

3 Algemene normen voor elektronische communicatie met de overheid

3.1 Inleiding

Communicatie tussen burger en overheid is essentieel voor een goed functionerende overheid. Een *recht* op communicatie met de overheid bestaat niet. Dat communicatie plaatsvindt, wordt echter als vanzelfsprekend voorondersteld. Zonder communicatie immers geen contact, en zonder dit contact kan de overheid geen diensten verlenen, belasting heffen of informatie verstrekken, is er geen bestaansrecht voor de overheid. Zonder communicatie kan de burger bijvoorbeeld niet deelnemen aan inspraak, geen aanvragen, klachten of bezwaarschriften indienen. Veel burgers zijn voor allerlei zaken afhankelijk van de overheid, en daar tegenover staat dat de overheid voor het uitvoeren van haar taken afhankelijk is van informatie die zij van burgers krijgt. De wijze waarop communicatie plaatsvindt, is vaak gereguleerd in vormvoorschriften.

In haar rapport gaat de commissie Wallage wel uit van een recht van de burger op communicatie met de overheid. Volgens deze commissie dient de burger te allen tijde contact te kunnen zoeken met de overheid. De burger moet er ook op kunnen vertrouwen dat de overheid snel en adequaat antwoordt. Tevens moet de burger er op kunnen vertrouwen dat de communicatie open, feitelijk juist, begrijpelijk en integer is. Hierbij merkt de commissie op, dit recht op communicatie niet als een formeel in de wet te verankeren recht op te vatten, maar als een politiek-bestuurlijk uitgangspunt voor overheidscommunicatie.¹⁰⁶

De elektronische communicatiemiddelen bieden een vlotte en laagdrempelige wijze van communiceren. Bestuurders en politici maken gebruik van deze middelen om hun profiel te vergroten en contact te kunnen hebben met burgers. Burgers maken hier ook gebruik van. Deze wijze van communiceren is vaak informeel van aard. Maar kunnen burgers, nu politici en bestuurders zich beschikbaar stellen voor deze laagdrempelige en informele wijze van communiceren, ook verwachten dat overheidsorganen in het algemeen op deze wijze te bereiken zijn? En: hoe ver moet de overheid gaan?

Dit hoofdstuk is als volgt opgebouwd: allereerst wordt in paragraaf 3.2 ingegaan op het toepassingsbereik van de regeling in de Algemene wet bestuursrecht (Awb). Vervolgens komen in paragraaf 3.3 de vormvoorschriften schriftelijk en ondertekening aan de orde. Dan wordt in paragraaf 3.4 ingegaan op het begrip nevenschikking, het uitgangspunt van de regeling, en in paragraaf 3.5 het kenbaar maken. Daarbij komt aan de orde wanneer verkeer langs

106 Commissie Wallage, p. 34.

elektronische weg is toegestaan. Aan welke voorwaarden dat verkeer moet voldoen wordt in paragraaf 3.6 beschreven, waarin de nadere eisen worden besproken. De voorwaarde dat het elektronisch verkeer moet voldoen aan de eisen van betrouwbaarheid en vertrouwelijkheid wordt in paragraaf 3.7 besproken. Tenslotte komt het moment waarop, in verband met de termijnen, een elektronisch verzonden bericht als verzonden dan wel als ontvangen wordt beschouwd aan de orde in paragraaf 3.8. Een conclusie volgt ten slotte in paragraaf 3.9, waar de vraag beantwoord kan worden of de normen die van toepassing zijn op elektronische communicatie met de overheid voldoen aan de rechtsstatelijke beginselen.

3.2 Toepassingsbereik

Afdeling 2.3 is op 1 juli 2004 in werking getreden en is aan de Awb toegevoegd om het gebruik van elektronische communicatiemiddelen tussen burger en bestuur te bevorderen, en wettelijke belemmeringen voor elektronische besluitvorming weg te nemen. Dit zonder afbreuk te doen aan waarborgen voor de rechtszekerheid en zorgvuldigheid van de besluitvorming. De essentie van afdeling 2.3 wordt gevormd door drie hoofdvragen: ten eerste wanneer verkeer langs elektronische weg is toegestaan, ten tweede aan welke voorwaarden het verkeer langs elektronische weg moet voldoen, om even betrouwbaar te zijn als conventioneel verkeer en ten slotte de vraag in welke gevallen verkeer langs elektronische weg kan worden gelijkgesteld met andere vormen van verkeer.¹⁰⁷

Afdeling 2.3 is bedoeld om antwoord te geven op vragen als:

- kan een bestuursorgaan zijn besluiten ook in elektronische vorm vastleggen en bekendmaken?
- kan een burger per e-mail een vergunning aanvragen?
- kan een gemeentebestuur een ontwerp-bestemmingsplan ter inzage leggen door het op zijn website te plaatsen?¹⁰⁸

Uit art. 2:13 Awb, waarin staat dat een bericht elektronisch kan worden verzonden, kan worden afgeleid dat elektronisch verkeer in de Awb niet dwingend wordt voorgeschreven. Alleen als van de elektronische weg gebruik wordt gemaakt, dan moeten de bepalingen van afdeling 2.3 in acht worden genomen. Het gaat hier dus om een facultatieve regeling.¹⁰⁹

Art. 2:13 Awb bepaalt dat in het verkeer tussen burgers en bestuursorganen een bericht elektronisch kan worden verzonden, mits de bepalingen van afdeling 2.3

107 *Kamerstukken II* 2001/02, 28 483, nr. 3, p. 2.

108 *Kamerstukken II* 2001/02, 28 483, nr. 3, p. 1.

109 Zie ook over afdeling 2.3 Awb Groothuis 2010.

in acht worden genomen. Ingevolge het tweede lid van art. 2:13 Awb zijn er twee uitzonderingen op deze hoofdregel. De eerste uitzondering is dat bij of krachtens wettelijk voorschrift is bepaald dat art. 2:13, eerste lid, Awb niet van toepassing is. In de uitspraak ‘aanvraag MEP-subsidie’ wordt op deze uitzonderingsgrond ingegaan. Het College van Beroep voor het bedrijfsleven oordeelt ten aanzien van deze uitzonderingsgrond, dat het uitsluiten van de werking van het eerste lid van art. 2:13 Awb uitdrukkelijk dient te geschieden.¹¹⁰

‘Het College overweegt dat uit de Memorie van Toelichting bij afdeling 2.3 valt af te leiden dat het uitsluiten van de werking van het eerste lid van art. 2:13 uitdrukkelijk dient te geschieden. Op p. 27 van de MvT is bij de toelichting op artikel 2:13, tweede lid, Awb sprake van een “verbod” bij de beschrijving van gevallen waarin elektronisch verkeer bij of krachtens de wet is uitgesloten. In de betrokken wet staat bepaald dat een aanvraag wordt ingediend “met gebruikmaking van het origineel van een ondertekend formulier” dat wordt vastgesteld bij ministeriële regeling. Deze Regeling schrijft voor dat een aanvraag wordt ingediend “met gebruikmaking van het origineel van een ondertekend formulier” dat is opgenomen in een bijlage bij de Regeling. Het College is van oordeel dat in beide wettelijke voorschriften niet een uitdrukkelijke bepaling valt te lezen die art. 2:13 Awb, eerste lid, zijn werking ontnemt.’

De tweede uitzondering is dat een vormvoorschrift zich tegen elektronische verzending verzet. Het vormvoorschrift moet dan een functie vervullen die langs de elektronische weg niet te bereiken is, zoals het aanplakken van een bord ‘onbewoonbaar verklaard’ aan een woning.¹¹¹

Voor het toepassingsbereik van afdeling 2.3 is niet van belang of er sprake is van openbare of niet-openbare communicatie. Art. 2:13 Awb spreekt immers van het elektronisch verzenden van berichten in het verkeer tussen burgers en bestuursorganen. Daarbij maakt het niet uit of het verkeer tussen bestuursorgaan en een enkele burger betreft, of verkeer tussen bestuursorgaan en een onbepaald aantal burgers. Omdat dit hoofdstuk de normen uit afdeling 2.3 in het algemeen behandelt, zal het onderscheid tussen openbare en niet-openbare communicatie, zoals besproken in het inleidende hoofdstuk, hier verder niet gemaakt worden.

Plaatsing van de regeling in hoofdstuk 2 van de Awb, Verkeer tussen burgers en bestuursorganen, heeft als gevolg dat de regeling van toepassing is op alle handelingen van bestuursorganen, zoals ook privaatrechtelijke rechtshandelingen of feitelijke handelingen. Afdeling 2.3 is daarom ook van toepassing op andere bestuurshandelingen dan besluiten. Aanvankelijk was de regeling niet van toepassing op het beroep bij de bestuursrechter maar in art.

110 CBB 4 juni 2008, *LJN* BD4039, *JB* 2008, 212, m.nt. M.O.-V. (Aanvraag MEP-subsidie).

111 *Kamerstukken II* 2001/02, 28 438, nr. 3, p. 37-38.

8:40a Awb is, met ingang van 1 juli 2010, afdeling 2.3 van overeenkomstige toepassing op het beroep bij de rechter verklaard. De (Nationale) ombudsman is in art. 1:1, tweede lid, onder f, Awb ook uitgezonderd van het begrip bestuursorgaan. Daarom is in art. 9:21 Awb bepaald dat op verkeer met een ombudsman hoofdstuk 2 van overeenkomstige toepassing is. Afdeling 2.3 is verder niet van toepassing op verkeer met de overige in het tweede lid van artikel 1:1 Awb uitgezonderde overheidsorganen.

3.3 Vormvoorschriften; schriftelijkheidseis en ondertekening

Het uitgangspunt van de wetgever is dat communicatie via de elektronische weg in beginsel gelijkwaardig is aan communicatie via de conventionele, papieren weg, mits zij dezelfde functie kan vervullen. Om te onderzoeken of communicatie via de elektronische weg dezelfde functie kan vervullen als communicatie via de conventionele weg, moet gekeken worden naar vormvoorschriften als de ondertekening, en het begrip schriftelijk. Hierbij moet dan de vraag beantwoord worden welke functies die vormvoorschriften in het conventionele verkeer vervullen, dus waarom zij gesteld zijn, en hoe deze functie in het elektronisch verkeer vervuld kan worden. Voor die functie moet een vervanger gevonden worden, die in het elektronisch verkeer toepasbaar is. De memorie van toelichting gebruikt hier de term functionele equivalenten.¹¹²

3.3.1 Het schriftelijkheidsvereiste

Ten eerste het *schriftelijkheidsvereiste*. Welke functies heeft het schriftelijkheidsvereiste? Het schriftelijkheidsvereiste in de Awb valt blijkens de memorie van toelichting onder te verdelen in drie aspecten:

- het duidelijk maken wat tot uitdrukking wordt gebracht (communicatiefunctie);
- het vastleggen wat tot uitdrukking wordt gebracht (bewijsfunctie);
- het maken van onderscheid met mondelinge handelingen (afbakingsfunctie).¹¹³

Wanneer deze functies even goed of beter via elektronische communicatie vervuld kunnen worden, is de elektronische weg een functioneel equivalent van de conventionele weg. Wanneer deze functies niet door elektronische communicatie vervuld kunnen worden, doet de elektronische weg afbreuk aan

112 *Kamerstukken II* 2001/02, 28 483, nr. 3, p. 7.

113 *Kamerstukken II* 2001/02, 28 483, nr. 3, p. 7.

de functie van het schriftelijkheidsvereiste. Het ligt dan niet voor de hand de elektronische weg toe te staan.

Een belangrijke eerste vraag is wat onder ‘schriftelijk’ verstaan moet worden. Aanvankelijk wilde de wetgever alles waar ‘schriftelijk’ stond, aanvullen met ‘of elektronisch vastgelegd’. Uiteindelijk is echter gekozen voor een ruime, dynamische uitleg van het begrip schriftelijk. Daarbij wordt aangesloten bij een MDW-rapport waarbij als definitie van geschrift wordt gegeven: ‘iedere drager van verstaanbare leestekens die (in onderling verband) een gedachteninhoud vertolken. Irrelevant is op welk materiaal deze leestekens zijn aangebracht. Eveneens is het irrelevant of die leestekens bestaan in ons welbekende karakters dan wel in Chinese, in stenografische of in eigen gevormd geheimschrift.’¹¹⁴ Schriftelijk kan dan ook worden opgevat als: weergave door middel van schrifttekens, ongeacht wat de drager van de schrifttekens is. De drager van die schrifttekens kan papier zijn, maar dus ook een diskette, de harde schijf van een computer of een andere elektronische informatiedrager.¹¹⁵

De elektronische wijze van communicatie moet dus evenals de conventionele wijze voldoen aan de communicatiefunctie, de bewijsfunctie en de afbakeningsfunctie. Deze laatste, de afbakeningsfunctie, is echter geen functie van het schriftelijkheidsvereiste, maar een eigenschap daarvan. De eis dat een bepaalde vorm van communiceren schriftelijk plaatsvindt (bijvoorbeeld het nemen van besluiten door een bestuursorgaan), wordt gesteld om de over te brengen boodschap duidelijk te maken en om deze boodschap vast te leggen. Dit wordt door de wetgever aangeduid als de communicatie- en bewijsfunctie. Doordat de boodschap schriftelijk is vastgelegd, onderscheidt deze zich van mondelinge communicatie. Dit is een onderscheidend kenmerk van deze vorm van communicatie en daarmee een eigenschap en geen functie. Bij de beoordeling of een bepaalde vorm van elektronische communicatie functioneel equivalent is, speelt de door de wetgever genoemde afbakeningsfunctie geen rol.

De bewijsfunctie, het vastleggen wat tot uitdrukking wordt gebracht, is in de elektronische context anders dan in een conventionele, schriftelijke situatie. Een boodschap die elektronisch wordt overgebracht, bestaat uit series van bits (bitstring). Een daarbij geleverde codering geeft aan in welke context de bits een betekenis krijgen.¹¹⁶ Bits kunnen in verschillende contexten een andere betekenis krijgen. Zelfs in dezelfde context kunnen bits een andere betekenis krijgen. Vastleggen wat tot uitdrukking moet worden gebracht, is in de

114 MDW-Rapport Hulst, p. 8.

115 *Kamerstukken I 2003/04*, 28 483, C p. 1.

116 Open een PDF bestand met het programma Word: er ontstaat een onleesbaar document. Open hetzelfde PDF bestand met het programma Acrobat Reader: er ontstaat een afbeelding die de weergave van de ‘werkelijke inhoud’ van het bestand bevat. Het hangt dus af van de interpretatie van de bits, of een elektronisch overgebrachte boodschap leesbaar is.

elektronische context dan ook geen functie van het schriftelijkheidvereiste. Dit is meer een functie van de elektronische handtekening, die hierna besproken wordt. Hoewel een elektronische handtekening nog niks zegt over de vraag met welk programma je het document moet openen. Wel garandeert de elektronische handtekening dat het document niet veranderd is. De bewijsfunctie kan bij elektronische communicatie, zonder gekwalificeerde elektronische handtekening, dan ook niet gewaarborgd worden. Bij het beoordelen of een bepaalde vorm van elektronische communicatie functioneel equivalent is van de conventionele schriftelijke, speelt de bewijsfunctie dan ook geen rol.

Dan blijft over als functie van het schriftelijkheidsvereiste de communicatiefunctie, het duidelijk maken wat tot uitdrukking moet worden gebracht. In een uitspraak van de rechtbank Zwolle, waar de rechtbank de vraag moest beantwoorden of een e-mailbericht een schriftelijke beëindiging van een arbeidsovereenkomst is als bedoeld in art. 16, derde lid, onder c, van de WW, oordeelde de rechtbank dat het e-mailbericht met de volgende inhoud: "Gisteren is de definitieve vaststellingsovereenkomst (inclusief de door u gewenste aanpassingen) per gewone post aan u toegestuurd.", niet anders kan worden opgevat als een akkoordverklaring van de werkgever met de door eiser voorgestelde wijzigingen. Derhalve is naar het oordeel van de rechtbank op dat moment een overeenkomst tussen partijen tot stand gekomen waarbij de arbeidsovereenkomst van eiser, onder de door eiser geamendeerde voorwaarden, is beëindigd. Nu, zoals gezegd, onder een schriftelijke overeengekomen beëindiging in de zin van artikel 16, derde lid, onder c van de Werkloosheidswet ook dient te worden begrepen een beëindiging per e-mail, heeft eiser zich terecht op het standpunt gesteld dat op dat moment de fictieve opzegtermijn een aanvang heeft genomen.¹¹⁷ Verder oordeelt de rechtbank:

‘Voor zover verweerder bedoeld zou hebben meer in het algemeen te stellen dat aan een beëindiging van een arbeidsovereenkomst per e-mail bepaalde eisen zouden moeten worden gesteld merkt de rechtbank op dat in het onderhavige geval niet gebleken is dat er aanleiding zou kunnen zijn om te twijfelen aan de intenties van eiser en zijn werkgever, zoals naar voren komend uit de e-mailcorrespondentie, de authenticiteit van de overgelegde e-mails.’

De rechtbank lijkt hier, hoewel niet met zoveel woorden, aan te sluiten bij de communicatiefunctie van het schriftelijkheidsvereiste: wordt duidelijk wat tot uitdrukking moet worden gebracht. Daar is in dit geval sprake van, de e-mailwisseling tussen eiser en zijn voormalig werkgever leidde tot een resultaat waar beide partijen mee in konden stemmen. Het moment van overeenstemming in de e-mailwisseling was volgens de rechtbank het moment waarop de overeenkomst tot stand kwam en niet het (drie weken latere) moment waarop de

117 Rb. Zwolle 24 maart 2009, LJN BH7555 (Beëindigen arbeidsovereenkomst per e-mailbericht).

overeenkomst door beide partijen getekend werd. De rechtbank oordeelt dat er geen reden is te twijfelen aan de authenticiteit van de e-mailberichten en wijdt geen overwegingen aan het al dan niet ontbreken van een elektronische handtekening. Overigens wordt de geldigheid van deze per e-mailcorrespondentie tot stand gekomen overeenkomst niet door een van de partijen bij de overeenkomst aangevochten, maar door het UWV.

Het lijkt er dan ook op dat het vormvoorschrift ‘schriftelijk’ materieel kan worden ingevuld: wat is de bedoeling geweest van de partijen en kon die bedoeling door het elektronische communicatiemiddel verwezenlijkt worden. De hier boven besproken uitspraak is daar een illustratie van. Zolang partijen zelf de betrouwbaarheid, vertrouwelijkheid en authenticiteit van het bericht niet betwisten, is er voor de rechter geen reden om dit wel te doen. Het vormvoorschrift schriftelijk kan dan materieel worden ingevuld, en de rechter toetst dit niet ambtshalve.

De communicatiefunctie is daarmee geschikt om te kunnen beoordelen of een elektronische boodschap functioneel equivalent is aan de conventionele, schriftelijke wijze van communiceren. Communiceren door middel van een elektronische boodschap op dragerniveau, zonder context, is niet goed mogelijk. Er ontstaat immers pas een leesbaar bericht, indien de elektronische boodschap vergezeld gaat van een code, waaruit blijkt in welke context de boodschap gelezen kan worden. Zoals hierboven besproken, levert een elektronische boodschap op dragerniveau een onleesbare rij bits op. Wil een elektronische boodschap leesbaar zijn, dan is daarvoor niet alleen een drager met schrifttekens vereist (zoals in de conventionele situatie papier met schrifttekens), maar is ook vereist dat de boodschap de benodigde codering bevat, die duidelijk maakt in welke context de boodschap gelezen kan worden.¹¹⁸

Daarom wordt in dit onderzoek uitgegaan van de volgende uitleg van het begrip schriftelijk: een elektronisch bericht is functioneel equivalent van een conventionele, papieren boodschap, wanneer door middel van de gebruikte tekens de bedoelde boodschap overgebracht kan worden, en de gebruikte tekens met codering in alle omstandigheden een gelijkwaardig weergave door middel van schrifttekens oplevert.

3.3.2 De ondertekening

Ten tweede de *ondertekening*. Welke functies vervult, blijktens de memorie van toelichting, het vormvereiste van ondertekening?

De functies van een ondertekening zijn:

- de identificatie van de afzender van het bericht;

118 Een dergelijke codering kan een .doc extensie zijn, waarmee duidelijk gemaakt wordt dat de boodschap moet worden gelezen in het programma Word.

