

Wet van
houdende regels inzake
overeenkomsten te sluiten
langs elektronische weg
(Wet overeenkomsten langs
elektronische weg)

MEMORIE VAN TOELICHTING

A. Algemeen

§ 1. Doel

1. Handel, financiële dienstverlening en andere commerciële activiteiten verlopen in snel groeiend tempo langs elektronische weg. Elektronische handel of *e-commerce* krijgt een steeds grotere maatschappelijke en economische betekenis.
2. Elektronische transacties (als samenvattend begrip) betreft niet alleen handel via internet, maar meer in het algemeen alle zakelijke handelingen via internet. De zakelijke handelingen kunnen bedrijven onderling (*business-to-business*), bedrijven en consumenten (*business-to-customer*) en bedrijven en overheden (*business-to-administration*) betreffen.
3. Met e-commerce hangen bijzondere aspecten samen. Zo heeft e-commerce in de regel een grensoverschrijdend karakter en raakt derhalve meerdere jurisdicties. Er is sprake van gedematerialiseerde communicatie, kennis, diensten en informatie: deze worden niet in een tastbare vorm neergelegd. Bij digitale vastlegging is informatie niet meer gebonden aan een bepaalde fysieke drager of plaats. Digitaal vastgelegde informatie is bovendien onuitputtelijk, in die zin, dat deze oneindig kan worden gekopieerd zonder dat dit leidt tot kwaliteitsverlies of vernietiging. Voorts kan een technologische turbulentie worden vastgesteld. Nieuwe informatietechnieken en -producten volgen elkaar in hoog tempo op, of convergeren tot nieuwe media. De ontwikkeling van de techniek, het maatschappelijk gebruik daarvan en de sociale en juridische problemen die daardoor worden opgeroepen, zijn in belangrijke mate onvoorspelbaar. Er is dus sprake van vergaande veranderingen, maar die brengen nog geen radicale breuk met het verleden mee. De centrale rol van de overheid blijft voorlopig beperkt tot ordening.
4. Het overheidsbeleid is onder meer gericht op het bevorderen van de transparantie en toegang tot de markt, alsmede de betrouwbaarheid van het elektronische verkeer, en het wegnemen van belemmeringen in de bestaande juridische infrastructuur. Daarnaast wordt een brede toegankelijkheid tot de elementaire voorzieningen beoogd: voorzieningen die nodig zijn voor het maatschappelijk functioneren van burgers en bedrijven.
5. Het onderhavige ontwerp, dat is ontleend aan de Nederlands-Antilliaanse Landsverordening overeenkomsten langs elektronische weg van 29 december 2000 (*Publicatieblad van de Nederlandse Antillen* 2000, no. 168), beoogt enerzijds onzekerheden weg te nemen en elektronisch verkeer te faciliteren, en anderzijds een aantal fundamentele waarden en normen in een elektronische omgeving te waarborgen. Hierbij gaat het om de vastlegging van rechten en verplichtingen, het verzekeren van rechtshandhaving en het bieden van rechtszekerheid. Uit het ontwerp volgt dat aan elektronische handtekeningen dezelfde rechtsgevolgen kunnen zijn verbonden als aan

schriftelijke handtekeningen, en dat aan rechtshandelingen niet de geldigheid kan worden ontzegd uitsluitend omdat deze langs elektronische weg zijn verricht. Ook een elektronisch document kan als bewijsmiddel worden gebruikt.

§ 2. *Begrenzing*

1. Het ontwerp brengt geen wijziging in de in Suriname van toepassing zijnde wet- en regelgeving, behoudens voor zover een afwijking expliciet uit het ontwerp blijkt. Uitgangspunt is geweest dat alleen die onderwerpen worden geregeld ten aanzien waarvan de behoefte tot een wettelijke regeling bestaat en waarin de bestaande wetten derhalve niet of niet adequaat voorzien. Het bestaande kader aan juridische normen uit de 'fysieke wereld' is namelijk in beginsel evenzeer van toepassing in de 'elektronische wereld'. Zo bevatten bijvoorbeeld het Burgerlijk Wetboek en het Wetboek van Koophandel grotendeels technologie-neutrale bepalingen. Dat neemt niet weg dat buiten twijfel moet worden gesteld dat overeenkomsten ook langs elektronische weg tot stand kunnen komen, dat aan elektronische handtekeningen niet de rechtsgeldigheid wordt ontzegd en dat beiden, net als een elektronisch document, ook in het bewijsrecht een rol kunnen spelen, al is de waardering daarvan in ieder concreet geval aan het oordeel van de rechter overgelaten.
2. Zo wordt het bijvoorbeeld niet nodig geacht bepalingen op het terrein van intellectuele eigendomsrechten op te nemen. Het handhaven van intellectuele eigendomsrechten in relatie tot e-commerce, waarbij het in de regel gaat om grensoverschrijdende, digitale contacten, is op zich niet altijd even eenvoudig. Slechts langs verdragsrechtelijke weg zou een adequaat en sluitend systeem denkbaar zijn. Daar staat tegenover dat het enkele feit dat transacties via internet tot stand komen, voor aanbieders doorgaans geen fundamenteel andersoortige intellectuele eigendomsproblemen met zich zal brengen, al zou dit van geval tot geval kunnen verschillen. Als centraal en verreweg grootste vraagstuk moet de wijze van bepaling van het toepasselijke recht in een concreet geval worden aangewezen. Naast de vraag of de rechthebbende naar Surinaams recht voldoende mogelijkheden heeft om zijn (auteurs- en merken)rechten jegens anderen geldend te maken, is de vraag of en in hoeverre *service providers* - in het ontwerp aangeduid als dienstenaanbieders - als intermediair uit hoofde van een onrechtmatige daad aansprakelijk kunnen worden gehouden voor inbreukmakende handelingen van aanbieders en hun wederpartijen (de gebruikers). Vergelijk Rb 's-Gravenhage 9 juni 1999, IER 1999, 47, p. 237, Scientology/XS4ALL e.a.: in beginsel niet, tenzij zij de inbreuk bevorderen of bewust laten plaatsvinden. In artikel 8 van het ontwerp is dit op vergelijkbare wijze geregeld.
3. Met betrekking tot *access providers* lijkt de aansprakelijkheidsvraag niet relevant, aangezien deze slechts inbelfaciliteiten bieden. Niettegenstaande deze conclusies moet worden gesteld dat de ontwikkelingen rond internet en e-commerce nog niet voldoende zijn uitgekristalliseerd om reeds nu verantwoorde wetgevingsinitiatieven te ontplooiën. Tegenover de civielrechtelijke bescherming staat vanzelfsprekend het probleem van de inbreuk op deze rechten vanuit 'cyberspace'. Op dit moment kunnen inbreuken slechts van geval tot geval worden gezien en strekt de genoemde bescherming zich niet verder uit dan tot de landsgrenzen. Gelet op de onzekerheid over deze ontwikkelingen, die ook andere wetgevers parten speelt, lijkt in dit opzicht een afwachtende houding verantwoord.

