere situaties waarin zowel binnen als buiten een contractuele verhouding eenzijdige rechtshandelingen gesteld worden. Dit is bijv. het geval bij een ingebrekestelling van een schuldenaar, een kennisgeving van niet conforme levering, enz.

In zijn algemeenheid geschieden die rechtshandelingen in de vorm van een kennisgeving gericht aan een andere persoon. Ook hier stelt zich het dubbele probleem: wanneer brengt de kennisgeving rechtsgevolgen teweeg en hoe kan men een kennisgeving bewijzen (hoe levert men het bewijs van het bewijs?).

64. Het bewijs van het bestaan van een schriftelijk bewijsstuk dat gebruikelijk via een kennisgeving geschiedt, is niet het voorwerp van een specifieke regeling. De wetgever heeft soms specifieke vormen voorgeschreven waardoor dit bewijs kan geleverd worden:

- indien een betekening gebeurt via exploot van gerechtsdeurwaarder dan wordt het bewijs geleverd door het exploot van betekening;
- indien de kennisgeving geschiedt via aangetekende brief (met ontvangstbewijs) dan wordt de kennisgeving bewezen door het voorleggen van de kopie van het geschrift, vergezeld van het bewijs van aangetekende zending (eventueel ontvangstbewijs);
- indien een kennisgeving geschiedt bij gewone brief wordt het bewijs in de regel geleverd door het voorleggen van de kopie van het verzonden exemplaar.

Kennisgevingen via fax, telex, e-mail zijn helemaal niet geregeld.

65. Deze belangrijke lacune in de wetgeving wordt opgelost door de invoering van het nieuwe artikel 2281 B.W.[47] [48], waar een aantal aanzienlijk nieuwe bepalingen zijn opgenomen:

a. indien een kennisgeving schriftelijk moet geschieden dan volstaat het dat de kennisgeving resulteert aan de kant van de geadresseerde in een schriftelijk stuk. Dit impliceert dat het origineel stuk waarin de kennisgeving vervat is niet noodzakelijk een schriftelijk stuk moet zijn, noch dat het origineel de bestemming moet bereiken om de rechtsgevolgen te initiëren.
   Het ontbreken van de handtekening op de kennisgeving leidt in beginsel niet tot de nietigheid van de kennisgeving. De geadresseerde kan wel om de toezending van het origineel verzoeken;
b. de kennisgeving brengt alle rechtsgevolgen teweeg zelfs indien de kennisgeving die bij de geadresseerde toekomt niet resulteert in een geschrift omdat de geadresseerde dit niet wenst. M.a.w. de geadresseerde behoeft zijn e-mail niet te printen om de rechtsgevolgen te doen ontstaan;
c. de kennisgeving gaat in op het ogenblik van de ontvangst van het bericht bij de geadresseerde.

E. Schriftelijke akten en derden

66. Een aspect dat door de wetgever op een afzonderlijke wijze werd geregeld is dat van de vaste datum van onderhandse akten (art. 1328 B.W.). Derden moeten de datum, vermeld op een onderhandse akte waaraan ze vreemd zijn, niet aanvaarden, tenzij de akte een vaste datum heeft (vermeld in een authentieke akte, geregistreerd of deze van het overlijden van één van de ondertekenaars). Dit recht kan enkel worden ingeroepen door derden met een concurrerend belang.

Daar de wetgever datumverschuiving wil tegengaan dient deze regel behouden te worden, enkel de wijze van vaststelling van vaste datum dient dringend geactualiseerd te worden.

Afdeling 3. Handtekening

67. De derde geldigheidsvereiste van een akte als schriftelijk bewijs is de handtekening van de partij waarvoor de rechtsgevolgen intreden. Wat de handtekening zelf betreft is de wetgever zo mogelijk nog beknopter dan voor het

[47] De zgn. wet Bourgeois van 20 oktober 2000.

[48] Rogier De Corte, "Een SMS-berichtje is geen kennisgeving", *Juristenkrant* 2001, afl. 22, 6.

begrip "geschrift". Begrip, functies, noch kenmerken werden door de wet ingericht. Het is de rechtspraak en de rechtsleer die deze leemtes invult.

A. Wat?

68. Het moet meteen duidelijk zijn dat een handtekening in het rechtsverkeer een ruimere functie heeft dan alleen het produceren van bewijsstukken. Wanneer men verzocht wordt een model van zijn handtekening te plaatsen, een presentielijst van een vergadering, de groene verzekeringskaart, zijn kredietkaart, een diploma of een contract, ... te ondertekenen zijn dit verschillende toepassingen van een handtekening. Daar de wetgever de handtekening enkel bespreekt als onderdeel van het schriftelijk bewijs gaat hij ervan uit dat een handtekening eveneens [1] een schriftelijk teken is [2] dat aangebracht is op een ander geschrift [3] door een fysiek persoon [4] om tot identificatie te dienen. Een schriftelijk teken dus naar keuze van de persoon die zich identificeert. En dit is meteen ook de kernfunctie van de handtekening m.n. (a) de identificatie en (b) authentificatie (de identificatie geschiedt immers aan de hand van een persoonlijk teken).[49]

Ook op dit vlak vat René Dekkers de situatie gevat samen[50]:

Een handtekening is een geschreven teken, waarmee een persoon zich gewoonlijk identificeert. Een min of meer willekeurig teken, door betrokkene zelf gekozen, en waaraan hij zich erkent.

De aard van het teken, de «tekening» in letterlijke zin, speelt geen rol. Maken bijv. handtekeningen uit:
- een onleesbaar teken;
- of integendeel schoonschrift;
- een handtekening met hetzelfde geschrift als de rest van de tekst, zonder versiering, zonder onderstreping;
- een teken, dat de naam weergeeft;
- het gebruik van de voornaam alleen (in familie- of vriendschapsbetrekking en);
- een handtekening met potlood, met krijt.

69. Het plaatsen van een handtekening is een handeling, in bepaalde gevallen een rechtshandeling, waarbij de betrokkene zich identificeert in een bepaalde rechtsbetrekking door een teken dat hijzelf heeft bedacht.[51]

Men kan ervan uitgaan dat een handtekening door de betrokkene moet geplaatst worden en niet via een stempel of een handtekeningmachine zijn aangebracht.

Wanneer een bepaald teken betwist wordt als zijnde een handtekening is het aan de rechter om uit te maken of een bepaald teken als een handtekening kan worden beschouwd. Zo is de rechtspraak van het Hof van Cassatie voldoende bekend met betrekking tot de handtekening op een eigenhandig geschreven testament.[52]

B. Functies van een handtekening

70. De andere functies (non-repudiatie, toe-eigening van de inhoud, behoud van de integriteit, ...) die men traditioneel aan een handtekening toeschrijft[53] zijn geen functies van de handtekening zelf, maar van het feit dat een handtekening in een bepaalde context wordt geplaatst. Ondertekent men een schriftelijk bewijs dan zal men de tekst aanvaarden die men ondertekent, ondertekent men een stuk *ne varietur* dan garandeert men de integriteit, ...

De kernfunctie van de handtekening is de identificatie en de daarbij horende authentificatie aan de hand van een persoonlijk teken.

Dit standpunt is thans wettelijk verankerd in art. 4 § 5 Wet Certificatiediensten waarin uitdrukkelijk wordt gesteld dat de rechtsgeldigheid van de handtekening niet afhangt van haar veiligheid, noch van haar vorm.

71. Indien men aanneemt dat de identificatie de kern is van de handtekening, dan geven een aantal wetteksten wel degelijk aanleiding tot bedenkingen:

a. dan kan een bepaling zoals art. 1322 lid 2 B.W. geen enkele goedkeuring wegdragen, daar het behoud van de integriteit wel een betrachting kan zijn, maar geen onderdeel van het wezen van een handtekening;
b. de kernfunctie werd precies miskend in art. 5 § 2 Wet Certificatiediensten, waar een elektronische handtekening wordt ingevoerd met een pseudoniem en waarbij de wetgever de verplichte vermelding van "pseudoniem" in het certificaat heeft weggelaten.[54] Deze bepaling is weggevallen, zodat niet kan worden nagegaan

[49] In deze zin is de handtekening inderdaad de vervanging (sinds de 16de eeuw) van het zegel door een zelf met de hand geplaatst teken.

[50] René Dekkers, *Handboek burgerlijk recht Deel II*, Bruylant Brussel 1971, nr. 654.

[51] Zo besliste het Hof van Cassatie dat het plaatsen van een kruisje, voor een persoon die niet schrijven kan, niet geldt als handtekening (Cass. 14 november 1901, *Pas*, I, 37).

[52] Mieke Coene, "Vormt de vereiste handtekening de valstrik van het eigenhandig testament", noot onder Cass.10 juni 1983, *T. Not*. 1986, 313-320.

[53] Zie hierover Bertel de Groote, "Het bewijs in de elektronische handel - enkele bedenkingen", *A.J.T.* 2000-2001, 881-901, nr. 20 en Etienne Davio, "Questions de certifications, signature en cryptographie", In X. *Internet face au droit*, Crid 1997: II. 2.1.

[54] In het eerste regeringsvoorontwerp bepaalde art. 10 «§ 1. Het certificaat bevat minstens onderstaande informatie: 1. de naam ..., of, in voorkomend geval, het pseudoniem ..., voorafgegaan door de vermelding dat het om een "pseudoniem" gaat;».

of al dan niet onder een pseudoniem is gehandeld.[55]

Men kan zich terecht de vraag stellen waarom men zich de moeite getroost om een volledig certificatiesysteem uit te werken d.w.z. het structureel leggen van een link tussen een teken en een persoon, wanneer dit mag gebeuren op basis van een pseudoniem, wanneer derden niet steeds verwittigd worden dat het om een pseudoniem gaat, noch het recht krijgen de achterliggende persoon te kennen. Hier is duidelijk de invloed van de privacy-fundi's voelbaar.