- de blijk van instemming met de inhoud van het bericht;
- het bieden van een waarborg tegen overhaast optreden.¹¹⁹

Om ook in een elektronische omgeving rechtsgeldig van handtekeningen gebruik te kunnen maken, is regelgeving ontwikkeld. De Nederlandse regelgeving vloeit voort uit Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999, betreffende een gemeenschappelijk kader voor elektronische handtekeningen. Deze richtlijn is geïmplementeerd in het Burgerlijk Wetboek en in de Telecommunicatiewet. Via de schakelbepaling art. 3:15c BW en de uitwerking daarvan in art. 2:16 Awb is de regeling uit het BW ook van toepassing binnen het bestuursrecht. In art. 2:16 Awb is bepaald dat de artikelen 15a, tweede tot en met zesde lid, en 15b van Boek 3 van het Burgerlijk Wetboek van overeenkomstige toepassing zijn.

Art. 2:16 Awb strekt ertoe de elektronische handtekening gelijk te stellen met de handgeschreven handtekening. Het artikel bepaalt namelijk dat aan het vereiste van ondertekening is voldaan door een elektronische handtekening, indien de methode die daarbij voor authenticatie is gebruikt, voldoende betrouwbaar is, gelet op de aard en de inhoud van het elektronische bericht en het doel waarvoor het wordt gebruikt.¹²⁰

Aan de hierboven genoemde functies (de identificatie van de afzender van het bericht, de blijk van instemming met de inhoud van het bericht en het bieden van een waarborg tegen overhaast optreden) wordt geacht te zijn voldaan indien een bericht met een elektronische handtekening is ondertekend. In elk geval blijkt uit deze functies dat de handtekening dient om de identiteit van de betrokkene of van het bericht vast te stellen. Authenticatie kan dan ook als een functie van de handtekening wordt beschouwd. Bij de twee andere door de wetgever aangeduide functies van een handtekening, de blijk van instemming en het bieden van een waarborg tegen overhaast optreden, is het maar de vraag in hoeverre deze functies door een elektronische handtekening worden gewaarborgd. Een elektronische handtekening wordt uiteindelijk door een apparaat geplaatst. Dit kan ook volledig automatisch, zonder medeweten van de 'eigenaar' van de handtekening gebeuren.

In de elektronische communicatie strekt de handtekening ook om te waarborgen dat het bericht gedurende de verzending niet gewijzigd is. Deze bewijsfunctie, het vastleggen wat tot uitdrukking moet worden gebracht, werd

119 *Kamerstukken II* 2001/02, 28 483, nr. 3, p. 8.

120 De termen authenticatie en authentificatie betekenen hetzelfde. Het begrip authenticatie wordt het meest gebruikt en staat in de Van Dale. Het begrip authentificatie wordt door de wetgever gebruikt, staat echter niet in de Van Dale. Ik zal het begrip authenticatie gebruiken, tenzij ik een wettekst citeer; dan volg ik de daar gebruikte terminologie.

door de wetgever als functie van de schriftelijkheidseis aangeduid, maar is meer een functie van de elektronische handtekening. Door gebruik te maken van een gekwalificeerde elektronische handtekening kan worden gewaarborgd dat het bericht onderweg niet is gewijzigd.

Vastleggen wat tot uitdrukking moet worden gebracht, is in de elektronische context dan ook geen functie van het schriftelijkheidvereiste, maar een functie van de elektronische handtekening. De bewijsfunctie kan bij elektronische communicatie zonder gekwalificeerde elektronische handtekening niet gewaarborgd worden.

De beoordeling of een bepaalde vorm van elektronische communicatie functioneel equivalent is voor de conventionele wijze, moet daarom ten aanzien van de elektronische handtekening plaatsvinden aan de hand van de identificatiefunctie (de identificatie van de afzender van het bericht) en de bewijsfunctie (het vastleggen van wat tot uitdrukking moet worden gebracht). Dit laatste betreft de integriteit van een bericht, de zekerheid dat het bericht onderweg niet gewijzigd is.

Wat onder een elektronische handtekening wordt verstaan, is in de hieronder besproken regelgeving vastgelegd. De genoemde functies spelen slechts een rol in een situatie waarin een elektronische handtekening ontbreekt en moet worden beoordeeld of het elektronische bericht aan de vormvereisten voldoet. Beoordeeld moet dan worden of er zekerheid bestaat over de identiteit van de afzender en de integriteit van het bericht.

3.3.2.1 Algemene omschrijving van de elektronische handtekening

Wat onder *elektronische handtekening* wordt verstaan, staat in art. 2, eerste lid, van Richtlijn 1999/93/EG en in art. 3:15a, vierde lid, BW: een handtekening die bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie.

Dit is een relatief abstracte definitie, waarvan de begrippen niet volledig zijn ingevuld, getuige ook overweging 8 uit de preambule van Richtlijn 1999/93/EG, waarin staat: 'De snelle technologische ontwikkelingen en de wereldwijde omvang van het internet vereisen een aanpak die openstaat voor verschillende technologieën en diensten.' Onder een elektronische handtekening als bedoeld in art. 3:15a, derde lid, BW zou dus ook een ingescande handtekening die onder een brief geplakt is, kunnen worden verstaan. Ook kan volgens Lodder, Dumortier en Bol onder omstandigheden een e-mailbericht onder deze ruime definitie komen te vallen: 'Hierin zijn immers gegevens (de inhoud van het bericht) verbonden aan andere gegevens (de in de header opgenomen afzender) en deze gegevens kunnen gebruikt worden om de

identiteit van de verzender vast te stellen. Of de e-mail als handtekening kan worden gezien, zal mede afhangen van het gebruikte e-mailadres. (...) Niet veel ontvangers van een e-mail van bill-gates@hotmail.com zullen denken met de Microsoft-voorman van doen te hebben. Anders is dit voor e-mailadressen van medewerkers van bedrijven of overheidsinstellingen, voorzover althans de gebruikte namen herleidbaar zijn. Een bericht dat daadwerkelijk afkomstig is van het adres bill-gates@microsoft.com zal in dat licht op zichzelf als een elektronisch ondertekend bericht kunnen worden gezien.¹²¹ Dat een e-mailbericht een elektronische handtekening kan zijn, wordt bevestigd op de website e-overheid. Hier staat: 'een gewone (bedoeld wordt gewone elektronische handtekening, AK) handtekening kan een e-mailbericht zijn waarin persoonsgegevens staan of een ingescande handtekening. Uiteraard moet deze handtekening voldoen aan art. 3:15a, vierde lid, BW, oftewel de elektronische handtekening moet bestaan uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die gegevens worden gebruikt als middel voor authenticatie.'¹²²

Bij deze opvatting zijn nog wel wat kanttekeningen te plaatsen. Hier wordt namelijk geen onderscheid gemaakt tussen identificatie en authenticatie. Identificatie houdt in de vaststelling van de identiteit van een persoon. Ik ben ... Authenticatie houdt in het bewijzen van de identiteit van betrokkene, het waarborgen dat het klopt.¹²³ Authenticatie is in die zin te vergelijken met legitimatie, het bewijzen dat iemand de persoon is wie deze zegt te zijn.

Volgens Van Eecke en Dumortier duidt authenticiteit op zekerheid over de identiteit van de afzender en de herkomst van de berichten.¹²⁴ Authenticatie duidt op het garanderen van de waarachtigheid van informatie en Van Eecke onderscheidt bij het authenticatieproces technisch gesproken drie aspecten:

- ten eerste gaat het om het vaststellen van de oorsprong van de informatie, het kunnen achterhalen van de identiteit van de auteur van de informatie;
- ten tweede gaat het om het vaststellen van de integriteit van de informatie, om het verkrijgen van zekerheid over het feit of een bericht al dan niet op een ongeoorloofde wijze gewijzigd is;
- ten derde gaat het om de niet-loochening, of de onmogelijkheid tot ontkenning door de auteur dat een bericht van hem is uitgegaan.¹²⁵

121 Lodder, Dumortier & Bol 2005, p. 25.

122 <http://www.e-overheid.nl/thema/juridisch/handtekeningen/>, geraadpleegd op 3 juni 2008.

123 Schellekens 2004, p. 15, hij schrijft: authentication is used here in the meaning of verification of identity of authority.

124 Van Eecke en Dumortier 1998, p. 233.

125 Van Eecke 2004, p. 275.

Het eerste aspect heeft betrekking op authenticatie in de zin van het bewijzen van de identiteit van de betrokkene. De twee daarna genoemde aspecten van authenticatie zijn anders en worden ook op een andere manier gerealiseerd. Ook de in het inleidende hoofdstuk genoemde beginselen van Franken van behoorlijk IT gebruik, worden deze drie aspecten apart genoemd. Het vaststellen van de oorsprong van de informatie is iets anders dan onweerlegbaarheid of onloochenbaarheid. Dit laatste is lastig te realiseren. Het ondertekenen bijvoorbeeld van een bericht in 2001 met een elektronische handtekening bevestigt de authenticiteit van het bericht. Maar die handtekening kan niet gebruikt worden om te bewijzen dat de ondertekenaar in 2009 dat bericht nog een keer getekend heeft, oftewel nog steeds achter de inhoud van het bericht staat. Niet alles wat geauthenticeerd is, is onweerlegbaar. Daarbij is een conventionele handtekening niet terug te trekken. Bij een elektronische handtekening kan dat wel, door het publiceren van de private sleutel door de houder van deze sleutel. Hierdoor kan de houder aangeven dat een ieder de handtekening had kunnen plaatsen, de sleutel is immers openbaar. Daarbij komt dat een elektronische handtekening ook volledig autonoom door een apparaat gezet kan worden, zonder medeweten van de houder. De onloochenbaarheid is daarom met een elektronische handtekening niet per definitie gegarandeerd.

Een e-mailbericht beschouwen als een elektronische handtekening is dan ook vergelijkbaar met het gelijkstellen van een naam onder een brief of een logo op een brief met een conventionele handtekening. Het e-mailadres is hooguit een middel voor identificatie. Het veld bij een e-mailadres waarin de naam staat, is te veranderen en daarom heeft een dergelijk bericht geen authenticerende eigenschappen, dat wil zeggen eigenschappen waarmee zekerheid gegeven kan worden over de afzender en de herkomst van het bericht. Dit voldoet ook niet aan de begripsomschrijving van de elektronische handtekening, waarin het gaat om elektronische gegevens die kunnen worden gebruikt 'als middel voor authenticatie'. Een e-mailbericht kan worden gebruikt als middel voor identificatie, niet als middel voor authenticatie.

3.3.2.2 De geavanceerde elektronische handtekening

Naast deze algemene omschrijving kent Richtlijn 1999/93/EG de *geavanceerde elektronische handtekening*. Hiervan is blijkens art. 2, tweede lid, van de Richtlijn sprake indien de elektronische handtekening aan de volgende vier eisen voldoet:

- a. zij is op unieke wijze aan de ondertekenaar verbonden;
- b. zij maakt het mogelijk de ondertekenaar te identificeren;

- c. zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; en
- d. zij is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord.

Volgens Lodder, Dumortier en Bol is er sprake van een dergelijke geavanceerde elektronische handtekening wanneer gebruik wordt gemaakt van asymmetrische cryptografie. In zo'n geval spreekt men ook wel van een digitale handtekening. Onder encryptie wordt verstaan een proces waarmee klare, leesbare gegevens met behulp van een wiskundige berekening (algoritme) worden versleuteld in gecodeerde, niet leesbare gegevens.¹²⁶ Op deze manier worden de data of een bericht onleesbaar voor onbevoegden. Een sleutel geeft vervolgens toegang tot de versleutelde informatie.

Bij *symmetrische encryptie* wordt door beide partijen gebruik gemaakt van dezelfde geheime sleutel.

Bij *asymmetrische encryptie* wordt gebruikt gemaakt van een sleutelbaar bestaande uit een geheime, private sleutel, welke enkel bekend is bij de gebruiker, en een publieke sleutel, die kan worden gebruikt om berichten te versleutelen die vervolgens alleen door de eigenaar van de bijbehorende private sleutel weer ontcijferd kunnen worden. Deze publieke sleutel kan, zoals de naam suggereert, bij iedereen bekend zijn. Vaak kent niet iedereen alle publieke sleutels. Daarom worden er certificaten uitgegeven die de sleutels binden aan identiteiten. Deze private en publieke sleutel zijn aan elkaar verbonden. Door het gebruik van asymmetrische cryptografie is het beheren en distribueren van sleutels eenvoudiger geworden omdat de publieke sleutel niet geheim gehouden hoeft te worden, en de private sleutel nooit getransporteerd of aan anderen bekend gemaakt hoeft te worden. Bij communicatie kan gebruik worden gemaakt van volledige versleuteling door middel van de publieke sleutel wanneer de afzender van een bericht wil dat dit bericht enkel gelezen kan worden door de houder van de private sleutel. Naast encryptie kan asymmetrische encryptografie ook gebruikt worden voor het creëren van een digitale handtekening. Door een elektronische handtekening te plaatsen met de private sleutel kan worden gegarandeerd dat het bericht afkomstig is van de houder van deze sleutel, aangezien deze de enige is die beschikt over deze sleutel. Dit plaatsen van een handtekening kan, heel grof gezegd, gezien worden als het versleutelen van het bericht met de private sleutel (welke weer ontcijferd kan worden met de publieke sleutel). Ten opzichte van encryptie worden dus de rol van de private en de publieke sleutel omgedraaid. Wanneer zowel zender als ontvanger een private sleutel hebben en tevens elkaars publieke sleutel, kunnen

126 Lodder, Dumortier & Bol 2005, p. 15.

de vertrouwelijkheid, de integriteit en de authenticiteit van de communicatie in beide richtingen gegarandeerd worden.

Wanneer men gebruik maakt van de digitale handtekening is echter veelal niet het bericht zelf ondertekend, doch een unieke waarde¹²⁷ welke op basis van een wiskundig algoritme is toegekend aan het bericht. Op basis van het bericht wordt deze waarde (de hashwaarde) gegenereerd en vervolgens asymmetrisch ondertekend. Wanneer in het bericht iets gewijzigd wordt, verandert tevens de hashwaarde en daarmee de elektronische handtekening. Door deze procedure kan voldaan worden aan de volgende criteria voor de geavanceerde elektronische handtekening:

- zij is op unieke wijze verbonden aan de ondertekenaar, want versleuteld door middel van diens private sleutel;
- zij is tot stand gekomen door middelen die de ondertekenaar onder zijn uitsluitende controle kan houden, zijnde de private sleutel;
- zij is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden dat elke wijziging achteraf kan worden opgespoord.

Wanneer na ondertekening het bericht gewijzigd wordt, zal dit immers een andere hashwaarde opleveren, welke niet meer overeenkomt met die welke reeds versleuteld aan het bericht is gehecht.

3.3.2.3 De gekwalificeerde elektronische handtekening

Aan drie criteria voor de geavanceerde elektronische handtekening is volgens de wetgever voldaan wanneer men gebruik maakt van een digitale handtekening met asymmetrische encryptie. Er is echter nog geen zekerheid over de daadwerkelijke identiteit van de ondertekenaar. Men kan de identiteit van een ander hebben aangenomen, en zodoende ook optreden als deze ander. Hoe kan de identiteit van de ondertekenaar dus gegarandeerd en gecontroleerd worden? Bij de digitale handtekening kan hiervoor gebruik worden gemaakt van certificaten. In dat geval is er sprake van een geavanceerde elektronische handtekening die gebaseerd is op een gekwalificeerd certificaat, zoals genoemd in art. 5, eerste lid, van de Richtlijn. Een dergelijke handtekening wordt ook wel *gekwalficeerde handtekening* genoemd. Een derde (de trusted third party, hierna te noemen TTP) controleert de identiteit van de ondertekenaar en voorziet hem vervolgens van een certificaat dat deze identiteit bevestigt. In een dergelijk

127 De waarde is echter niet uniek. Er zijn namelijk oneindig veel berichten die dezelfde hashwaarde opleveren. Het is echter onmogelijk (het zou te veel tijd kosten) om twee berichten te construeren die dezelfde hashwaarde opleveren. Deze eigenschap heet *collision resistance*. Strikt genomen is de hashwaarde dus niet uniek, maar uniek genoeg.

certificaat staat een bevestiging in de vorm: de publieke sleutel van mevrouw X is K, en de bevestiging is vervolgens ondertekend met de private sleutel van de TTP. Vervolgens rijst de vraag in hoeverre deze certificaten op hun beurt betrouwbaar zijn. Hiervoor kan gebruik worden gemaakt van een zogenaamde Public Key Infrastructure. Een dergelijke infrastructuur voorziet erin dat de ondertekende certificaten via meerdere van deze certificatie dienstverleners uiteindelijk bij een certificatie dienstverlener komt die vertrouwd wordt door de ontvanger van het bericht. In de praktijk zal een dergelijke keten van certificatie dienstverleners er als volgt uitzien:

Identiteit verzender wordt bevestigd door TTP A → Identiteit TTP A wordt bevestigd door TTP B → Identiteit TTP B wordt bevestigd door TTP C → [...] → Identiteit TTP X wordt bevestigd door TTP Y → Ontvanger heeft de sleutel van TTP Y in zijn bezit. Omdat de ontvanger alle TTP's vertrouwt wat betreft het correct uitgeven van certificaten heeft hij aldus zekerheid over de identiteit van de verzender.

In art. 3:15a BW wordt uitgegaan van deze derde vorm van de elektronische handtekening. In het eerste lid van dit artikel staat dat een elektronische handtekening slechts dezelfde rechtsgevolgen heeft als een handgeschreven handtekening indien de methode die daarbij is gebruikt voor authenticatie, voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische gegevens worden gebruikt en op alle overige omstandigheden van het geval. Hieraan is blijkens het tweede lid voldaan wanneer de elektronische handtekening aan de volgende eisen voldoet:

- a. zij is op unieke wijze aan de ondertekenaar verbonden;
- b. zij maakt het mogelijk de ondertekenaar te identificeren;
- c. zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
- d. zij is op zodanige wijze aan het elektronische bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;
- e. zij is gebaseerd op een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss, van de Telecommunicatiewet; en
- f. zij is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen als bedoeld in art. 1.1, onderdeel vv, van de Telecommunicatiewet.

Een elektronische handtekening die aan al deze eisen voldoet, is een gekwalificeerde elektronische handtekening. Nu hoeft blijkens het derde lid van art. 3:15a BW een elektronische handtekening niet per se een gekwalificeerde elektronische handtekening te zijn. Het derde lid bepaalt namelijk dat een

methode als bedoeld in het eerste lid, niet als onvoldoende betrouwbaar kan worden aangemerkt op de enkele grond dat de methode niet voldoet aan de onderdelen e en f uit het tweede lid, of niet is gebaseerd op een door een certificatieinstantie verleend als bedoeld in artikel 18.16, eerste lid, Telecommunicatiewet afgegeven certificaat. Een geavanceerde elektronische handtekening kan ook dan als voldoende betrouwbaar worden aangemerkt.

3.3.2.4 Huidig stelsel

Het stelsel van elektronische handtekeningen zoals dit nu door de overheid ontwikkeld wordt, past als volgt binnen dit wettelijke systeem. Het stelsel DigiD kent de zekerheidsniveaus laag en midden. Bij het zekerheidsniveau ‘laag’ wordt door de burger gebruik gemaakt van een inlogcode, die bestaat uit een gebruikersnaam met een wachtwoord. Bij het zekerheidsniveau ‘midden’ wordt aan die inlogcode een authenticatie door middel van een sms bericht toegevoegd. Het zekerheidsniveau ‘hoog’ zou moeten voldoen aan de eisen die gesteld worden aan een gekwalificeerde elektronische handtekening. Hierin wil de rijksoverheid voorzien door het ontwikkelen van de eNik, de elektronische identiteitskaart. Hiermee zou het voor de burger mogelijk worden om versleutelde berichten te versturen. Deze is echter nog niet ingevoerd, en invoering lijkt op korte termijn ook nog niet te verwachten.

Is de combinatie van gebruikersnaam, wachtwoord en eventueel per sms ontvangen authenticatiecode voldoende om te kunnen dienen als geavanceerde of mogelijkgevoerd gekwalificeerde elektronische handtekening? Voldoet deze combinatie aan de criteria zoals eerder opgesomd? Zij:

– is *op unieke wijze verbonden aan de ondertekenaar*; aangezien vóór uitgifte van de gebruikersnaam/wachtwoord de identiteit van de aanvrager is gecontroleerd aan de hand van het BSN. Pas na aanvraag van deze gebruikersnaam/wachtwoord is het voor de ondertekenaar mogelijk de authenticatiemogelijkheden uit te breiden met een telefoonnummer. Wanneer dit telefoonnummer daadwerkelijk gebruikt wordt om een authenticatiecode naar te versturen, zal dit altijd pas zijn nadat eerst is ingelogd met de gebruikersnaam en het wachtwoord van de ondertekenaar. Alvorens gebruik te kunnen maken van beveiligingsniveau ‘midden’ zal dus altijd eerst ingelogd moeten zijn op basis van beveiligingsniveau ‘laag’. Controle op het gebruik van een gebruikersnaam/wachtwoord door een ander ontbreekt echter.