§ 3. *Opzet*

1. Gelet op de snelheid waarmee technische ontwikkelingen plaatsvinden en de onzekerheid

in welke richting e-commerce zich kan en zal ontwikkelen, is gekozen voor een zo flexibel mogelijke opzet van de wet. Enerzijds komt dat tot uitdrukking in het gebruik van algemeen geformuleerde begrippen en bepalingen, en anderzijds in de mogelijkheden om bij staatsbesluit nadere regels omtrent één of meerdere onderwerpen te kunnen stellen. Aldus kan makkelijk op veranderingen, vernieuwingen en knelpunten worden ingespeeld.

2. In het ontwerp komt eerst de commerciële communicatie aan de orde (artikelen 2 tot en met 4). Dit betreft het aanbieden en aanprijzen van goederen, diensten, personen en bedrijven op in de eerste plaats internet. Daarna wat de aanbieder van commerciële communicatie verplicht moet vermelden (artikel 5). Dan komen achtereenvolgens de overeenkomsten langs elektronische weg (artikel 6), de elektronische handtekening (artikel 7), de aansprakelijkheid van dienstenaanbieders (artikel 8) en certificatie-dienstverleners (artikel 9), de bescherming van persoonsgegevens (artikel 10) en vertrouwelijke informatie (artikel 11), cryptografie (artikel 12) en buitengerechtelijke geschillenbeslechting (artikel 13) aan de orde. Ten slotte zijn er bepalingen inzake toezicht (artikelen 14 en 15), opsporing (artikel 16), bestuursdwang (artikelen 17 tot en met 29), door de Minister te geven aanwijzingen (artikel 30), strafrechtelijke sanctionering (artikel 32) en geheimhouding (artikel 33).

§ 4. Toepassingsbereik

1. De ontwerpwet is van toepassing op e-commerce activiteiten. Voor de toepasselijkheid is het aanbieden van commerciële communicatie daarbij een belangrijk criterium. De nationaliteit of woon- of vestigingsplaats van de aanbieder van commerciële communicatie is daarbij op zich niet relevant. Van belang is of de Surinaamse rechtssfeer wordt geraakt. In de toelichting op het begrip commerciële communicatie wordt hierop nader ingegaan.
2. Al staat dat daar niet met zoveel woorden in, de ontwerpwet beoogt buiten twijfel te stellen dat overeenkomsten langs elektronische weg tot stand kunnen komen. In verbintenisrechtelijke zin kan commerciële communicatie een concreet 'aanbod' inhouden, bijvoorbeeld bepaalde producten voor een bepaalde prijs.
3. Voor het tot stand komen van een overeenkomst langs elektronische weg is vereist dat de aanbieder van commerciële communicatie de instemming van de wederpartij met het aanbod ontvangt. Dit uitgangspunt is logisch en is gebaseerd op het gemene recht: wanneer een brief houdende een aanvaarding naar een verkeerd postbusnummer wordt gestuurd en de aanbieder niet bereikt, komt immers ook geen overeenkomst tot stand. Dit uitgangspunt geldt derhalve onverkort voor het tot stand komen van overeenkomsten langs elektronische weg. Elders ziet men ingewikkelde regelingen (bijvoorbeeld in de Europese Unie), waar als constitutief vereiste geldt dat de aanbieder deze instemming op zijn beurt weer aan de wederpartij moet bevestigen en zelfs dat de wederpartij de ontvangst daarvan weer moet bevestigen.
4. Een langs elektronische weg gedaan aanbod kan door de wederpartij echter ook schriftelijk worden aanvaard. Er is desondanks sprake van een overeenkomst die langs elektronische weg tot stand is gekomen en die derhalve valt binnen het bereik van de wet, omdat daarvoor alleen is vereist dat het aanbod langs elektronische weg wordt gedaan. Verwezen wordt ook naar het begrip commerciële communicatie.
5. Daartegenover wordt opgemerkt dat indien het aanbod niet maar de aanvaarding wel langs elektronische weg plaatsvindt, er dan geen sprake is van een overeenkomst langs elektronische weg.
6. Wordt het aanbod gedeeltelijk langs elektronische weg gedaan en gedeeltelijk op andere

wijze (bijvoorbeeld per brief) dan valt de overeenkomst wel onder de werking van de wet.

7. Aanbod en aanvaarding worden overigens door het gemene verbintenissenrecht geregeld. Eén van de hoofdregels is dat een door een aanbieder gedaan aanbod onherroepelijk en niet regionaal of in de tijd begrensd is, tenzij dit bij het aanbod uitdrukkelijk en ondubbelzinnig anders is vermeld. In de regel zal bovendien een aanbod niet worden aangemerkt als een uitnodiging tot het doen van een aanbod, tenzij dit uitdrukkelijk en ondubbelzinnig is vermeld.
8. Soms kunnen geen overeenkomsten langs elektronische weg tot stand komen: bijvoorbeeld wanneer het gaat om rechtshandelingen die slechts door tussenkomst van een notaris tot stand kunnen komen, of wanneer het gaat om rechtshandelingen waarvoor wettelijke vormvoorschriften bestaan, behoudens voor zover elektronische wegen worden gebruikt waarmee aan de betreffende vormvoorschriften wordt voldaan. Wanneer bijvoorbeeld de schriftelijke vorm is voorgeschreven, voldoet ook een faxbericht daaraan. Bij vormvoorschriften moet een onderscheid worden gemaakt tussen (dwingende) bewijsvoorschriften enerzijds en constitutieve vereisten anderzijds.

§ 5. Handhaving

1. Handhaving van rechtsnormen en -waarden bij grensoverschrijdende activiteiten is bijzonder lastig. Een deel van de bepalingen in de ontwerpwet heeft betrekking op de relatie tussen een aanbieder van commerciële communicatie en zijn wederpartij. Het al dan niet afdwingen van de op die relatie van toepassing zijnde wettelijke normen ligt in handen van de betrokken partijen. De relatie tussen een aanbieder van commerciële communicatie en een dienstenaanbieder (service provider) is eveneens contractueel van karakter wanneer het om een rechtstreekse relatie gaat. Ook in dat geval is het aan partijen om de naleving al dan niet af te dwingen.
2. Bij artikel 11, eerste lid, waar het gaat om het vertrouwelijk behandelen van informatie met een zodanig karakter, is het evenzeer aan partijen om op grond van een contractuele relatie of uit hoofde van een onrechtmatige daad, tegen een inbreuk te ageren. Dat neemt niet weg dat een op artikel 11, derde lid, gebaseerd staatsbesluit strafrechtelijk te sanctioneren verboden kan bevatten.
3. Daarnaast zijn er bepalingen die zien op de aansprakelijkheid jegens de aanbieder van commerciële communicatie, de wederpartij en (andere) derden: zo is de dienstenaanbieder (service provider) niet aansprakelijk wanneer hij slechts 'doorgeefluik' van informatie is (artikel 8). Deze bepalingen beperken dus de mogelijkheden om de service provider in rechte aan te spreken, doorgaans op grond van het leerstuk onrechtmatige daad.
4. Ten slotte zijn er bepalingen op de naleving waarvan de overheid ziet, hetzij in de vorm van het geven van een aanwijzing hetzij langs strafrechtelijke weg. De strafrechtelijke bepalingen zijn doorgaans te herkennen aan het woord 'verboden'. Strafbepalingen inzake computercriminaliteit zullen in het Wetboek van Strafrecht worden opgenomen. Een mengvorm is te vinden in artikel 4, tweede lid, waarin het verbod is vastgelegd om commerciële communicatie te bedrijven met geadresseerden die te kennen hebben gegeven daarop geen prijs te stellen: deze geadresseerden kunnen aangifte doen en/of met een beroep op dit artikel uit hoofde van een onrechtmatige daad tegen ongewenste informatie ageren.

