DigiD: goed geregeld?

Het verschijnsel DigiD rechtsstatelijk bekeken

J. Vlug[1] [2]

1 Inleiding

"DigiD: je eigen inlogcode voor de hele overheid", luidt de wervende tekst op digid.nl. Negen miljoen burgers doen inmiddels mee, met de digitale - vooringevulde! - belastingaangifte als *killer app*.
De *succes story* van DigiD heeft echter ook schaduwkanten. Sinds de introductie in 2004 vond een reeks van beveiligingsincidenten plaats. Het beheer van DigiD bleef zelden langer dan enkele jaren op één plek en de ontwikkeling stokte, waardoor DigiD nog steeds leunt op het suboptimale gebruik van de *username/password*-combinatie[3]. Bij problemen werd de burger vaak van het kastje naar de muur gestuurd.
Dit alles doet de vraag rijzen welke regels eigenlijk van toepassing zijn op DigiD. Daartoe wordt in dit artikel een inventarisatie gemaakt van de juridische issues rond DigiD, zoals het gebruik van het burgerservicenummer (bsn), de koppeling met het GBA, de vraag of DigiD ook een elektronische handtekening is, de aard van de rechtsverhouding tussen burger en DigiD en de vraag of het gebruik van DigiD (feitelijk) mag worden afgedwongen. Daarnaast worden ook grondrechtelijke aspecten belicht. Bovenal staat de vraag centraal of een wezenlijke voorziening als DigiD niet zou moeten steunen op specifieke regelgeving. Deze vraag wordt met name bezien vanuit het (staatsrechtelijk) legaliteitsbeginsel. Ten slotte wordt DigiD in perspectief geplaatst door van een aantal Europese landen de ontwikkelingen op het gebied van *eID*[4] de status te nemen.

2 Geschiedenis en achtergrond DigiD

Aan het einde van de 20e eeuw raakt de toepassing van ICT onder invloed van de penetratie van internet in een stroomversnelling. Ook de Nederlandse overheid ziet dan nieuwe mogelijkheden en

[1] Mr. J. Vlug is werkzaam bij het College bescherming persoonsgegevens (CBP) en schrijft dit artikel op persoonlijke titel.
Met dank aan R.J.N. Schlössels (hoogleraar staats- en bestuursrecht, RU) en B.P.F. Jacobs (hoogleraar beveiliging en correctheid van programmatuur, RU).
[2] Het onderzoek dat ten grondslag lag aan dit artikel werd afgesloten per 1 juli 2012.
[3] Eventueel aangevuld met sms-authenticatie. zie verder onder 3.2.
[4] De in Europa gangbare afkorting voor *elektronic identification*.

zet de eerste stappen in wat thans wel iOverheid[5] wordt genoemd: het actieprogramma Elektronische snelwegen[6] gaat van start. Dit programma is de eerste in een reeks die uiteindelijk (wellicht) wordt afgesloten met het programma Andere Overheid[7] [8] [9].

Binnen deze programma's werd reeds in een vroeg stadium onderkend dat voor elektronische dienstverlening door de overheid c.q. elektronische communicatie tussen overheid en burger een - liefst overheidsbrede -authenticatievoorziening[10] nodig is. In 2004 werd door het Bureau Keteninformatisering Werk & Inkomen (BKWI)[11] een eerste versie van zo'n authenticatievoorziening ontwikkeld voor gebruik in het domein van belastingen, werk en inkomen (het sofi-domein). Kort daarna werd het beheer van deze voorziening overgedragen aan de Belastingdienst (2005) en vervolgens aan GBO Overheid (2006-2010). DigiD wordt nu beheerd door Logius, een onderdeel van het ministerie van BZK.[12]

3 Schets van de gegevensverwerking

3.1 Werking

De elementaire functie van DigiD is authenticatie van de burger die via internet contact zoekt met een bestuursorgaan (of een andere organisatie die het bsn mag gebruiken[13] en is aangesloten op DigiD) - verder te noemen: afnemer[14] [15].

Authenticatie vormt - in dit verband - een onderdeel van de toegangscontrole tot een afgeschermd onderdeel van de website van de afnemer, waarop de burger bijvoorbeeld zijn gegevens kan inzien of waarop een bepaalde dienst wordt aangeboden. Bij zo'n toegangscontrole worden in het algemeen de volgende stappen doorlopen:

---

[5] Wetenschappelijke Raad voor het Regeringsbeleid, *iOverheid*, Amsterdam University Press 2011.
[6] Elektronisch snelwegen, Kamerstukken II 1995/96 - 1997/98, 24 565.
[7] Ook wel "Modernisering van de overheid" geheten (Kamerstukken II 2005/06-2011/12, 29 362).
[8] Tussen deze programma's liepen ook nog: Wetgeving voor de elektronische snelweg (Kamerstukken II 1997/98 - 2002/03, 25 880) en Actieprogramma Elektronische Overheid (Kamerstukken II 1998/99 - 2006/07, 26 387).
[9] Zie voor een beknopte geschiedenis van de Elektronische overheid: J. Holvast, 'Elektronische overheid' in J.M.A. Berkvens/J.E.J. Prins (red.), *Privacyregulering in theorie en praktijk,* Deventer: Kluwer 2007.
[10] Zie verder onder 3.1.
[11] Zie www.bkwi.nl.
[12] Zie www.logius.nl.
[13] Wie wel en niet mogen aansluiten op DigiD is niet in regelgeving bepaald. Een buitengrens is de bevoegheid het bsn te kunnen gebruiken omdat zonder uitwisseling van bsn geen gebruik kan worden gemaakt van DigiD.
[14] Zie artikel 1.1 Gebruiksvoorwaarden DigiD versie 5.1 (augustus 2010), te vinden op www.digid.nl.
[15] Een lijst van aangesloten organisaties staat op www.digid.nl.