72. Verdere specifieke kenmerken van een handtekening zijn de volgende:

- een persoon kan over meerdere handtekeningen beschikken: één voor zijn briefwisseling, één voor de ondertekening van financiële documenten, één voor bedrijfsdocumenten, ...
- een persoon kan ook vrij zijn handtekening wijzigen, tenzij de wet of een overeenkomst voor bijzondere toepassingen (bijv. de notaris) een andere regeling invoert;
- een handtekening kan alleen door een fysiek persoon worden geplaatst, dit is trouwens de reden waarom men aanneemt dat een rechtspersoon geen handtekening kan plaatsen. Deze vereiste vervalt bij het plaatsen van een elektronische handtekening, zodat een elektronische handtekening rechtsgeldig kan geplaatst worden zonder tussenkomst van een fysiek persoon.

C. Technologie-onafhankelijke benadering

73. Bij het aanpassen van de wetgeving aan de eisen van de virtuele wereld werd ook hier de eerder uitgedrukte wil van de regering niet gerealiseerd:

> Op de tweede plaats zou in het Burgerlijk Wetboek een functionele en technologie-onafhankelijke definitie van [het] begrip[...]... "handtekening" opgenomen moeten worden, zodat ... handtekening niet louter een met de hand op het document geschreven handtekening kan beschouwd worden. Door het inlassen van een open en technologie-onafhankelijke definitie van [het ...] begrip[...], kan de zeer restrictieve cassatierechtspraak, vooral m.b.t. het begrip "handtekening" opengebroken worden.
>
> (Nota aan de Ministerraad, Naar een juridische regeling van de digitale handtekening van Stefaan De Clerck, Minister van Justitie, en Elio Di Rupo, Vice-Premier en Minister van Economie en Telecommunicatie.)

Uiteindelijk werd in het B.W. geen open en technologie-onafhankelijke definitie van handtekening opgenomen, zoals het oorspronkelijk de bedoeling was van de regering. Het B.W. bevatte geen omschrijving van het begrip *handtekening*, zodat de toevoeging van het lid 2 aan art. 1322 B.W. moeilijk als een functionele omschrijving kan worden beschouwd. Anderzijds is de benadering in de Wet Certificatiediensten, zelfs na vele verbeteringen, te technisch.

Een open, technologie-onafhankelijke omschrijving vereist het invoeren van een nieuwe bepaling in het B.W. waarin (a) de kernfunctie van de handtekening werd aangegeven en (b) de rechtsgevolgen van de handtekening zelf werden aangeduid. Het artikel zou moeten gaan in de richting van: "een teken, ongeacht de vorm (manueel, elektronisch of mechanisch), waardoor een persoon zich identificeert".

Ondanks herhaalde vermeldingen in parlementaire stukken dat gekozen werd voor een open en technologie-onafhankelijke omschrijving, is dit apert niet gerealiseerd. Elke functionele omschrijving ontbreekt, terwijl de Wet Certificatiediensten verstrikt zit in technologische details.

74. Zeer goed bruikbaar daarentegen is de benadering in de *Model Law on Electronic Commerce* van Uncitral van 1996[56]:

> Article 7. *Signature*
>
> (1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:
>
> (a) a method is used to identify that person and to indicate that persons approval of the information contained in the data message; and
>
> (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.
>
> (2) Paragraph (1) applies wether the requirement therein is in the form of an obligation or wether the law simply provides consequences for the absence of a signature.
>
> (3) The provisions of this article do not apply for the following ...

D. Is het elektronisch of digitaal?

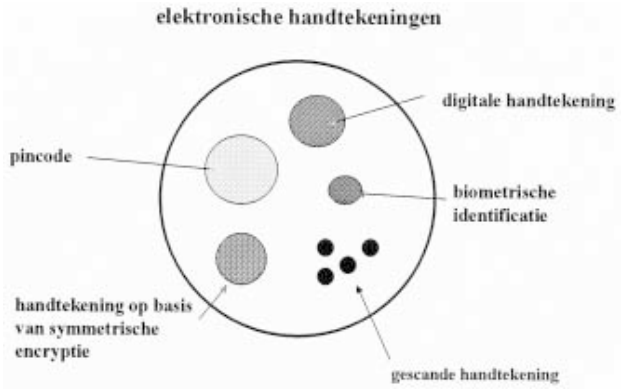
75. In de literatuur en in de oorspronkelijke wetsontwerpen wordt er soms nog een onderscheid gemaakt tussen het begrip "elektronische handtekening" en "digitale handtekening". De wetgever maakt in de actuele teksten dit onderscheid niet meer, daarenboven is dit onderscheid vanuit terminologisch standpunt onjuist, wat niet wil zeggen dat er geen verschillende vormen van elektronische handtekening zouden bestaan.

[55] De verplichte vermelding dat het om een pseudoniem gaat moet enkel in geval van een gekwalificeerd certificaat worden vermeld (Bijlage I, c).

[56] X., UNCITRAL, *Model Law on Electronic Commerce with Guide to Enactement, United Nations, 1996*, New York 1997, 72 p.

76. Elektronisch noemde men alle handtekeningen die op één of andere wijze "gecomputeriseerd" waren. Het betreft elke elektronische gegevensverzameling met de bedoeling iemand te identificeren: pincode, biometrische identificatie, een elektronische handtekening op basis van encryptie, zowel symmetrische als asymmetrische encryptie, een gescande handtekening, … kortom een generieke verzamelnaam.

Een digitale handtekening, één species van de elektronische vormen, is deze die gebaseerd is op asymmetrische encryptie, d.w.z. op basis van het gebruik van een sleutelpaar: een private en een publieke sleutel. Deze handtekening is in vergelijking met de andere elektronische handtekeningen fraude-bestendig.



77. Zuiver terminologisch is het onderscheid ook onjuist. Het begrip *digitaal* heeft betrekking op de aard van de gebruikte signalen: analoge of digitale signalen. Analoge signalen zijn signalen met een groot bereik (bijv. van zwart over alle grijstinten naar wit), digitale signalen kennen slechts twee waarden (voorgesteld door 0 of 1). Computers werken in de regel met digitale signalen.

Het begrip *elektronisch* wijst op de wijze van verwerking: een verwerking kan mechanisch zijn, pneumatisch, hydraulisch, elektronisch, ... Een elektronische verwerking geschiedt via elektronische schakelingen. Computersystemen werken elektronisch.

Deze begrippen hebben inhoudelijk geen onderscheidend vermogen wat de handtekening betreft en de wetgever gebruikt ze niet meer, zodat dit onderscheid naar de geschiedenis kan verwezen worden. Thans zijn het synoniemen.

78. Het onderscheid dat thans gemaakt wordt is drieërlei:

[1] een geavanceerde elektronische handtekening op basis van een gekwalificeerd certificaat;

[2] een geavanceerde elektronische handtekening zonder een gekwalificeerd certificaat

[3] [gewone] elektronische handtekening;

Het vertoont eerder een piramidale opbouw:

Hoofdstuk III. Elektronisch bericht – Elektronische handtekening – Encryptie

79. Er zijn tientallen soorten elektronische berichten. Hierna wordt één voorbeeld uitgewerkt m.n. een e-mailbericht. Een e-mailbericht is een kort tekstbestand dat een afzender verzendt via het internet naar een bestemmeling.

De afzender moet vanzelfsprekend beschikken over de nodige hard- en software voor het opmaken én verzenden van e-mails. De bestemmeling moet beschikken over een e-mailadres en eveneens de nodige hard- en software om de e-mailberichten te ontvangen en te kunnen lezen.

Nadat de afzender een bericht verstuurde komt dit bericht na enkele ogenblikken toe bij de provider van de bestemmeling, d.i. de postmeester van de bestemmeling. De bestemmeling kan bij zijn postmeester ten alle tijde zijn berichten opvragen en lezen. Een internetinstallatie kan ook zo opgesteld worden dat de bestemmeling verwittigd wordt wanneer een bericht toekomt.

1. Gewoon bericht

80. Wanneer een bepaalde persoon, *Afzender*, een bericht of een boodschap (*B*) wenst te verzenden aan *Bestemmeling*, wordt bijv. volgend bericht klaargemaakt en via e-mail verzonden.

from:	*Afzender*
to:	*Bestemmeling*
date:	10 juli 2001
subject:	aanpassing factuur nr 10.830

Geachte heer *Bestemmeling*,

Ik ontving zopas uw factuur nr. 10.830 van 17 mei 2001 m.b.t. de levering van 27 autobanden. De factuur vermeldt onterecht 270 autobanden. Kunt u zo snel mogelijk de kredietnota overmaken voor het verschil.

Hoogachtend,
Afzender

Wanneer *Afzender* dit bericht via e-mail over het internet verstuurt aan *Bestemmeling*, heeft *Bestemmeling* [a] geen zekerheid dat *Afzender* het bericht heeft verstuurd en [b] dat indien het bericht van *Afzender* komt het niet werd gewijzigd door onbevoegden. Daarenboven [c] kan in de regel iedereen dit bericht lezen.

Het plaatsen van een elektronische handtekening komt tegemoet aan de onzekerheden sub [a] en [b]. Encryptie, versleuteling of onleesbaar maken, komt tegemoet aan de onzekerheid sub [c].

2. Elektronische handtekening

81. Het plaatsen van een elektronische handtekening geschiedt door aan het bericht *B* een bestand toe te voegen (✍). Het verzonden bericht bestaat derhalve uit twee componenten: het bericht *B* zelf, aangevuld met het bestand ✍. Dit laatste bestand geldt als elektronische handtekening. Beide componenten of bestanden vormen één document dat via internet wordt verzonden.

from:	*Afzender*
to:	*Bestemmeling*
date:	10 juli 2001
subject:	aanpassing factuur nr 10.830

Geachte heer *Bestemmeling*,

Ik ontving zopas uw factuur nr. 10.830 van 17 mei 2001 m.b.t. de levering van 27 autobanden. De factuur vermeldt onterecht 270 autobanden. Kunt u zo snel mogelijk de kredietnota overmaken voor het verschil.