B. Artikelsgewijze toelichting

Artikel 1

In de ontwerpwet wordt over 'aanbieder' van commerciële communicatie gesproken. Het is niet nodig dit begrip in de wet te omschrijven. Het gaat om de natuurlijke of rechtspersoon die zaken en diensten langs elektronische weg aanbiedt. Het begrip 'wederpartij' is evenmin gedefinieerd. Het gaat om de natuurlijke of rechtspersoon tot wie de commerciële communicatie zich richt en met wie beoogd wordt overeenkomsten langs elektronische weg aan te gaan. Het kan gaan om consumenten of om partijen die beroeps- of bedrijfsmatig aan het economisch verkeer deelnemen.

Commerciële communicatie

1. In het ontwerp wordt commerciële communicatie gereguleerd voor zover deze plaatsvindt vanuit Suriname of gericht is op inwoners, bedrijven, instellingen en dergelijke in Suriname: ook commerciële communicatie uitsluitend binnen Suriname valt hieronder. Het maakt geen verschil of de uiting zich exclusief op Suriname richt dan wel mede op Suriname is gericht. Van een in de Noorse taal gestelde webpage zal dat minder snel worden aangenomen dan van een in de Engelse taal gestelde webpage, maar beiden kunnen op Suriname zijn gericht. Vanzelfsprekend zijn aan de (internationale) reikwijdte van de wet beperkingen verbonden, maar deze zullen van geval tot geval blijken en hierna nog aan de orde komen. Voor wat betreft de overgrote meerderheid van de gevallen mag overigens worden verwacht dat de wederpartij van overeenkomsten langs elektronische weg buiten Suriname wonen of gevestigd zijn.
2. Aan het onderscheid tussen het actief verzenden van informatie aan een beoogde wederpartij (bijvoorbeeld per e-mail) of het door hem opvragen van de informatie (het op zijn scherm toveren van een bepaalde webpage) wordt in deze wet in beginsel geen betekenis toegekend. Dit onderscheid speelt alleen bij 'ongevraagde' commerciële communicatie een rol (artikel 4).
3. Het gaat om commerciële communicatie die direct of indirect is gericht op het tot stand komen van overeenkomsten langs elektronische weg. Er is afgezien van het in de omschrijving opnemen van de beperking 'met winstoogmerk' of 'tegen betaling'. Er zijn immers ook zakelijke transacties zonder winstoogmerk of waarbij geen betaling plaatsvindt, maar waarvan het wenselijk wordt geacht deze te reguleren. Onder de werking van het ontwerp vallen commerciële en in beginsel alle andere zakelijke activiteiten.
4. Onder het bereik van de ontwerpwet valt onder meer de webpage van:
 - het bedrijf dat producten te koop, te huur of ter leasing aanbiedt;
 - degene die zich als tuinman, schilder of chauffeur aanbiedt;
 - degene die aanbiedt tegen betaling toegang tot bepaalde informatie te verschaffen;
 - degene die zich als consultant, architect, advocaat of accountant aanbiedt;
 - commerciële communicatie tussen overheden en tussen de overheid en burgers (voor zover deze niet separaat zijn of worden gereguleerd);
 - de particulier die zijn auto te koop aanbiedt, en
 - de religieuze organisatie die geschriften te koop aanbiedt (ook als dat tegen slechts of minder dan de kostprijs is).
5. Het gaat in deze gevallen om enigerlei vorm van aanbieden en aanprijzen van zaken, diensten, bedrijven en personen, waaronder reclame en direct marketing, langs elektronische weg, direct of indirect bestemd om overeenkomsten langs elektronische weg tot stand te brengen. Het gaat bij de toepassing van de ontwerpwet overigens niet

- alleen om een webpage, maar om iedere uiting langs elektronische weg.
6. Niet onder het bereik van de ontwerpwet valt daarentegen bijvoorbeeld de webpage van:
 - de leesmoeder die om niet haar diensten aanbiedt;
 - het bedrijf dat of de organisatie die personeel werft;
 - de onderwijsorganisatie die leerlingen of studenten werft;
 - de religieuze organisatie die zichzelf aanprijst en gelovigen oproept om zich bij haar aan te sluiten (tenzij hieraan -mede- commerciële overwegingen ten grondslag liggen en beoogd wordt een overeenkomst tot stand te brengen).
 7. Het gaat om het aanbieden of aanprijzen van goederen, diensten, bedrijven en personen. Naar nieuw BW vallen onder het begrip 'goederen' zowel stoffelijke objecten (lichamelijke zaken) als rechten (onlichamelijke zaken). Bij deze rechten moet bijvoorbeeld ook aan software(applicaties) worden gedacht.

Dienstenaanbieder (service provider)

Het begrip dienstenaanbieder (service provider) is zodanig geformuleerd dat daaronder in beginsel alle aanbieders van elektronische mogelijkheden voor communicatiediensten vallen, met inbegrip van bijvoorbeeld degene die de mogelijkheid biedt om via een website informatie op internet aan te bieden, cellulaire telefonie, en radio- en televisiecommunicatie. De onderhavige ontwerp- wet laat echter de werking van weten die laatstgenoemde service providers bestrijken onverlet. Een beperking van het toepassingsgebied van de wet is bovendien nog te vinden in de omschrijving van het begrip commerciële communicatie: de uitingen moeten langs elektronische weg plaatsvinden en direct of indirect zijn bestemd om overeenkomsten tot stand te brengen. Het begrip dienstenaanbieder is desondanks ruim geformuleerd met het oog op de aansprakelijkheidsregeling in artikel 8, om aldus buiten twijfel te stellen dat een dienstenaanbieder die in feite niet meer is dan een 'doorgeefluik' in beginsel niet jegens bijvoorbeeld een wederpartij van de aanbieder aansprakelijk is voor de inhoud van de doorgegeven uiting.

Langs elektronische weg

Het gaat hier om onder meer elektronische en optische mogelijkheden tot het overbrengen of opslaan van gegevens. Daaronder vallen bijvoorbeeld de fax, e-mail en internet. Het gemene verbintennisrecht geeft voldoende aanknopingspunten voor de beantwoording van de vraag voor wiens risico het onvolledig of onjuist overkomen van een mededeling komt. Hoofregel is dat degene die een bepaalde elektronische techniek kiest dat risico draagt.

Minister

Omdat de ontwerpwet de regels van het Burgerlijk Wetboek aanvult, ligt het voor de hand de Minister van Justitie en Politie met de uitvoering en toepassing van de wet te belasten.

Artikel 2

1. Het moet duidelijk zijn wanneer sprake is van commerciële communicatie. Zo moet bijvoorbeeld duidelijk zijn wanneer wetenschappelijke resultaten worden gebruikt om de verkoop van een product te stimuleren. Er mag niet van misleiding sprake zijn. Het gaat hier om normen die ten aanzien van reclame en dergelijke ook gelden voor media als televisie en kranten.
2. In het tweede lid wordt gesproken over degene 'namens wie' commerciële communicatie

plaatsvindt. Dat zal veelal degene zijn voor wiens rekening dat plaatsvindt, maar noodzakelijk is dat niet. Er is derhalve gekozen voor een ruime formulering. Het is van openbaar belang dat duidelijk is wie welke aanprijzing of welk aanbod doet, opdat beoogde wederpartijen in staat zijn ervoor te kiezen wel of geen zaken met deze aanbieder te doen.