– maakt *identificatie van de ondertekenaar niet mogelijk*; op geen enkel moment in de aanvraagprocedure van een DigiD vindt individuele identificatie plaats. Zowel niet op het moment dat de DigiD inlogcode wordt aangevraagd als op het moment dat het telefoonnummer wordt opgegeven (hierbij wordt

uitgegaan van dezelfde persoon als die de DigiD inlogcode heeft aangevraagd). Iedereen kan immers met een BSN van een ander een DigiD aanvragen. Een belangrijke drempel ligt dan wel in het feit dat per post een wachtwoord thuisgestuurd wordt. Dit biedt echter ook geen afdoende waarborgen: denk bijvoorbeeld aan huisgenoten in studentenhuizen. Een DigiD aanvragen op een BSN van een ander is dan ook mogelijk, het activeren ervan door middel van de thuis gestuurde code werpt daarbij een belangrijke drempel op. Er kan echter gesteld worden, dat alleen wanneer op basis van bijvoorbeeld het in persoon laten zien van een legitimatiebewijs een DigiD code wordt verstrekt of een telefoonnummer wordt opgegeven, kan worden gezegd dat de identificatie voldoende is. In de toekomst is een dergelijk (elektronisch) identiteitsbewijs voorzien voor het beveiligingsniveau ‘hoog’.¹²⁸

– *is tot stand gekomen met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; wanneer de ondertekenaar zijn gebruikersnaam en wachtwoord voor zich zelf houdt, kan hier redelijkerwijs van worden uitgegaan. Het intypen van deze gegevens op een website, zoals de DigiD gebruikt wordt, biedt echter niet altijd voldoende waarborgen voor het onder uitsluitende controle houden van de middelen.*

– *is niet op zodanige wijze aan de gegevens waarop zij betrekking heeft, verbonden, dat elke wijziging achteraf kan worden opgespoord. Bij ondertekening door middel van een DigiD kunnen gegevens na ondertekening gewijzigd worden, aangezien de DigiD niet gegenereerd wordt op basis van het document dat ondertekend wordt.*

Een DigiD voldoet dan ook niet aan de eisen die gesteld worden aan een *geavanceerde elektronische handtekening*. Het biedt immers niet de mogelijkheid om berichten versleuteld te versturen. Een DigiD doet niet meer dan toegang bieden tot een website van de overheid. Een DigiD is niet verbonden aan het bericht, maar biedt een (beperkte) mogelijkheid tot identificatie en authenticatie van de afzender van het bericht.

Doordat de DigiD niet voldoet aan de eisen die gesteld worden aan een geavanceerde handtekening, kan de DigiD ook niet voldoen aan de eisen die gesteld worden aan een *gekwalficeerde handtekening*. Wil er sprake zijn van een gekwalficeerde elektronische handtekening, dan zal er, naast de mogelijkheid berichten versleuteld te versturen, gebruik moeten worden gemaakt van een zogenaamd gekwalficeerd certificaat. Deze mogelijkheid is er niet. Vooral nog biedt DigiD dan ook niet de mogelijkheid te ondertekenen door middel van een gekwalficeerde elektronische handtekening. Hierin is voor de toekomst voorzien in het nog te ontwikkelen beveiligingsniveau ‘hoog’.

128 Zie ook: <http://www.digid.nl/burger/vraag-en-antwoord/zekerheidsniveaus/#irfaq1>

Waarschijnlijk zal dit niet via de DigiD gaan lopen, maar via de te ontwikkelen eNik, zoals hierboven genoemd. De beveiligingsniveaus ‘laag en midden’ maken gebruik van de combinatie van inloggen door middel van gebruikersnaam/wachtwoord en eventueel de authenticatie per sms. Strikt genomen is een DigiD ook niet te kwalificeren als elektronische handtekening. DigiD geeft geen functionaliteit om een handtekening vast te hechten of logisch te associëren aan een document. Een DigiD laat iemand inloggen bij een website, waarbij identificatie plaats vindt door het BurgerServiceNummer. Eventueel is een DigiD in een procesflow wel te beschouwen als een elektronische handtekening, wanneer het dan wel aan een bericht verbonden is.

Art. 2:16 Awb bepaalt dat aan het vereiste van ondertekening is voldaan door een elektronische handtekening, indien de methode die voor authenticatie is gebruikt, voldoende betrouwbaar is, gelet op de aard en de inhoud van het elektronische bericht en het doel waarvoor het wordt gebruikt. De artikelen 3:15a, tweede tot en met zesde lid, en 3:15b van het BW worden van overeenkomstige toepassing verklaard, voor zover de aard van het bericht zich daartegen niet verzet. Hiermee wordt verwezen naar de gekwalificeerde elektronische handtekening. Wanneer gebruik wordt gemaakt van een gekwalificeerde elektronische handtekening, dan wordt de methode voor authenticatie vermoed voldoende betrouwbaar te zijn. Het zesde lid van art. 3:15a BW bepaalt dat tussen partijen van het tweede en derde lid kan worden afgeweken.

Zoals hierboven al uiteengezet, is het momenteel niet of nauwelijks mogelijk om binnen het elektronisch bestuurlijk verkeer gebruik te maken van de gekwalificeerde elektronische handtekening, zoals geregeld in art. 3:15a, tweede lid, BW. Een dergelijk systeem moet namelijk door de overheid ondersteund worden, en tot op heden bieden de meeste overheidswebsites (als ze al iets aanbieden) alleen de mogelijkheid een DigiD te gebruiken. Een DigiD is een methode voor authenticatie. Bestuursorganen die ondertekening met dit middel ondersteunen, nemen kennelijk aan dat de methode die voor authenticatie wordt gebruikt, voldoende betrouwbaar is. Een andere methode van authenticatie, die door het bestuursorgaan voldoende betrouwbaar wordt geacht, voldoet eveneens. Dit is afhankelijk van de aard en de inhoud van het elektronische bericht en het doel waarvoor het gebruikt wordt.

Het is daarom heel goed denkbaar dat een bestuursorgaan voor verschillende categorieën berichten waarbij ondertekening vereist is, verschillende voorwaarden zal gaan stellen ten aanzien van de elektronische handtekening. Het bestuursorgaan kan met betrekking tot de methode van authenticatie differentiëren naar gelang de aard van het berichtenverkeer.

Blijkens de laatste zinsnede van art. 2:16 Awb kunnen bij wettelijk voorschrift aanvullende eisen gesteld worden.

Uit jurisprudentie blijkt vooralsnog weinig informatie te verkrijgen over de wijze waarop de hierboven besproken regeling in de praktijk toegepast wordt. In elk geval is duidelijk dat het gebruiken van een gekwalificeerde elektronische handtekening op dit moment slechts op kleine schaal mogelijk is en voornamelijk voor beroepsbeoefenaars. De DigiD voldoet niet aan de eisen van een gekwalificeerde handtekening.

In 2006 oordeelt de rechtbank Maastricht dat een elektronisch ingediend bezwaarschrift moet zijn voorzien van een elektronische handtekening.¹²⁹ Het betreft een bezwaarschrift dat per e-mail tegen een besluit van de Informatie Beheer Groep was ingediend. Ambtshalve overweegt de rechtbank dat op grond van art. 6:5 Awb een bezwaarschrift dient te worden ondertekend. Eiseres diende haar bezwaarschrift in door een e-mailbericht dat verzonden was via hotmail. Daarom komt de rechtbank tot de conclusie dat niet is voldaan aan de vereisten die aan een elektronische handtekening op grond van art. 2:16 Awb jo art. 3:15a BW worden gesteld. Het bezwaarschrift moest daarom niet-ontvankelijk verklaard worden. De annotator bekritiseert deze uitspraak als een tamelijk rigide uitleg van afdeling 2.3 Awb, waarbij de rechtbank is voorbijgegaan aan art. 6:6 Awb waaruit blijkt dat een bestuursorgaan een bezwaarschrift niet-ontvankelijk kan verklaren wanneer niet aan het ondertekeningvereiste is voldaan.

Daarbij is de rechtbank in deze uitspraak voorbij gegaan aan de verschillende niveaus die er bestaan op het gebied van de elektronische handtekening. Zoals hierboven is aangegeven, zijn Lodder, Dumortier & Bol van mening dat een e-mailbericht onder omstandigheden aangemerkt kan worden als een elektronische handtekening. Had de studente in het e-mailbericht haar inschrijvingsnummer van de studiefinanciering vermeld, dan was er sprake van elektronische gegevens (het inschrijfnummer in het bericht) die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens (de in de header van het e-mailbericht genoemde afzender) en die worden gebruikt als middel voor identificatie van de afzender. Een mailadres biedt echter geen zekerheid over de identiteit van de afzender. Een ieder kan op een willekeurige naam immers een mailadres aanmaken. Hieruit blijkt dat deze definitie van een elektronische handtekening discutabel is. Uit het mailbericht kan misschien de identiteit van de afzender afgeleid worden, er is daarmee nog geen zekerheid over deze identiteit. Met andere woorden, authenticatie, het verschaffen van zekerheid over de identiteit van de afzender, heeft niet plaats

129 Rb. Maastricht 27 maart 2006, *LJN* AW6886, *JB* 2006, 162 m.nt. M.O.-V (Hotmail bezwaar bij IBG).

gevonden. Het bestuursorgaan had echter wel, ingevolge art. 2:16 Awb, kunnen beslissen dat de methode die gebruikt werd voor authenticatie (hoe discutabel ook) voldoende betrouwbaar was, gelet op de aard en de inhoud van het elektronische bericht. Dit is geen rechtsregel van openbare orde, de rechter toetst hier niet ambtshalve aan.¹³⁰

Verder is het ingevolge art. 2:15 Awb aan het bestuursorgaan om te bepalen of de elektronische weg geopend is, gelet op het gereed zijn van de organisatie en werkprocessen aan de kant van het bestuursorgaan voor het afhandelen van elektronisch verkeer. Zo moet het bestuursorgaan bijvoorbeeld ook een systeem inrichten om elektronische handtekeningen te kunnen lezen. Indien een bestuursorgaan een dergelijk systeem (nog) niet heeft, maar de elektronische weg voor het indienen van bezwaarschriften wel opengesteld heeft, kan het bestuursorgaan zelf bepalen of de indiener van het bezwaarschrift voldoende geïdentificeerd kan worden, bijvoorbeeld door het opgeven van een inschrijf- of correspondentienummer. Indien het bestuursorgaan van oordeel is dat er gebreken kleven aan het elektronisch ingediende bezwaarschrift, dan moet de indiener de gelegenheid krijgen dit gebrek te herstellen, zoals dit ook bij niet gemotiveerde pro forma bezwaarschriften gebruikelijk is. Indien er gebreken aan het bericht kleven omdat de betrouwbaarheid bijvoorbeeld in het geding is, of er vragen zijn ten aanzien van de authenticiteit van het bericht, kan het bestuursorgaan de indiener in de gelegenheid stellen om dit verzuim te herstellen op grond van art. 6:6 Awb.

De rechtbank in Zwolle gaat in een uitspraak niet in op deze vraag.¹³¹ In deze zaak is door de Stichting Centraal Bureau Rijvaardigheidsbewijzen een rijbewijs ongeldig verklaard. Belanghebbende dient tegen dit besluit per e-mailbericht een bezwaarschrift in. Dit bezwaar wordt ongegrond verklaard. In de beroepszaak oordeelt de rechtbank als volgt:

‘Niet duidelijk is of verweerster kenbaar heeft gemaakt dat de mogelijkheid van het elektronisch maken van bezwaar bestaat. Indien verweerster al de mogelijkheid van het elektronisch maken van bezwaar heeft geopend, voldoet eisers bezwaarschrift niet aan het vereiste van een (elektronische) handtekening. Verweerster heeft eiser echter niet in de gelegenheid gesteld om een verzuim te herstellen middels het alsnog schriftelijk indienen van een bezwaarschrift of het alsnog ondertekenen van het elektronische bezwaarschrift. Nu ervan mag worden uitgegaan dat het gebrek aan het bezwaarschrift desgevraagd zou zijn hersteld, ziet de rechtbank uit proceseconomische motieven aanleiding aan het voorgaande voorbij te gaan en te komen tot een inhoudelijke beoordeling van het geschil.’

Ook hier gaat de rechtbank eraan voorbij dat een e-mailbericht onder omstandigheden kan voldoen aan de definitie van een elektronische handtekening als bedoeld in art. 3:15a, vierde lid, BW. De authenticiteit van het

130 Damen e.a. Bestuursrecht 2 2009, p. 231.

131 Rb. Zwolle 17 januari 2007, *LJN AZ7162* (Elektronisch bezwaar bij CBR).

bericht kan op deze manier voldoende gewaarborgd zijn. Kennelijk bedoelt de rechtbank dat een gekwalificeerde elektronische handtekening ontbreekt. Overigens moet het bestuursorgaan wel voor de elektronische infrastructuur gezorgd hebben, die het mogelijk maakt om een bericht te voorzien van bijvoorbeeld een DigiD of een elektronische handtekening.¹³² Terecht gaat de rechtbank aan dit gebrek voorbij, zodat het beroep inhoudelijk behandeld kan worden.

Dat het doel van een handtekening is het vaststellen van de identiteit van de indiener van een bezwaarschrift, blijkt uit een uitspraak van de rechtbank Rotterdam. In deze zaak verklaarde het college van burgemeester en wethouders van Rotterdam de indiener van een bezwaarschrift niet-ontvankelijk, omdat zij het (op conventionele wijze ingediende) bezwaarschrift niet had ondertekend. De rechtbank overweegt:¹³³

‘...dat een niet-ontvankelijkheidsverklaring van het bezwaar in een dergelijk geval achterwege dient te blijven indien de identiteit van de indiener van het bezwaar op andere wijze kan worden vastgesteld dan wel aan diens identiteit niet kan worden getwijfeld. Indien geen ondertekend bezwaarschrift is ingediend, maar wel een ondertekend antwoordstrookje over het al dan niet bijwonen van de hoorzitting, dient verweerder een afweging te maken of hij in redelijkheid gebruik kan maken van zijn bevoegdheid om het bezwaar niet-ontvankelijk te verklaren. (...) Er bevinden zich in het (bijstands)dossier van verweerder door eiseres ondertekende stukken waardoor er geen grond is om aan de authenticiteit van de handtekening op het antwoordstrookje te twijfelen. De rechtbank is van oordeel dat, nu de ondertekening van het antwoordstrookje voldoende is om aan te nemen dat de identiteit van de indiener van het bezwaarschrift bekend is en dit ondertekende antwoordstrookje voor het einde van de hersteltermijn door verweerder is ontvangen, verweerder niet in redelijkheid gebruik had kunnen maken van zijn bevoegdheid om het bezwaar niet-ontvankelijk te verklaren.’

Deze uitspraak sluit aan bij de hierboven genoemde doelen van de elektronische handtekening en laat zien dat het bestuursorgaan ook op andere wijze kan nagaan of de identiteit van de indiener van een bepaald geschrift kan worden vastgesteld.

3.3.3 Conclusie vormvoorschriften schriftelijk en ondertekening

Aan de vormvereisten, schriftelijk en ondertekening, wordt volgens de wetgever voldaan indien de elektronische wijze van communicatie functioneel equivalent is aan de conventionele wijze van communicatie. De vormvereisten schriftelijk en handtekening zijn in de elektronische communicatie wezenlijk anders dan in de conventionele, papieren wijze van communiceren.

132 Hierin voorzag de website van het CBR niet op 3 juli 2008.

133 Rb. Rotterdam 2 juli 2009, *LJN* BJ2435 (Bezwaar zonder handtekening).

De wetgever heeft ervoor gekozen om het begrip ‘schriftelijk’ ruim uit te leggen. Hierdoor wordt onder schriftelijk verstaan: weergave door middel van schrifttekens. Een elektronische drager met schrifttekens (bits) is echter niet te lezen zonder de daarbij horende codering, die aangeeft in welke context de informatie gelezen kan worden. Aan de ruime interpretatie van het begrip schriftelijk, in de zin dat elke drager die schrifttekens bevat, als schriftelijk wordt aangemerkt, moet worden toegevoegd dat een elektronische boodschap ook de codering dient te bevatten waaruit blijkt in welke context een bericht gelezen kan worden. Zonder deze codering is met een drager met elektronische schrifttekens (bits) immers niks te beginnen

Van functionele equivalentie bij de eis dat communicatie schriftelijk moet plaatsvinden, is sprake wanneer de elektronische wijze van communicatie evenals de conventionele wijze voldoet aan de communicatiefunctie, de bewijsfunctie en de afbakeningsfunctie. Deze laatste, de afbakeningsfunctie, is echter geen functie van het schriftelijkheidsvereiste, maar een eigenschap daarvan. De eis dat een bepaalde vorm van communiceren schriftelijk plaatsvindt (bijvoorbeeld het nemen van besluiten door een bestuursorgaan), wordt gesteld om de over te brengen boodschap duidelijk te maken en om deze boodschap vast te leggen. Dit wordt door de wetgever aangeduid als de communicatie- en bewijsfunctie. Doordat de boodschap schriftelijk is vastgelegd, onderscheidt deze zich van mondelinge communicatie. Dit is een onderscheidend kenmerk van deze vorm van communicatie en daarmee een eigenschap en geen functie.

De bewijsfunctie, het vastleggen wat tot uitdrukking wordt gebracht, is in de elektronische context anders dan in een conventionele, schriftelijke situatie. Een boodschap die elektronisch wordt overgebracht, bestaat uit series van bits (bitstring), waarbij de daarbij geleverde codering aangeeft in welke context de bits een betekenis krijgen. Bits kunnen in verschillende contexten dan ook een andere betekenis krijgen. Zelfs in dezelfde context kunnen bits een andere betekenis krijgen. Vastleggen wat tot uitdrukking moet worden gebracht, is in de elektronische context dan ook geen functie van het schriftelijkheidvereiste, maar een functie van de elektronische handtekening. De bewijsfunctie kan bij elektronische communicatie zonder gekwalificeerde elektronische handtekening dan ook niet gewaarborgd worden. Bij het beoordelen of een bepaalde vorm van elektronische communicatie functioneel equivalent is van de conventionele schriftelijke, speelt de bewijsfunctie dan ook geen rol.

De beoordeling of een bepaalde vorm van elektronische communicatie functioneel equivalent is aan de conventionele schriftelijke wijze, moet daarom plaats vinden aan de hand van de communicatiefunctie. Dit houdt in dat elektronische communicatie een functioneel equivalent is van de conventionele

schriftelijke communicatie, indien door middel van de elektronische communicatie duidelijk gemaakt kan worden wat tot uitdrukking moet worden gebracht. Deze communicatiefunctie moet materieel ingevuld worden, dat wil zeggen dat zolang betrokkenen de middels het bericht overgebrachte boodschap niet betwisten, de boodschap geacht moet worden schriftelijk te zijn. De rechter toetst hier niet ambtshalve aan.

Het begrip functioneel equivalent is ook van toepassing op de elektronische handtekening. De functies van een ondertekening zijn: de identificatie van de afzender van het bericht, de blijk van instemming met de inhoud van het bericht en het bieden van een waarborg tegen overhaast optreden. Deze functies zijn ingevuld door de regeling van de elektronische handtekening in het Burgerlijk Wetboek en de Telecommunicatiewet. Door de schakelbepalingen 3:15c BW en 2:16 Awb is deze regeling ook van toepassing op elektronisch verkeer tussen burger en bestuursorgaan.

Het uitgangspunt van art. 2:16 Awb is dat aan het vereiste van ondertekening is voldaan door een elektronische handtekening, indien de methode die daarbij voor authenticatie is gebruikt voldoende betrouwbaar is, gelet op de aard en de inhoud van het elektronische bericht en het doel waarvoor het wordt gebruikt.

In de elektronische communicatie strekt de handtekening ook om te waarborgen dat het bericht gedurende de verzending niet gewijzigd is. Deze bewijsfunctie, het vastleggen van wat tot uitdrukking moet worden gebracht, werd door de wetgever als functie van de schriftelijkheidseis aangeduid, maar is meer een functie van de elektronische handtekening. Door gebruik te maken van een gekwalificeerde elektronische handtekening kan worden gewaarborgd dat het bericht onderweg niet is gewijzigd, oftewel dat de integriteit van het bericht gewaarborgd is.

Bij twee andere door de wetgever aangeduide functies van een handtekening, de blijk van instemming en het bieden van een waarborg tegen overhaast optreden, is het de vraag in hoeverre deze functies door een elektronische handtekening worden gewaarborgd. Een elektronische handtekening wordt uiteindelijk door een apparaat geplaatst. Dit kan ook volledig automatisch, zonder medeweten van de 'eigenaar' van de handtekening gebeuren.

De eisen die aan de elektronische handtekening dan wel aan het middel van authenticatie gesteld worden, kunnen differentiëren naar gelang de aard en de inhoud van het bericht.