-identificatie
-authenticatie
-autorisatie

In het geval van DigiD bestaat de *identificatie* uit het invoeren van de gebruikersnaam; de *authenticatie* verifieert of de gebruikersnaam inderdaad wordt gebruikt door zijn "eigenaar" door hem een (geheim) wachtwoord te vragen[16]. De *autorisatie* geeft op basis van zogenaamde toegangsprofielen specifieke toegangsrechten die per burger kunnen verschillen.

De burger kan pas gebruik maken van DigiD als hij een DigiD-*account* (combinatie gebruikersnaam-wachtwoord) heeft gekregen. Voorafgaand aan de verstrekking van zo'n account vindt een aantal controles plaats, waarbij onder andere het GBA-V[17] wordt geraadpleegd. De burger dient daarnaast akkoord te gaan met de Gebruiksvoorwaarden DigiD[18].

Van burgers met een DigiD-account - ruim 9 miljoen[19] - worden de volgende gegevens bij Logius opgeslagen:

- bsn;
- A-nummer[20];
- gebruikersnaam;
- wachtwoord (versleuteld);
- e-mailadres (optioneel);
- mobiel telefoonnummer (optioneel)[21].

Als een burger een afgeschermd onderdeel van de website van een afnemer benadert kan op die website het DigiD logo worden aangeklikt waarna hij wordt doorgeleid naar de DigiD website. Op de DigiD website worden gebruikersnaam en wachtwoord ingevuld en als deze combinatie "klopt" wordt hij weer teruggestuurd naar de website van de afnemer. DigiD geeft daarbij A-nummer en bsn

[16] Soms vindt ook nog sms-authenticatie plaats (zie verder onder 3.2).
[17] Zie verder onder *A-nummer.*
[18] Zie voor een nadere beschouwing van deze Gebruiksvoorwaarden verder onder *Duiding van de rechtsbetrekking tussen burger en DigiD.*
[19] www.logius.nl/producten/toegang/nieuwsbericht/titel/ruim-9-miljoen-gebruikers-digid.
[20] Zie verder onder 5.3.2.2.
[21] In verband met sms-authenticatie (zie verder onder 3.2).

mee, opdat de afnemer gericht toegang kan verlenen tot de gegevens van deze burger en specifieke diensten aan deze burger kan verlenen.

3.2 Zekerheidsniveaus

DigiD onderkent (in theorie) drie zekerheidsniveaus: basis, midden en hoog.[22] Deze niveaus zijn gerelateerd aan de vertrouwelijkheid van de gecommuniceerde gegevens. Het niveau "hoog" wordt niet aangeboden. Hiervoor zou een chipkaart nodig zijn, die er de facto (nog) niet is. Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties onderzoekt nog steeds de mogelijkheid tot invoering van deze zogenaamde eNIK. De eNIK bestaat uit een chip die wordt toegevoegd aan de Nederlandse identiteitskaart. Er wordt dus geen aparte kaart voor gemaakt.

De combinatie gebruikersnaam-wachtwoord vormt het zekerheidsniveau "basis"; indien dit wordt aangevuld met sms-authenticatie is sprake van zekerheidsniveau "midden". Bij sms-authenticatie wordt na het (correct) invullen van gebruikersnaam-wachtwoord door DigiD een sms met een code gestuurd naar de inloggende burger. Deze code moet worden overgetypt op het DigiD-inlogscherm, waarna de gevraagde toegang wordt verkregen. Dit is een extra drempel tegen onbevoegd gebruik van de DigiD-account.

4 DigiD en digitale veiligheid

DigiD kent geen onbekommerde geschiedenis. Berucht was het advies van de Belastingtelefoon in 2007 om voor het doen van elektronische belastingaangifte zo nodig de DigiD van iemand anders, bijvoorbeeld de buurman, te "lenen". En recent trok de DigiNotar affaire[23], ook in relatie tot DigiD, veel aandacht.

4.1 Problemen rond DigiD

Er bestaat al jaren een v.o.f. Digi-D[24]. In de loop der tijd stuurden honderden burgers per abuis (vertrouwelijke) informatie per email naar dit bedrijf. Digi-d en DigiD zijn al jaren verwikkeld in een

[22] Zie www.digid.nl.
[23] Zie M.M. Groothuis, 'De DigiNotar-affaire: een indringende waarschuwing', Computerrecht 2011/151.
[24] www.digi-d.nl

rechtszaak[25]. Het onderliggende probleem (en de kans op miscommunicatie) is nog steeds niet verholpen.

In 2006 bleek dat in de DigiD-database één mobiel telefoonnummer[26] aan meerdere burgers kon zijn gekoppeld, terwijl de per sms verzonden DigiD-inlogcode strikt persoonlijk is (of: zou moeten zijn). Jacobs en Jochems uitten in 2007 twijfels over de veiligheid van DigiD.[27] Zij concludeerden onder meer dat de rond DigiD getroffen organisatorische maatregelen onvoldoende bescherming bieden tegen identiteitsfraude.