Artikel 3

1. Het algemeen belang is ermee gediend wanneer bepaalde transacties ook op traditionele wijze tot stand kunnen komen. Zo is het (op dit moment) niet wenselijk wanneer reguliere bancaire transacties uitsluitend langs elektronische weg zouden kunnen plaatsvinden. Belangrijke delen van de bevolking, waaronder veel ouderen, zouden hiervan immers worden uitgesloten, omdat zij niet de vaardigheden en/of de middelen hebben om transacties op deze wijze tot stand te brengen.
2. Ter zake van andere transacties kan het wenselijk zijn nadere regels te stellen, bijvoorbeeld met betrekking tot de verkoop van geneesmiddelen en elektronische recepten. Omdat moeilijk is te bepalen welke ontwikkelingen kunnen en zullen plaatsvinden is ervoor gekozen om de mogelijkheid te creëren deze regels bij staatsbesluit in het leven te roepen.
3. Bij staatsbesluit kunnen voorts categorieën van personen worden aangewezen (bijvoorbeeld minderjarigen) tot wie het verboden is commerciële communicatie te richten en kunnen categorieën van commerciële communicatie (bijvoorbeeld tabak) worden aangewezen die zijn verboden. Daarbij moet uiteraard rekening worden gehouden met de aan sommige elektronische wegen inherent verbonden beperkingen voor wat betreft de reikwijdte van de wet en van eventueel daarop gebaseerde staatsbesluiten, houdende algemene maatregelen. Vanuit Suriname kan informatie vanuit nagenoeg alle plekken in de wereld worden opgevraagd: dat laat zich niet goed verbieden.
4. Voorts kunnen bij staatsbesluit verplichte mededelingen worden voorgeschreven, bijvoorbeeld dat een bepaald product schadelijk is voor de gezondheid of dat het aangeboden niet geschikt is voor minderjarigen.
5. In hoofdstuk 11 van de ontwerpwet is de regeling van de bestuursdwang opgenomen. Langs die weg kan de Minister ingrijpen wanneer activiteiten van een aanbieder naar zijn oordeel onwettig zijn, of wanneer het gaat om activiteiten in strijd met de openbare orde, de goede zeden, of wanneer het belang van de staatsveiligheid of andere openbare belangen dat vorderen. In plaats van bestuursdwang kan de Minister desgewenst overgaan tot het opleggen van een last onder dwangsom (artikel 26). Op grond van artikel 30 kan de Minister de aanbieder één of meer aanwijzingen geven.

Artikel 4

1. Zoals ongevraagd reclamefolders in een brievenbus kunnen worden gedeponereerd, kan door een aanbieder ongevraagd commerciële communicatie tot één of meer beoogde wederpartijen worden gericht. Commerciële communicatie is 'ongevraagd' wanneer de ontvanger deze buiten zijn wil ontvangt, bijvoorbeeld op zijn e-mailadres. Commerciële communicatie kan niet een ongevraagd karakter dragen wanneer deze zelf wordt opgevraagd, bijvoorbeeld door te surfen op het net om van bepaalde webpages kennis te nemen. De mogelijkheid moet bestaan om tegen ongevraagde commerciële communicatie bezwaar aan te teken. Is dat eenmaal gedaan dan is het een aanbieder verboden om nog langer ongevraagde commerciële communicatie naar de betrokkene te sturen.

2. Uit het tweede lid volgt dat de aanbieder een goed herkenbare en eenvoudige mogelijkheid moet geven om bezwaar te maken tegen nieuwe ongevraagde uitingen. De meest voor de hand liggende mogelijkheid is een daarop gerichte vraag die de ontvanger met 'ja' of 'nee' kan beantwoorden met een simpele 'druk op de knop'. Met een 'eenvoudige mogelijkheid' wordt bedoeld dat van de ontvanger niet kan worden verlangd dat hij (alleen) schriftelijk bezwaar mag maken of (alleen) telefonisch, laat staan slechts gedurende bijvoorbeeld kantooruren.
3. Een probleem kan zich voordoen wanneer de ontvanger over bijvoorbeeld meerdere e-mail adressen beschikt: een kantoor dat voor iedere medewerker een eigen e-mailaansluiting heeft. Het ligt dan op de weg van de ontvanger om de aanbieder specifiek aan te geven voor welke adressen zijn bezwaar geldt.

Artikel 5

1. Aan beoogde wederpartijen moet zo duidelijk en volledig mogelijk inzicht worden verschaft in de transactie die zij overwegen aan te gaan. In het eerste lid van dit artikel is opgesomd hetgeen de aanbieder verplicht is te vermelden. Het gaat er om dat de wederpartij voldoende wordt geïnformeerd, hetgeen deels zal geschieden door het vermelden van de kernbedingen (en wezenlijke voorwaarden) van de transactie, en anderzijds door melding te maken van de toepasselijke algemene voorwaarden, waarvan dan weer op eenvoudige wijze kennis moet kunnen worden genomen (artikel 6). Met het oog op het gegeven dat het in de regel om grensoverschrijdende transacties gaat is de lijst redelijk uitgebreid. Dat is van belang omdat een wederpartij minder makkelijk inlichtingen over bijvoorbeeld de aanbieder kan inwinnen. Het spreekt voor zich dat ter zake van een bepaalde voorgenomen transactie één of meer van de verplicht te vermelden gegevens niet van toepassing kunnen zijn: deze kunnen dan uit de aard der zaak niet worden vermeld. Aan de andere kant draagt de lijst géén limitatief karakter. Het is aan partijen en eventueel de rechter om te beoordelen wat redelijkerwijs had behoren te worden vermeld en dus of sprake is van een wezenlijke omissie en welke gevolgen daaraan moeten worden verbonden.
2. Het gemene verbintenissenrecht geeft voldoende aanknopingspunten voor de beantwoording van de vraag naar de aansprakelijkheid voor de schade die het gevolg is van onjuiste of onvolledige informatie. Hoofddregel is dat de aanbieder jegens de wederpartij aansprakelijk is voor schade die de wederpartij lijdt als gevolg van onjuiste of onvolledige informatie die hij ter zake van een langs elektronische weg gesloten overeenkomst heeft verstrekt. Partijen kunnen in beginsel van deze hoofddregel afwijken door middel van een duidelijk en ondubbelzinnig beding.
3. Wanneer het gaat om beroepsbeoefenaren (zoals advocaten, belastingadviseurs) moet blijkens het derde lid worden vermeld waarbij zij zijn aangesloten of waar zij staan ingeschreven, met een omschrijving van de van toepassing zijnde beroepsregels. Het gaat er niet om dat deze regels in extenso worden besproken, maar wel dat het bestaan daarvan wordt vermeld, met inbegrip van een bestaande klachtprocedure. De bedoeling is dat geen misverstand bestaat over het beroep dat wordt uitgeoefend en dat met name consumenten ervan op de hoogte zijn bij wie zij zich in voorkomend geval kunnen beklagen. De sanctie op overtreding kan bestaan uit het toepassen van bestuursdwang.
4. De aanbieder hoeft de verplichte mededelingen, bedoeld in de eerste drie leden, niet noodzakelijk langs elektronische weg te doen. Weliswaar kan met 'papierwerk' niet dezelfde snelheid van communiceren worden bereikt als wanneer bijvoorbeeld een e-mail wordt verstuurd, maar niets verzet zich ertegen om (ook) traditionele communicatiemiddelen te gebruiken. Zeker in het geval van een meer langdurige relatie

kan het wenselijk worden geacht om in een raam- of basisovereenkomst een aantal afspraken vast te leggen, waarna de individuele transacties langs elektronische weg plaatsvinden. Het is aan de betrokken partijen om te bepalen hoe zij van de gegeven vrijheid gebruik maken: de wet beoogt de mogelijkheden te verruimen en niet te beperken.