Een elektronisch bericht is daarmee functioneel equivalent aan de vormvereisten schriftelijk en ondertekening indien daarmee de boodschap kan worden

overgebracht, de identiteit van de afzender kan worden vastgesteld (de authenticiteit) en indien de integriteit van het bericht vaststaat.

3.4 Uitgangspunt van nevenschikking

Een belangrijk uitgangspunt dat steeds in de regeling van afd. 2.3 terugkomt, is het uitgangspunt van de nevenschikking. Dit houdt in dat de toename van elektronisch verkeer niet ten koste mag gaan van diegenen die daar geen gebruik van kunnen maken. Er mag geen verdringing zijn van de conventionele weg, want voor diegenen die niet (kunnen) beschikken over de nieuwe communicatiemiddelen, moet de overheid nog via de conventionele, papieren weg bereikbaar zijn. De nevenschikking is een van de wezenlijke onderdelen van afdeling 2.3. en wordt op wettelijk niveau gegarandeerd. Dit blijkt uit art. 2:14, eerste en tweede lid, en art. 2:15, eerste lid.

Art. 2:14 bepaalt dat een bericht dat tot een of meer geadresseerden is gericht, elektronisch wordt verzonden voor zover de geadresseerde heeft kenbaar gemaakt langs deze weg voldoende bereikbaar te zijn. Het gaat hier bijvoorbeeld om beschikkingen. Het tweede lid bepaalt dat berichten die niet tot een of meer geadresseerden zijn gericht, niet uitsluitend elektronisch verzonden mogen worden. Deze bepaling betreft bijvoorbeeld de besluiten van algemene strekking, zoals verordeningen en beleidsregels. Deze mogen dus niet uitsluitend elektronisch verzonden worden en moeten ook altijd op de conventionele wijze aan personen die niet over internet beschikken, verzonden of bekendgemaakt worden, tenzij bij wet anders is bepaald. Art. 2:15, eerste lid, regelt dit voor het bestuursorgaan: de burger kan alleen van de elektronische weg gebruik maken, voor zover het bestuursorgaan deze weg heeft opengesteld.

Art. 3:42, tweede lid, Awb werd aanvankelijk ook beschouwd als bepaling waarin het uitgangspunt van de nevenschikking was neergelegd. Hierin is namelijk bepaald dat besluiten van algemene strekking niet elektronisch bekend gemaakt mogen worden. Van dit verbod kan bij wettelijk voorschrift worden afgeweken. In de Wet elektronische bekendmaking is deze bepaling gewijzigd.¹³⁴ Deze wijziging heeft tot gevolg dat besluiten die niet tot een of meer belanghebbenden zijn gericht en die afkomstig zijn van de rijksoverheid, in beginsel in de elektronische Staatscourant worden bekendgemaakt. Besluiten die niet tot een of meer belanghebbenden zijn gericht en die afkomstig zijn van een

134 Wetsvoorstel tot Wijziging van de Bekendmakingswet en enkele andere wetten in verband met de elektronische bekendmaking en beschikbaarstelling in geconsolideerde vorm van wetten, algemene maatregelen van bestuur, anders dan bij wet of algemene maatregel van bestuur vastgestelde algemeen verbindende voorschriften en andere besluiten die niet tot een of meer belanghebbenden zijn gericht (Wet elektronische bekendmaking) *Kamerstukken II* 2006/2007, 31 084, nr. 2.

niet tot de centrale overheid behorend bestuursorgaan, worden bekendgemaakt in een van overheidswege uitgegeven blad of een dag-, nieuws- of huis-aan-huisblad, dan wel op andere geschikte wijze. Elektronische bekendmaking vindt uitsluitend plaats in een van overheidswege uitgegeven blad, tenzij bij wettelijk voorschrift anders is bepaald.

Deze wetswijziging is op 1 juli 2009 in werking getreden.

Het uitgangspunt van de nevenschikking komt in de volgende aspecten tot uiting:

- uitgangspunt is dat de burger bepaalt in welke vorm het verkeer plaats vindt, indien het bestuursorgaan over beide mogelijkheden (de conventionele en de elektronische wijze) beschikt;
- voor zover het bestuursorgaan over bepaalde zaken alleen maar op de conventionele wijze communiceert, heeft de burger geen keus: hij kan elektronisch verkeer niet afdwingen.¹³⁵

Het derde, in de memorie van toelichting genoemde aspect:

- het is het bestuursorgaan niet toegestaan bepaalde zaken alleen nog maar langs elektronische weg te doen, tenzij alle betrokkenen hiermee instemmen, heeft door de Wet elektronische bekendmaking een deel van zijn zeggingskracht verloren.

Een aantal belangrijke uitzonderingen op dit beginsel zullen hieronder besproken worden.

3.4.1 Belastingwetgeving

In art. 8, tweede lid, van de Algemene wet inzake rijksbelastingen (AWR) is voor ondernemers bepaald dat aangifte slechts elektronisch kan plaatsvinden. Dit geldt voor de groep die administratieplichtig is op grond van art. 52, tweede lid, AWR. Dit zijn: lichamen, natuurlijke personen die een bedrijf of zelfstandig een beroep uitoefenen, natuurlijke personen die belastbare winst uit onderneming als bedoeld in artikel 3.3 van de Wet inkomstenbelasting 2001 genieten, natuurlijke personen die inhoudingsplichtige zijn en natuurlijke personen die een werkzaamheid als bedoeld in de artikelen 3.91 en 3.92 van de Wet inkomstenbelasting 2001 verrichten. In art. 20 van de Uitvoeringsregeling AWR wordt vervolgens bepaald dat aangifte door een administratieplichtige als bedoeld in artikel 52, tweede lid, van de wet langs elektronische weg wordt gedaan indien het betreft: de inkomstenbelasting ingeval de administratieplichtige binnenlands belastingplichtige is; de

135 *Kamerstukken II* 2001/02, 28 483, nr. 3, p. 8.

vennootschapsbelasting ingeval de administratieplichtige binnenlands belastingplichtige is; de omzetbelasting: ingeval de administratieplichtige of diens fiscale vertegenwoordiger als bedoeld in de Wet op de omzetbelasting 1968, in Nederland woont of is gevestigd en de loonbelasting. Op grond van het derde lid van art. 20 van de Uitvoeringsregeling kan de inspecteur al dan niet op verzoek bij voor bezwaar vatbare beschikking ontheffing verlenen van een van de in het tweede lid bedoelde verplichtingen indien het langs elektronische weg aangifte doen onredelijk bezwarend is voor de administratieplichtige. Deze ontheffing geldt voor maximaal een jaar.

In een uitspraak uit 2007 gaat de rechtbank Arnhem in op deze ontheffingsmogelijkheid.¹³⁶ De betrokken belastingplichtige en zijn echtgenote waren administratieplichtig als bedoeld in art. 52 AWR en moesten elektronisch aangifte doen. Betrokkene wilde dit niet, omdat hij zoals blijkt uit de uitspraak, niet beschikte over toegang tot internet en zijn echtgenote niet in staat bleek om de elektronische aangifte via haar aansluiting op internet te versturen. Betrokkene was verder principieel tegen elektronisch berichtenverkeer en had geen zin om zich te verdiepen in computers en internet alleen om de belastingdienst ter wille te zijn.

Allereerst constateert de rechtbank dat de regeling in de AWR een afwijking is van het algemene beginsel van nevenschikking zoals dit in afd. 2.3 Awb staat opgenomen. De rechtbank constateert oneffenheden in het wetgevingsproces, met name op het punt van een ontbrekende en ondeugdelijke motivering ten aanzien van de afwijking in de AWR van de Awb. Ondanks deze gebreken oordeelt de rechtbank dat dit niet meebrengt dat de AWR als bijzondere wet op dit punt buiten toepassing moet blijven. De voorrangregel, dat de bijzondere wet voor de algemene wet gaat, blijft ook in dit geval gelden. De rechtbank concludeert dan ook dat art. 8, tweede lid, AWR en art. 20 van de Uitvoeringsregeling niet hoeven te wijken voor art. 2:15 Awb, en dat betrokkenen derhalve verplicht zijn om elektronisch aangifte te doen, tenzij zij een ontheffing hebben van deze verplichting.

Blijkens de tekst van art. 20 van de Uitvoeringsregeling wordt ontheffing verleend wanneer het doen van elektronische aangifte onredelijk bezwarend is voor de administratieplichtige. Op het formulier waarmee de ontheffing kon worden aangevraagd stond dat ontheffing alleen zou worden verleend wanneer de administratieplichtige niet over een computer beschikt. Eisers hebben daarom geen ontheffing aangevraagd. De rechtbank oordeelt dat het ontbreken van een ontheffing de eisers daarom niet kan worden tegengeworpen. De rechtbank verwijst naar de parlementaire behandeling van de

136 Rb. Arnhem 25 april 2007, *LJN* BA4054, *NTR* 2007, 905 (Geen elektronische aangifte bij belastingdienst).

bepaling, waarbij is opgemerkt dat bij de invulling van het criterium ‘onredelijk bezwarend’ als uitgangspunt zou worden gehanteerd dat er geen ontheffing wordt verleend indien de administratieplichtige de administratie geautomatiseerd voert, of de aangifte laat opstellen door een derde die daarbij gebruik maakt van geautomatiseerde systemen. De rechtbank oordeelt dat verweerder de brief van eiser waarin hij aangeeft van mening te zijn dat het doen van elektronische aangifte voor hem onredelijk bezwarend is, had moeten aanmerken als een verzoek om een ontheffing. De rechtbank onderzoekt vervolgens zelf of aan eisers ontheffing had moeten worden verleend:

‘De rechtbank is van oordeel dat eisers aannemelijk hebben gemaakt dat zij in 2005 niet in staat waren om zonder hulp van derden de aangifte elektronisch te versturen. Gezien de beperkte omvang van hun ondernemingen en de daaraan gekoppelde (relatief) beperkte administratieplicht, is de rechtbank van oordeel dat niet van eisers mag worden verwacht dat zij investeren in het opdoen of inkopen van kennis op het gebied van computers en interne, uitsluitend om aan hun elektronische aangifteverplichting te kunnen voldoen. Evenmin kunnen zij worden verplicht om het doen van aangifte uit te besteden aan een derde. De daarmee gemoeide kosten zijn in het licht van de beperkte inkomsten uit hun ondernemingen relatief te hoog. De rechtbank acht het doen van elektronische aangifte voor eisers in 2005 daarom onredelijk bezwarend. Dit brengt mee dat de rechtbank van oordeel is dat verweerder aan eisers ontheffing had moeten verlenen.’

In een uitspraak met grotendeels identieke overwegingen ten aanzien van het beginsel van nevenschikking en de voorrang van de bijzondere wet, oordeelt de rechtbank Haarlem in een zaak, waarbij bezwaar en beroep is ingesteld tegen een boetebeschikking die is opgelegd wegens het niet tijdig doen van aangifte op elektronische wijze als volgt:¹³⁷

‘In casu is niet in geschil dat eiseres tijdig de papieren aangifte heeft ingediend. Hoewel dit geen aangifte is op de voorgeschreven wijze, volgt hieruit wel dat de aangifte van eiseres tijdig klaar was voor de verzending. Eiseres heeft aangevoerd dat zij op 11 januari 2006 heeft getracht de aangifte elektronisch te verzenden. Eiseres stelt dat zij wel in het persoonlijk domein kon komen, maar de aangifte daarin niet op kon halen. Verweerder stelt dat niet uit het systeem blijkt dat eiseres op die dag in het persoonlijk domein is geweest. Verweerder heeft echter ter zitting ook verklaard dat er landelijk veel problemen zijn geweest met het inloggen. De rechtbank acht het aannemelijk dat eiseres op 11 januari 2006 heeft gepoogd de aangifte elektronisch te verzenden. (...). Gezien de onder 4.13 opgenomen feiten en omstandigheden is de rechtbank van oordeel dat eiseres alle van haar in redelijkheid te vergen zorg heeft betracht om te bewerkstelligen dat de aangifte tijdig op de juiste wijze bij verweerder werd ingediend. Hierin ligt besloten dat er sprake is van afwezigheid van alle schuld van eiseres. Dat er nog andere manieren waren om de aangifte in te dienen doet daar niet aan af, nu elke manier deugdelijk dient te werken.’

137 Rb. Haarlem 16 augustus 2007, *LJN* BB2114, r.o. 4.13 en 4.14, *NTFR* 2007, 1581 (Inlogproblemen bij belastingdienst).

In de eerste genoemde zaak wordt een afweging gemaakt tussen de verplichting om de aangifte elektronisch in te dienen en de lasten die dit voor de administratieplichtige met zich mee brengt. In dit specifieke geval, gezien de omvang van de onderneming van de betrokkene, werd het als onredelijk bezwarend aangemerkt de betrokkene te verplichten de aangifte elektronisch in te dienen. In de tweede zaak functioneerde kennelijk de software waarmee elektronisch aangifte moest worden gedaan, niet. Aangezien bleek dat betrokkene alle zorg had betracht om tijdig de elektronische aangifte te verzenden en vervolgens tijdig de aangifte op papier had ingediend, mocht het bestuursorgaan betrokkene geen boete opleggen wegens het niet tijdig doen van aangifte op de voorgeschreven wijze.

3.4.2 Bekendmakingswet

In de Wet elektronische bekendmaking die op 1 juli 2009 inwerking is getreden, is het beginsel van de nevenschikking expliciet verlaten.¹³⁸ Deze wet gaat uit van elektronische bekendmaking van wetten en besluiten van algemene strekking, waarbij de conventionele bekendmaking komt te vervallen. De voorgestelde wijzigingen betreffen niet alleen de bekendmaking van besluiten die algemeen verbindende voorschriften inhouden, maar ook besluiten waarop het bekendmakingsregime van art. 3:42 Awb van toepassing is. Het naast elkaar bestaan van twee bekendmakingsystemen wordt ongewenst genoemd, vanwege het risico van het optreden van verschillen in de gepubliceerde tekst dan wel verschillen in de datum van publicatie. In de memorie van toelichting wordt hierover gesteld dat er van beperking van de toegankelijkheid door alleen elektronische bekendmaking mogelijk te maken geen sprake is, aangezien de groep abonnees hoofdzakelijk uit professionele beroepsbeoefenaars bestaat, die tevens toegang tot internet hebben.¹³⁹ De officiële publicatiebladen vormen daarom in de praktijk geen alternatief voor burgers die (nog) geen toegang hebben tot het internet.

Ook wordt in de memorie van toelichting bij dit wetsvoorstel gesteld dat de toepassing van elektronische communicatiemiddelen de transparantie vergroot. Dit omdat elektronische informatie op zeer veel plaatsen toegankelijk is, 24 uur per dag bereikbaar is en vaak kosteloos kan worden geraadpleegd. De gedrukte versies van het Staatsblad en de Staatscourant zijn daartegen slechts op een verkoopadres in Den Haag verkrijgbaar. Een abonnement op het Staatsblad kost ca € 850 per jaar en dit blad heeft ca 700 abonnees. Een abonnement op de Staatscourant kostte in 2005 € 317; dit blad heeft 8000 abonnees.¹⁴⁰

138 *Kamerstukken II* 2006/07, 31 084, nr. 2.

139 *Kamerstukken II* 2006/07, 31 084, nr. 3, p. 11.

140 *Kamerstukken II* 2006/07, 31 084, nr. 3, p. 6.

Elektronische bekendmaking van wetten, algemeen verbindende voorschriften en andere besluiten van algemene strekking, zonder deze nog op de conventionele wijze bekend te maken, vergroot volgens dit wetsvoorstel dan ook de toegankelijkheid en transparantie van deze regelingen en besluiten. De groep die door de elektronische bekendmaking bereikt zal kunnen worden, is aanzienlijk groter dan de groep die bereikt wordt door de huidige uitgifte van de conventionele, papieren versie.

3.4.3 Dienstenwet en Dienstenrichtlijn

Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006, betreffende diensten op de interne markt (de Dienstenrichtlijn) beoogt blijkens overweging 5 uit de preambule, belemmeringen voor de vrijheid van vestiging van dienstverleners in de lidstaten en voor het vrije verkeer van diensten tussen lidstaten te verwijderen. Verder beoogt de Dienstenrichtlijn de afnemers en verrichters van diensten de nodige rechtszekerheid te bieden, zodat twee fundamentele vrijheden (het vrije verkeer van diensten en de vrijheid van vestiging door dienstverrichters) daadwerkelijk kunnen worden uitgeoefend. Een van de middelen waarmee dit doel bereikt moet worden, is het wegnemen van overmatig belastende procedures en formaliteiten. In overweging 52 van de preambule staat dat de invoering van een elektronisch systeem voor de afwikkeling van procedures en formaliteiten een noodzakelijke voorwaarde is om te komen tot die administratieve vereenvoudiging. In de richtlijn staat dit in het eerste lid van art. 8 als volgt geformuleerd: ‘De lidstaten zien erop toe dat alle procedures en formaliteiten betreffende de toegang tot en de uitoefening van een dienstenactiviteit eenvoudig, op afstand en met elektronische middelen via het betrokken één-loket en met de relevante bevoegde instanties kunnen worden afgewikkeld.’ Dit betekent dat de procedures, waaronder het aanvragen van eventueel vereiste vergunningen, elektronisch moeten kunnen worden afgehandeld. Dit voorschrift is in zoverre een inbreuk op het uitgangspunt van de nevenschikking, dat het bevoegde bestuursorgaan hierdoor verplicht wordt om procedures elektronisch af te handelen. Het bestuursorgaan heeft niet meer de mogelijkheid om de elektronische weg niet open te stellen.

In de wet ‘Implementatie van Europese regelgeving betreffende het verkeer van diensten op de interne markt (Dienstenwet)’ wordt deze verplichting geïmplementeerd.¹⁴¹ In art. 5 van deze wet staat:

1. Onze Minister draagt zorg voor de inrichting, instandhouding, werking en beveiliging van een centraal loket met behulp waarvan:

141 *Kamerstukken II* 2007/08, 31 579, nr. 2 en het gewijzigd voorstel van wet *Kamerstukken I*, 2008/09, 31 579A.

a. ten behoeve van dienstverrichters:

1. informatie toegankelijk wordt gemaakt die van belang is voor het verkrijgen van toegang tot of de uitoefening van diensten;
2. berichtenverkeer dat betrekking heeft op procedures en formaliteiten wordt uitgewisseld tussen dienstverrichters en bevoegde instanties.

(...)

2. Het centraal loket is gemakkelijk langs elektronische weg bereikbaar.

(...)

De wet voorziet in de inrichting van een centraal loket onder de verantwoordelijkheid van de minister van Economische zaken. Dit is het één-loket zoals dat is genoemd in de richtlijn. Het centraal loket is blijkens het tweede lid van art. 5 gemakkelijk langs elektronische weg bereikbaar.

Zoals hierboven al uiteengezet, vormt art. 8 Dienstenrichtlijn een inbreuk op het uitgangspunt van de nevenschikking voor het bestuursorgaan. Een bestuursorgaan heeft niet meer de keuze om de elektronische weg open te stellen, het moet de elektronische weg openstellen. De conventionele weg staat echter nog steeds open, de keus is aan de dienstverrichter.¹⁴²

In het vijfde en zesde lid van art. 12 Dienstenwet staat:

5. Een bevoegde instantie verzendt een bericht met de verzochte informatie als bedoeld in het eerste lid, of een mededeling als bedoeld in het derde lid, langs elektronische weg, voor zover een dienstverrichter waarvoor het bericht bestemd is aan de bevoegde instantie kenbaar heeft gemaakt dat hij langs deze weg voldoende bereikbaar is.
6. Het vijfde lid geldt, voor zover van toepassing, in afwijking van artikel 2:14, eerste lid, van de Algemene wet bestuursrecht.

Het gaat in deze bepaling om berichten van informatieve aard, om het verlenen van bijstand aan dienstverrichters. Art. 13 Dienstenwet geeft regels over berichtenverkeer die betrekking hebben op procedures en formaliteiten. Op grond van het eerste lid van deze bepaling verloopt alle elektronische berichtenverkeer tussen dienstverrichter en de bevoegde instantie via dit elektronische loket. Art. 13, eerste lid, luidt als volgt:

Onze minister biedt een dienstverrichter respectievelijk een bevoegde instantie de mogelijkheid berichten die betrekking hebben op procedures en formaliteiten via het centraal loket te verzenden en te ontvangen.

De verplichting voor bevoegde instanties zich aan te sluiten bij het centraal loket staat opgenomen in art. 14 van de wet. Daar staat:

142 De verschillende onderdelen van de Dienstenwet zijn op verschillende data in december 2009 in werking getreden, bij koninklijk besluit van 26 november 2009, houdende vaststelling van het tijdstip van inwerkingtreding van de Dienstenwet, het Dienstenbesluit centraal loket en enkele artikelen van het Aanpassingsbesluit dienstenrichtlijn.