In 2008 werd DigiD geïntroduceerd bij de elektronische belastingaangifte waarna 730.000 digitale belastingaangiften zoek raakten. De oorzaak bleek een softwarefout bij de Belastingdienst die niet tijdig werd ontdekt omdat de integratietest te laat werd uitgevoerd.[28]

Eind 2009 maakte GOVCERT bekend dat communicatie via GSM (inclusief SMS) is af te luisteren.[29] Vanwege de SMS-authenticatie verzwakt dit ook de beveiliging van DigiD. De minister van VWS besloot dan ook direct een pas op de plaats te maken bij het ontwikkelen van de zgn. EPD-DigiD.[30]

Kort daarna vond een grootschalige toeslagenfraude plaats via DigiD: de huur-, zorg- en kinderopvangtoeslagen van honderden mensen werden overgemaakt naar de rekeningnummers van de fraudeurs. De fraude bleek kinderspel en werd veroorzaakt doordat de software van de Belastingdienst niet controleerde of het gebruikte DigiD wel bij de aanvrager hoorde.[31]

Oktober 2011 werd door Webwereld uitgeroepen tot "Lektober".[32] Als eerste was DigiD aan de beurt.[33] Een aantal (gemeentelijke) websites met DigiD[34], die kwetsbaar bleken voor een zgn. cross site scripting (XSS)[35] aanval, maakten het mogelijk een DigiD-sessie over te nemen. Naar aanleiding hiervan moesten alle afnemers van DigiD vóór 1 april 2012 een ICT-beveiligingsassessment doorlopen.[36] Deze deadline is inmiddels opgeschoven naar 1 januari 2013 voor "grootverbruikers" (Belastingdienst, DUO en UVW) en naar 1 januari 2014 voor gemeenten, provincies en Unie van Waterschappen.[37]

---

[25] Rechtbank 's-Gravenhage 17 november 2010 (Digi-D/DigiD), zaaknummer 371238, KG ZA 10-891.
[26] Opgenomen ten behoeve van sms-authenticatie (zie verder onder 3.2).
[27] Bart Jacobs en Marc Jochems, 'DigiD en privacy', *Automatisering Gids,* 19 oktober 2007.
[28] Automatisering Gids, 27 februari 2008.
[29] Zie Factsheet 2009-05 (december 2009) op govcert.nl.
[30] Kamerstukken II 2010/11, 27 529, nr. 61, p. 8.
[31] NRC Handelsblad 19 september 2011 'Fraudeurs bestelen burgers via DigiD'.
[32] www.webwereld.nl/nieuws/108052/lektober--iedere-dag-een-privacylek-op-webwereld.html
[33] www.webwereld.nl/nieuws/108107/lek1--blunder-logius-maakt-digid-fraude-kinderspel.html
[34] www. webwereld.nl/nieuws/108111/lek2--7-gemeenten-kwetsbaar-voor-digid-lek.html en www.webwereld.nl/nieuws/108184/lektober-superknaller--megalek-treft-50-gemeenten.html
[35] Zie nl.wikipedia.org/wiki/Cross-site_scripting
[36] Kamerstukken II 2011/12, 26 643, nr. 193.
[37] Kamerstukken II 2011/12, 26 643, nr. 222. De door de Tweede Kamer aangenomen motie Gesthuizen/El Fassed (Kamerstukken II 2011/12, 26 643, nr. 238) beoogde het opschuiven van deze deadline ongedaan te maken. De minister van BZK heeft echter aangegeven geen uitvoering te kunnen geven aan deze motie.

Het Nationaal Cyber Security Centrum (NCSC)[38] waarschuwde recent voor kwetsbaarheden op webservers van het ICT-servicecentrum van Binnenlandse Zaken. DigiD was kwetsbaar voor DDoS-aanvallen.[39]

Niet in alle gevallen worden de problemen veroorzaakt door DigiD zelf. Vaak zijn het (ook) de "afnemers" die steken laten vallen. Maar volgens de Nationale Ombudsman kan de verantwoordelijke voor DigiD - de minister van BZK - hiermee niet wegkomen. Hij is uitermate kritisch over DigiD: "Als de overheid een bank was, zou die failliet zijn"[40]. Burgers die in verband met het gebruik van DigiD slachtoffer worden van identiteitsfraude, worden volgens hem van het kastje naar de muur gestuurd; het is onduidelijk wie verantwoordelijk is voor DigiD.[41] De Nationale Ombudsman baseert zich hierbij op klachten van burgers.[42]

4.2 Digitale veiligheid bij overheidsorganisaties

De Onderzoeksraad voor de Veiligheid onderzocht in 2012 het DigiNotar-incident en trok daarbij ook conclusies inzake digitale veiligheid in het algemeen en specifiek bij overheidsorganisaties.[43] De Onderzoeksraad verstaat onder digitale veiligheid:

"voorkomen dat (persoons)gegevens van burgers en bedrijven gecompromitteerd raken doordat onbevoegden er kennis van kunnen nemen, ze manipuleren of misbruiken"[44]

De onderzoeksraad concludeert dat de digitale overheid kwetsbaarheden kent: enerzijds kwetsbaarheden voor burgers en bedrijven wier gegevens door de overheid verwerkt worden, anderzijds kwetsbaarheden voor de vitale infrastructuur als ICT-systemen uitvallen door verstoringen. De Onderzoeksraad concludeert dat de overheid de regie moet nemen bij het beheersen van deze kwetsbaarheden. De Onderzoeksraad is vervolgens van mening dat de rijksoverheid een stelselverantwoordelijkheid heeft voor digitale veiligheid bij overheidsorganisaties en dat deze verantwoordelijkheid doortastender moet worden ingevuld *door actiever gebruik te*

[38] Het vroegere Govcert.nl.
[39] Nieuwsbericht op computable.nl van 27 januari 2012 (http://www.computable.nl/artikel/nieuws/security/4370954/1276896/ncsc-wijst-logius-op-lek-in-digidserver.html)
[40] AD, 8 augustus 2011.
[41] Idem.
[42] Zoals bijvoorbeeld de Ombudsmanrapporten 2008/214 en 2008/268.
[43] Onderzoeksraad voor de Veiligheid, *Het DigiNotarincident - waarom digitale veiligheid de bestuurstafel te weinig bereikt*, juni 2012.
[44] Onderzoeksraad 2012, p. 65.

maken van haar regelgevende bevoegdheid en haar centrale positie in het openbaar bestuur.[45] Er kan nauwelijks twijfel over bestaan dat (al) deze conclusies ook DigiD regarderen.