5. In het vierde lid is vastgelegd dat bij of krachtens staatsbesluit nadere regels ter zake van te verstrekken informatie kunnen worden gegeven. Omdat niet is te voorzien of het derde lid mogelijk een te verstrekkende bepaling is of overbodig voor sommige categorieën beroepsbeoefenaren, is de mogelijkheid van ontheffing opgenomen. Het gaat daarbij niet om ontheffing ten behoeve van *individuele* beroepsbeoefenaren.
6. In het vijfde lid zijn regels gesteld ten aanzien van de 'lokkertjes' waarvan een aanbieder zich kan bedienen. Het wordt wenselijk geacht dat de voorwaarden om voor kortingen, premies en geschenken in aanmerking te komen precies en duidelijk worden vermeld, bijvoorbeeld dat een bepaalde korting alleen wordt gegeven wanneer een bepaald aantal producten wordt gekocht. Deze bepaling beoogt in de eerste plaats consumenten te beschermen.

Artikel 6

1. Het is van belang dat de wederpartij de voorwaarden waarmee hij zich akkoord verklaart zelf kan opslaan op een voor hem makkelijk toegankelijke wijze dan wel deze schriftelijk van de aanbieder van commerciële communicatie ontvangt (lid 1). De aanbieder is verplicht ervoor te zorgen dat deze voorwaarden zodanig worden opgeslagen dat de wederpartij deze eenvoudig digitaal kan kopiëren dan wel om voor schriftelijke toezending zorg te dragen.
2. De kans op fouten bij e-commerce activiteiten is groter dan bij bijvoorbeeld transacties die in een winkel plaatsvinden: wie virtueel boodschappen doet ziet niet of in de regel minder makkelijk wat hij in zijn 'karretje' heeft liggen, dan degene die met zijn karretje in de supermarkt rondloopt. Bovendien druk je makkelijk een keer teveel op de muisknop. Wanneer de mogelijkheid op herkenning en herstel van fouten niet wordt geboden, en er is sprake van een fout, is de overeenkomst vernietigbaar. De aanbieder van commerciële communicatie staan immers in de regel de technische voorzieningen ter beschikking om een eenvoudige terugkoppeling mogelijk te maken en hij kan daar bij de inrichting van zijn webpages reeds rekening mee houden.

Artikel 7

1. Een bericht kan in een elektronische omgeving makkelijker worden gemanipuleerd dan in een 'papieren' omgeving, omdat in een elektronische omgeving de gegevens en de drager van de gegevens niet onlosmakelijk met elkaar zijn verbonden. In de elektronische omgeving is het des te belangrijker de identiteit van de afzender en de juistheid van het bericht te kunnen vaststellen. Daartoe kunnen organisatorische, technische en juridische beveiligingsmethoden worden toegepast.
2. Er is vanaf gezien het begrip elektronische (of: digitale) handtekening wettelijk te omschrijven. Het gaat om een langs elektronische weg verstuurd identificatie van de afzender: de ontvanger kan verifiëren dat de informatie van de verzender afkomstig is én dat de inhoud tijdens de verzending niet is veranderd. Deze identificatie vindt (thans) plaats met behulp van zogeheten certificatedienstverleners: op betrouwbaarheid getoetste derden.
3. Een schriftelijke handtekening heeft verschillende functies: identificatie (uniek aan één persoon gebonden), authenticiteit van de handtekening (de onmogelijkheid om de eigen

handtekening te kunnen ontkennen), wilsuiking van de betrokkene, autorisatie van een rechtshandeling, toerekening van een verklaring aan de betrokkene, kennisneming van de inhoud van een document (aangenomen mag worden dat de ondertekenaar de inhoud kent als hij het heeft ondertekend), integriteit en compleetheid van een document (door ondertekening wordt enige garantie gegeven dat er geen gegevens zijn toegevoegd of verwijderd; vergelijk het paraferen), authenticatie van het geschrift (met het zetten van een handtekening benadrukt de ondertekenaar de echtheid van het geschrift), vaststellen origineel (ter onderscheiding van een kopie) en een waarschuwingfunctie (degene die zijn handtekening plaatst, weet dat hij zich bindt). Een elektronische handtekening kan niet al deze functies op dezelfde wijze vervullen: daarvoor zijn aanvullende hulpmiddelen en procedures nodig.

4. Strikt genomen is een digitale handtekening een species van de elektronische handtekening. Tot de elektronische handtekeningen behoren in de praktijk immers ook gescande handtekeningen en biometrische identificatiemethoden zoals gescande oogirissen en vingerafdrukken. Deze gescande 'handtekeningen' kunnen zelf ook weer langs elektronische weg worden verstuurd. In de wet is van een ruim begrip elektronische handtekening uitgegaan.
5. Het verschil tussen een schriftelijke en een elektronische handtekening zal zich met name bij de ontkenning daarvan doen gevoelen. Een schriftelijke handtekening is een weergave van het handschrift van de ondertekenaar en een eigen persoonlijke creatieve uiting van de betreffende persoon. Bij de ontkenning van een schriftelijke handtekening zal de betrokkene doorgaans stellen dat het niet om zijn handtekening gaat. Bij een elektronische handtekening zal deze ontkenning veelal niet plaatsvinden, maar zal de betrokkene stellen dat deze handtekening niet door of in zijn opdracht is gebruikt maar door een onbevoegde. De bepaling van de authenticiteit van een handtekening in een digitale omgeving dient dus te worden opgesplitst in enerzijds de vaststelling van de echtheid en anderzijds de vaststelling of de handtekening door of namens de betrokkene is gebruikt. Wie dient te bewijzen dat een elektronische handtekening onbevoegd is gezet? In de regel zal dat de betrokkene zijn, omdat hem de (technische) mogelijkheden ter beschikking staan om misbruik te voorkomen en dus te waarborgen dat de wederpartij te goeder trouw erop mag afgaan dat de handtekening door een bevoegde persoon is gebruikt. De elektronische handtekening moet dan wel zodanig persoonsgebonden zijn dat deze niet ook door de ontvanger van het bericht zelf kan worden gebruikt.
6. De elektronische handtekening en het gebruik van cryptografische technieken ('public key' in dit geval) zijn met elkaar verbonden. Er wordt gebruik gemaakt van zogeheten 'trusted third parties' (TTP), waartoe ook de Surinaamse notarissen naar verwachting zullen gaan behoren, en van digitale certificaten. Deze certificaten kunnen onder andere voor identificatie worden gebruikt: ze koppelen de identiteit van de gebruiker aan een publieke encryptiesleutel. Deze certificaten lijken enigszins op 'access cards' zoals bedrijven en overheden die soms gebruiken en waarmee toegang tot bepaalde afdelingen of ruimtes kan worden verkregen. Het is minder juist ze als een 'digitaal paspoort' of 'digitaal rijbewijs' te beschouwen.
7. Digitale of elektronische handtekeningen vloeien voort uit 'public key' cryptografie. Daarbij wordt gebruik gemaakt van sleutelparen. De *publieke* sleutel wordt aan andere gebruikers beschikbaar gemaakt in een publiek domein (bijvoorbeeld internet). De *private* sleutel blijft in het bezit van de gebruiker. Deze twee sleutels vormen het publiek/privaat sleutelpaar. De publieke sleutel kan gebruikt worden om berichten te versleutelen die vervolgens alleen met de private sleutel kunnen worden ontcijferd. De private sleutel kan worden gebruikt om berichten te versleutelen die vervolgens alleen met