Hoogachtend,
Afzender

82. De elektronische handtekening (✍) op zichzelf bestaat op zijn beurt uit een combinatie van twee handelingen [1] het maken van een *hash* van het bericht *B* en [2] het versleutelen van dit *hash*-bestand. Het resultaat van deze twee activiteiten noemt men een elektronische handtekening en deze biedt de garantie dat het bericht wel degelijk van de afzender komt en tijdens zijn reis niet werd gewijzigd.

[1] De hash van het bericht *B* is een klein controlebestand in de vorm van een cijfer code die bekomen wordt door een wiskundig irreversibel algoritme toe te passen op het bericht *B* zelf. Dit *hash*-bestand (een cijfercombinatie) laat toe vast te stellen of het bericht al dan niet werd gewijzigd.

[2] Na de aanmaak van het *hash*-bestand wordt dit *hash*-bestand bewerkt door de afzender met zijn private sleutel om te vermijden dat het *hash*-bestand op zijn beurt zou worden gewijzigd.[57]

Eenmaal bewerkt vormt dit *hash*-bestand de eigenlijke elektronische handtekening.

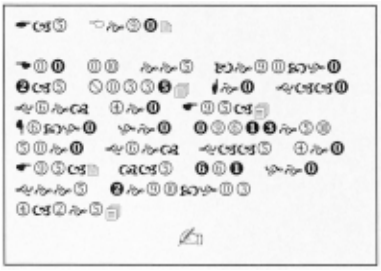
bericht *B*	**leesbare mededeling in eenvoudig tekst formaat**
✍	***hash* van bericht *B* laat integriteitscontrole toe** ✚ bewerking *hash*-bestand met private key van afzender laat identificatie toe

83. Een elektronische handtekening is derhalve sterk verschillend van een handgeschreven handtekening: het is een bestand dat toegevoegd wordt aan het bericht *B* dat moet worden ondertekend en is voor elk document wezenlijk verschillend[58] omdat het een cijfercode bevat die een afgeleide is van het bericht *B*.

84. Het aldus verstuurde bericht komt in leesbaar formaat toe bij *Bestemmeling* die het toegevoegde bestandje (✍) controleert door gebruik van de publieke sleutel van *Afzender*[59] en zo twee zaken kan vaststellen: [1] het bericht werd niet gewijzigd (*hash*-techniek) en [2] het bericht werd verzonden door de houder van de private sleutel.

3. Versleuteling

85. Wil *Afzender* het bericht onleesbaar maken voor derden, d.w.z. onleesbaar voor alle personen behalve *Bestemmeling*, dan moet hij het bericht dat voorzien is van zijn elektronische handtekening, encrypteren of versleutelen met de publieke sleutel van *Bestemmeling*.



Dit bericht kan door niemand worden ontcijferd, behalve door *Bestemmeling* door middel van zijn private key.

[57] Deze bewerking geschiedt met de *private key* van de afzender. Art. 2, 6° Wet Certificatiediensten noemt dit de gegevens voor het aanmaken van een handtekening. Verder geregeld in art. 7 § 1 en Bijlage III.

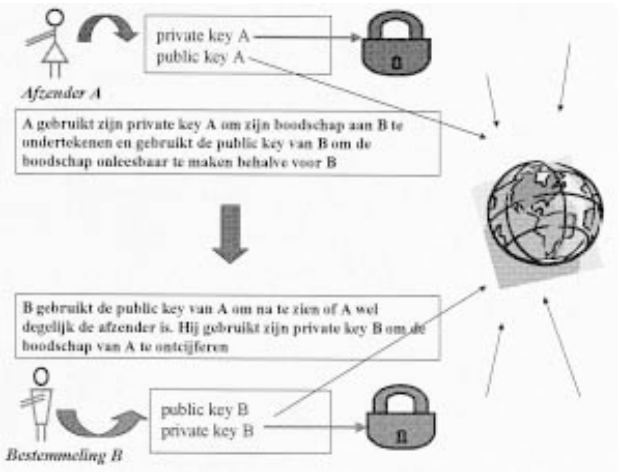
[58] Terwijl voor een handgeschreven handtekening het om hetzelfde teken gaat ongeacht op welk document het geplaatst wordt.

[59] In art. 2, 8° Wet Certificatiediensten wordt dit aangeduid als gegevens voor verificatie.

86. De versleuteling is in beginsel vrij.[60]

87. Voor de hierboven omschreven vorm van versleuteling wordt gebruik gemaakt van de asymmetrische encryptie[61], dit betekent het gebruik van een sleutelpaar: twee sleutels die bij elkaar horen: een publieke sleutel (*public key*) die voor iedereen toegankelijk is en de privé sleutel (*private key*) waarvan de partij, die het sleutelpaar maakte, de bewaring heeft en voor niemand, behalve voor hem, toegankelijk is.

Het systeem is zeer eenvoudig: een bericht, versleuteld met de *public key* van *Bestemmeling* kan alleen door *Bestemmeling* gelezen worden. Hij ontsleutelt dit bericht via zijn *private key*. In het gegeven voorbeeld heeft *Afzender* de *public key* van *Bestemmeling* opgespoord en hiermee de boodschap *B* versleuteld. Het bericht komt bij *Bestemmeling* toe en wordt door hem gelezen nadat het ontsleuteld is via zijn *private key*, waar hij als enige toegang toe heeft.



4. Certificatie

88. Het hierboven geschetste verhaal is nog niet af. Op welke wijze kan *Afzender* de zekerheid hebben dat de zgn. *public key* van *Bestemmeling*, effectief van *Bestemmeling* is en geen vervalsing? In de hypothese dat *Afzender Bestemmeling* niet kent, en dit is meestal het geval op internet, vormt dit een ernstig veiligheidsprobleem. Trouwens hoe kan *Afzender* een *public key* van *Bestemmeling* vinden?

Hier treedt de certificatiedienstverlener in beeld of ook wel *trusted third party* (TTP) genoemd: het is de persoon of instelling die het verband garandeert tussen de sleutel en de houder van de sleutel. Dit gebeurt door het ter beschikking stellen van een certificaat.

Hoofdstuk IV.
De elektronische handtekening

89. Hierna wordt zeer kort, op basis van de wet 9 juli 2001 op het juridisch kader voor elektronische handtekeningen en certificatiediensten, aandacht besteed aan drie aspecten: de voornaamste begrippen over handtekening, wie kan houder zijn van een elektronische handtekening en het juridisch statuut van de elektronische handtekening.

90. De *summa divisio* in de soorten handtekeningen is thans de "*handgeschreven handtekening*" en de "*digitale of elektronische handtekening*". Om volledig te zijn moet hieraan nog de "*mechanisch geplaatste handtekening*" worden toegevoegd. [1] De handgeschreven handtekening werd hierboven reeds toegelicht. Het is een door een fysiek persoon bedacht en geplaatst teken ter identificatie. [2] Wordt deze handtekening niet door de fysieke persoon zelf aangebracht, maar mechanisch (bijv. door een handtekeningtoestel, door een printer[62] of plotter, ...) dan kan men spreken van een mechanisch geplaatste handtekening.[63] [3] De digitale of elektronische handtekening, in tegenstelling tot een analoge handtekening zoals een handgeschreven handtekening, heeft betrekking op een identificatiehandeling door het gebruik van een elektronische gegevensverzameling.

[60] Telecomwet 21 maart 1991 - art. 109*ter*F. «Het gebruik van versleuteling is vrij.
De terbeschikkingstelling aan het publiek van versleutelingsdiensten aangewezen door de Koning is onderworpen aan een voorafgaande aangifte aan het Instituut. Deze aangifte moet per aangetekende brief gebeuren uiterlijk vier weken vóór de aanvang van de activiteiten.»

[61] Het tegenovergestelde is symmetrische encryptie. Dit is het onleesbaar maken van de boodschap aan de hand van een sleutel, die dan opnieuw dient gebruikt te worden om te ontsleutelen. Sleutel en boodschap vormen een onlosmakelijk geheel. Bij asymmetrische encryptie wordt gewerkt met twee verschillende sleutels, een sleutelpaar dus: een publieke sleutel om de gegevens te coderen en een private om ze weer te decoderen. De private sleutel moet geheim blijven. De publieke sleutel mag verspreid worden op het internet, met de publieke sleutel alleen kan men immers niets anders doen dan versleutelen. Iedereen mag je publieke sleutel kennen, maar jij bent de enige die de private sleutel bezit.

[62] Wanneer een persoon zijn handtekening scant, zodat het via zijn tekstverwerking afgedrukt wordt op de door hem verzonden brieven, gaat het over een mechanisch geplaatste handtekening.

[63] Deze frequent voorkomende vorm van handtekening wordt niet vermeld noch geregeld. Derden die documenten ontvangen met een dergelijke handtekening zullen zich kunnen baseren op de vertrouwensleer om deze vorm van handtekening tegen de titularis in te roepen.

91. Een elektronische handtekening is derhalve een handtekening die op elektronische wijze is geplaatst op een elektronisch document. In de loop van de overigens vrij recente geschiedenis werden zeer veel begrippen en onderscheiden gelanceerd. Thans maakt het wetsontwerp als belangrijkste onderscheid "de geavanceerde elektronische handtekening" en de niet-geavanceerde elektronische handtekening, hierna genoemd "[gewone] elektronische handtekening".

Afdeling 1. Gewone en geavanceerde elektronische handtekening

92. Waar voorheen het onderscheid werd gemaakt tussen de elektronische handtekening en de digitale handtekening, wordt nu een onderscheid gemaakt tussen de [gewone] elektronische handtekening en de geavanceerde elektronische handtekening. Het onderscheid is van technische aard: de geavanceerde handtekening is gebaseerd op de techniek van de asymmetrische encryptie en wordt als veel fraude-ongevoeliger ervaren dan elke andere vorm van elektronische handtekening en de tussenkomst van een certificatiedienst is noodzakelijk.