5 Juridisch kader

5.1 Grondrechtelijke invalshoek

Op het eerste gezicht lijkt DigiD niet meer dan een (neutraal) stukje techniek tussen burger en overheid. Maar de schijn bedriegt: de beveiliging ervan, de toegang, de geboden diensten en de keuzevrijheid om DigiD al dan niet te gebruiken zijn geen neutrale aangelegenheden maar de resultanten van beleidskeuzes. De vormgeving van dit "stukje techniek" heeft direct impact op de burger en heeft gevolgen voor zijn relatie met de overheid. Het is de toegangspoort naar zijn persoonsgegevens, naar overheidsinformatie en naar voorzieningen waarop hij recht heeft. En het is zijn digitale identiteit in zijn communicatie met de overheid. Op bepaalde punten is daarom een grondrechtelijke benadering denkbaar.

In de eerste plaats speelt de *bescherming van persoonsgegevens* een rol: niet alleen de bij DigiD opgeslagen persoonsgegevens (zie par. 3.1) maar ook de persoonsgegevens bij de "afnemers" die via DigiD ontsloten worden. Bescherming van persoonsgegevens is onderdeel van het recht op privéleven (artikel 8 EVRM) en is verder als grondrecht erkend in artikel 16 VWEU en in artikel 10 Grondwet. Zie verder par. 5.3.

De *toegang tot overheidsinformatie* is niet als grondrecht in Grondwet en EVRM opgenomen. In de jurisprudentie van het EHRM zijn de artikelen 8 en 10 EVRM in bepaalde gevallen echter wel zo uitgelegd, dat de overheid bepaalde informatie moest verstrekken. Bij artikel 8 EVRM betreft het gevallen waarin de burger specifiek belang bij de informatie heeft (Guerra-arrest[46]). Een beroep op artikel 10 EVRM is in dit verband slechts mogelijk indien het gaat om openbare informatie, en dan nog slechts in uitzonderingsgevallen.[47] Voorts kan erop worden gewezen dat de Staatscommissie 'Grondrechten in het digitale tijdperk' (1999) op verzoek van de regering heeft geadviseerd over de vraag of het wenselijk is een grondrecht met betrekking tot de toegankelijkheid van (elektronische) (overheids-)informatie in te voeren. De Staatscommissie beantwoordde deze vraag bevestigend en stelde de volgende formulering voor:

[45] Onderzoeksraad 2012, p. 85.
[46] EHRM 19 februari 1998, NJ 1990, 690 *(Guerra)*.
[47] EHRM 14 april 2009, NJ 2010, 209 (*TASZ v. Hongarije)*

1. *Ieder heeft recht op toegang tot bij de overheid berustende informatie. Dit recht kan bij of krachtens de wet worden beperkt.*
2. *De overheid draagt zorg voor de toegankelijkheid van bij de overheid berustende informatie.* [48]

Tot welke overheidsinformatie geeft DigiD toegang? In het algemeen niet tot openbare overheidsinformatie, want deze wordt ontsloten via bijvoorbeeld overheid.nl waarvoor geen persoonlijke login nodig is. Wel kan informatie die specifiek op de burger (of zijn woonomgeving) is toegesneden of geselecteerd worden aangeboden via DigiD. Op zulke informatie zou artikel 8 EVRM - in lijn met het Guerra-arrest - van toepassing kunnen zijn. Overigens is hier een gedeeltelijke samenloop met het inzagerecht zoals we dat kennen uit de Wbp en dat uiteindelijk eveneens valt terug te voeren op artikel 8 EVRM.[49]

Tenslotte kan in dit verband nog worden gewezen op het onder artikel 8 EVRM beschermde *right to identity* als grondrechtelijke waarborg tegen identiteitsdiefstal.[50]

Het voert in dit verband te ver deze grondrechtelijke beginselen compleet uit te werken in relatie tot DigiD. Wel is het belangrijk te signaleren dat bepaalde aspecten van DigiD in grondrechtelijk perspectief kunnen worden geplaatst.

5.2 Afdeling 2.3 Awb (Wet elektronisch bestuurlijk verkeer)

5.2.1 algemeen

Het elektronisch verkeer tussen bestuursorgaan en burger wordt in algemene zin gereguleerd door Afdeling 2.3 van de Awb[51].

Artikel 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 Awb in acht worden genomen. "Verzending" is hier bedoeld in de "ruimste zin van het woord": hieronder wordt "iedere

[48] Rapport Commissie 'Grondrechten in het digitale tijdperk' (1999), p. 190.
[49] EHRM 7 juli 1989, NJ 1991, 659 (*Gaskin)*
[50] EHRM 17 juli 2008, NJ 2009, 524 (*Reklos & Davourlis t. Griekenland)*
[51] Let echter op: niet alle afnemers van DigiD zijn bestuursorganen (zie paragraaf 3.1).

vorm van elektronische gegevensuitwisseling met een ander" verstaan. Ook het plaatsen van een stuk op een website wordt hieronder bijvoorbeeld begrepen.[52]

Gezien deze ruime uitleg van "verzending" wordt aangenomen dat Afdeling 2.3 Awb van toepassing is op DigiD. Hieronder worden daarom enige bepalingen uit deze afdeling toegepast op DigiD.

5.2.2 elektronische handtekening (artikel 2:16 Awb)

Bij een analyse van DigiD dient onderscheid te worden gemaakt naar DigiD als authenticatiemiddel en het gebruik ervan in vervolgsessies door zgn. afnemers[53] als UWV, gemeenten etc. In deze vervolgsessies kan eventueel sprake zijn van een - met behulp van DigiD gezette - elektronische handtekening.