1. Een bevoegde instantie die betrokken is bij de afwikkeling van procedures en formaliteiten:
 - a. draagt zorg voor aansluiting op het centraal loket;
 - b. verzendt daarop betrekking hebbende berichten via het centraal loket, voor zover een dienstverrichter waarvoor een bericht is bestemd via het centraal loket aan de bevoegde instantie kenbaar heeft gemaakt dat hij langs deze weg voldoende bereikbaar is.
 - c. draagt er zorg voor dat zij via het centraal loket voldoende bereikbaar is voor daarop betrekking hebbende berichten van een dienstverrichter.
2. (...)
3. Het eerste lid geldt, voor zover van toepassing, in afwijking van artikel 2:14, eerste lid, van de Algemene wet bestuursrecht.

Duidelijk is dat de Dienstenrichtlijn een inbreuk vormt op het uitgangspunt van de nevenschikking. Op grond van deze richtlijn worden de bevoegde organen verplicht om elektronisch te communiceren. Bij de implementatie van deze richtlijn in de Dienstenwet is ervoor gekozen om een centraal loket in te stellen, onder verantwoordelijkheid van de minister van Economische Zaken.

Op dit moment is echter nog geen Europees systeem beschikbaar waarmee een elektronische handtekening geplaatst kan worden. De DigiD maakt gebruik van het Burger Service Nummer, waar buitenlandse dienstverrichters niet over beschikken.¹⁴³

3.4.4 Wet ruimtelijke ordening en Wet algemene bepalingen omgevingsrecht

De bedoeling van de Wro, die op 1 juli 2008 in werking is getreden, is dat alle bestemmingsplannen elektronisch raadpleegbaar worden. Dit staat nader geregeld in het Besluit ruimtelijke ordening (Bro). Op 1 juli 2009 is de verplichting uit art. 1.2.1 Bro in werking getreden tot het in digitale vorm beschikbaar stellen van bestemmingsplannen. In de memorie van toelichting bij de Wro staat dat digitalisering een belangrijk hulpmiddel is voor het bereiken van efficiënte, effectieve en voor burgers toegankelijke besluitvormingsprocessen op het terrein van de ruimtelijke ordening. Volgens de regering kunnen digitale plannen sneller worden gemaakt, getoetst en geactualiseerd dan analoge plannen. Het planproces zal daardoor efficiënter en effectiever kunnen verlopen. Digitaal beschikbare informatie kan tussen overheden onderling en tussen overheid en burger op een snelle manier worden uitgewisseld. Ook de gebruiker van ruimtelijke plannen kan via internet op een eenvoudige en snelle manier informatie beschikbaar krijgen en raadplegen.¹⁴⁴ Een gelijklopende motivering is te vinden in de nota van toelichting bij het

143 Er zijn wel initiatieven om interoperabiliteit van eID systemen (zoals de DigiD) op EU schaal mogelijk te maken, bijvoorbeeld STORK: <http://www.eid-stork.eu/>.

144 *Kamerstukken II* 2002/03, 28 916, nr. 3, p. 70-71.

Besluit ruimtelijke ordening.¹⁴⁵ In deze nota van toelichting staat ook uitgelegd wat onder een digitaal bestemmingsplan wordt verstaan:

‘Een digitaal bestemmingsplan is een elektronisch weergegeven plan waarin een koppeling is gelegd tussen geografische en administratieve gegevens met gebruikmaking van een objectgerichte kaart. Door te “klikken” op een deel van het objectgerichte kaartbeeld worden alle relevante gegevens en beleidsinformatie van dat deel (object) op het kaartbeeld getoond. Het object op het kaartbeeld is dus de ingang tot de achterliggende informatie. Veel voorkomende objecten op het kaartbeeld zijn bijvoorbeeld: bestemmingsvlakken, bouwvlakken en aanduidingen. In tegenstelling tot wat gebruikelijk is bij een traditioneel vervaardigd bestemmingsplan, behoeft de ligging van een bestemming bij een digitaal bestemmingsplan niet te blijken uit het gebruikte kaartmateriaal en de ondergrond waarop een kaart is getekend, maar slechts of juist uit de geografische coördinaten volgens het Rijksdriehoekstelsel. Met gebruikmaking van de coördinaten kan in de eerste plaats exact de plaats van een object in een gebied worden bepaald. Daarnaast is koppeling mogelijk met andere (digitale) informatie die volgens dat stelsel is opgebouwd.’

Om recht te doen aan het uitgangspunt van de nevenschikking is in art. 1.2.2, vierde lid, Besluit ruimtelijke ordening bepaald dat de volledige geautoriseerde verbeelding van het plan op papier beschikbaar moet zijn bij de hoofdzetel van het betrokken bestuursorgaan. Verder is in het derde lid van dit artikel bepaald dat bij dat bestuursorgaan de digitale versie langs elektronische weg geraadpleegd moet kunnen worden. Het tweede lid van art. 1.2.2 Bro bepaalt dat de elektronische beschikbaarstelling een toegankelijke en begrijpelijke verbeelding van het betrokken document omvat.

Ten aanzien van de authenticiteit staat vervolgens in art. 1.2.3 Bro bepaald dat bij ministeriële regeling regels worden gesteld voor het waarborgen van de authenticiteit van de documenten. De nota van toelichting bepaalt hierover dat authenticiteit betrekking heeft op de oorsprong van de informatie: is de informatie het oorspronkelijke document, is de informatie werkelijk van de afzender afkomstig en is de afzender werkelijk degene voor wie hij zich uit geeft. Een van de elementen van de maatregelen om de authenticiteit te waarborgen is volgens deze toelichting dat gewerkt zal worden met een elektronische handtekening, die voldoet aan de eisen die de Awb daaraan stelt.¹⁴⁶

Voor de ruimtelijke plannen van alle overheden komt een landelijke toegangspoort, namelijk www.ruimtelijkeplannen.nl

Voor de toepassing van afdeling 3.4 Awb, vereist art. 3.8, eerste lid, Wro dat het ontwerp-bestemmingsplan tevens langs elektronische weg beschikbaar wordt gesteld. Volgens de Afdeling houdt deze verplichting in dat het ontwerpbestemmingsplan langs elektronische weg moet kunnen worden

145 *Kamerstukken II 2006/07, bijlage bij 30 218, nr. 23, p. 8.*

146 *Kamerstukken II 2006/07, bijlage bij 30 218, nr. 23, p. 9.*

geraadpleegd, niet dat het ook in zijn geheel moet kunnen worden gedownload.¹⁴⁷

De Wet algemene bepalingen omgevingsrecht (Wabo), die op 1 oktober 2010 in werking is getreden, bepaalt in art. 2.8, eerste lid:

Bij of krachtens algemene maatregel van bestuur worden regels gesteld met betrekking tot de wijze waarop de aanvraag om een omgevingsvergunning geschiedt en de gegevens en bescheiden die door de aanvrager worden verstrekt met het oog op de beslissing op de aanvraag. Bij de maatregel kan – in afwijking van de artikelen 2:14, eerste lid, en 2:15 van de Algemene wet bestuursrecht – worden bepaald dat de aanvraag geheel of gedeeltelijk elektronisch wordt ingediend of in ontvangst wordt genomen. Daarbij kan worden bepaald dat de verplichtingen slechts gelden in daarbij aangewezen categorieën gevallen.

De algemene maatregel van bestuur waarnaar verwezen wordt, is het Besluit omgevingsrecht (Bor). Daar bepaalt art. 4.1 dat een aanvraag langs elektronische weg kan worden ingediend. In art. 4.3, eerste lid, Bor wordt afgeweken van het uitgangspunt van de nevenschikking voor bestuursorganen:

In afwijking van artikel 2:15, eerste en tweede lid, van de Algemene wet bestuursrecht, neemt het bevoegd gezag een aanvraag die langs elektronische weg wordt ingediend, in ontvangst.

Het bestuursorgaan heeft hier geen keuze meer, het moet elektronische communicatie mogelijk maken.

3.4.5 Overig

Naast de hierbovengenoemde afwijkingen op het uitgangspunt van de nevenschikking probeert de overheid ook meer door ‘zachte druk’ burgers ertoe te krijgen om elektronisch te communiceren. De elektronische communicatie is dan de norm, de conventionele de uitzondering. Voor de conventionele vorm moet de burger dan meer moeite doen,¹⁴⁸ of het bestuursorgaan geeft aan dat de aanvraag die op conventionele wijze plaats vindt, een langere behandeltermijn heeft.¹⁴⁹ Volgens Overkleeft-Verburg is de belangrijkste drijfveer hiervoor het behalen van efficiencywinst voor de overheid zelf, en staat het halen van reductie van bestuurslasten hierbij voorop.¹⁵⁰

Ook komt het voor dat, wanneer beide vormen in formele zin naast elkaar mogelijk zijn, de gebruikers van de conventionele communicatievorm in

147 ABRvS 21 april 2010, *LJN* BM1793, *AB* 2010, 163 m.nt. de Gier (Downloaden ontwerpbestemmingsplan).

148 Overkleeft-Verburg 2008, p. 24.

149 Damen 2010b, p. 161.

150 Overkleeft-Verburg 2009, p. 71.

het nadeel zijn doordat een elektronisch aanvraagformulier het bestuursorgaan eerder bereikt. Bijvoorbeeld in een situatie van een subsidieregeling met een subsidieplafond, waarbij is bepaald dat aanvragen op volgorde van ontvangst in behandeling worden genomen. Wordt een dergelijke subsidieregeling opengesteld bij het begin van de dag, om 0.00 uur, dan kan het subsidieplafond al bereikt zijn door elektronische aanvragen, voordat de conventionele aanvragen het bestuursorgaan überhaupt hebben kunnen bereiken.¹⁵¹ In een dergelijk geval heeft het uitgangspunt van de nevenschikking niet veel praktische betekenis meer. Wil er echt sprake zijn van nevenschikking, dan moet het bestuursorgaan er ook voor zorgen dat beide communicatievormen daadwerkelijk, in materiële zin, gelijk aan elkaar zijn.

3.4.6 Conclusie nevenschikking

Het uitgangspunt van de nevenschikking is ingevoerd door de wetgever om enerzijds de burger tegemoet te komen die niet over internet beschikt, en anderzijds bestuursorganen tegemoet te komen die hun werkprocessen (nog) niet hebben aangepast aan elektronisch berichtenverkeer. Inmiddels zijn er meerdere uitzonderingen op dit uitgangspunt.

De uitzonderingen hebben met elkaar gemeen dat zij betrekking hebben op burgers in de uitoefening van hun beroep. De verplichting om elektronisch aangifte te doen betreft immers ondernemers. Ook de elektronische bekendmaking van Staatsblad en Staatscourant raakt de beroepsbeoefenaars, want deze vormen volgens de parlementaire stukken hoofdzakelijk het abonneebestand van deze bladen. De uitzondering op grond van de Dienstenrichtlijn betreft overigens niet een verplichting voor de burger om elektronisch te communiceren; deze heeft de keuze. De verplichting geldt hier de overheid. Deze is verplicht om elektronisch berichtenverkeer mogelijk te maken.

De jurisprudentie, voor zover aanwezig, over de verplichting voor de burger om elektronisch te communiceren, betreft de belastingwetgeving. De jurisprudentie ziet er afgewogen uit en oordeelt dat het voor een burger onredelijk bezwarend kan zijn om verplicht te worden elektronisch aangifte te doen. Overigens speelde de geringe omvang van het bedrijf hierbij een nadrukkelijke rol. Ook biedt de jurisprudentie ruimte om af te wijken van de verplichting om elektronisch aangifte te doen indien de software, waarmee de

151 Zoals gebeurde bij de Subsidie stimulering energiebesparende maatregelen van de provincie Groningen, <http://www.provinciegroningen.nl/energiekgroningen/energieloket/subsidiebesparende maatregelen>.

aangifte gedaan had moeten worden, niet functioneerde. Betrokkene had voldoende zorg betracht om tijdig elektronisch aangifte te doen.

Met betrekking tot het uitgangspunt van de nevenschikking is, als het gaat om burgers, meer en meer sprake van zachte dwang, uitgeoefend door de overheid jegens de burger, om digitaal te communiceren. Ook lijkt het uitgangspunt in de praktijk aan betekenis te verliezen, doordat burgers die elektronisch communiceren, bijvoorbeeld bij het aanvragen van subsidie op grond van een regeling met een subsidieplafond, in het voordeel zijn ten aanzien van hen die gebruik maken van de conventionele weg. Ten aanzien van beroepsbeoefenaars wordt het uitgangspunt van de nevenschikking verlaten. Dat stuit in het algemeen niet op problemen. Wel blijkt uit de beperkte jurisprudentie dat een uitlaatklep noodzakelijk is. Indien elektronische communicatie onredelijk bezwarend is, moet onder omstandigheden conventionele communicatie mogelijk gemaakt worden.

Ook worden wetten, algemeen verbindende voorschriften en bestemmingsplannen elektronisch bekend gemaakt, en is de elektronische bekendmaking leidend. Overheidsorganen hebben ook niet altijd meer de keuze: de Dienstenwet bepaalt dat in het kader van te verrichten diensten elektronisch moet kunnen worden gecommuniceerd.

Geconstateerd kan worden dat, ondanks het uitgangspunt van de nevenschikking, elektronische communicatie de norm wordt, en de conventionele wijze van communicatie de uitzondering aan het worden is.

3.5 Kenbaar maken dat elektronisch verkeer mogelijk is

Elektronische communicatie is op grond van de Awb in het algemeen alleen dan mogelijk als zowel het bestuursorgaan als de burger kenbaar hebben gemaakt dat de elektronische weg openstaat. Voor de burger volgt dit uit art. 2:14, eerste lid, Awb en voor het bestuursorgaan volgt dit uit art. 2:15 eerste lid, Awb. Over de wijze waarop de burger kenbaar maakt langs elektronische weg bereikbaar te zijn, wordt in de memorie van toelichting bij afdeling 2.3 opgemerkt dat voorlopig van uitdrukkelijk kenbaar maken moet worden uitgegaan.¹⁵² De bekendheid van een e-mailadres van de burger bij het bestuursorgaan is in de huidige situatie niet voldoende. De burger zal moeten aangeven voor een bepaald bericht of voor een bepaalde berichtenuitwisseling elektronisch bereikbaar te zijn en tevens op welk adres hij bereikbaar is. In de memorie van toelichting wordt aangenomen dat het elektronisch indienen van een verzoek niet hetzelfde is als kenbaar maken langs elektronische weg bereikbaar te zijn. Dit kenbaar maken moet door de burger expliciet tot uitdrukking worden

152 *Kamerstukken II 2001/02, 28 483, nr. 3, p. 11.*

gebracht. Bij ontbreken van een expliciete verklaring van een burger mag een bestuursorgaan niet zonder daarnaar bij de burger te hebben geïnformeerd, gebruik maken van de elektronische weg. Verzoekt een burger expliciet om toezending op klassieke wijze, dan moet het bestuursorgaan hieraan voldoen.¹⁵³ Overigens houdt de wetgever in de memorie van toelichting een slag om de arm ten aanzien van de voorwaarde dat het kenbaar maken door de burger door middel van een expliciete verklaring moet plaats vinden. Dit wordt duidelijk uit de opmerking dat de enkele bekendheid van een e-mailadres in de huidige situatie niet zonder meer voldoende is. Vervolgens wordt opgemerkt dat gewoonten en conventies door de snelle ontwikkelingen snel aan wijzigingen onderhevig zijn en dat er daarom is gekozen voor algemene bewoordingen die ruimte laten aan de praktijk en jurisprudentie om rekening te houden met nieuwe ontwikkelingen.¹⁵⁴ Verzoekt een burger een bestuursorgaan om elektronisch te communiceren, en voldoet het bestuursorgaan aan dit verzoek, dan kan de burger er ook op vertrouwen dat de correspondentie op elektronische wijze wordt verzonden.¹⁵⁵ In deze zaak had appellante het bestuursorgaan verzocht om haar alle correspondentie over haar aanvraag per e-mail toe te zenden wegens haar verblijf in het buitenland. Het bestuursorgaan had aan dit verzoek voldaan en e-mailde haar de correspondentie, behalve het primaire besluit waartegen zij bezwaar wilde maken. Dit bezwaar maakte zij dan ook te laat omdat zij de (papieren) brief te laat aantrof. De CRvB oordeelt in r.o. 2.3:

‘De onder 1.2 genoemde brief van 16 februari 2008, die zich onder de gedingstukken bevindt, is gericht aan de PUR, Raadskamer WUBO, en vermeldt alleen het specifieke correspondentienummer voor de Wubo. Een dergelijke brief aan verweerster ontbreekt onder de gedingstukken. Gelet op het samenloopkarakter van de aanvraag acht de Raad echter het eventueel ontbreken van een expliciet verzoek om ook Wuv-stukken via e-mail toe te zenden niet doorslaggevend. In aanmerking genomen dat door de PUR niet afwijzend is gereageerd op de brief van appellante van 16 februari 2008 doch integendeel het besluit over de toepassing van de Wubo wel via e-mail is toegezonden, kon en mocht appellante er naar het oordeel van de Raad op rekenen dat ook het primaire besluit Wuv via e-mail zou worden toegezonden. Een en ander betekent dat verweerster het primaire besluit Wuv in feite aan het verkeerde adres heeft gezonden.’

3.5.1 Toepassing art. 2:15 Awb

Uit art. 2:15 Awb volgt dat een bericht alleen elektronisch naar een bestuursorgaan kan worden verzonden indien het bestuursorgaan kenbaar heeft gemaakt dat deze weg geopend is. In een uitspraak van het Gerechtshof

153 CRvB 14 oktober 2010, *LJN* BO1902 (Overuren jeugdtheater).

154 *Kamerstukken II* 2001/02, 28 483, nr. 3, p. 12.

155 CRvB 10 december 2009, *LJN* BK7208, *AB* 2010, 131 m.nt. A.M. Klingenberg (Wuv-besluit).

Leeuwarden werd geanticipeerd op art. 2:15 Awb.¹⁵⁶ Het ging hier, samengevat, om een beroepschrift dat op tijd per e-mail bij de officier van justitie was ingediend, maar te laat per brief. Welk tijdstip van ontvangst moest nu gelden, het tijdstip van ontvangst van het e-mailbericht dat op tijd was, of het tijdstip van ontvangst van de (papieren) brief, die te laat was? Het Hof oordeelde hier dat ‘niet is gebleken dat de officier van justitie heeft kenbaar gemaakt dat hij langs elektronische weg voldoende bereikbaar is en dat voor de ontvangst van beroepschriften een procedure is ontwikkeld, die recht doet aan de eisen van onder meer art. 6:5 Awb.’ Er was dus niet op grond van art. 2:15 Awb kenbaar gemaakt dat de elektronische weg geopend was en er kon dus niet per e-mail beroep ingesteld worden. Het (papieren) beroep was te laat en werd daarom niet-ontvankelijk verklaard.

Voor bestuursorganen geldt, net als bij burgers, dat het bestaan van een e-mailadres nog niet betekent dat de elektronische weg openstaat.¹⁵⁷ Ook hier vereist het kenbaar maken een expliciete verklaring van het bestuursorgaan. Dit kenbaar maken kan plaatsvinden in een algemene regeling als in een bericht aan een of meer geadresseerden, bijvoorbeeld door plaatsing in een huis-aan-huis blad, of op de website. Indien een elektronisch bericht naar het bestuursorgaan wordt verzonden, zonder dat dit heeft kenbaar gemaakt dat deze weg openstaat, kan het bestuursorgaan op die grond weigeren het bericht te accepteren. Dit is echter geen verplichting, het staat het bestuursorgaan vrij om het bericht toch te accepteren. Uit het zorgvuldigheidsbeginsel volgt dat in een geval waarin een bericht elektronisch is ingediend terwijl deze weg niet opengesteld is, het bestuursorgaan betrokkene erop zal moeten wijzen dat het bericht op een andere wijze ingediend zal moeten worden.

Dit blijkt uit een uitspraak over het indienen van bedenkingen per e-mail, uit de periode voor de inwerkingtreding van afd. 2.3 Awb.¹⁵⁸ Deze werden door het betrokken bestuursorgaan niet geaccepteerd aangezien de bedenkingen niet schriftelijk (waarmee werd bedoeld: op papier) waren ingediend. De Afdeling constateerde dat door de bedenkingen per e-mail in te dienen, niet is voldaan aan de in art. 3:24, eerste lid, Awb genoemde eis van schriftelijkheid. Wel overweegt de Afdeling in r.o. 2.2.4:

‘Dit laat echter onverlet dat uit art. 3:2 Awb en het algemene rechtsbeginsel dat een besluit met de nodige zorgvuldigheid dient te worden genomen volgt dat een bestuursorgaan, wanneer appellanten per e-mail kenbaar hebben gemaakt bedenkingen te hebben, hen er op zou moeten attenderen dat zij deze bedenkingen alsnog op de in de Awb voorgeschreven

156 Hof Leeuwarden 9 juli 2003, *LJN* AI0434, *JB* 2003, 277 (Beroep per e-mail niet-ontvankelijk).

157 *Kamerstukken II* 2001/02, 28 483, nr. 3, p. 13.