A. De [gewone] elektronische handtekening

93. Het meest ruime begrip is de [gewone] elektronische handtekening en deze handtekening wordt op twee plaatsen op verschillende wijze gedefinieerd:

> *Art. 1322 B.W.:* « ... een geheel van elektronische gegevens dat aan een bepaalde persoon kan worden toegerekend en het behoud van de integriteit van de inhoud van de akte aantoont.».
>
> *Wet Certificatiediensten, art. 2, 1°* «elektronische handtekening»: gegevens in elektronische vorm, vastgehecht aan of logisch geassocieerd met andere elektronische gegevens, die worden gebruikt als middel voor authentificatie;

Hoewel de omschrijving in art. 1322 B.W. verschilt van deze in art. 2, 1° van de Wet Certificatiediensten dekken beide omschrijvingen dezelfde lading: het is een noodzakelijke maar voldoende vereiste voor een elektronische handtekening:

a. dat het gaat om een verzameling van "elektronische gegevens"[64];
b. met de bedoeling een handtekening te plaatsen.

Deze nieuwe omschrijving omvat dan zowel een gescande handtekening, een pincode, een biometrische identificatie als een handtekening bekomen door symmetrische of asymmetrische encryptietechnieken.

Het verschil in formulering tussen art. 1322 B.W. en art. 2, 1° Wet Certificatiediensten lijkt geen rechtsgevolgen teweeg te brengen. De essentie van het begrip "handtekening" werd in beide definities vergeten met name de identificatie. De vermelding van de integriteit in art. 1322 B.W. kan er voor lief worden bijgenomen, omdat deze bepaling voorkomt onder de hoofding Schriftelijk Bewijs in het B.W., en het behoud van de integriteit er een waardevol, doch niet onmisbaar onderdeel van is. De vermelding van de authentificatie in art. 2, 1 Wet Certificatiediensten lijkt eerder een ongelukkige vertaling te zijn van de identificatievereiste.

B. Een eenvoudig geavanceerde elektronische handtekening

94. Het begrip "geavanceerde elektronische handtekening" wordt omschreven in art. 2, 2° van de Wet Certificatiediensten. Het is de [gewone] elektronische handtekening, maar met bijzondere waarborgen:

> Art. 2, 2° «geavanceerde elektronische handtekening»: elektronische gegevens vastgehecht aan of logisch geassocieerd met andere elektronische gegevens, die worden gebruikt als middel voor authentificatie en aan de volgende eisen voldoen :
> *a)* zij is op unieke wijze aan de ondertekenaar verbonden;
> *b)* zij maakt het mogelijk de ondertekenaar te identificeren;
> *c)* zij wordt aangemaakt met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
> *d)* zij is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke latere wijziging van de gegevens kan worden opgespoord.

Het verschil tussen geavanceerde en een [gewone] elektronische handtekening ligt in hoofdzaak op het gebied van de kwaliteit van de elektronische handtekening. Voor een geavanceerde elektronische handtekening worden een aantal kwaliteitsvereisten gesteld die niet gevraagd worden aan de andere elektronische handtekening:

- de unieke band tussen teken en ondertekenaar (voorwaarde *a)*);
- de middelen voor aanmaak van de handtekening (dit is de *private key*) moeten onder de uitsluitende controle van de ondertekenaar kunnen gehouden worden (voor waarde *c)*);
- de opsporing van latere wijzigen moet mogelijk zijn (gebruik van *hash*-code) (voorwaarde *d)*).

De vereisten voor het plaatsen van een gekwalificeerde elektronische handtekening kunnen op dit ogenblik enkel gerealiseerd worden via de techniek van de asymmetrische encryptie, zoals in het vorige Hoofdstuk werd toegelicht.

[64] De uitprint van een gescande handtekening via de tekstverwerker onderaan een brief beantwoordt derhalve niet aan deze omschrijving, omdat de handtekening niet bestaat uit elektronische gegevens, doch enkel uit een fysieke weergave ervan.

C. Een geavanceerde elektronische handtekening op basis van een gekwalificeerd certificaat

95. Daar het begrip geavanceerde elektronische handtekening hoofdzakelijk betrekking heeft op de technische aanmaakaspecten van de handtekening, met name het gebruik maken van de asymmetrische encryptietechnieken, maakt de wetgever in deze categorie nog een onderscheid naar gelang de aard van het erbij horende certificaat, d.w.z. de identificatie en de authentificatie.

De wetgever stelt een geavanceerde elektronische handtekening enkel gelijk met een handgeschreven handtekening indien de geavanceerde elektronische handtekening gerealiseerd werd op basis van een gekwalificeerd certificaat. Dit betekent dat het certificaat een aantal vermeldingen zal moeten bevatten.

Afdeling 2. Houder van een elektronische handtekening

96. De houder van een elektronische handtekening kan zowel een *fysiek persoon* als een *rechtspersoon* zijn. Niet alleen uit de logica van de tekst, maar ook uit het expliciet weglaten van deze mogelijkheid[65], kan men afleiden dat een feitelijke vereniging zonder rechtspersoonlijkheid geen titularis kan zijn van een elektronische handtekening.

97. Het toekennen van een elektronische handtekening aan *rechtspersonen* kan volgens sommigen de leer van de orgaantheorie voor de rechtspersoon in het gedrang brengen. Art. 3 Wet Certificatiediensten stelt enkel dat deze regeling de bevoegdheid voor het stellen van rechtshandelingen in het vennootschapsrecht niet wijzigt, terwijl art. 8 § 3 de specifieke verplichtingen oplegt in hoofde van de certificatiedienst, met name het bijhouden van de identiteit van de natuurlijke persoon die de rechtspersoon vertegenwoordigt en de handtekening gebruikt.

98. Bijzonder merkwaardig is art. 5 § 2 Wet Certificatiediensten met betrekking tot het gebruik van een *pseudoniem*, dat zowel door een fysiek als door een rechtspersoon zou kunnen gebruikt worden.

> Art. 5. «§ 1. ...
> § 2. Wanneer de houder van het certificaat een pseudoniem gebruikt en wanneer het onderzoek dit vereist, is de certificatiedienstverlener die het certificaat heeft afgegeven ertoe gehouden alle gegevens betreffende de identiteit van de titularis mee te delen in de omstandigheden en volgens de voorwaarden waarin de artikelen 90*ter* tot 90*decies* van het Wetboek van Strafvordering voorzien.»

Het gebruik van pseudoniemen kan inderdaad in een aantal gevallen in het sociaal verkeer een meerwaarde betekenen. Het is immers de uiting van een wens om naamloos op te treden. Art. 5 § 2 Wet Certificatiediensten heeft deze naamloosheid nochtans omgebogen tot een geval van relatieve anonimiteit. Ten aanzien van deze wetsbepaling dringen zich toch twee bedenkingen op:

- het valt te betreuren dat de wetgever de verplichting de vermelding aan te brengen dat het om een pseudoniem gaat, niet meer in de tekst van de wet zelf heeft opgenomen.[66] Het kan derhalve denkbaar zijn dat een deelnemer aan een virtuele communicatie (al dan niet met juridische implicaties) enkel te doen heeft met iemand die zich van een pseudoniem bedient, zonder dat hij hiervan op de hoogte wordt gesteld. Men kan zich hierbij de vraag stellen of de certificatiediensten, zelfs zonder deze wettelijke verplichting, aansprakelijk kunnen gesteld worden indien derden schade zouden lijden door het feit dat hen de kennis onthouden werd dat het om een pseudoniem ging;
- het laatste gedeelte van deze bepaling is volkomen onbegrijpelijk met name dat het vrijgeven van de identiteit door de certificatiedienst enkel mag geschieden onder dezelfde voorwaarden als een gerechtelijke telefoonaftap. Hierdoor wordt de identificatie van personen volledig naar de strafrechtelijke sfeer overgebracht. Blijkbaar heeft men enkel gedacht aan of was men nog steeds gebiologeerd door kinderporno. Identificatie is enkel mogelijk voor de misdrijven in die artikelen opgenomen. Onrechtmatige daden die niet onder het strafrecht vallen mogen blijkbaar ....

99. Tenslotte wordt algemeen aanvaard dat elke fysieke persoon en elke rechtspersoon over meerdere elektronische handtekeningen kan beschikken, zowel bij dezelfde als bij verschillende certificatieautoriteiten. Waar men zich in de fysieke wereld van meerdere handtekeningen kan bedienen, kan men dit ook in de virtuele wereld.

Afdeling 3. Juridisch statuut van een elektronische handtekening

100. De omschrijving van de juridische waarde van een elektronische handtekening is in wezen de kern van de

[65] In het oorspronkelijk regeringsontwerp luidde art. 2, 4° als volgt: «certificatiehouder: een natuurlijke, een privaat- of publiekrechtelijke rechtspersoon, een overheidsbestuur of een feitelijke vereniging aan wie een certificatie-autoriteit een certificaat heeft afgeleverd;».

[66] In het oorspronkelijk regeringsontwerp was de verplichting voor de certificatie-autoriteit ingeschreven dat in geval van gebruik van een pseudoniem, die uitdrukkelijk moest worden vermeld. Thans is deze verplichting enkel in de Bijlage opgenomen.

nieuwe wetgeving. Bij nader inzien is dit helaas het zwakke punt van de nieuwe regeling.

De juridische situatie van de handgeschreven handtekening kan als volgt worden samengevat:

a. een handtekening geplaatst op een authentieke akte, waarvoor de openbare ambtenaar de bevoegdheid had de handtekening te ontvangen, geniet een volstrekte erkenning. Enkel een betichting wegens valsheid in geschrifte kan dit "volledig bewijs" ongedaan maken;
b. voor alle andere handtekeningen [1] moet de rechter een teken als handtekening erkennen indien dit wordt betwist (de eventuele vraag naar de geldigheid van de handtekening zelf) en [2] moet de persoon die de handtekening heeft geplaatst zijn handtekening formeel erkennen of ontkennen. In het eerste geval is er "volledig bewijs", in het tweede geval start een gerechtelijk onderzoek naar de echtheid van de handtekening.