De elektronische handtekening in het verkeer tussen burgers en bestuursorganen wordt geregeld in artikel 2:16 Awb. Artikel 2:16 Awb verwijst daarbij naar de artikelen 3:15a lid 2 tot en met lid 6 BW.

De definitie van de elektronische handtekening luidt als volgt (artikel 3:15a lid 4 BW):

"een handtekening (...) die bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd met andere elektronische gegevens en die worden gebruikt als middel voor authentificatie[54]".

Aan het element van *vasthechting* of *logische associatie* aan het te ondertekenen bestand wordt in het algemeen weinig aandacht geschonken. De Memorie van Toelichting bij de Wet elektronisch bestuurlijk verkeer merkt - terecht - wel op dat 'de elektronische handtekening (...) strikt genomen alleen betrekking [heeft] op de authenticiteit van het *bericht* (cursivering auteur)'.[55] [56] Zeer recent oordeelde de Rb. Rotterdam in een aanbestedingszaak dat het enkele feit dat bij een inlogprocedure van de digitale aanbestedingsportal de authenticatie van de inschrijver en de beveiliging van de data op orde waren, nog niet maakt dat er ten aanzien van enkele documenten - waarvan de ondertekening een voorwaarde was om een geldige inschrijving te kunnen doen - sprake is een

[52] Kamerstukken II 2001/02, 28 483, nr. 3, p. 37.
[53] Zie paragraaf 3.1.
[54] Dit is de tekst van de wet. Beter is volgens mij "authenticatie". Zo ook M.B. Voulon, 'Wetsvoorstel elektronische handtekeningen', Computerrecht 2001 p. 287, noot 5.
[55] Kamerstukken II 2001/02, 28 483, nr. 3, p. 21.
[56] Zie ook M.B. Voulon, 'Toezicht op certification service providers (CSP's)', *Computerrecht* 2012, 1, p. 33.

elektronische handtekening in de zin van artikel 3:15a lid 4 BW. [57] Indien geen (authenticerende) elektronische gegevens worden vastgehecht aan of logisch geassocieerd met het bericht dat de burger via DigiD aan het bestuursorgaan verzendt kan geen sprake zijn van een elektronische handtekening in de zin van artikel 3:15a lid 4 BW. Bij de digitale belastingaangifte is bijvoorbeeld geen sprake van een elektronische handtekening: weliswaar wordt de identiteit van de indiener gecontroleerd, maar deze wordt niet vastgehecht of verbonden met het aangiftebestand.

Voor zover binnen een DigiD-vervolgsessie wel sprake zou zijn van een elektronische handtekening in de zin van artikel 3:15a lid 4 BW, rijst de vraag hoe deze dient te worden gekwalificeerd. In artikel 3:15a BW wordt een onderscheid gemaakt tussen een geavanceerde elektronische handtekening en een "gewone" elektronische handtekening. Een geavanceerde elektronische handtekening moet voldoen aan de eisen die artikel 3:15a lid 2 BW stelt:

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

DigiD voldoet in elk geval niet aan de onder e en f gestelde (PKI-)eisen en kan daarom niet gelden als een *geavanceerde* elektronische handtekening. Wel kan eventueel sprake zijn van een "gewone" elektronische handtekening, maar dan uitsluitend indien werkelijk sprake is van vasthechting of logische associatie aan het document dat wordt ondertekend. Alleen dan levert DigiD een elektronische handtekening op in de zin van artikel 3:15a lid 4 BW die kan dienen ter ondertekening conform artikel 2:16 Awb.

[57] Rb. Rotterdam 16 april 2012, LJN BW5991.

5.2.3 beginsel van nevenschikking (artikel 2:14 lid 1 Awb)

Het beginsel van nevenschikking houdt in dat de burger de keuze heeft of hij al dan niet elektronisch wenst te worden benaderd door het bestuursorgaan:

"Het kabinet kiest voor "nevenschikking" en niet voor "verdringing" van conventionele gegevensuitwisseling door elektronisch verkeer. Dit betekent dat de papieren weg mogelijk blijft: ook als het bestuur langs elektronische weg kan reageren, behoudt de burger de mogelijkheid aan te geven dat hij uitsluitend via papieren geschriften dan wel mondeling contact wenst. De elektronische weg komt naast en niet in plaats van het conventionele verkeer."[58]

In hoeverre de burger nog daadwerkelijk vrij is om al dan niet DigiD te gebruiken in zijn contacten met de overheid is ondertussen de vraag. Enig veldonderzoek[59] bracht aan het licht dat enkele transacties in de praktijk niet mogelijk zijn zonder DigiD.[60] Het betrof de volgende transacties: inschrijven voor een studie (studielink.nl), registreren in BIG-register, aanvragen vergoeding depositogarantiestelsel voor de DSB Bank (DNB) en aangifte Tanken zonder betalen (Bureau verkeershandhaving OM).

Zulke voorbeelden van "verdringing"[61] zijn in strijd met het beginsel van nevenschikking, dat een belangrijk uitgangspunt vormde bij het Wetsvoorstel elektronisch bestuurlijk verkeer[62]. Dit beginsel is onder andere tot uitdrukking gebracht in artikel 2.14 lid 1 Awb.[63]

5.3 Wet bescherming persoonsgegevens

Omdat in DigiD persoonsgegevens worden verwerkt, is de Wet bescherming persoonsgegevens (Wbp) van toepassing.