- de publieke sleutel kunnen worden ontcijferd.
8. Bij elektronische handtekeningen wordt met een zogeheten hashfunctie gewerkt. Technisch gesproken is de definitie van een hashfunctie: een transformatieproces waarbij een input m van variabele lengte wordt omgezet in een waarde van vaste lengte, de hashwaarde h . De hashfunctie is een methode om een document van willekeurige lengte op een kortere manier weer te geven. Deze kortere weergave heeft altijd dezelfde lengte, ongeacht de grootte van het originele document. Hashfuncties hebben twee unieke eigenschappen waardoor ze geschikt zijn voor het gebruik van cryptografie. Ten eerste is een hashwaarde een numerieke weergave van een document. Ten tweede is het proces 'eenrichtingsverkeer'. Deze eigenschappen hebben tot gevolg dat er geen informatie uit de hashwaarde is af te leiden met betrekking tot de inhoud van het originele document, en dat het niet mogelijk is het originele document vanuit de hashwaarde te herleiden.
 9. Het gebruik van een hashwaarde in cryptografie stelt de verzender van een bericht in staat om eerst de hashwaarde van het bericht te berekenen en deze vervolgens samen met het bericht aan de ontvanger te versturen. Wanneer de ontvanger het bericht ontvangt, kan deze met dezelfde hash algoritme opnieuw de hashwaarde van het document berekenen en deze waarde vergelijken met de meegezonden hashwaarde. Indien de twee waarden identiek zijn, kan de ontvanger er zeker van zijn dat het ontvangen document gelijk is aan het verzonden document.
 10. Er kan niet alleen op de hashwaarde worden vertrouwd om de inhoud van een bericht te garanderen. Als een 'elektronische af luisteraar' het document en de hashwaarde zou onderscheppen, kan het document veranderd, opnieuw gehashed en doorgezonden worden. De ontvanger zal dan niet weten dat de inhoud van het bericht is gewijzigd. Het gehele pakket (document en hashwaarde) zou met behulp van public key cryptografie kunnen worden versleuteld, waardoor de identiteit van de afzender wordt gegarandeerd, maar dat kost onacceptabel veel tijd.
 11. De elektronische handtekening is een zeker zo veilige methode voor het garanderen van de inhoud en identiteit. Een elektronische handtekening is de hashwaarde van het originele document, dat is gecijferd met de private sleutel van de afzender. Door de elektronische handtekening aan het originele document toe te voegen, kan de ontvanger verifiëren dat het document van de verzender afkomstig is én dat de inhoud tijdens de verzending niet is veranderd.
 12. Een hoge mate van betrouwbaarheid van de elektronische handtekening betekent overigens niet 100% betrouwbaarheid, maar dat geldt evenzeer in een 'papieren' omgeving. De mate waarin betrouwbaarheid nodig is zal in de praktijk afhankelijk zijn van de aard en/of omvang van de transactie. Naarmate de transacties gevoeliger zijn zullen de betrokken partijen meer aan allerlei soorten bescherming moeten doen, bijvoorbeeld electronic monitoring (het volgen van processen en handelingen), time stamping (zekerheid over het tijdstip waarop informatie is verwerkt), firewall (toegangsbeveiliging), EDP-audit (Electronic Data Processing), cryptografie, certificatie, call back-procedure (de verzendende computer maakt contact met de ontvangende computer, identificeert zich en verbreekt de verbinding, waarna de ontvangende computer terugbelt), enzovoort (P. Kolkman en R. van Kralingen, *Verschuivend vertrouwen. Methoden voor het waarborgen van betrouwbaarheid in het elektronische rechtsverkeer*, IteR reeks, nr. 12, 1998, blz. 205-289).
 13. De onderhavige ontwerpwet beoogt duidelijkheid te verschaffen door aan elektronische handtekeningen niet de rechtskracht te ontfemen en door het gebruik daarvan te vergemakkelijken. Deze erkenning strekt zich ook uit tot bepaalde certificaten en certificatedienstverleners. Het is nog niet duidelijk hoe de elektronische handtekening

zich zal ontwikkelen. Evenmin staat de noodzaak vast om gebruikers te verplichten in relatie tot bijvoorbeeld consumenten van een certificatedienstverlener gebruik te maken. De wettelijke regeling is daarom globaal van opzet.

14. In het eerste lid van artikel 7 wordt de term 'rechtskracht' van een elektronische handtekening gebruikt. Daarmee wordt tot uitdrukking gebracht dat aan een elektronische handtekening rechtens dezelfde gevolgen verbonden kunnen zijn als aan een schriftelijke handtekening.
15. In Suriname bestaat een open systeem van bewijsmiddelen, zodat een elektronische handtekening reeds nu als bewijsmiddel in een procedure kan worden gebruikt. Mogelijke misverstanden hierover zijn met de wet uit de wereld geholpen. Het wordt in dit stadium niet nodig geacht de vrije waardering van het bewijs door de rechter te sturen of te beperken. Van geval tot geval zal de betrokken rechter de concrete feiten en omstandigheden in zijn onderzoek en oordeel moeten betrekken, en nagaan op wie de bewijslast en het bewijsrisico van de echtheid van een elektronische handtekening rusten (vgl. HR 19 november 1993, NJ 1994, 622 inzake COVA). Bij belangrijke transacties doen partijen er verstandig aan een overeenkomst langs elektronische weg bij een onafhankelijke derde (Trusted Third Party) in bewaring te geven, bij wie ingeval een geschil rijst een (gewaarmerkt) elektronisch afschrift kan worden verkregen.
16. Evenals bij iedere andere vorm van identificatie is een (digitaal) certificaat zo betrouwbaar als de autoriteit en procedures die daar achter staan. Een rijbewijs heeft daardoor een ander karakter dan een bibliotheekpas. Met een rijbewijs garandeert de overheid als betrouwbare 'derde partij' dat die informatie juist en waar is. Bij 'digitale' certificaten verzorgen certificatedienstverleners deze verificatie. Iedere natuurlijke persoon of rechtspersoon kan certificatedienstverlener worden wanneer deze wil instaan voor de identiteit van degenen aan wie hij een digitaal certificaat uitgeeft: een bedrijf voor zijn werknemers, de universiteit voor zijn studenten, enz. Om wildgroei te voorkomen zijn in de wet een aantal waarborgen opgenomen. Zo zal een (digitaal) certificaat voor bewijsdoeleinden kunnen worden erkend wanneer de certificatedienstverlener die het heeft afgegeven aan bepaalde -bij staatsbesluit te stellen- voorschriften voldoet dan wel een zodanige certificatedienstverlener zich borg stelt voor een door een ander afgegeven certificaat (lid 2).