De inpassing van de elektronische handtekening in dit kader bleek voor de wetgever geen evidentie. Zo toont de Memorie van Toelichting bij art. 4 § 4 Wet Certificatiediensten in hoge mate de verwarring die er heerste[67]:

> Paragraaf 4 wil een verband leggen tussen, enerzijds, de hervorming van de regels over het bewijs zoals bepaald in het Burgerlijk Wetboek, meer bepaald de invoering van de open en functionele definitie van het begrip handtekening en, anderzijds, deze wet. Immers, elke geavanceerde elektronische handtekening gecombineerd met een gekwalificeerd certificaat — en dus afgegeven door een geaccrediteerde certificatiedienstverlener en aangemaakt door een veilig middel voor het aanmaken van een handtekening — is een handtekening in de zin van artikel 1322,2 e lid van het Burgerlijk Wetboek en voldoet dus aan de diverse eisen die aan een handtekening worden gesteld, zelfs indien een rechter zich over deze laatste niet kan uitspreken. Er kan worden gesteld dat de beveiliging die voor de certificatiedienstverleners is opgezet de geavanceerde elektronische handtekening een veiligheids- en betrouwbaarheidsgraad verschaft die minstens gelijk is aan die van een handgeschreven handtekening.
>
> In dit stadium moet worden onderstreept dat een certificaat met de bij artikel 12 bepaalde inhoud (bijlage I bij het voorstel van richtlijn), behoudens artikel 12, 1°, kan worden afgegeven zowel door een geaccrediteerd certificatiedienstverlener als door een niet-geaccrediteerd certificatiedienstverlener die evenwel zou beweren dat hij voldoet aan de accreditatievoorwaarden (zie bijlage II van het ontwerp van richtlijn) zonder daar voor een aanvraag te hebben ingediend. Wel blijft er een fundamenteel verschil bestaan tussen die twee hypotheses omdat enkel een elektronische handtekening die steunt op een certificaat waarvan de inhoud overeenstemt met artikel 12 en dat is afgegeven door een geaccrediteerd certificatiedienstverlener automatisch zal worden gelijkgeschakeld met een handgeschreven handtekening zoals bepaald bij artikel 4 § 4, en zulks door de uiterst beveiligde omstandigheden die gepaard gaan met de aanmaak ervan. Dat wil niet zeggen dat een elektronische handtekening die steunt op een certificaat waarvan de inhoud beantwoordt aan artikel 12 en die is afgegeven door een niet-geaccrediteerde certificatiedienstverlener maar die desondanks toch voldoet aan de eisen in verband met de accreditatie (zie bijlage II van het ontwerp van richtlijn) geen enkele juridische erkenning zou genieten (in dit geval wat de ontvankelijkheid betreft). Ze wordt echter niet automatisch gelijkgeschakeld met een handgeschreven handtekening, maar er wordt verondersteld dat daadwerkelijk is bewezen dat aan de voorwaarden is voldaan. Die verschillende behandeling is te verklaren door praktische en veiligheidsoverwegingen. De geaccrediteerde certificatiedienstverleners worden voortdurend door het Bestuur gecontroleerd en verrichten hun werk in optimale betrouwbaarheids- en veiligheidsomstandigheden. Een dienstverlener die zich beroept op een certificaat afgegeven door een geaccrediteerd certificatiedienstverlener kan dus worden vrijgesteld van de verplichting om het bewijs van zijn kwaliteit te leveren. Dat geldt niet als het certificaat werd afgegeven door een dienstverlener die zich niet heeft willen onderwerpen aan de controle die gepaard gaat met de accreditatie. In dat geval wordt door niemand meer geverifieerd noch geattesteerd dat aan de eisen in verband met het afgeven van certificaten is voldaan. Om de rechter hiervan eventueel te overtuigen, moet daarvan dus het bewijs worden geleverd.
>
> Meer algemeen moet voorts worden vermeld dat, ook al komt een «gewone» elektronische handtekening die niet voldoet aan de eisen van artikel 4 § 4 niet in aanmerking voor de assimilatieclausule, zij toch niet kan worden verworpen louter en alleen omdat zij een elektronische vorm aanneemt, of omdat zij niet gebaseerd is op een gekwalificeerd certificaat afgegeven door een geaccrediteerde certificatiedienstverlener, of nog omdat zij niet is aangemaakt door een veilig middel voor het aanmaken van een handtekening. Elke elektronische handtekening is dus ontvankelijk in geval van betwisting. Om evenwel te voldoen aan de eisen van artikel 4 § 4 moet de persoon die zich beroept op een elektronisch ondertekend document de rechter

[67] Wetsontwerp 16 december 1999 betreffende de werking van de certificatiedienstverleners met het oog op het gebruik van elektronische handtekeningen, *Parl. St.*, Kamer 50-0322/001, p. 14.

overtuigen van de bewijskracht ervan. Er bestaat een parallellisme met het begrip «begin van bewijs door geschrift», waarvan sprake is in artikel 1347 van het Burgerlijk Wetboek.
Het geschrift bedoeld in artikel 1347 voldoet niet aan de vereisten om te worden beschouwd als een bewijsstuk in de zin van artikel 1341 van het Burgerlijk Wetboek, doch beantwoordt aan sommige specifieke kenmerken inzake vorm, oorsprong en inhoud. Hiervoor verwijzen wij naar de overvloedige rechtsleer terzake.

101. Uiteindelijk zijn bij de invoering van de bepalingen betreffende de elektronische handtekening de bestaande regels overeind gebleven en heeft de wetgever 3 nieuwe regels aan het bestaande arsenaal toegevoegd: [1] het non-discriminatiebeginsel, [2] het assimilatiebeginsel en [3] een bijzondere regeling voor de openbare sector. Deze toegevoegde regels hebben enkel werking voor de elektronische handtekening.

A. Het non-discriminatiebeginsel

102. Het invoeren van het non-discriminatiebeginsel van een elektronische handtekening met een handgeschreven handtekening is een verplichting die voortvloeit uit art. 5.2 van de Richtl. nr. 1999/93 van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen:

Artikel 5. Rechtsgevolgen van elektronische handtekeningen
1. ....
2. De lidstaten zorgen ervoor dat een elektronische handtekening geen rechtsgeldigheid wordt ontzegd en dat zij niet als bewijsmiddel in gerechtelijke procedures kan worden geweigerd louter op grond van het feit dat:
– de handtekening in elektronische vorm is gesteld, of
– niet is gebaseerd op een gekwalificeerd certificaat, of
– niet is gebaseerd op een door een geaccrediteerd certificatiedienstverlener afgegeven certificaat, of
– zij niet met een veilig middel is aangemaakt.

Deze bepaling is letterlijk overgenomen in art. 4 § 5 Wet Certificatiediensten, zodat de inwerking van deze bepaling in het Belgisch recht niet meer tot betwisting aanleiding kan geven.

103. De draagwijdte van deze bepaling is dubbel en uitermate belangrijk: het heeft betrekking op de toelaatbaarheid (ontvankelijkheid) van het bewijsmiddel en het regelt de geldigheid van de (elektronische) handtekening.

§ 1. Ontvankelijkheid van de elektronische handtekening

104. Art. 1341 B.W. bepaalt dat het bewijs van een rechtshandeling in civiele zaken met een waarde boven 375,- € enkel mag geleverd worden aan de hand van een authentieke of een onderhandse akte. Krachtens deze bepaling zijn alle andere bewijsmiddelen niet toelaatbaar. De rechter mag geen andere bewijsmiddelen toelaten.

Art. 4 § 5 Wet Certificatiediensten verhindert dat de rechter een elektronisch bestand, voorzien van een elektronische handtekening, als niet toelaatbaar zou afwijzen als bewijsmiddel voor civiele rechtshandelingen omdat het geschrift en de handtekening in elektronische vorm zijn.[68]

§ 2. Geldigheid van de elektronische handtekening

105. Art. 4 § 5 Wet Certificatiediensten bepaalt eveneens dat de rechtsgeldigheid van een elektronische handtekening niet mag afhankelijk gemaakt worden van een aantal kwaliteitsvoorwaarden van die handtekening, zoals het beroep doen op een certificatiedienst, het gebruik van veilige middelen, ...

Positief betekent dit dat een elektronische handtekening rechtsgeldig is enkel op basis van het voorhanden zijn van de kenmerken: identificatie en authentificatie.

106. Tenslotte moet de vraag gesteld worden of in gevolge de aanvaarding van de tekst van art. 4 § 5 Wet Certificatiediensten (letterlijke overname van de non-discriminatie van art. 5.2 Richtl.) art. 1322 lid 2 van het B.W. nog enige zin of functie heeft. Het antwoord kan enkel ontkennend luiden. De functie van deze bepaling was precies de non-discriminatie in te voeren. Art. 4 § 5 doet dit alleen duidelijker en volledig.

B. Het assimilatiebeginsel

107. Naast de regeling van de toelaatbaarheid en de geldigheid als bewijsmiddel (non-discriminatie) moesten de rechtsgevolgen worden geregeld. Ook hier waren twee mogelijkheden: een eigen rechtsstelsel voor de elektronische handtekening ontwikkelen of de elektronische handtekening wat de rechtsgevolgen betreft, volledig assimileren met de handgeschreven handtekening.

De wetgever heeft in art. 4 § 4 Wet Certificatiediensten gekozen voor het assimilatiebeginsel.

[68] Positief houdt deze bepaling in dat een elektronisch bestand gelijk wordt gesteld met een geschrift en een elektronische handtekening met een handgeschreven handtekening.