---

[58] Kamerstukken II 2001/02, 28 483 nr. 3, p. 3.
[59] Steekproef uitgevoerd in januari 2012 (update: juni 2012).
[60] In zulke gevallen wordt meestal als regel gehanteerd dat burgers die kunnen beschikken over een eigen DigiD deze moeten gebruiken om in te loggen. Uitzonderingen worden dus slechts gemaakt voor burgers die geen DigiD kunnen bemachtigen. Dit zijn bijvoorbeeld mensen die in het buitenland woonachtig zijn (en geen AOW genieten).
[61] Zie ook J.E.J. Prins, 'Verdringing: sluipend feit van deze tijd?', *Computerrecht* 2005, 1, p. 2.
[62] Kamerstukken II 2001/02, 28 483 nr. 3, p. 8-9.
[63] Kamerstukken II 2001/02, 28 483 nr. 3, p. 38. Letterlijk genomen betreft dit slechts de verzending *aan* de burger, terwijl het bij DigiD transacties *tussen* burger en overheid betreft. Aangenomen moet worden dat de strekking van artikel 2:14 lid 1 Awb met zich meebrengt dat het gebruik van DigiD voor de burger niet (feitelijk) verplicht mag zijn.

Bij de bestudering van het elektronisch verkeer tussen burger en bestuursorgaan via DigiD in het licht van de Wbp dient een scherp onderscheid te worden gemaakt tussen de *authenticatie* zoals beschreven in par. 3.1 enerzijds en de *transactie* met het bestuursorgaan (bijv. de aangifte inkomstenbelasting) anderzijds.

Voor de *authenticatie* en de daarbij door Logius gebruikte gegevens is de minister van BZK verantwoordelijk. Bij de *transactie* tussen burger en bestuursorgaan wordt DigiD door het bestuursorgaan ingezet als beveiligingsmiddel. De transactie zelf valt onder de verantwoordelijkheid van het betreffende bestuursorgaan en staat dus los van DigiD. De Wbp-rolverdeling tussen minister van BZK (als leverancier van DigiD) en het betreffende bestuursorgaan wordt beheerst door het in de praktijk weerbarstige leerstuk van de verantwoordelijke en de bewerker (artikel 1 sub d en e Wbp).

De toepassing van de Wbp op DigiD valt verder buiten het kader van dit onderzoek, met uitzondering van artikel 13 Wbp (beveiliging) en artikel 24 Wbp (gebruik persoonsnummers), die in deze casus van bijzonder belang zijn.

5.3.1 Artikel 13 Wbp (beveiliging)

Artikel 13 Wbp verplicht de verantwoordelijke passende technische en organisatorische maatregelen te nemen om de persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Artikel 13 Wbp is bij uitstek een open norm en is dus lastig toe te passen.

In par. 4.1 zagen we dat DigiD nogal wat beveiligingsincidenten heeft gekend. Mogelijk leverden deze incidenten overtreding op van artikel 13 Wbp door de minister van BZK, het betrokken bestuursorgaan of beide. Gezien het open karakter van artikel 13 Wbp en de complexiteit van de verantwoordelijkheidsvraag kan hierover geen uitsluitsel worden gegeven.

5.3.2 Artikel 24 Wbp (gebruik persoonsnummers)

DigiD verwerkt de persoonsnummers bsn en A-nummer. Hieronder
wordt ingegaan op de toelaatbaarheid hiervan.

De Europese richtlijn 95/46/EC draagt de Lidstaten op de voorwaarden vast te stellen waaronder een persoonsnummer mag worden gebruikt (artikel 8 lid 7 Richtlijn 95/46/EC). Dit heeft zijn uitwerking gekregen in artikel 24 Wbp. Dit artikel is onderdeel van Hoofdstuk 2, paragraaf 2 Wbp getiteld 'De

verwerking van bijzondere persoonsgegevens'[64]. Een persoonsnummer is dus een bijzonder persoonsgegeven, al is de verwerking ervan niet verboden in artikel 16 Wbp. Artikel 24 Wbp geeft specifiek voor persoonsnummers invulling aan het zgn. doelbindingsprincipe zoals geformuleerd in artikel 9 Wbp en luidt als volgt:

1. *Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald.*
2. *Bij algemene maatregel van bestuur kunnen andere dan in het eerste lid bedoelde gevallen worden aangewezen waarin een daarbij aan te wijzen nummer als bedoeld in het eerste lid, kan worden gebruikt. Daarbij kunnen nadere regels worden gegeven over het gebruik van een zodanig nummer.*

5.3.2.1 bsn

Het gebruik van het bsn is geregeld in de Wet algemene bepalingen burgerservicenummer (Wabb). Artikel 10 Wabb geeft "overheidsorganen"[65] de *bevoegdheid* het bsn te gebruiken in het kader van de uitvoering hun taak. Dat deze bevoegdheid ook de minister van BZK toekomt terzake van de DigiD-verwerking staat niet ter discussie.

Strikt genomen kan artikel 10 Wabb niet worden gelezen als een *verplichting* het bsn te gebruiken, waardoor hiermee nog niet wordt voldaan aan het vereiste van artikel 24 Wbp ("bij wet voorgeschreven"). Het College bescherming persoonsgegevens (CBP) meent echter dat "voorgeschreven" in artikel 24 Wbp ruim geïnterpreteerd dient te worden, namelijk als alle persoonsnummers die hun basis in de wet vinden.[66] Zelfs indien het CBP hierin niet zou worden gevolgd, behoeft nog geen strijd met artikel 24 Wbp te bestaan: artikel 11 Wabb biedt immers eveneens een uitweg. Artikel 11 Wabb verplicht namelijk bij gebruik van een ander nummer dan bsn - in casu het A-nummer - tot het eveneens vermelden van het bsn.

[64] Dit is conform de systematiek in Richtlijn 95/46/EC.
[65] Zoals gedefinieerd in artikel 1 sub c Wabb.
[66] Uitspraak CBP 15 mei 2003 (z2002-1291).