Artikel 8

1. Een dienstenaanbieder (service provider) is niet aansprakelijk wanneer hij slechts 'doorgeefluik' van informatie is. Wel is hij blijkens het tweede lid gehouden informatie te verwijderen of de toegang daartoe onmogelijk te maken wanneer dat door of namens de Minister wordt gelast, alsmede wanneer het hem duidelijk moet zijn dat de informatie onwettig is of onwettige activiteiten betreft. Wat dit laatste betreft rust op de dienstenaanbieder geen eigen of actieve onderzoeksplicht. Onwettig is bijvoorbeeld een auteursrechtinbreuk of een webpage die oproept tot rassendiscriminatie.
2. In het tweede lid wordt de Minister de mogelijkheid gegeven om de verwijdering van informatie te gelasten en/of de toegang daartoe te verbieden onder de in het derde lid genoemde beperkingen. Dit instrument is uitdrukkelijk niet als politiek instrument bedoeld, maar beoogt evident kwalijke praktijken tegen te gaan. Dat betekent dat een tot oordelen geroepen rechter niet kan volstaan met een marginale toetsing, maar de rechten doelmatigheid ten volle moet toetsen. Het instrument mag bijvoorbeeld niet worden gebruikt voor het weren van politiek onwelgevallige informatie of erotisch getinte informatie. Aan laatstgenoemde uitingen kunnen uiteraard zekere beperkingen worden verbonden die zoveel mogelijk moeten waarborgen dat deze informatie niet ongevraagd

wordt toegezonden, of die de toegankelijkheid voor bijvoorbeeld minderjarigen beperken.

3. De dienstenaanbieder die zelf weet krijgt van onwettige informatie of activiteiten is gehouden de informatie te verwijderen of ontoegankelijk te maken (lid 2). Voor de dienstenaanbieder zal het niet altijd eenvoudig zijn vast te stellen of van onwettige activiteiten of informatie sprake is. Bij twijfel moet hij de strijdende partijen naar de rechter verwijzen. Hij kan natuurlijk ook de Minister vragen of er grond voor een aanwijzing bestaat.
4. De mogelijkheid van ontoegankelijk maken zal als eerste stap voor hem in de regel de meest veilige zijn, omdat aan het op eigen initiatief overgaan tot verwijdering grotere risico's kleven. Vanwege zijn contractuele verplichtingen zal de dienstenaanbieder er in de regel bovendien verstandig aan doen om de houder van de website van zijn voornemen in kennis te stellen. Vanzelfsprekend doet de dienstenaanbieder er verstandig aan de mogelijkheid van eigenmachtig afsluiten of ontoegankelijk maken van de webpage in zijn algemene voorwaarden adequaat te regelen. In het algemeen bestaat voor de dienstenaanbieder niet de verplichting om de naam en adresgegevens van de betreffende site houder bekend te maken, hetgeen immers een schending van de privacy zou kunnen betekenen. Bij twijfel kan hij het op een kort geding laten aankomen: wordt hij veroordeeld deze gegevens te verstrekken, dan doet hij zulks op grond van een rechterlijk bevel, zodat hem geen schending van de privacy kan worden verweten.

Artikel 9

1. Gelet op de rol van certificatie dienstverleners en (digitale) certificaten, is het noodzakelijk de aansprakelijkheid van certificatie dienstverleners wettelijk te regelen. Een wettelijke regeling is nodig omdat niet alleen de relatie tussen de certificatie dienstverlener en diens opdrachtgever aan de orde is, maar ook belangen van derden (waaronder consumenten) in het spel zijn. Juist deze derden zullen op het opgewekte vertrouwen afgaan en aan hen moet een meer toegesneden instrument dan het reguliere leerstuk van de onrechtmatige daad ter beschikking staan. Met dit artikel staat vast dat het belang van deze derden een rechtens te beschermen belang is en dat zij niet afzonderlijk behoeven aan te tonen dat aan het relativiteitsvereiste is voldaan.
2. Op de certificatie dienstverlener rust de bewijslast: hij moet aantonen niet nalatig te zijn geweest. Op dit punt voldoet de derde derhalve aan zijn stelplicht wanneer hij deze nalatigheid stelt dan wel wanneer deze uit zijn stellingen voortvloeit.
3. De certificatie dienstverlener is niet aansprakelijk voor in het digitale certificaat opgenomen beperkingen die voor derden kenbaar zijn (lid 3). Een beperking kan bijvoorbeeld ook gelegen zijn in het maximum bedrag dat met de overeenkomst waarvoor het certificaat wordt gebruikt gemoeid mag zijn.

Artikel 10

Het is noodzakelijk persoonsgegevens te beschermen en misbruik daarvan zoveel mogelijk te voorkomen. In het ontwerp is dan ook een verbod opgenomen om persoonsgegevens zonder toestemming van de betrokkene aan derden te verstrekken. Deze bepaling kan eventueel te zijner tijd vervallen wanneer een afzonderlijke wet inzake privacy in werking treedt.

Artikel 11

Het is wenselijk om wettelijk vast te leggen dat vertrouwelijke informatie ook als zodanig moet worden behandeld. Deze bepaling is niet beperkt tot bijvoorbeeld

creditcard gegevens, maar heeft een zeer brede strekking.

Artikel 12

De encryptie is bij de toelichting op artikel 7 al aan de orde gekomen. Denkbaar is dat bij staatsbesluit het verplichte gebruik van cryptografische technieken in bepaalde gevallen wordt voorgeschreven, bijvoorbeeld ter zake van persoonsgebonden gegevens (creditcard gegevens). In het algemeen schept encryptie de mogelijkheid om belangrijke of gevoelige informatie tijdens het transport over publieke netwerken, zoals internet, te beschermen. Misbruik daarvan moet zoveel mogelijk worden bestreden. Bij staatsbesluit kunnen daartoe wenselijk geachte regels worden gegeven.