108. De oorspronkelijk door de Kamer aangenomen tekst luidde als volgt:

Art. 4. § 1 - § 3

§ 4. Onverminderd de artikelen 1323 en volgende van het Burgerlijk Wetboek voldoet een geavanceerde elektronische handtekening, gerealiseerd op basis van een gekwalificeerd certificaat en aangemaakt door een veilig middel voor het aanmaken van een handtekening, aan de vereisten van artikel 1322, tweede lid[69], van het Burgerlijk Wetboek, ongeacht of deze handtekening gerealiseerd wordt door een natuurlijke dan wel door een rechtspersoon.

Deze bepaling gaf aanleiding tot heel wat kritiek wegens onduidelijkheid. Het kwam erop neer dat de wetgever bepaalde dat een geavanceerde handtekening op basis van een gekwalificeerd certificaat, «kon» gelijkgesteld worden met een handgeschreven handtekening. Duidelijkheid is inderdaad iets anders.

Ingevolge amendering door de Senaat werd de tekst als volgt gewijzigd en luidt nu:

Art. 4. § 1 - § 3

§ 4. Onverminderd de artikelen 1323 en volgende van het Burgerlijk Wetboek wordt een geavanceerde elektronische handtekening, gerealiseerd op basis van een gekwalificeerd certificaat en aangemaakt door een veilig middel voor het aanmaken van een handtekening, geassimileerd met een handgeschreven handtekening ongeacht of deze handtekening gerealiseerd wordt door een natuurlijke dan wel door een rechtspersoon.

109. Door deze wijziging werd *in extremis* meer duidelijkheid gecreëerd: de geavanceerde elektronische handtekening gerealiseerd op basis van een gekwalificeerd certificaat *wordt volledig geassimileerd* met een handgeschreven handtekening.

De assimilatie geldt enkel voor:

- de geavanceerde elektronische handtekening, d.w.z. een handtekening op basis van de asymmetrische encryptie. Deze assimilatie geldt dus niet voor een gescande handtekening, voor biometrische identificatie, enz. zonder dat de rechter echter deze laatste handtekeningen als zodanig niet-toelaatbaar of niet-rechtsgeldig zou mogen verklaren (non-discriminatie);
- daarenboven moet de handtekening gerealiseerd zijn op basis van een gekwalificeerd certificaat. De tussenkomst van een certificaatdienstverlener is derhalve vereist.[70]

110. Belangrijk is nochtans vast te stellen dat er een sterk verschil bestaat tussen deze assimilatie en de bepaling die in het eerste regeringsontwerp voorkwam, waar een dergelijke handtekening werd geacht, behoudens tegenbewijs, te zijn uitgegaan van de houder van het certificaat.

In het huidige art. 4 § 5 Wet Certificatiediensten wordt aan een derde, die te goeder trouw handelt met een persoon die beschikt over een geavanceerde elektronische handtekening op basis van een gekwalificeerd certificaat, slechts een zeer zwakke bescherming gegeven op het vlak van de non-repudiatie. Indien de houder van het certificaat geconfronteerd wordt met zijn handtekening en deze op stellige wijze ontkent, wordt de procedure van een gerechtelijk onderzoek naar de echtheid gestart.

Wat een dergelijke procedure in deze context betekent, is niet helemaal, zelfs helemaal niet duidelijk.

Dergelijke zware eisen stellen (geavanceerde elektronische handtekening én gekwalificeerd certificaat) zonder daaraan de nodige rechtsgevolgen te verbinden is zeer bevreemdend.

De rechtsregeling in het initiële wetsontwerp nl. dat behoudens tegenbewijs, deze handtekening kon worden toegeschreven aan de certificaathouder, bood een meer evenwichtige oplossing, daar in geval van repudiatie de bewijslast rustte bij de houder van de handtekening.

C. Openbare sector

111. De wetgever geeft enkele specificaties voor het gebruik van de elektronische handtekening in de openbare sector.

Art. 4. § 1 - § 3.

§ 3. De Koning kan, bij een besluit vastgesteld na overleg in Ministerraad, voor het gebruik van elektronische handtekeningen in de openbare sector eventuele aanvullende eisen stellen. Deze eisen moeten objectief, transparant, evenredig en niet discriminerend zijn en mogen slechts op de specifieke kenmerken van de betrokken toepassing betrekking hebben. Zij mogen geen belemmering vormen voor grensoverschrijdende diensten voor de burgers.

[69] Art. 1322 lid 2 B.W. bepaalt: «Kan, voor de toepassing van dit artikel, voldoen aan de vereiste van een handtekening, een geheel van elektronische gegevens dat aan een bepaalde persoon kan worden toegerekend en het behoud van de integriteit van de inhoud van de akte aantoont.»

[70] In de memorie van toelichting wordt een onderscheid gemaakt in de juridische behandeling tussen [1] een geavanceerde elektronische handtekening (dus met gekwalificeerd certificaat) afgegeven door een geaccrediteerde certificatiedienstverlener en [2] eenzelfde elektronische handtekening afgegeven door een niet geaccrediteerde certificatiedienstverlener. Dit onderscheid is in de wet niet meer terug te vinden.

In deze sector moet op een verdere uitwerking worden gewacht.

Hoofdstuk V. Certificatie

112. De belangrijkste rol van een certificatiedienstverlener is het zichtbaar maken en attesteren van de band tussen de houder van de handtekening en de handtekening. Dit verband wordt bevestigd in een digitaal certificaat, afgegeven door de certificatiedienstverlener.

Hierna worden de begrippen certificatiedienstverlener en certificaat nader toegelicht.

Afdeling 1. Certificatiedienstverlener

A. Wat is een certificatiedienstverlener?

113. Het begrip *certificatiedienstverlener* wordt in art. 1, 10° Wet Certificatiediensten omschreven als elke natuurlijke persoon of rechtspersoon die certificaten afgeeft en beheert of andere diensten in verband met elektronische handtekeningen verleent. Een ruime bepaling dus die zowel betrekking kan hebben op gespecialiseerde bedrijven (VeriSign) als op gewone beroepsorganisaties die certificatiediensten aan hun leden verlenen, zoals het notariaat en de balie.

B. Taken van een certificatiedienstverlener

114. De kerntaak van een certificatiedienstverlener is het [1] controleren van het sleutelpaar, [2] het afleveren van certificaten aan certificaathouders en [3] het bijhouden van een elektronisch register van de verleende certificaten (art. 10).

De gegevens die de certificatiedienstverlener nodig heeft voor controle van de certificaathouder mag hij enkel bij de certificaathouder vergaren.

C. Geen voorafgaande machtiging

115. Een zeer belangrijke bepaling m.b.t. het juridisch statuut van de certificaatdienstverlener is, in uitvoering van de Europese richtlijn, in art. 4 § 2, lid 1 van de Wet Certificatiediensten opgenomen: een certificatiedienstverlener kan niet verplicht worden aan de overheid een voorafgaande machtiging aan te vragen.

D. Soorten

116. In de wet wordt een dubbel onderscheid gemaakt tussen de certificaatdienstverleners, op de eerste plaats zijn er certificaatdienstverleners die gekwalificeerde certificaten uitreiken of niet en vervolgens zijn er certificaatdienstverleners die een accreditatie aanvragen en andere niet.

§ 1. Gekwalificeerde en niet-gekwalificeerde certificatenverstrekkers

117. Elke certificaatdienstverlener kan certificaten afleveren. Het is de essentie van hun taak. Enkel een gekwalificeerd certificaat samen met een geavanceerde elektronische handtekening biedt rechtens assimilatie met een handgeschreven handtekening. Art. 4 § 2, lid 2 Wet Certificatiediensten bepaalt dat elke certificatiedienstverlener gekwalificeerde certificaten kan afleveren. Wanneer hij dit doet moet hij aan de overheid vooraf volgende mededelingen doen:

- zijn naam;
- zijn geografisch adres waar hij gevestigd is;
- zijn coördinaten, waardoor hij gemakkelijk te bereiken is, met inbegrip van zijn adres voor elektronische post;
- in voorkomend geval, zijn beroep, referenties en identificatienummers (handelsregister, BTW);
- het bewijs dat er een verzekering onderschreven werd ter dekking van zijn verplichtingen bedoeld in artikel 14.

Ze ontvangen dan een ontvangstbewijs binnen vijf werkdagen volgend op hun mededeling.

Dit impliceert dat elke certificaatdienstverlener alle denkbare certificaten mag ontwikkelen die hij dienstig acht. Enkel wanneer hij een certificaat creëert waarop hij de vermelding “gekwalificeerd certificaat” aanbrengt valt hij onder de wettelijke bepalingen.

118. Daar Hoofdstuk V van de wet enkel van toepassing is op de certificatiedienstverlener die gekwalificeerde certificaten aflevert, ongeacht of ze geaccrediteerd zijn, impliceert dit dat het statuut van een certificatiedienstverlener die geen gekwalificeerde certificaten aflevert niet geregeld is.

§ 2. Geaccrediteerd en niet-geaccrediteerd

119. Certificatiedienstverleners kunnen om een accreditatie verzoeken. Bekomen zij de accreditatie dan spreekt men van een geaccrediteerde certificatiedienstverlener. Accreditatie wordt aangevraagd aan het bestuur en steunt op de controle [a] of de gekwalificeerde certificaten voldoen aan Bijlage I van de wet en [2] of de aanmaakmiddelen overeenkomen met de vereisten van Bijlage III. De Koning bepaalt de verdere voorwaarden van de accreditatie.

Er wordt geen onderscheid gemaakt tussen certificatiedienstverleners die geaccrediteerd zijn of die niet geaccrediteerd zijn. Het enige verschil bestaat hierin dat ingevolge de accreditatie een aantal kwaliteitsvoorwaarden door het bestuur *a priori* werden onderzocht, zonder accreditatie moet de eindgebruiker die criteria *a posteriori* onderzoeken.