158 ABRvS 10 september 2003, *LJN* AJ3308, *AB* 2004, 34 m.nt. Michiels, *BR* 2003, 1050, *JB* 2003, 295, *JM* 2004, 3 m.nt. Zigenhorn (Bedenkingen per e-mail).

wijze kunnen inbrengen, alvorens de per e-mail ingebrachte bedenkingen niet in behandeling te nemen.⁷

In dit geval was dat niet gebeurd. Appellanten hadden de bedenking echter pas om 19.18 uur op de laatste dag van de termijn gemaaild. Daarom was het voor het bestuursorgaan onmogelijk om appellanten er nog op te attenderen dat de bedenkingen nog binnen de termijn op een andere wijze ingediend hadden moeten worden. Dus was er in casu geen reden om te oordelen dat het besluit onzorgvuldig of in strijd met art. 3:2 Awb was genomen.

Een bestuursorgaan kan op grond van art. 2:15 Awb differentiëren. Zo kan hetzelfde bestuursorgaan voor het ene beleidsterrein elektronische communicatie wel mogelijk maken, en voor het andere niet. Dit is onder meer afhankelijk van de eisen die aan de communicatie gesteld worden, van de aard van de communicatie en van de inrichting van de organisatie van het bestuursorgaan (is die ingericht op elektronisch berichtenverkeer?). Overigens neemt de rechtbank Arnhem voor bestuursorganen die de elektronische weg niet opengesteld hebben, bijvoorbeeld voor faxverkeer, wel aan dat het bestuursorgaan de fax moet doorsturen naar de rechtbank, met toepassing van art. 6:15 Awb.¹⁵⁹ In deze casus had de belanghebbende per fax bezwaar gemaakt bij de belastingdienst, terwijl beroep ingesteld had moeten worden. De belastingdienst maakt het indienen van bezwaar per fax niet mogelijk. Desondanks had de dienst het faxbericht door moeten sturen naar de bevoegde rechtbank.

Expliciete kenbaarmaking is niet vereist indien er sprake is van een bestendige bestuurlijke praktijk. In een uitspraak over een Wob-verzoek, oordeelt de Afdeling:¹⁶⁰

‘Vaststaat dat beide politieregio’s niet uitdrukkelijk kenbaar hebben gemaakt dat de elektronische weg voor het doen van Wob-verzoeken is geopend. Anders dan de rechtbank heeft aangenomen, kan een bestendige bestuurlijke praktijk waarbij Wob-verzoeken reeds vele malen via de elektronische weg zijn ingediend en hierop is besloten grond bieden voor het oordeel dat aan de verzoeker kenbaar is gemaakt dat de elektronische weg voor dergelijke verzoeken is geopend.’

Een vraag die overblijft na het lezen van deze uitspraak is of een derde, die niet elektronisch met het bestuursorgaan heeft gecommuniceerd, zich dan ook op

159 Rb. Arnhem, 16 augustus 2007, *LJN* BB1983 (Doorzendplicht bij elektronisch verkeer).

160 *ABRvS* 29 april 2008, *LJN* BD0772, *AB* 2008, 202 m.nt. P.J. Stolk, *JB* 2008, 130 (Kenbaar maken door bestendige praktijk).

deze bestendige praktijk kan beroepen. In elk geval past de Afdeling hier art. 2:15 Awb naar haar bedoeling toe.¹⁶¹

In een volgende uitspraak wordt art. 2:15 weer op een formalistische wijze toegepast. Deze uitspraak gaat evenals de vorige over een Wob-verzoek, ingediend bij een politieregio. Het verzoek was elektronisch ingediend via het e-mailadres info@rijnmond.politie.nl. In deze uitspraak oordeelt de Afdeling dat uit het feit dat op de website van een bestuursorgaan aan het publiek de gelegenheid wordt geboden om vragen te stellen door het invullen van een formulier, op zichzelf niet voortvloeit dat de elektronische weg geopend is voor het indienen van verzoeken als bedoeld in art. 3, eerste lid, van de Wob. Uit het feit dat aan het op de website van de politieregio Rotterdam-Rijnmond geplaatste vragenformulier het e-mailadres info@rijnmond.politie.nl was verbonden, kan gelet op het algemene karakter van het formulier en het e-mailadres, niet worden afgeleid dat dit formulier behalve voor het stellen van publieksvragen ook voor het indienen van verzoeken als bedoeld in art. 3, eerste lid, van de Wob was bestemd.¹⁶² De vraag is wat het verschil is tussen een verzoek om informatie als waarvoor het betreffende e-mailadres bedoeld is, een publieksvraag, en een verzoek om informatie als bedoeld in art. 3 Wob. Wordt op een website van een overheidsorgaan de mogelijkheid geboden om informatie op te vragen, dan omvat dit naar mijn mening de mogelijkheid om een Wob-verzoek in te dienen. In de memorie van toelichting bij de Wob werd destijds door de regering opgemerkt:¹⁶³

‘Voorop staat dat elk verzoek om informatie over een bestuurlijke aangelegenheid dient te worden aangemerkt als een verzoek op grond van de WOB. Bij een verzoek om informatie hoeft dus niet uitdrukkelijk een beroep op de WOB te worden gedaan. De wijze waarop het verzoek is gedaan, kan derhalve verschillend zijn: mondeling in een persoonlijk onderhoud, telefonisch, schriftelijk per brief of per telegram. Wij achten het niet noodzakelijk de manieren waarop een verzoek kan worden gedaan uitdrukkelijk in de wet te noemen. (...) Bovendien kan het noemen van bepaalde wijzen van verzoeken vragen oproepen indien in de toekomst andere vormen algemeen mogelijk worden die thans nog niet worden gebruikt, bijvoorbeeld via beeldschermen.’

Vast staat dat het verzoek een Wob-verzoek betrof. Volgens de parlementaire geschiedenis van de Wob moet elk verzoek om informatie over een bestuurlijke aangelegenheid aangemerkt worden als een Wob-verzoek. Verder blijkt dat de wetgever destijds de keuze heeft gemaakt het Wob-verzoek vormvrij te houden,

161 Deze uitspraak wordt herhaald in ABRvS 4 augustus 2010, *LJN* BN3186 (Politieregio Amsterdam-Amstelland), alleen was in deze casus geen sprake van een bestendige bestuurlijke praktijk.

162 ABRvS 3 december-2008, *LJN* BG5897, *AB* 2009, 8 m.nt. P.J. Stolk, *JB* 2009, 15 m.nt. M.O.-V. (Politie Rijnmond).

163 *Kamerstukken II* 1986/87, 19 859, nr. 3, p. 23.

waarbij de mogelijkheid van nieuwe communicatietechnieken uitdrukkelijk is genoemd. In de onderhavige uitspraak wordt onderscheid gemaakt tussen ‘normale’ verzoeken om informatie, de zogenaamde publieksvragen, en ‘Wob-verzoeken’. Het ligt echter niet voor de hand dat de ‘normale’ verzoeken niet een bestuurlijke aangelegenheid betreffen. Dit onderscheid komt daarom nogal kunstmatig over. Indien een bestuursorgaan een e-mailadres op zijn internetwebsite publiceert waarbij uit de benaming van het e-mailadres blijkt dat het bedoeld is om informatie mee aan te vragen, dan moet door middel van dit e-mailadres ook een Wob-verzoek kunnen worden gedaan.

3.5.2 Conclusie kenbaar maken

De voorwaarde dat elektronische communicatie alleen dan mogelijk is indien kenbaar gemaakt is dat geadresseerde langs deze weg voldoende bereikbaar is, geldt zowel voor de overheid als voor de burger. Ten aanzien van communicatie met de burger door de overheid lijkt mij dit een terechte eis. De overheid zal zich ervan moeten vergewissen of de burger door middel van het opgegeven e-mailadres voldoende bereikbaar is.

Ten aanzien van communicatie met de overheid door de burger lijkt deze eis echter onnodig formalistisch te zijn. Een overheidsorgaan met een e-mailadres als bijvoorbeeld `info@bestuursorgaan.nl` geeft daarmee aan dat via dit e-mailadres informatie kan worden opgevraagd. Volgens de Afdeling voldoet een dergelijk e-mailadres echter niet aan de eis dat expliciet kenbaar moet zijn gemaakt dat de elektronische weg openstaat. Deze jurisprudentie vormt een onnodige formalisering en beperking van de elektronische communicatie.

3.6 Nadere eisen aan en consequenties van het gebruik van de elektronische weg

In art. 2:15, eerste lid, Awb is verder bepaald dat het bestuursorgaan nadere eisen kan stellen voor de manier van aanleveren van gegevens door de burger. Deze eisen worden gesteld met het oog op een uniforme behandeling en een veilig dataverkeer. Zij zijn over het algemeen technisch van aard.¹⁶⁴ De gestelde eisen moeten noodzakelijk zijn voor de verwerking van het binnengekomen bericht, betrekking hebben op de betrouwbaarheid en vertrouwelijkheid van het bericht, en een ordelijke en efficiënte behandeling van het bericht mogelijk maken. Gedacht wordt bijvoorbeeld aan de eis dat bij het indienen van berichten gebruik wordt gemaakt van bepaalde software. Verder kan het bestuursorgaan op grond van het tweede lid van art. 2:15 Awb elektronisch verschaftte gegevens

164 *Kamerstukken II 2001/02, 28 483, nr. 3, p. 13 en p. 39.*

en bescheiden weigeren, voor zover de aanvaarding daarvan tot een onevenredige belasting voor het bestuursorgaan zou leiden. Deze bepaling dient ertoe overbelasting van het bestuursorgaan te voorkomen. Omvangrijke documenten die aan een elektronisch bericht worden gehecht, kunnen geweigerd worden, en zullen op conventionele wijze verstuurd moeten worden.

In de memorie van toelichting wordt vastgesteld dat het bestuursorgaan bij deze bepaling een grote mate van beleidsvrijheid heeft.¹⁶⁵ Daarbij wordt als voorbeeld genoemd een rapport van de Nationale ombudsman, waarin deze overwoog dat het niet uitbrengen van een aangifte-diskette voor het besturingssysteem Apple Macintosh van het programma om elektronisch belastingaangifte te doen, niet onbehoorlijk was.¹⁶⁶ De belastingdienst volstond met het uitbrengen van een versie voor het besturingssysteem MS-Dos en Windows. Blijkens de memorie van toelichting liet de regering meewegen dat op grond van het uitgangspunt van de nevenschikking de conventionele weg steeds achter de hand blijft.¹⁶⁷ In het voorgaande stuk hebben we gezien dat deze laatste overweging zijn zeggingskracht verloren heeft. In paragraaf 2.4 over de nevenschikking concludeerde ik dat elektronische communicatie meer en meer het uitgangspunt wordt, en conventionele de uitzondering. Dit blijkt uit een aantal wettelijke uitzonderingen op het uitgangspunt van de nevenschikking en uit zachte dwang die overheidsorganen uitoefenen op de burger om elektronisch te communiceren. De vraag is dan ook of het gerechtvaardigd is dat de overheid, die of door wettelijke verplichtingen of door zachte dwang, burgers verplicht om elektronisch te communiceren, de burger dan ook dwingend kan opleggen een bepaald systeem te gebruiken. Het bovenstaande oordeel van de Nationale ombudsman komt uit een periode dat conventionele communicatie het uitgangspunt was, en elektronische de uitzondering. Heeft de burger echter niet meer de keuze, zoals dat nu meer en meer het geval gaat worden, dan moet de overheid de elektronische communicatie aanbieden in een vorm die het voor de gebruikers van gangbare systemen mogelijk maakt te communiceren. De overheid zou de elektronische communicatiemiddelen zo moeten inrichten, dat burgers niet gedwongen worden bepaalde software aan te schaffen. Dit leidt daarom tot de conclusie dat de overheid niet moet standaardiseren op de toepassing, maar gebruik zou moeten maken van open bestandsformaten, met een open specificatie.¹⁶⁸ Dit zal overigens geen volledige oplossing bieden, er kunnen altijd nieuwe (incompatibele) versies ontstaan.

165 *Kamerstukken II* 2001/02, 28 483, nr. 3, p. 13.

166 No 27 augustus 1999, AB 1999, 435 m.nt. P.J.S (Apple en belastingdienst).

167 *Kamerstukken II* 2001/02, 28 483, nr. 3, p. 14.

168 Dergelijke software is niet beschermd door patenten, vaak is de broncode van deze software bekend bij een ieder.

Voor communicatie op grond van de Dienstenrichtlijn is het uitgangspunt van de nevenschikking eveneens verlaten. Hier is het echter de overheid die verplicht is om elektronisch te communiceren. Deze verplichting voor overheidsorganen om elektronisch te communiceren brengt wat mij betreft met zich mee, dat dit ook de verplichting inhoudt techniekneutraal te communiceren, dat wil zeggen door gebruik te maken van open standaarden.¹⁶⁹

Daar komt nog bij, dat burgers het stellen van nadere eisen niet aan de bestuursrechter kunnen voorleggen. Tegen een weigering op grond van art. 2:15 Awb kan geen bezwaar worden gemaakt en beroep worden ingesteld. Deze uitzondering staat in art. 8:4, aanhef en onder k, Awb. In het licht van de hierboven genoemde wijzigingen op het uitgangspunt van de nevenschikking, is dit niet meer juist. Deze nadere eisen kunnen een grote belemmering opwerpen voor de burger om elektronisch te communiceren met de overheid, terwijl de burger hiertoe in een aantal gevallen tegelijkertijd verplicht wordt. Een dergelijke belemmering moet daarom aan de bestuursrechter ter toetsing voorgelegd kunnen worden. Art. 8:4, aanhef en onder k, Awb moet daarom komen te vervallen. Veel nadere eisen zullen een voorbereidingsbesluit als bedoeld in art. 6:3 Awb zijn, of een handeling van feitelijke aard. Daardoor valt er niet een grote toevloed van procedures hierover te verwachten. Wanneer een burger daadwerkelijk rechtstreeks in zijn belangen getroffen wordt als bedoeld in art. 6:3 Awb, dan zou deze tegen de nadere eisen bezwaar en beroep in moeten kunnen stellen.

3.6.1 Conclusie nadere eisen

Het stellen van nadere eisen is een bevoegdheid die het bestuursorgaan een grote mate van beleidsvrijheid geeft. Deze grote mate van beleidsvrijheid past echter niet meer in de situatie waarin burgers wettelijk, dan wel door zachte dwang, verplicht worden om elektronisch te communiceren. Ook de verplichting die op grond van de Dienstenrichtlijn geldt voor overheidsorganen om elektronisch te communiceren, impliceert de verplichting om deze communicatie zo breed mogelijk toepasbaar te maken. De wetgever is van oordeel dat een beslissing op grond van art. 2:15 Awb geen appellabel besluit in de zin van art. 1:3 inhoudt omdat de beslissing of van feitelijke aard is, of een voorbereidingsbeslissing als bedoeld in art. 6:3 Awb betreft.¹⁷⁰ Toch is art. 8:4, aanhef en onder k, aan de Awb toegevoegd. Bezwaar en beroep tegen het stellen van nadere eisen is dan ook niet mogelijk. Hierbij zijn de volgende kanttekeningen te plaatsen. Het

169 Het huidige kabinet gaat, om verschillende redenen, ook uit van het belang van het gebruik van open standaarden gezien het programma Nederland Open in Verbinding (NOiV) van het ministerie van Economische Zaken.

170 *Kamerstukken II* 2001/02, 28 483, nr. 3, p. 44.

uitgangspunt was, zoals hierboven al bleek, dat de conventionele wijze van communicatie altijd nog mogelijk zou zijn. Dat dit uitgangspunt meer en meer verlaten wordt, is hierboven aangetoond. Dat maakt het uitsluiten van het instellen van bezwaar en beroep tegen het stellen van nadere eisen dan ook niet meer juist. Deze nadere eisen kunnen een grote belemmering opwerpen voor de burger om elektronisch te communiceren met de overheid en het is vreemd dat een dergelijke belemmering niet aan de bestuursrechter ter toetsing voorgelegd kan worden. Art. 8:4, aanhef en onder k, Awb moet komen te vervallen. Voor een grote belasting van de rechterlijke macht zal niet hoeven worden gevreesd. Veel nadere eisen zullen een voorbereidingsbesluit als bedoeld in art. 6:3 Awb zijn, of een handeling van feitelijke aard. En alleen indien de nadere eis de belanghebbende rechtstreeks in zijn belang treft, kan deze daar bezwaar en beroep tegen instellen. Een dergelijke beroepsmogelijkheid doet recht aan het steeds groter wordende belang dat burgers hebben bij elektronische communicatie en het kunnen opheffen van mogelijke belemmeringen daarbij.

3.7 Betrouwbaarheid en vertrouwelijkheid

De artikelen 2:14, derde lid, en 2:15, derde lid, Awb bepalen dat de elektronische verzending van berichten moet plaatsvinden op een voldoende betrouwbare en vertrouwelijke manier. De betrouwbaarheid en vertrouwelijkheid moeten dus gewaarborgd zijn. Hoe wordt dit bereikt? In elk geval is daarvan sprake indien de veiligheid even groot is vergeleken met de situatie dat er van conventioneel verkeer gebruik zou worden gemaakt. Verder hangt de vraag naar een voldoende mate van betrouwbaarheid en vertrouwelijkheid blijkens deze bepalingen af van de aard en inhoud van een bericht en het doel waarvoor het wordt gebruikt. Voor verschillende soorten berichtenverkeer kunnen dan verschillende betrouwbaarheidseisen worden ontwikkeld.

Betrouwbaarheid en vertrouwelijkheid zijn verschillende normen. De *betrouwbaarheid* ziet op de aard van het berichtenverkeer, terwijl *vertrouwelijkheid* ziet op de toegang tot het berichtenverkeer door personen die al dan niet inzage zouden moeten hebben in dit verkeer. Betrouwbaarheid en vertrouwelijkheid zijn open normen. In de memorie van toelichting wordt voor een goede uitwerking van deze twee open normen verwezen naar de in hoofdstuk 1 besproken beginselen van behoorlijk IT-gebruik van Franken.¹⁷¹

Betrouwbaarheid heeft volgens de memorie van toelichting betrekking op de eerste zes genoemde beginselen, en vertrouwelijkheid heeft betrekking op

171 *Kamerstukken II 2001/02, 28 483, nr. 3, p. 15.*

de exclusieve toegankelijkheid van het stuk.¹⁷² De eis van de vertrouwelijkheid houdt in dat het bericht terecht komt bij degene voor wie het bestemd is, en dat het niet door een ander kan worden gelezen. Ten aanzien van dit criterium wordt in de parlementaire stukken geen nadere toelichting gegeven. De vertrouwelijkheid moet in elk geval even groot zijn als in de situatie waarin er van conventioneel verkeer gebruik zou worden gemaakt. De vertrouwelijkheid van elektronische berichten moet dus gewaarborgd worden op een wijze die gelijk is aan de vertrouwelijkheid van berichten die op een conventionele wijze naar het bestuursorgaan worden verzonden. Verder hangt de vereiste mate van vertrouwelijkheid af van de aard en inhoud van het bericht, en het doel waarmee dit verzonden is.