5.3.2.2 A-nummer

Het A-nummer is "bij wet voorgeschreven" (namelijk in artikel 34 lid 1 sub a onder 7 Wet Gemeentelijke basisadministratie persoonsgegevens (Wet GBA)). De vraag is nu met name of de verstrekking van het A-nummer vanuit de gemeentelijke basisadministratie (GBA; het vroegere bevolkingsregister) aan DigiD aan de vereisten van artikel 24 Wbp voldoet.

DigiD verkrijgt het A-nummer niet rechtstreeks uit het GBA maar via GBA Verstrekkingen (GBA-V). GBA-V is een centrale, landelijke database die kopieën bevat van alle persoonslijsten die in de gemeentelijke GBA's zijn opgenomen. Deze sturen een volledig nieuwe "persoonslijst" naar GBA-V zodra één of meer van de gegevens op een persoonslijst wijzigt. Het betreft dus een gesynchroniseerde kopie.

GBA-V wordt beheerd door de minister van BZK (artikel 66b Besluit GBA). Er zijn geen indicaties dat in afwijking hiervan een ander dan de minister van BZK als verantwoordelijke in de zin van de Wbp heeft te gelden.

De persoonslijst (waarin o.a. het A-nummer[67]) wordt dus door een GBA aan GBA-V verstrekt (1), die hiervan een kopie opslaat (2) waarna GBA-V het A-nummer doorgeeft aan DigiD (3) zodra een nieuwe DigiD-account wordt aangemaakt.

De verstrekking van het A-nummer door GBA aan GBA-V is mogelijk op basis van artikel 91 Wet GBA lid 1 juncto artikel 66a lid 2 Besluit GBA. De opslag bij en de verstrekking door GBA-V aan DigiD zijn als zodanig niet geregeld. De minister van BZK lijkt er, door GBA-V te positioneren als technisch onderdeel van de verstrekkingssystematiek van de GBA, van uit te gaan dat het steeds een via-verstrekking betreft zonder een zelfstandige rol voor GBA-V, waarbij het verstrekkingenregime van de (Wet) GBA geldt.[68] Deze zienswijze lijkt echter onjuist: het centraal bijhouden van een landelijke kopie is een geheel andere verwerking dan het decentraal onderhouden van de GBA zelf. Dit komt ook tot uiting in het feit dat GBA en GBA-V niet dezelfde verantwoordelijke hebben.

Nu de verstrekking door GBA-V aan DigiD niet binnen de grenzen van artikel 24 lid 1 Wbp valt, dient gekeken te worden naar artikel 24 lid 2 Wbp, dat de mogelijkheid creëert om bij algemene maatregel van bestuur gevallen aan te geven waarin een persoonsnummer alsnog mag worden gebruikt.

[67] Zie artikel 34 lid 1 sub a onder 7 Wet GBA.
[68] Wijziging Besluit GBA, Staatsblad 2005,536 p. 8 en 10; Besluit beheer DigiD, Staatscourant 18 augustus 2006, nr. 160, p. 7.

Hierbij valt het oog op het Tijdelijk Besluit nummergebruik overheidstoegangsvoorziening (2004)[69]. Deze amvb is nog steeds in werking en daarmee minder tijdelijk dan men op grond van de titel zou aannemen. In 2004 was echter nog de verwachting dat de overheidstoegangsvoorziening (OTV) - het huidige DigiD - bij formele wet zou worden geregeld. In deze wet zou onder meer de basis worden gelegd voor het gebruik van de persoonsnummers bsn en A-nummer[70] en zou de zorg voor de instandhouding van de OTV aan een bestuursorgaan worden opgedragen[71]. De amvb betreft echter slechts het gebruik van deze persoonsnummers in de context van de OTV en dient dus uitsluitend tot doel te voldoen aan artikel 24 Wbp.

Door dit Tijdelijk besluit nummergebruik overheidstoegangsvoorziening is verwerking van het A-nummer in het kader van DigiD op grond van artikel 24 lid 2 Wbp toegelaten. [72]

5.4 Besluit beheer DigiD

Sinds 2006 bestaat het Besluit beheer DigiD[73]. Hierin wordt de minister van BZK belast met de zorg voor de instandhouding van de overheidstoegangsvoorziening DigiD. Meer wordt hier niet geregeld. Uit deze ministeriële regeling en uit de melding bij het College bescherming persoonsgegevens [74] moet worden afgeleid dat de minister van BZK de verantwoordelijke[75] is voor DigiD.
De kwalificatie van het Besluit beheer DigiD is overigens lastig. Het is een ministerieel besluit waarin een ministeriële zorgtaak in het leven wordt geroepen of in ieder geval wordt opgedragen. De basis is schimmig: het Tijdelijk besluit nummergebruik overheidstoegangsvoorziening waarnaar wordt verwezen kan niet gelden als grondslag voor dit ministerieel besluit, omdat deze amvb geen delegatiebepaling kent en ook een heel ander onderwerp regelt. De regeling lijkt dus een zelfstandige ministeriële regeling. Dit is in principe rechtsstatelijk bezwaarlijk, zij het dat dit ministerieel besluit organisatorisch van aard is en een intern karakter heeft, waardoor de burger niet (rechtstreeks) wordt geraakt.

[69] Stb. 2004, 584. Gewijzigd bij besluit van 2 september 2009, houdende aanpassing van enige algemene maatregelen van bestuur in verband met de invoering van het burgerservicenummer (Aanpassingsbesluit burgerservicenummer), Stb. 2009, 378.
[70] Nota van Toelichting, Stb. 2004, 584, p. 3.
[71] Nota van Toelichting, Stb. 2004, 584, p. 10.
[72] Zo ook het CBP in zijn advies van 18 juni 2004 (z2004-694).
[73] Staatscourant 2006, 160, p. 7.
[74] Meldingsnr. 1320472 in meldingsregister op www.cbpweb.nl.
[75] In de zin van artikel 1 sub d Wbp.