Afdeling 2. Certificaat

A. Begrip

120. Een certificaat is een elektronische bevestiging uitgaande van een certificatiedienstverlener waarin [1] een bepaalde *public key* wordt gekoppeld aan een bepaalde persoon en [2] waarbij deze persoon wordt geïdentificeerd (art. 2, 3° Wet Certificatiedienstverlening). Een certificaat koppelt een persoon aan een handtekening.

Bestemmeling wil de handtekening van *Afzender* controleren. Dit moet hij doen aan de hand van de *public key* van *Afzender*. Het certificaat bevestigt dat *Afzender* wel degelijk de de titularis is van die *public key*.

Indien *Afzender* een pseudoniem gebruikt, moet dit alleen vermeld worden op gekwalificeerde certificaten.

121. De aansprakelijkheid van de certificatiedienstverlener speelt zich af precies rond deze certificaten. De aansprakelijkheid voor het afleveren van de eenvoudige certificaten werd in de Wet Certificatiediensten niet geregeld, zodat de gewone regels van aansprakelijkheid van toepassing zijn, zowel wat de beoordeling van het foutcriterium betreft als eventueel de geldigheid van de clausules van aansprakelijkheidsontheffing. De aansprakelijkheid voor het uitschrijven van gekwalificeerde certificaten is wel in de wet geregeld.

B. Soorten

122. Er zijn twee soorten certificaten: het gewone certificaat en het gekwalificeerd certificaat. Beiden zijn geldig indien in het certificaat [1] de *public key* wordt toegewezen aan een bepaalde persoon (authentificatie) en [2] deze persoon wordt geïdentificeerd.

§ 1. Een eenvoudig certificaat

123. Een eenvoudig certificaat is een certificaat waarin beide hierboven omschreven functies voorkomen, zonder de vermelding dat het om een gekwalificeerd certificaat gaat. Een handtekening op basis van een dergelijk certificaat *moet niet* geassimileerd worden met een handgeschreven handtekening, zonder dat de rechter nochtans deze handtekening ontoelaatbaar of ongeldig mag verklaren omdat die handtekening niet vergezeld is van een gekwalificeerd certificaat.

§ 2. Een gekwalificeerd certificaat

124. Elke certificatiedienstverlener kan in de regel, ongeacht enige accreditatie, gekwalificeerde certificaten afleveren. Het volstaat dat het certificaat voldoet aan de voorwaarden van de wet.

Een gekwalificeerd certificaat moet de vermelding *"gekwalificeerd certificaat"* bevatten en daarenboven aan volgende voorwaarden voldoen wat [A] het certificaat en [B] de certificatiedienst betreffen.

A. HET CERTIFICAAT MOET VOLDOEN AAN EEN AANTAL KWALITEITSVEREISTEN OPGESOMD IN BIJLAGE I BIJ DE WET:

a) de vermelding waaruit blijkt dat het certificaat als gekwalificeerd certificaat wordt afgegeven;
b) de identificatie van de certificatiedienstverlener en het land waar hij gevestigd is;
c) de naam van de ondertekenaar of een pseudoniem dat als dusdanig is geïdentificeerd;
d) de mogelijkheid om, in voorkomend geval, een specifiek attribuut van de ondertekenaar te vermelden, rekening houdend met het gebruik waarvoor het certificaat bestemd is;
e) gegevens voor het verifiëren van de handtekening die overeenstemmen met de gegevens voor het aanmaken van de handtekening onder controle van de ondertekenaar;
f) de vermelding van het begin en het einde van de geldigheidsduur van het certificaat;
g) de identiteitscode van het certificaat;
h) de geavanceerde elektronische handtekening van de certificatiedienstverlener die het certificaat afgeeft;
i) in voorkomend geval de beperkingen op het gebruik van het certificaat, en;
j) in voorkomend geval de grenzen met betrekking tot de waarde van de transacties waarvoor het certificaat kan worden gebruikt.

B. HET CERTIFICAAT MOET AFGELEVERD WORDEN DOOR EEN CERTIFICATIEDIENSTVERLENER DIE VOLDOET AAN DE KWALITEITSVEREISTEN VAN BIJLAGE II BIJ DE WET, ONGEACHT EEN EVENTUELE ACCREDITATIE:

a) het bewijs te leveren dat ze voldoende betrouwbaar zijn om certificatiediensten te leveren;
b) te zorgen voor de werking van een snelle en veilige directorydienst en van een veilige en prompte herroepingsdienst;
c) erop toe te zien dat de datum en het uur van uitgifte en herroeping van een certificaat nauwkeurig kunnen worden bepaald;
d) aan de hand van passende en met het nationaal recht in overeenstemming zijnde middelen de identiteit en, in voorkomend geval, de specifieke attributen te controleren van de persoon aan wie een gekwalificeerd certificaat wordt afgegeven;
e) personeel tewerk te stellen met specifieke kennis, ervaring en kwalificaties noodzakelijk voor het verlenen van de diensten en, in het bijzonder, met beheersbe-

kwaamheid, gespecialiseerde kennis inzake technologie van elektronische handtekeningen en een goede praktische kennis van de passende beveiligingsmethoden; ze dienen tevens administratieve en beheersprocedures en –methoden toe te passen, die aangepast zijn aan en overeenstemmen met de erkende normen;

f) betrouwbare systemen en producten te gebruiken, die beschermd zijn tegen de wijzigingen en die de technische en cryptografische veiligheid garanderen van de processen die ze ondersteunen;

g) maatregelen te treffen tegen het vervalsen van certificaten en wanneer de certificatiedienstverlener gegevens genereert in verband met het aanmaken van de handtekening, de vertrouwelijkheid van dat proces te garanderen;

h) over voldoende financiële middelen te beschikken om te functioneren overeenkomstig de vereisten van deze wet en vooral om de aansprakelijkheid te nemen voor schade, door bijvoorbeeld een passende verzekering te sluiten;

i) alle relevante informatie over een gekwalificeerd certificaat te registreren gedurende de nuttige termijn van 30 jaar, in het bijzonder om een certificatiebewijs te kunnen voorleggen bij gerechtelijke procedures. Die registraties mogen elektronisch gebeuren;

j) de gegevens voor het aanmaken van de handtekening van de persoon waar aan de certificatiedienstverlener sleutelbeheersdiensten heeft verleend, noch op te slaan noch te kopiëren;

k) vooraleer een contractuele verbintenis tot stand te brengen met een persoon die om een certificaat verzoekt ter ondersteuning van zijn elektronische handtekening, die persoon via een duurzaam communicatiemiddel op de hoogte te brengen van de exacte gebruiksmodaliteiten en –voorwaarden van de certificaten, met inbegrip van de opgelegde beperkingen voor het gebruik ervan, van het bestaan van een vrijwillig accreditatiestelsel en van de procedures qua klachten en regeling van de geschillen. Deze informatie, die elektronisch kan worden doorgegeven, dient schriftelijk en in gemakkelijk te begrijpen woorden geformuleerd te zijn. Relevante elementen van die informatie dienen tevens, op verzoek, ter beschikking te worden gesteld van derden die zich beroepen op het certificaat;

l) betrouwbare systemen te gebruiken om de certificaten in controleerbare vorm op te slaan zodat:
   a) enkel daartoe gemachtigde personen gegevens kunnen invoeren en wijzigen;
   b) de authenticiteit van de informatie kan worden gecontroleerd;
   c) de certificaten enkel publiekelijk beschikbaar zijn in de gevallen waarin de certificaathouder zijn toestemming heeft verleend en
   d) elke technische wijziging waarbij die veiligheidsvereisten in het gedrang komen, duidelijk is voor de gebruiker.

125. Gekwalificeerde certificaten kunnen verleend worden voor een specifiek gebruik (art. 14 § 3 Wet Certificatiediensten) of voor een maximumwaarde van een transactie (art. 14 § 4 Wet Certificatiediensten). Indien deze beperkingen duidelijk zijn aangegeven wordt de aansprakelijkheid van de certificatiedienstverlener beperkt tot dat specifiek gebruik of dat beperkt bedrag.

126. Gekwalificeerde certificaten kunnen worden herroepen hetzij op vraag van de certificaathouder, hetzij door de certificatiedienstverlener in de 4 gevallen vermeld in art. 12 § 2: foutieve of vervalste gegevens, beslissing van de rechtbank, stopzetting van activiteit en overlijden van de certificatiehouder.

C. Aansprakelijkheid

127. De aansprakelijkheid van de certificatiedienstverleners van gekwalificeerde certificaten is samengebracht in art. 14 van de Wet Certificatiediensten.[71] In de regel staan ze in voor de schade die zij toebrengen aan een derde die zich als een voorzichtig huisvader op een dergelijk certificaat heeft gesteund.[72] Ze staan in voor de juistheid van de gegevens op het ogenblik van het aanmaken van het certificaat.

Zij dragen verder de verantwoordelijkheid van de herroeping van het certificaat in de gevallen die de wet opsomt (art. 12).

Conclusie

128. Net zoals voor de andere wetten, waarin de gemeenschap de confrontatie heeft aangegaan met de eisen van de informatiemaatschappij, is deze wet niet als een schoolvoorbeeld van duidelijkheid aan te wijzen.[73] Zowel de genese van de teksten als de uiteindelijk goedgekeur-

[71] Ze moeten over de nodige financiële middelen beschikken om hun aansprakelijkheid te kunnen garanderen, desnoods moeten ze die verzekeren (Bijlage II, h). Enkel dienstverleners die een gekwalificeerd certificaat afleveren moeten zich laten verzekeren (art. 4 § 2 lid 2).

[72] Zo kan de vraag gesteld worden of de niet-vermelding op een certificaat dat een handtekening gevoerd wordt onder een pseudoniem op zichzelf geen fout uitmaakt.

[73] Dit was ook zo voor de wet van 8 december 1992 op de Verwerking Persoonsgegevens en op de wet van 31 augustus 1998 op de Rechtsbescherming Databanken.

de versie zijn niet gebaseerd op een duidelijke en doordachte analyse van het bestaande rechtssysteem. Het zal opnieuw aan de rechtspraktijk zijn om een aantal zaken op te lossen die eigenlijk door de wetgever hadden moeten geregeld worden, zoals bijv. de verhouding tussen art. 1322 lid 2 B.W. en art. 4 § 5 Wet Certificatiediensten (het non-discriminatiebeginsel).