De eerste vier door Franken genoemde criteria hebben te maken met authenticiteit en integriteit. Authenticatie houdt volgens de omschrijving in par. 3.3.2.1 immers het bewijzen van de identiteit van de betrokkene in, het waarborgen dat het klopt. Hieruit vloeit voort dat het onweerlegbaar zou moeten zijn dat het bericht van betrokkene afkomstig is. Zoals ik echter ook al heb beschreven in par. 3.3.2.1, kan echter zelfs niet met een elektronische handtekening de onweerlegbaarheid volledig gewaarborgd worden. Zodra betrokkene zijn private sleutel bijvoorbeeld openbaar maakt, staat niet meer onweerlegbaar vast dat het bericht van betrokkene afkomstig is. Het door Franken genoemde beginsel transparantie heeft te maken met het ook door hem genoemde beginsel van de integriteit van de informatie. Integriteit betekent onschendbaarheid, de ongeschonden toestand. Met integriteit van een elektronisch bericht wordt dan ook bedoeld de situatie dat het bericht aankomt in de staat waarin het verzonden werd. Dit houdt in dat wijzigingen in het bericht opgespoord moeten kunnen worden

In de nota van toelichting bij het Besluit ruimtelijke ordening (Bro) staat dat betrouwbaar en vertrouwelijk elektronisch verkeer tussen burger en overheid moet voldoen aan drie kwaliteitscriteria: authenticiteit, integriteit en exclusiviteit. Hierbij wordt authenticiteit uitgelegd als betrekking hebbende op de oorsprong van de informatie; is de informatie het oorspronkelijke document, is de informatie werkelijk van de afzender afkomstig en is de afzender werkelijk degene voor wie hij zich uitgeeft. Een van de elementen van de maatregelen om de authenticiteit te waarborgen is volgens deze toelichting dat gewerkt zal worden met een elektronische handtekening, die voldoet aan de eisen die de Awb daaraan stelt. Integriteit houdt volgens de toelichting de zekerheid in, dat de informatie juist en volledig is en niet onderweg door onbevoegden of door falende techniek is gewijzigd. Exclusiviteit ziet op het toegankelijk zijn van de informatie voor uitsluitend degene waarvoor de informatie is bestemd.¹⁷³

172 *Kamerstukken II* 2001/02, 28 483, nr. 3, p. 16.

173 *Kamerstukken II* 2006/07, bijlage bij 30 218, nr. 23, p. 9.

Dan blijven nog over de door Franken genoemde criteria van beschikbaarheid en flexibiliteit. Deze passen niet in de noties van authenticiteit, integriteit en betrouwbaarheid, terwijl de wetgever ze blijkens de toelichting kennelijk toch heeft willen laten vallen onder het begrip betrouwbaarheid. Deze criteria staan ook niet opgenomen in de hierboven genoemde toelichting bij het Bro. Beschikbaarheid en flexibiliteit zijn ook geen criteria die te maken hebben met authenticiteit en integriteit van elektronische berichten.

Het begrip beschikbaarheid ziet volgens Franken op de wijze waarop informatie wordt overgedragen. Elektronische 'communicatie is pas mogelijk als de diverse componenten van een informatiesysteem (apparatuur, software, verbindingsmiddelen) gestandaardiseerd zijn. Daartoe moeten normen worden gedefinieerd met betrekking tot de functies van de systemen en de wijze van interactie met en tussen deze systemen.'¹⁷⁴ Aan deze standaarden die gelden voor het elektronisch berichtenverkeer, zijn volgens Franken aspecten verbonden die te maken hebben met mededingingsrecht en met intellectuele eigendom. Uit het feit dat een bepaalde softwarefabrikant een monopolie heeft op de verkoop van bepaalde software kan dan ook voortvloeien dat diegenen die andere software gebruiken, bepaalde informatie niet kunnen bereiken indien de overheid deze software gebruikt. Dit wringt als er van uitgegaan wordt dat contact zoeken met de overheid op een zo laagdrempelig mogelijke wijze moet kunnen plaatsvinden. Onder beschikbaar moet dan ook worden verstaan het gebruiken van die standaarden bij elektronische communicatie, die waarborgen dat elektronische berichtgeving voor een grote groep burgers bereikbaar en toegankelijk is.

Het begrip flexibiliteit betreft volgens Franken de mogelijkheid dat technologische toepassingen gemakkelijk kunnen worden aangepast aan nieuwe gebruikseisen. Hieronder verstaat hij dat nieuwe regelingen en nieuwe feiten gemakkelijk en zonder al te veel kosten kunnen worden ingevoerd. Niet alleen het inputmateriaal, maar ook de gebruikte programma's moeten gemakkelijk te wijzigen zijn.¹⁷⁵ Onder het begrip flexibiliteit moet dan ook worden verstaan de mogelijkheid dat de door de overheid gebruikte communicatietechnologie gemakkelijk en zonder veel kosten aan nieuwe gebruikseisen kan worden aangepast.

In antwoord op de vraag hoe betrouwbaar en vertrouwelijk de elektronische communicatie moet zijn, staat in de memorie van toelichting:¹⁷⁶

'De neiging bestaat bij elektronisch verkeer een hogere mate van betrouwbaarheid en vertrouwelijkheid te eisen dan bij conventionele communicatie. Dit is niet gewenst, want ook

174 Franken 1993, p. 19.

175 Franken 1993, p. 21.

176 *Kamerstukken II* 2001/02, 28 483, nr. 3, p. 16-17.

de handtekening op papier biedt geen absolute garanties tegen vervalsingen. Er zijn in theorie drie maten van betrouwbaarheid en vertrouwelijkheid te onderscheiden:

- van maximale betrouwbaarheid en vertrouwelijkheid is sprake indien de beveiliging geheel conform de maximaal (technische) mogelijkheden plaatsvindt.
- van voldoende betrouwbaarheid en vertrouwelijkheid is sprake indien de veiligheid even groot is vergeleken met de situatie dat er uitsluitend van conventioneel verkeer gebruik zou worden gemaakt.
- van pro forma betrouwbaarheid en vertrouwelijkheid is sprake indien de beveiliging slechts één stap verwijderd is van het bieden van geen enkele beveiliging; zij bestaat bijvoorbeeld uit de (elektronische) mededeling «verboden toegang».

Absolute betrouwbaarheid en vertrouwelijkheid bestaan niet. De maximale betrouwbaarheid en vertrouwelijkheid zijn afhankelijk van de stand der techniek en de (financiële) inspanningen die men er voor over heeft. (...)

Wanneer precies sprake is van voldoende mate van betrouwbaarheid en vertrouwelijkheid is in algemene zin moeilijk te zeggen. In sommige gevallen van uitwisseling van informatieve berichten is er weinig behoefte aan bescherming. Een e-mailbericht zonder een elektronische handtekening of een sms-bericht kan al voldoende zijn. Zodra echter van belang is dat de authenticiteit, de integriteit of andere hiervoor genoemde beginselen voldoende zijn gewaarborgd, dienen maatregelen ter bescherming te worden genomen. De aard en de inhoud van het bericht en het doel waarvoor het wordt gebruikt, zijn bepalend voor de mate van betrouwbaarheid en vertrouwelijkheid die vereist is. De mate van betrouwbaarheid en vertrouwelijkheid dient even groot te zijn als in het conventionele verkeer. Aan de verlening van een vergunning bijvoorbeeld moeten hogere eisen worden gesteld dan aan de verstrekking van algemene inlichtingen die ook langs andere kanalen verkrijgbaar zijn.’

De algemene omschrijvingen van de begrippen betrouwbaar en vertrouwelijk lijken op de omschrijvingen waaraan een elektronische handtekening moet voldoen. Zijn de normen van betrouwbaarheid en vertrouwelijkheid en de eis dat elektronische communicatie een elektronische handtekening bevat, nu identiek en dus uitwisselbaar? In de memorie van toelichting staat hierover:¹⁷⁷

‘Een bijzondere manier waardoor voor een belangrijk deel de betrouwbaarheid kan worden gerealiseerd, is de elektronische handtekening. Daarop heeft artikel 2:16 betrekking. Dit artikel geeft een nadere uitwerking aan het beginsel van authenticiteit.’

Volgens de wetgever is de regeling van de elektronische handtekening dus een specialis van de eis dat bij elektronische communicatie de betrouwbaarheid gewaarborgd moet zijn.

Art. 2:14 Awb betreft berichten die door een bestuursorgaan naar een burger verzonden worden. De ontvanger van het bericht moet er zeker van zijn dat het bericht afkomstig is van het bestuursorgaan. Afhankelijk van de aard en de inhoud van het bericht en het doel waarvoor het gebruikt wordt, moet de burger

177 *Kamerstukken II 2001/02, 28 438, nr. 3, p. 16.*

die het bericht ontvangt, de authenticiteit en de integriteit van het bericht kunnen vaststellen.

Art. 2:14 betreft zowel berichten die naar een of meer geadresseerden worden verzonden, als berichten die een openbare kennisgeving inhouden.¹⁷⁸

Art. 2:14 heeft dan ook betrekking op berichten die door een overheidsorgaan op een website worden geplaatst. Het risico van de verzending langs elektronische weg ligt bij de verzender, tenzij komt vast te staan dat het probleem is veroorzaakt door de ontvanger.¹⁷⁹

Hieruit kan worden afgeleid dat het risico van problemen door een niet functionerende overheidswebsite bij het betreffende overheidsorgaan ligt. De norm uit art. 2:14, derde lid, die bepaalt dat berichten op een betrouwbare manier verzonden moeten worden, geldt ook voor berichten die een overheidsorgaan op een website plaatst met als doel dat een ieder deze berichten kan lezen. Het overheidsorgaan moet dan niet alleen instaan voor de (technische) betrouwbaarheid van de website, maar ook voor de toegankelijkheid en het document format. De betrouwbaarheid moet even groot zijn, vergeleken met de situatie dat er van conventioneel verkeer gebruik gemaakt wordt. Een burger moet dan ook gerechtvaardigd op een mededeling op een overheidswebsite kunnen vertrouwen, indien op een gelijksoortige mededeling die op conventionele wijze werd gedaan, ook gerechtvaardigd kan worden vertrouwd. Stelt de overheid de elektronische weg open, dan kan zij ingevolge art. 2:14 daar dan ook niet minder bescherming voor de burger aan verbinden.

Art. 2:15 betreft berichten die door een burger naar een bestuursorgaan worden verzonden. Het bestuursorgaan beschikt over de middelen om de authenticiteit van het bericht vast te stellen, bijvoorbeeld door middel van een elektronische handtekening.

3.7.1 Conclusie betrouwbaarheid en vertrouwelijkheid

In art. 2:14, derde lid, en 2:15, derde lid, is de algemene eis gesteld dat elektronische berichten op een voldoende betrouwbare en vertrouwelijke manier verzonden worden. De regeling van de elektronische handtekening uit art. 2:16 is een nadere invulling van de eis van betrouwbaarheid, maar vervangt deze niet. Het begrip betrouwbaarheid wordt volgens de wetstoelichting ingevuld door de beginselen van behoorlijk IT gebruik van Franken. Met de eisen die in art. 3:15a, tweede lid, BW aan de elektronische handtekening gesteld worden, wordt in meer of mindere mate voldaan aan de beginselen authenticiteit, integriteit, onweerlegbaarheid en transparantie. Met de elektronische handtekening is niet

¹⁷⁸ *Kamerstukken II* 2001/02, 28 483, nr. 3, p. 38.

¹⁷⁹ *Kamerstukken I*, 2001/02, 28 483, nr. 3, p. 39.

voldaan aan de beginselen beschikbaarheid en flexibiliteit. De eis van beschikbaarheid heeft te maken met de toegankelijkheid van de elektronische systemen voor burgers: kan een ieder er gebruik van maken? Ook heeft het te maken met de beschikbaarheid van elektronische informatie voor burgers. Aan de eis van flexibiliteit wordt voldaan wanneer het technologische systeem waarvan gebruik gemaakt wordt, op eenvoudige wijze is aan te passen aan nieuwe gebruikseisen. Patenten en auteursrecht kunnen echter aan de eis van flexibiliteit in de weg staan. De conclusie kan daarom getrokken worden dat, om te voldoen aan de eis van flexibiliteit, de technologische systemen die door de overheid worden gebruikt, alleen aan deze wettelijk norm voldoen wanneer daarin gebruik wordt gemaakt van open standaarden.

Een volgend aspect is dat volgens de memorie van toelichting de verzender van het elektronische bericht moet instaan voor de betrouwbaarheid en vertrouwelijkheid daarvan. Dit leidt tot de conclusie dat disclaimers die op een groot aantal websites van bestuursorganen staan en regelmatig onder e-mailberichten afkomstig van bestuursorganen te vinden zijn, in strijd zijn met art. 2:14 Awb. Indien het bestuursorgaan immers niet kan instaan voor de betrouwbaarheid en vertrouwelijkheid van de elektronische berichtgeving, dan had het niet voor deze weg moeten kiezen. Dit geldt ook voor de technische kwaliteiten: kiest een bestuursorgaan ervoor om via een website met burgers te communiceren, dan staat dit bestuursorgaan ervoor in dat deze website in technische opzicht goed functioneert en beschikbaar is. De risico's voor een niet functionerende website liggen aan de kant van het bestuursorgaan.

De eis van betrouwbaarheid geldt zowel voor berichten die door een bestuursorgaan naar een burger worden verzonden, als voor de omgekeerde situatie. Voor de laatste situatie ontstaat er een infrastructuur van de elektronische handtekening. In de situatie dat een bestuursorgaan op elektronische wijze berichten naar een burger verstuurt, moet ook hierbij de betrouwbaarheid gewaarborgd zijn.

3.8 Begin en einde termijn

In het bestuursrecht spelen termijnen een grote rol. Het is daarom van belang om te weten wanneer een termijn begint. Art. 2:17, eerste lid, Awb bepaalt dat als moment van verzending door een bestuursorgaan het tijdstip geldt waarop het bericht een systeem bereikt waarover het bestuursorgaan geen controle meer heeft, of, indien het bestuursorgaan en de geadresseerde gebruik maken van hetzelfde systeem voor gegevensverwerking, het tijdstip waarop het bericht toegankelijk wordt voor de geadresseerde. Als tijdstip waarop een bericht van een burger is ontvangen, geldt op grond van art. 2:17, tweede lid, Awb, het tijdstip waarop het bericht het systeem van het bestuursorgaan heeft bereikt.

In een pre-afdeling 2.3 uitspraak oordeelt de Centrale Raad van Beroep hierover als volgt.¹⁸⁰ Het betreft een bij het UWV per e-mail ingediend bezwaarschrift. Appellant had telefonisch contact opgenomen met het UWV op 10 maart 2003. In dit telefoongesprek werd hem verteld dat hij tot en met 12 maart 2003 een bezwaarschrift kon indienen, en dat hij zijn bezwaarschrift ook per e-mail kon indienen. Op 12 maart 's avonds, de dag waarop de termijn afliep, probeert appellant vier keer om het bezwaarschrift per e-mail te verzenden. Vier keer krijgt hij echter het bericht dat de e-mail niet is aangekomen. De ochtend daarna lukte het wel om het bezwaarschrift te e-mailen, maar het was te laat en werd niet-ontvankelijk verklaard wegens termijnoverschrijding. De Raad oordeelde hierover dat een bezwaarschrift tijdig is ingediend indien het voor het einde van de termijn is ontvangen, art. 6:9 Awb. Het was onomstreden dat de eerdere bezwaarschriften het bestuursorgaan niet hadden bereikt. De Raad is daarbij van oordeel dat de keuze voor het middel en de daarbij mogelijke feilen voor het risico van appellant dienen te komen. De stelling van appellant dat, gezien art. 6:9, tweede lid, Awb de eerste poging als moment van ontvangst bij het bestuursorgaan moet worden beschouwd, wordt verworpen.

In een andere zaak (ook van voor de invoering van Afdeling 2.3) was er een e-mail zoekgeraakt bij de Sociale verzekeringsbank (Svb).¹⁸¹ De Svb erkende dat er een e-mail was binnen gekomen, maar het tijdstip waarop en de inhoud van de e-mail (een verzoek om informatie of een bezwaarschrift) waren niet meer na te gaan. De Svb stelde dat de e-mail een verzoek om informatie betrof, de eiser stelde dat de e-mail een tijdig ingediend bezwaarschrift betrof. De rechtbank Haarlem verwijst naar de hierboven reeds genoemde jurisprudentie van de CRvB waaruit volgt dat de indiener van een bezwaar- of beroepschrift in beginsel het risico loopt dat zijn geschrift de geadresseerde niet of te laat bereikt. Ook de keuze van de wijze van verzending, zoals in dit geval per e-mail, komt in beginsel voor rekening en risico van verzender. In dit geval was echter niet in geschil dat er een e-mail bericht verzonden was, en tevens was niet in geschil dat er naar aanleiding van de e-mail telefonisch contact is geweest tussen verweerder en de zoon van de eiser. De rechtbank is daarom van oordeel dat het feit dat de e-mail in het ongereede is geraakt en dus niet meer te traceren is wanneer deze is ontvangen en wat de inhoud was, voor rekening van verweerder dient te komen. Eiseres had daarom het voordeel van de twijfel behoren te krijgen en het bezwaar had ontvankelijk verklaard moeten worden.

180 CRvB 23 maart 2005, *LJN* AT3617, *AB* 2005, 193 m.nt. Ortlep, *USZ* 2005, 214 (Te late e-mail).

181 Rb. Haarlem 31 oktober 2005, *LJN* AV1672, *USZ* 2006, 71 m.nt. Groothuis (Zoekgeraakt e-mailbericht).

In de memorie van toelichting en in jurisprudentie wordt gesteld dat de risico's van de keuze voor het volgen van de elektronische weg bij het verzenden van berichten bij de verzender liggen. In een uitspraak over een zoekgeraakt faxbericht stelt de Centrale Raad van Beroep, onder verwijzing naar eerdere jurisprudentie, dat

‘de aan deze wijze van indiening verbonden risico's voor rekening van de verzender dienen te komen’.¹⁸²

De verzendbevestiging van de ontvanger toonde weliswaar de status ‘OK’, maar dit vormt volgens de Raad geen sluitend bewijs dat het faxbericht in goede orde is ontvangen. Helaas komt in deze uitspraak de vraag naar de ontvangstregistratie van het bestuursorgaan niet aan de orde. In latere uitspraken komt de Raad terug van deze jurisprudentie, nadat de Hoge Raad had geoordeeld dat indien een belanghebbende een verzendregistratie heeft overlegd, het bestuursorgaan hier gemotiveerd op in moet gaan.¹⁸³ In twee uitspraken van 7 februari 2007 oordeelt de Raad:¹⁸⁴

‘Volgens vaste jurisprudentie is het indienen van een bezwaarschrift door middel van een faxbericht op zichzelf aan te merken als een toelaatbare wijze van verzending. De aan deze wijze van verzending verbonden risico's dienen voor rekening van de verzender te komen. Dit brengt met zich mee dat, als door de geadresseerde wordt gesteld dat het verzonden bericht niet is ontvangen, het op de weg van de verzender ligt de verzending aannemelijk te maken. Indien de verzender de verzending aannemelijk heeft gemaakt, ligt het op de weg van de geadresseerde om de ontvangst van het faxbericht op een niet ongeloofwaardige manier te ontkennen.’

In beide zaken acht de Raad de verzending van het bericht voldoende aannemelijk gemaakt door het overleggen van een verzendjournaal. Het ontvangende bestuursorgaan kon echter naar het oordeel van de Raad de ontvangst van het bericht niet op een niet ongeloofwaardige manier ontkennen. Dat kwam in beide gevallen zowel door het ontbreken van een ontvangstjournaal, als door het niet op orde zijn van de onderhavige dossiers. In beide gevallen was er sprake van verzending door middel van een faxbericht, een verzending die ook onder de regeling in afd. 2.3 Awb valt.

De hierboven genoemde jurisprudentie past in de rechtspraak over bewijsperikelen rond termijnen. De bewijsregels zijn als volgt: a. het is aan de

182 CRvB 1 september 2006, *LJN* AY9485, *JB* 2006, 310 m.nt. M.O.-V. (Niet ontvangen faxbericht).

183 HR 22 september 2006, *LJN* AY8658, *AB* 2007, 1 m.nt. B.W.N. de Waard, *JB* 2006, 300 (Niet ontvangen faxbericht).

184 CRvB 7 februari 2007, *LJN* BA0213 en *LJN* AZ8886, *RSV* 2007, 148, *JB* 2007, 78 m.nt. M.O.-V (Incompleet elektronisch dossier).

verzender om aannemelijk te maken dat is verzonden; b. slaagt de verzender daarin, dan is het aan de ontvanger om 'niet ongeloofwaardig' te ontkennen dat hij heeft ontvangen; c. slaagt die daarin, dan is het aan de verzender om aannemelijk te maken dat desondanks is ontvangen.¹⁸⁵ Het was altijd eenvoudiger voor bestuursorganen om aan de bewijsregels te voldoen dan voor burgers. Een belanghebbende kan de verzending van een bezwaar- of beroepschrift niet eenvoudig aantonen door het overleggen van een verzendjournaal. Een bestuursorgaan kan dit wel. De Afdeling accepteert voetstoots het overleggen van een computeruitdraai van de geautomatiseerde administratie door het bestuursorgaan. Uit deze uitdraai volgt volgens de Afdeling, gelet op de vermelding in de uitdraai van naam en adres van de ontvanger, data van factuur en herinneringsbrief, de vaste werkwijze en de omstandigheid, dat niet is gebleken van problemen bij de verwerking en verzending in de desbetreffende periode, dat voldoende aannemelijk is gemaakt dat de genoemde brieven inderdaad zijn verzonden.¹⁸⁶

Door gebruik te maken van elektronisch verkeer is het voor een burger eenvoudiger geworden om aan te tonen dat een bericht verzonden is. De burger kan dat doen door het overleggen van een verzendjournaal: het bestuursorgaan moet daar dan gemotiveerd op ingaan. Bij de conventionele wijze van verzending kan de burger alleen maar bewijzen dat het stuk verzonden is, als het stuk aangetekend of met bewijs van ontvangst is verzonden.¹⁸⁷ Voor het bestuursorgaan geldt zowel bij de conventionele weg, als bij de elektronische weg, dat het kan aantonen dat een bericht is verzonden door het overleggen van een verzendregistratie.¹⁸⁸

3.8.1 Conclusie begin en einde termijn

Met het toenemen van het elektronisch verkeer zullen dergelijke bewijsvragen meer gaan spelen. Voor diegenen die een elektronisch bericht naar een bestuursorgaan willen zenden, geldt in elk geval dat zij moeten bijhouden of en wanneer bepaalde berichten verzonden zijn, en dat zij bij twijfel contact moeten opnemen met het bestuursorgaan om na te gaan of een bericht ontvangen dan wel verzonden is. Het bestaan van een plicht voor bestuursorganen om logfiles dan wel een verzend- of gespreksregistratie bij te houden valt nog niet uit de jurisprudentie af te leiden. Wel kan het ontbreken van een dergelijke registratie

185 ABRvS 24 november 2007, *LJN* BB6318, *AB* 2008, 3 m.nt. A.T. Marseille (Herplanten Ede), de genoemde bewijsregels komen uit de noot.