Artikel 13

1. Er bestaat behoefte aan efficiënte, snelle en relatief goedkope geschillenbeslechting, bij voorkeur buiten de burgerlijke rechter om. Deze buitengerechtelijke geschillenbeslechting moet voldoen aan de beginselen van onafhankelijkheid, transparantie, hoor en wederhoor, doeltreffendheid van de procedure, wettigheid van de beslissing, vrijheid van de partijen en de mogelijkheid tot vertegenwoordiging en (zodanig onder bepaalde voorwaarden) van hoger beroep. Het kan gaan om arbitrage of bindend advies: het eerste is een vorm van rechtspraak, het tweede leidt tot een uitspraak die tussen partijen de kracht van een overeenkomst heeft, waarvan de nakoming zodanig via de burgerlijke rechter (al dan niet in kort geding) moet worden afgedwongen. Nadat is onderzocht of en op welke wijze deze vorm van geschillenbeslechting in het leven moet worden geroepen, kan dat relatief eenvoudig door middel van een staatsbesluit, houdende algemene maatregelen (lid 1). Er zou ook een eventueel reeds bestaand orgaan voor buitengerechtelijke geschillenbeslechting kunnen worden aangewezen.
2. Partijen kunnen zich voor de beslechting van hun geschillen onderwerpen aan het college als in het eerste lid bedoeld, wanneer deze geschillen betrekking hebben op commerciële communicatie, overeenkomsten langs elektronische weg (met inbegrip van de precontractuele fase, de uitvoering van de transactie en leerstukken als dwang, dwaling, bedrog en misbruik van omstandigheden), aansprakelijkheid van de dienstenverlener, bescherming van de vertrouwelijkheid en privacy, alsmede certificaten en (aansprakelijkheid van) certificatedienstverleners (lid 2). Partijen kunnen vooraf, al dan niet in toepasselijke algemene voorwaarden, maar ook nadat een geschil is gerezen, overeenkomen de weg van buitengerechtelijke geschillenbeslechting te bewandelen. Het is dus aan partijen of zij van deze mogelijkheid gebruik willen maken.
3. Het college zal, evenals een burgerlijke rechter, het op het geschil van toepassing zijnde recht moeten vaststellen. De in dit artikel bedoelde mogelijkheden van buitengerechtelijke geschillenbeslechting laten de bevoegdheid van de burgerlijke rechter om in kort geding desgevraagd voorlopige voorzieningen te treffen onverlet.
4. Bij staatsbesluit kunnen andere categorieën van geschillen worden aangewezen waarvan de beslechting buitengerechtelijk zou kunnen plaatsvinden (lid 3). Het kan allerhande met e-commerce samenhangende onderwerpen betreffen: geschillen over het ter beschikking gestelde netwerk, geschillen met access providers, geschillen op het terrein van intellectuele eigendomsrechten (voor zover die er niet reeds nu onder vallen), enzovoort.

Artikelen 14 en 15

Deze bepalingen hebben betrekking op het toezicht op de naleving van het bepaalde bij of krachtens deze wet. Hoewel ter zake van grote delen van het internet sprake is van

zelfregulering is het gewenst daarnaast ten behoeve van het algemeen belang te beschikken over adequaat toezicht op de naleving van de onderhavige wetgeving. In artikel 14, eerste lid, wordt bepaald dat de zorg voor een adequate handhaving van het bepaalde bij of krachtens de onderhavige wet, behoort tot de taak van bij staatsbesluit aangewezen ambtenaren en personen. Voor alle duidelijkheid zij opgemerkt dat het hier steeds gaat om bestuurlijk toezicht op de naleving van het bij of krachtens deze wet bepaalde. De strafrechtelijke handhaving wordt uitgevoerd door opsporingsambtenaren die bij staatsbesluit, krachtens het Wetboek van Strafvordering worden benoemd. De aan opsporingsambtenaren toegekende bevoegdheden die verder gaan dan die van de toezichthouders, zijn ook opgenomen in voornoemd wetboek. Artikelen 14, tweede en derde lid, regelt de bevoegdheden van de toezichthouders.

Artikel 16

Gelet op het specialistische karakter van de onderwerpelijke materie is het gewenst dat naast de reguliere politie ook opsporingstaken kunnen worden uitgevoerd door speciaal daarvoor opgeleide personen die daartoe als bijzondere opsporingsambtenaar kunnen worden aangewezen. Artikel 16 strekt ertoe zulks mogelijk te maken.

Artikelen 17 tot en met 29

1. Deze artikelen bevatten bestuurlijke sanctiemiddelen die kunnen worden toegepast bij het handelen in strijd met het bij of krachtens deze wet bepaalde. De onderhavige ontwerp-wet kent de volgende bestuurlijke sanctiemiddelen:
 - *Bestuursdwang*. De Minister kan vorderen dat de overtreder van een bij of krachtens de onderhavige wet gesteld verbod een bepaalde activiteit terugdraait of alsnog verricht. Het nadeel van dit middel is echter in de praktijk dat de kosten vaak niet zijn te verhalen op de overtreder omdat deze daartoe financieel niet in staat is. De Minister ziet zich dan gesteld voor gemaakte kosten die ten laste van de overheidsfinanciën blijven. Dat maakt de animo om dit middel toe te passen er niet groter op.
 - *Dwangsom*. Aantrekkelijker dan het tegenhouden of stopzetten van een activiteit of de toepassing van bestuursdwang is het middel van de bestuurlijke dwangsom. De Minister kan de overtreder van het bij of krachtens de onderhavige wet bepaalde een dwangsom opleggen voor elke dag dat de overtreding voortduurt. De dwangsom wordt per tijdseenheid of per overtreding vastgesteld. Het bestuursorgaan bepaalt de hoogte van de dwangsom. Dit bedrag dient in redelijke overeenstemming te zijn met de ernst van de overtreding. Als er een wanverhouding bestaat tussen de hoogte van de dwangsom en de ernst van de overtreding zal uiteindelijk de rechter moeten bepalen wat redelijk is. Verbeurde dwangsommen komen toe aan de Staat. De dwangsom kan bij dwangbevel worden ingevorderd; de daaraan verbonden kosten komen uiteraard voor rekening van de overtreder.
2. Er zij op gewezen dat het in artikel 26 om een bestuurlijke en niet om een strafrechtelijke dwangsom gaat. Het gaat hier om een eigen sanctiebevoegdheid van het overheidsbestuur die voortvloeit uit zijn bestuurlijke verantwoordelijkheid. Een dergelijke sanctie dient een ander doel dan een strafrechtelijke sanctie. De bedoeling van een bestuurlijke sanctie is dat een einde wordt gemaakt aan een situatie die de wetgever uit een oogpunt van het beschermde belang in de desbetreffende wettelijke regeling onaanvaardbaar acht.

Artikel 30

De Minister kan aan een aanbieder van commerciële communicatie of dienstenaanbieder

een of meer aanwijzingen geven, wanneer dat voor een richtige uitvoering van de wet nodig mocht blijken. In dit laatste ligt een beperking opgesloten. De beginselen van behoorlijk bestuur brengen in de regel mee dat de belanghebbende vooraf van het voornemen op de hoogte wordt gesteld en de gelegenheid krijgt zijn bezwaren naar voren te brengen. Het gaat om een volle toetsing, derhalve zowel om de doel- als de rechtmatigheid.

Artikelen 31 en 32

In deze artikelen is de strafrechtelijke sanctionering van een aantal bepalingen in de ontwerpwet opgenomen. Expliciet is aangegeven wanneer sprake is van een misdrijf en wanneer van een overtreding. Zulks heeft, zoals uit de afzonderlijke bepalingen blijkt, gevolgen voor de maximum strafmaat.

Artikel 33

Het is passend dat evenzeer tot geheimhouding zijn gehouden al diegenen die bij de uitvoering van deze wet zijn betrokken en de beschikking krijgen over vertrouwelijke gegevens, maar niet reeds uit andere hoofde tot een dergelijke geheimhouding zijn verplicht. Artikel 33 strekt ertoe dit in het ontwerp vast te leggen.

Paramaribo, de

R.R. Venetiaan