129. Het valt te betreuren dat de wetgever niet van de gelegenheid heeft gebruik gemaakt om zowel het begrip *geschrift* als het begrip *handtekening* op een functionele wijze in het Burgerlijk Wetboek op te nemen, zodat op een naadloze wijze deze teksten in een virtuele omgeving konden worden toegepast.

De werkwijze die thans is gevolgd kan tot nieuwe problemen aanleiding geven: de wetgever heeft zich niet uitgesproken over wat een "geschrift" of een "handtekening" is. Enkel de rechtsgeldigheid van een elektronische handtekening werd erkend. Door het feit dat een elektronische handtekening alleen op een elektronisch document kan worden geplaatst, wordt bij wijze van noodzakelijke afleiding (de onterechte gelijkstelling van de elektronische handtekening met het elektronisch document) het elektronisch document als geschrift erkend.

130. Tenslotte zijn er bijkomend nog een drietal kritische vaststellingen te doen. Ze hebben betrekking op de rechtsgevolgen en op de identificatie.

A. Rechtsgevolgen

131. Er werd een systeem uitgewerkt van een geavanceerde elektronische handtekening op basis van een gekwalificeerd certificaat, d.i. een handtekening met een zeer hoog zekerheidsgehalte. De rechtsbescherming die op basis van deze handtekening wordt geboden aan de persoon die hiermee in contact komt, is te gering, m.a.w. de mogelijkheden van repudiatie blijven te hoog. Het is niet meer van deze tijd dat het formeel ontkennen van een dergelijke handtekening volstaat om de rechtsgevolgen op de helling te zetten. Het ware beter geweest op algemene wijze een oplossing te vinden voor alle handtekeningen:

a. handtekeningen geplaatst ten aanzien van een openbare ambtenaar: erkenning van de handtekening tot inschrijving wegens valsheid (thans bestaand systeem);
b. voor een geavanceerde elektronische handtekening met gekwalificeerd certificaat: de toewijzing van de handtekening aan de houder van het certificaat, tot bewijs van het tegendeel;
c. voor alle andere handtekeningen (handgeschreven handtekening, mechanisch geplaatste handtekeningen en [gewone] elektronische handtekening): uitdrukkelijke ontkenning, gevolgd door een gerechtelijk echtheidsonderzoek.

B. Pseudoniem

132. Het feit dat een gecertificeerde handtekening kan worden toegekend op basis van een pseudoniem, zonder dat de derde steeds van dit feit op de hoogte moet worden gesteld in het certificaat[74], lijkt niet aanvaardbaar en ondermijnt het doel van de certificatie die de wetgever voor ogen had.

C. Identificatie

133. Tenslotte lijkt evenmin aanvaardbaar dat bij onrechtmatig gedrag op internet het slachtoffer het recht niet toekomt de identiteit van de dader te kennen (art. 5 § 2 Wet Certificatiediensten). Identificatie is enkel mogelijk indien er misdrijven werden gepleegd en mits politioneel optreden.

Bibliografie

Wetgeving

Richtlijn nr. 1999/93 van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen, *PB. L*. 19 januari 2000, 12.

Wet 20 oktober 2000 tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en de buitengerechtelijke procedure (*B.S.* 22 december 2000).[75]

Wet 9 juli 2001 houdende vaststelling van bepaalde regels i.v.m. het juridisch kader voor elektronische handtekeningen en certificatiediensten (Wet Certificatiediensten), *B.S*. 29 september 2001.

Literatuur

Mireille ANTOINE en D. GOBERT, "Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification", *T.B.B.R.* 1998, 285-310.

Mireille ANTOINE en D. GOBERT, "La directive européenne sur la signature électronique. Vers la sécurisation des transactions sur l'internet?", *J.T. dr. eur*. 2000, 73-78.

Mireille ANTOINE, M. ELOY, M. en J. BRAKELAND, *Le droit de la preuve face aux nouvelles technologies de l'information. Aspects techniques et juridiques du transfert et de la conservation des documents*. Reeks "Cahiers

[74] Thans moet het alleen vermeld worden in een gekwalificeerd certificaat.

[75] *Parl. St. Kamer*, zitting nr. 50, B.Z. 1999, nr. 0038.

du Centre de recherches informatique et droit", nr. 7. Story-Scientia, Brussel, 1992, 244 p.

G. Luc BALLON, "EDI en Belgisch recht", in X., EDI en België, 175-197.

G. Luc BALLON, "Het bewijs en de moderne technieken" *Computerr*., deel 1: 1990, 228-244; deel 2: 1991, 14-16.

G. Luc BALLON, "Ik gaf mijzelf (g)een naam - over anoniem en pseudoniem optreden in het openbaar", *T.P.R.* 1981, 557-592.

V. CAMBIER, "L'authentification du consentement du consommateur dans les paiements électroniques", *REDC* 1998, 171-186.

Mieke COENE, "Vormt de vereiste van handtekening de valstrik van het eigenhandig testament?", *Tijd. Not*. 1986, 313-320.

Etienne DAVIO, "Questions de certification, signature et cryptographie" in X. *Internet face au droit*, Crid, Story Scientia, 1997, 65-109.

Etienne DAVIO, "Preuve et certification sur internet" *T.B.H*. 1997, 660-670.

Bertel DE GROOTE, "Het bewijs in de elektronische handel - enkele bedenkingen", *A.J.T.* 2000-2001, 881-901.

Jos DUMORTIER, "Digitale handtekening en de hervorming van het bewijsrecht", in X., *Recht in beweging*, 123-143.

Jos DUMORTIER, "Juridische aspecten van de elektronische en de digitale handteke ning" in X., *Mediarecht*, 20 p. Kluwer Editorial, Diegem, losbl., z.p.

Jos DUMORTIER en S. VAN DEN EYNDE, "De juridische erkenning van de elektronische handtekening in België" *Computerr*. 2001, 185-194.

Jos DUMORTIER en Patrick VAN EECKE, "De Europese ontwerprichtlijn over digitale handtekening: waarom is het misgelopen?", *Computerr*. 1999, 3-10.

Jos DUMORTIER en Patrick VAN EECKE, "Een juridisch kader voor Trusted Third Parties in België", *Computerr*. 1998, 228-234.

Jos DUMORTIER en Patrick VAN EECKE, "Naar een juridische regeling van de digitale handtekening in België", *Computerr*. 1997, 145-159.

Jos DUMORTIER en Patrick VAN EECKE, "Recente ontwikkelingen van Recht en Informatica. Digitale handtekening en de hervorming van het bewijsrecht", in X., *Recht in beweging* , 123-143, KU Leuven, Leuven, 2000, 276 p.

Didier GOBERT en Etinne MONTERO, "La signature dans les contrats et les paiements électroniques: l'approche fonctionnelle", in X., *Commerce électronique: le temps des certitudes*, 53-97.

Didier GOBERT en Etienne MONTERO, "L'ouverture de la preuve littérale aux écrits sous forme électronique", *J.T.* 2001, 114-128.

B. KOOPS, R. VAN KRALINGEN en L. VAN DER WEES, "De rol van Trusted Third Parties in het elektronisch handelsverkeer", *Computerr*. (Ned.) 1998, 206-211.

Filip LOGGHE, "Van verscheidenheid naar eenheid en terug. De ondertekening van een eigenhandig testament", *A.J.T.* 1998-99, 878-880.

Dominique MOUGENOT, "Droit de la preuve et technologies nouvelles: synthèse et perspectives" in X., *Droit de la preuve*, Formation permanente CUP, octobre 1997, 45-105.

W. OOSTERVEEN, "De elektronische handtekening", in X., *De elektronische snelweg*, 47-56.

Jean-Luc SNYERS, "De elektronische authentieke akte en de notariële elektronische archivering", *Limb. Rechtsl*. 2000, 283-305.

Reinhard STEENNOT, "Bankieren via internet: het belang van de elektronische handtekening", *Bank Fin*. 2000, 630-640.

Reinhard STEENNOT, "Juridische problemen in het kader van de elektronische handel", *T.B.H.* 1999, 664-676.

Matthias E. STORME, "De invoering van de elektronische handtekening in ons bewijsrecht - Een inkadering van en commentaar bij de nieuwe wetsbepalingen" *R.W.* 2000-2001, 1505-1525.

D. SY, "Naar nieuwe vormen van handtekening? Het probleem van de handtekening in het elektronisch rechtsverkeer", *Computerr*. 1998, 153-166.

R. VAN ESCH, "De elektronische handtekening", in X., *De elektronische snelweg*, 31-37.

Marc VAN QUICKENBORNE, "Quelques réflexions sur la signature des actes sous seing privé", noot onder Cass. 28 juni 1982, *R.C.J.B.* 1985, 65-104.

Wilfried WILMS, "Van handtekening naar elektronische notaris - de validering van elektronische communicatie", *R.W.* 1995-96, 837-842.

X., *Authenticiteit en Informatica*, Bruylant, Brussel, 2000, 496 p.

X., *Commerce Électronique: le temps des certitudes.*
Reeks "Cahiers du Centre de Recherches Informatique et Droit", nr. 17. Bruylant, Brussel, 2000, 225 p.

X., *De elektronische snelweg*, Reeks "Privaatrecht in de 21e Eeuw", Kluwer, Deven ter, 1999, 83 p.

X., *Le consentement électronique*, Collection droit et consommation, Bruylant, 2000, 370 p.

X., *Telebanking, Teleshopping and the Law*. Reeks "Computer Law Series", afl. 1. Kluwer Law and Taxation Publishers, Deventer, 1988, 379 p.

X., *The legal aspects of digital signatures*, Vol. I-V, European Commission, Mys & Breesch, 1998.