186 ABRvS 23 december 2005, *LJN* AU9187, *AB* 2006, 101 m.nt. I. Sewandono (Aannemelijke computeruitdraai).

187 Damen e.a. 2 2009, p. 167.

188 Damen e.a. 2 2009, p. 165.

ertoe leiden dat de ontvangst van een bericht door het bestuursorgaan niet op een niet ongeloofwaardige wijze ontkend kan worden, maar in beide aangehaalde uitspraken speelde naast het ontbreken van een ontvangstregistratie ook het niet op orde zijn van de dossiers een rol. De vraag of enkel het ontbreken van een ontvangstregistratie op zich zelf kan leiden tot een ‘niet ongeloofwaardige ontkening’, is nog niet beantwoord. Het lijkt mij echter redelijk om de verplichting tot het bijhouden van een ontvangstregistratie door het bestuur aan te nemen. Wanneer een burger door het overleggen van een verzendregistratie aantoont een bericht verzonden te hebben, dan kan een bestuursorgaan dit alleen dan op een niet ongeloofwaardige wijze ontkennen wanneer het een ontvangstregistratie kan tonen waaruit blijkt dat het bericht niet ontvangen is. Hiermee lijkt de bewijspositie van de burger iets voordeliger uit te vallen wanneer deze gebruik maakt van de elektronische weg dan wanneer de burger gebruik maakt van de conventionele weg.

3.9 Samenvatting en conclusies

3.9.1 Samenvatting

De facultatieve regeling van afd. 2.3 Awb geeft regels ten aanzien van communicatie langs elektronische weg tussen burger en bestuursorgaan, maar schrijft deze vorm van communicatie niet voor. Het gaat bij deze regeling om berichten die langs elektronische weg verzonden worden.

De wetgever wilde de ontwikkeling van normen op dit punt niet volledig overlaten aan de wisselwerking van praktijk en jurisprudentie, omdat dit naar verwachting zou leiden tot een periode van (rechts)onzekerheid die ongewenst lang zou duren.¹⁸⁹ Dit is een terechte keuze geweest.

Wat een bericht is, wordt in afdeling 2.3 niet gedefinieerd. Een bericht in de zin van afdeling 2.3 kan elk bericht zijn dat een bestuursorgaan aan een burger of een burger aan een bestuursorgaan wil zenden. In afdeling 2.3 is niet voorgeschreven dat een bericht schriftelijk moet zijn. Hierdoor kan een bericht ook heel goed mondeling zijn, bijvoorbeeld een podcast, of een film die door een bestuursorgaan op een website wordt geplaatst.

Ook het begrip verkeer langs elektronische weg wordt niet gedefinieerd. In de memorie van toelichting worden voorbeelden genoemd als e-mail, websites, intra- of internet en sms-berichten. Van verzending langs elektronische weg is sprake indien het transport van het bericht volledig dan wel gedeeltelijk via elektronische middelen plaatsvindt. Hierdoor vallen berichten die op een elektronische gegevensdrager langs conventionele weg worden verzonden

189 *Kamerstukken II 2001/02, 28483, nr. 3, p. 2.*

(bijvoorbeeld een diskette die per post wordt verzonden), ook onder de regeling uit afdeling 2.3.

Een elektronisch bericht hoeft niet per definitie schriftelijk te zijn. Alleen als het vormvereiste schriftelijk wordt gesteld, dan moet het bericht aan die eis voldoen.

Over de vormvoorschriften schriftelijk en ondertekening is bepaald dat communicatie via de elektronische weg in beginsel gelijkwaardig is aan communicatie via de conventionele, papieren weg, mits zij dezelfde functies kan vervullen. Hiervoor wordt de term functionele equivalenten gebruikt. Een elektronisch bericht voldoet aan dit vormvereiste wanneer door middel van het bericht de boodschap kan worden overgebracht, en de gebruikte tekens met codering onder alle omstandigheden een gelijkwaardig resultaat opleveren.

In art. 2:16 Awb wordt de gekwalificeerde elektronische handtekening uit het BW van overeenkomstige toepassing verklaard, voor zover de aard van het bericht zich daartegen niet verzet. Maar ten eerste is het op dit moment niet mogelijk om in het verkeer tussen burger en bestuursorgaan van de gekwalificeerde elektronische handtekening gebruik te maken. Het middel DigiD voldoet noch aan de eisen die aan de gekwalificeerde handtekening worden gesteld, noch aan de eisen die aan de geavanceerde handtekening worden gesteld. Ten tweede vergt het gebruik van een gekwalificeerde elektronische handtekening meer van de gebruiker dan het gebruik van een conventionele handtekening. Het is daarom de vraag of dit zware authenticatiemiddel nodig is in alle gevallen waarin een handtekening vereist is. Het ligt voor de hand om te differentiëren: bij bepaalde soorten berichten zou het bestuursorgaan heel goed aan de hand van de inhoud van het bericht, bijvoorbeeld door het gebruik van correspondentienummers, de identiteit van de afzender voldoende kunnen vaststellen. Hoe vaak wordt er in het geval van een op de conventionele wijze ingediend bezwaarschrift nagegaan of de handtekening daadwerkelijk afkomstig is van de indiener van het geschrift? Voor elektronische communicatie worden dan in sommige gevallen zwaardere eisen gesteld dan in het geval van conventionele communicatie. De eisen die aan de elektronische handtekening dan wel aan het middel van authenticatie gesteld worden, moeten differentiëren naar gelang de aard en de inhoud van het bericht.

Een elektronisch bericht is daarmee functioneel equivalent van de vormvereisten schriftelijk en ondertekening indien daarmee de boodschap kan worden overgebracht, de identiteit van de afzender kan worden vastgesteld (de authenticiteit) en indien de integriteit van het bericht vaststaat.

Uitgangspunt van afdeling 2.3 Awb is het principe van de nevenschikking. Dat houdt in dat de overheid ook altijd nog op de conventionele wijze bereikbaar moet zijn. Van dit uitgangspunt kan worden afgeweken in een bijzondere wet. Dit gebeurt inmiddels in de Algemene wet inzake

rijksbelastingen, in de Bekendmakingswet, in de Wet ruimtelijke ordening en in de Dienstenwet. De Dienstenwet betreft echter niet een verplichting voor de burger om elektronisch te communiceren, maar een verplichting voor de overheid. Ondanks het beginsel van de nevenschikking wordt steeds meer elektronische communicatie de norm, en conventionele de uitzondering.

Berichten kunnen elektronisch verzonden worden, indien de geadresseerde heeft kenbaar gemaakt langs deze weg voldoende bereikbaar te zijn, art. 2:14, eerste lid, Awb. Bij een onbekend aantal geadresseerden, zoals bij besluiten van algemene strekking, kan dit niet. Daarom gold daarvoor dat de verzending van berichten die niet tot een of meer geadresseerden zijn gericht, niet uitsluitend elektronisch gebeurt, art. 2:14, tweede lid, en art. 3:42, tweede lid, Awb. Op deze bepaling bestaat inmiddels een uitzondering door de Wet elektronische bekendmaking. Gevolg van het feit dat elektronische communicatie meer en meer de regel wordt, is dat de voorwaarde voor het kenbaar maken door burgers minder vaak geldt.

Art. 2:15, eerste lid, Awb bepaalt dat een bericht elektronisch aan een bestuursorgaan kan worden verzonden voor zover het bestuursorgaan heeft kenbaar gemaakt dat deze weg geopend is. Het bestuursorgaan kan hierin differentiëren, dus ten aanzien van het ene beleidsterrein de elektronische weg wel openstellen en ten aanzien van het andere niet. Ten aanzien van communicatie door de burger met de overheid lijkt deze eis onnodig formalisme en onduidelijkheid voor de burger in de hand te werken.

Verder heeft het bestuursorgaan beleidsvrijheid ten aanzien van de nadere eisen die het kan stellen aan het gebruik van de elektronische weg. Beslissingen die het bestuursorgaan ten aanzien van de nadere eisen neemt, zijn echter niet appellabel. Naar mijn mening ten onrechte, omdat nu niet aan de bestuursrechter de vraag kan worden voorgelegd welke nadere eisen nog redelijk zijn en welke niet meer. Wel kan hierover worden geklaagd bij een klachtenvoorziening, en uiteindelijk in veel gevallen bij de Nationale ombudsman. Uitgangspunt hierbij was blijkens de parlementaire geschiedenis dat de conventionele, papieren wijze van communicatie altijd nog voorhanden was. Nu dit uitgangspunt van de nevenschikking op een aantal gebieden verlaten is, zal de wetgever moeten teruggekomen op de beslissing om het stellen van nadere eisen niet-appellabel te maken.

Veel nadere eisen zullen geen besluit, maar een voorbereidingshandeling in de zin van art. 6:3 Awb inhouden. Het laten vervallen van art. 8:4, aanhef en onder k, Awb zal als gevolg hebben dat die nadere eisen die als een besluit in de zin van de Awb zijn aan te merken en die de belanghebbende los van het voor te bereiden besluit rechtstreeks in zijn belang treffen, appellabel zijn. Dit is gerechtvaardigd door het verlaten van het

uitgangspunt van de nevenschikking, en het gevolg daarvan, dat elektronische communicatie de norm wordt.

In de art. 2:14, derde lid en 2:15, derde lid, Awb is de algemene eis gesteld dat elektronische berichten op een voldoende betrouwbare en vertrouwelijke manier verzonden worden. De regeling van de elektronische handtekening uit art. 2:16 Awb is een nadere invulling van de eis van betrouwbaarheid, maar vervangt deze niet. Het begrip betrouwbaarheid wordt volgens de wetstoelichting ingevuld door de beginselen van behoorlijk IT gebruik van Franken. Door gebruik te maken van een gekwalificeerde elektronische handtekening wordt in meer of mindere mate voldaan aan de beginselen authenticiteit, integriteit, onweerlegbaarheid en transparantie.

Met de elektronische handtekening is niet voldaan aan de beginselen van beschikbaarheid en flexibiliteit die Franken formuleerde. De eis van beschikbaarheid heeft te maken met de toegankelijkheid van de elektronische systemen voor burgers: kan een ieder er gebruik van maken? Ook heeft het te maken met de beschikbaarheid van elektronische informatie voor burgers. Aan de eis van flexibiliteit wordt voldaan wanneer het technologische systeem waarvan gebruik gemaakt wordt, op eenvoudige wijze is aan te passen aan nieuwe gebruikseisen. Patenten en auteursrecht kunnen hieraan echter in de weg staan. De conclusie kan daarom getrokken worden dat, om te voldoen aan de eis van flexibiliteit, de technologische systemen die door de overheid worden gebruikt, alleen aan deze wettelijk norm voldoen wanneer daarin gebruik wordt gemaakt van open standaarden.

Een volgend aspect is dat volgens de memorie van toelichting de verzender van het elektronische bericht moet instaan voor de betrouwbaarheid en vertrouwelijkheid daarvan. Dit geldt zowel voor berichten die door de burger naar het bestuursorgaan worden verzonden, als voor berichten die door het bestuursorgaan naar de burger worden verzonden. Dit leidt tot de conclusie dat disclaimers die op een groot aantal websites van bestuursorganen staan en regelmatig onder e-mailberichten afkomstig van bestuursorganen te vinden zijn, in strijd zijn met art. 2:14 Awb. Indien het bestuursorgaan immers niet kan instaan voor de betrouwbaarheid en vertrouwelijkheid van de elektronische berichtgeving, dan had het niet voor deze weg moeten kiezen. Dit geldt ook voor de technische kwaliteiten: kiest een bestuursorgaan ervoor om via een website met burgers te communiceren, dan staat dit bestuursorgaan ervoor in dat deze website in technische opzicht goed functioneert en beschikbaar is. De risico's voor een niet functionerende website liggen dan aan de kant van het bestuursorgaan.

De eis van betrouwbaarheid geldt zowel berichten die door een bestuursorgaan naar een burger worden verzonden, als de omgekeerde situatie. Voor de laatste situatie ontstaat er een infrastructuur van de elektronische

handtekening. In de situatie dat een bestuursorgaan op elektronische wijze berichten naar een burger verstuurt, moet ook hierbij de betrouwbaarheid en dan met name de authenticiteit van de berichten gewaarborgd zijn. Bij communicatie door de overheid met de burger is deze eis echter nieuw. Bij veel overheidscommunicatie is de eis niet gesteld dat deze ondertekend is. Door de eis van betrouwbaarheid wordt er, afhankelijk van de aard en de inhoud van het bericht en het doel waarvoor het gebruikt wordt, een vorm van authenticatie van overheidscommunicatie ingevoerd die voorheen niet bestond.

Door het reeds ingeburgerde gebruik van faxapparatuur is er inmiddels vrij veel jurisprudentie over het begin en einde van de termijn bij elektronische communicatie. Bij verzending van een elektronisch bericht naar een bestuursorgaan geldt dat de verzender moet bijhouden of en wanneer een bepaald bericht verzonden is. Bij twijfel moet contact worden opgenomen met het bestuursorgaan om na te gaan of een bericht ontvangen dan wel verzonden is. Het bestaan van een plicht voor bestuursorganen om logfiles dan wel een verzend- of gespreksregistratie bij te houden valt nog niet uit de jurisprudentie af te leiden. Wel kan het ontbreken van een dergelijke registratie ertoe leiden dat de ontvangst van een bericht door het bestuursorgaan niet op een niet ongeloofwaardige wijze ontkend kan worden, maar in de beide aangehaalde uitspraken speelde naast het ontbreken van een ontvangstregistratie ook het niet op orde zijn van de dossiers een rol. Door gebruik te maken van elektronische communicatiemiddelen is het voor een burger eenvoudiger geworden om aan te tonen dat een bericht verzonden is. De vraag of alleen het ontbreken van een ontvangstregistratie op zich zelf kan leiden tot een ‘niet ongeloofwaardige ontkenning’, is nog niet beantwoord. Het lijkt mij echter redelijk om de verplichting tot het bijhouden van een ontvangstregistratie aan te nemen.

3.9.2 Conclusies

In dit hoofdstuk wordt een antwoord gegeven op de vraag welke normen van toepassing zijn op elektronische vormen van communicatie met de overheid en of deze normen adequaat zijn.

Dit is de eerste subvraag van de centrale probleemstelling, die luidt:

Welke zijn de bestuursrechtelijke normen voor elektronische overheidscommunicatie, zijn ze in het licht van de gangbare beginselen van de democratische rechtsstaat nog adequaat en, zo nee, tot welke wijzigingen zou dit moeten leiden?

In de inleiding werden voorwaarden genoemd waaraan de normen voor elektronische communicatie met de overheid moeten voldoen. De eerste betrof de voorwaarde dat in normen die elektronische communicatie met de overheid reguleren, de transparantie en de toegang tot informatie en daarmee tot de

communicatiemiddelen gewaarborgd moeten zijn. Ten tweede moeten deze normen de integriteit en de authenticiteit van de elektronische communicatiemiddelen waarborgen. En ten slotte moet de vertrouwelijkheid van de communicatie gewaarborgd zijn.

Besproken zijn de normen die invulling geven aan het uitgangspunt van de nevenschikking, aan de vormvoorschriften schriftelijk en ondertekening, aan de norm die inhoudt dat alleen dan elektronisch gecommuniceerd kan worden indien kenbaar gemaakt is dat deze weg openstaat, aan de nadere eisen die aan het gebruik van de elektronische weg gesteld kunnen worden, aan de norm dat elektronische communicatie op een betrouwbare en vertrouwelijke manier moet plaatsvinden en aan de regeling over het begin en het einde van de termijn.

De eis van de elektronische handtekening kan tot onnodig formalisme leiden. Het bestuursorgaan heeft hier de keuze om te differentiëren naar gelang de aard en de inhoud van het bericht. In alle gevallen om een elektronische handtekening vragen (nog los van de praktische beschikbaarheid van dit middel) is niet nodig. Afdeling 2.3 biedt bestuursorganen de ruimte om andere middelen te gebruiken om een bericht te authenticeren.

Het uitgangspunt van de nevenschikking wordt door de wetgever in steeds meer situaties verlaten. Dit heeft een aantal consequenties. De bepaling dat elektronische communicatie alleen mogelijk is, wanneer betrokkenen hebben aangegeven langs deze weg bereikbaar te zijn, verliest hierdoor namelijk haar belang. In een aantal gevallen geldt de eis van kenbaar maken door burgers niet meer. Dat elektronisch wordt gecommuniceerd staat al vast. De burger die dit niet wil, moet er extra moeite voor doen om op de conventionele wijze met de overheid te kunnen communiceren.

Het verlaten van het uitgangspunt van de nevenschikking leidt ook tot de conclusie dat toegang tot elektronische communicatiemiddelen essentieel is om in de samenleving te kunnen functioneren. Voor het functioneren in de samenleving is de mogelijkheid om met de overheid te kunnen communiceren, of om informatie van de overheid te kunnen ontvangen, een basisvereiste. Geschiedt deze communicatie elektronisch, dan moeten burgers gemakkelijk over deze middelen kunnen beschikken.

Het verlaten van het uitgangspunt van de nevenschikking strookt ook niet met de interpretatie in jurisprudentie over art. 2:15, eerste lid, Awb. Hieruit volgt dat alleen elektronisch met de overheid kan worden gecommuniceerd, indien deze dat kenbaar heeft gemaakt. Deze eis werkt voor de burger onnodig formalisme en onduidelijkheid in de hand. Beter zou het zijn de norm uit deze bepaling om te draaien, zoals inmiddels in veel gevallen ook al voor de burger geldt: elektronische communicatie is mogelijk, tenzij het overheidsorgaan met redenen omkleed aangeeft waarom dit niet mogelijk is.

Verder leidt het verlaten van het uitgangspunt van de nevenschikking tot de conclusie dat art. 8:4, aanhef en onder k, Awb moet komen te vervallen. Zodra elektronische communicatie de norm wordt, moeten burgers nadere eisen die op grond van art. 2:15, eerste lid, Awb, aan deze communicatie gesteld worden en die hen rechtstreeks in hun belang treffen, voor de rechter kunnen brengen. De ongebreidelde beleidsvrijheid die nu het gevolg is van art. 2:15, eerste lid, Awb in samenhang met art. 8:4, aanhef en onder k, Awb is dan ook niet adequaat, want hierdoor kan de toegang tot communicatie met de overheid zonder rechterlijke toets beperkt worden.

In art. 2:14, derde lid, en art. 2:15, derde lid, wordt de eis gesteld dat elektronische berichten op een voldoende betrouwbare en vertrouwelijke manier verzonden worden. De verzender moet instaan voor de betrouwbaarheid en vertrouwelijkheid daarvan. Disclaimers op overheidswebsites en onder e-mailberichten die door een bestuursorgaan zijn verzonden, waarbij het orgaan aangeeft hiervoor niet in te staan, zijn dan ook in strijd met art. 2:14 Awb.

Uit deze eis vloeit eveneens voort dat de vertrouwelijkheid van de berichtenuitwisseling gewaarborgd moet zijn. De overheid dient dan ook zorg te dragen voor een adequate beveiliging van de informatie die zij uitwisselt.

Bij het begin en einde van termijnen is de bewijspositie van de burger die gebruik maakt van elektronische communicatiemiddelen voordeliger dan de burger die gebruik maakt van de conventionele weg. Bestuursorganen zullen een ontvangstregistratie moeten bijhouden.