5.5 Contractuele relatie tussen burger en de minister van BZK?

Bij het aanvragen van DigiD moet de burger akkoord gaan met de Gebruiksvoorwaarden DigiD.[76] Hiermee komt een gebruiksovereenkomst tot stand tussen de minister van BZK en de burger. Maar hoe zit dat precies? Is het acceptabel als de overheid zijn relatie met de burger contractueel in plaats van bestuursrechtelijk regelt?[77] De overheid handelt hier evident "als overheid"[78] en niet als koper van pennen of computers. Staat de privaatrechtelijke weg überhaupt open bij een algemene voorziening waarvan nu reeds 9 miljoen burgers gebruik maken? En hoe vrij is de burger bij de afweging al dan niet te contracteren?

Overeenkomsten met de overheid bestaan in verschillende gedaantes, afhankelijk van de mate waarin met de overeenkomst beleid wordt gemaakt. Het spectrum loopt grofweg van de "gewone" overeenkomst (bijv. de koop van pennen of computers) tot zogenaamde bevoegdhedenovereenkomsten, waarbij de overheid zich contractueel vastlegt op een bepaald gebruik van zijn publiekrechtelijke bevoegdheid. DigiD lijkt zich ergens midden in dit spectrum te bevinden: het kan deels gezien worden als een dienst, een faciliteit, die naar keuze al dan niet kan worden afgenomen, maar anderzijds is het een pure overheidsvoorziening die door een private partij nooit als zodanig kan worden geleverd.[79] Er is zowel sprake van een algemeen belang als van een monopoliepositie, zij het dat de burger er in principe voor kan kiezen om niet te participeren en om zijn transacties met de overheid op een andere wijze te verrichten. De rechtsbetrekking tussen burger en DigiD is echter veeleer publiekrechtelijk dan privaatrechtelijk van aard. De minister van BZK verzorgt DigiD namelijk niet als gewone contractspartij maar in het kader van het in de Awb geregelde bestuurlijk elektronisch verkeer met de burger.

Artikel 2:15 lid 1, tweede zin Awb bepaalt dat het bestuursorgaan nadere eisen kan stellen aan het gebruik van de elektronische weg. Hieruit vloeit mijns inziens niet dwingend voort, dat deze eisen publiekrechtelijk dienen te worden geregeld. Volgens het Windmill-arrest is de privaatrechtelijke weg slechts afgesloten indien het gebruik ervan de publiekrechtelijke regeling op onaanvaardbare wijze

[76] Gebruiksvoorwaarden DigiD versie 5.1 (augustus 2010), te vinden op www.digid.nl.
[77] Zie hierover uitgebreid Van Ommeren, 'Een andere visie op de verhouding tussen publiek- en privaatrecht', Ars Aequi 2012, p. 568-570.
[78] Volgens Tak handelt de overheid *altijd* als overheid (A.Q.C. Tak, Overheid en Burgerlijk Wetboek, Naar een invullende rechtsleer, Recht en kritiek 1993, p. 178).
[79] Uiteraard kunnen private partijen wel de bouwstenen leveren.

doorkruist.[80] Dit is hier niet het geval, omdat de Gebruiksvoorwaarden DigiD niet conflicteren met de uitgangspunten van afdeling 2.3 Awb en zij evenmin bepalingen bevatten ten nadele van de burger.

Ik neem daarom aan, dat beide wegen in dit geval naast elkaar bestaan. De privaatrechtelijke rechtsverhouding wordt ondertussen wel beïnvloed door de algemene beginselen van behoorlijk bestuur.[81]

6 Een wettelijke basis voor DigiD?

6.1 De wet die er niet kwam

Reeds vanaf het begin van de ontwikkeling van DigiD had de wetgever het voornemen een wettelijke regeling voor DigiD (en eNIK) te treffen.

In 1998 geeft het kabinet in de nota *Wetgeving voor de elektronische snelweg*[82] aan dat zij zal *"voorstellen de Wet op de identificatieplicht met het oog op de elektronische identificatie uit te breiden"*.[83] Dit voorstel wordt gedaan *"met het oog op het personaliseren van chipcards en andere elektronische identiteitsbewijzen die een strikt persoonlijke toegang geven tot de elektronische snelweg."*[84]

In 2004 werd een motie van Van der Ham en Szabó aangenomen waarin de regering wordt verzocht *"te streven naar algemeen verbindende afspraken"* voor onder andere het *"gemeenschappelijk gebruik van de elektronische identificatie"*.[85]

In het eerder aangehaalde Tijdelijk Besluit nummergebruik overheidstoegangsvoorziening (2004) wordt in de Nota van Toelichting het volgende opgemerkt:

"Het is de verwachting dat de OTV wordt geregeld in een wet in formele zin. In die wet wordt dan bijvoorbeeld de zorg voor de instandhouding van de OTV geregeld, worden rechten en verplichtingen

[80] HR 26 januari 1990, NJ 1991, 393 (*Windmill*).
[81] Artikel 3:14 BW; HR 27 maart 1987, NJ 1987, 727 (*Amsterdam/IKON)*; HR 26 april 1996, NJ 1996, 728 (*Rasti Rostelli).*
[82] Kamerstukken II 1997/98 , 25 880, nrs. 1-2.
[83] Kamerstukken II 1997/98 , 25 880, nrs. 1-2, p. 9.
[84] Kamerstukken II 1997/98 , 25 880, nrs. 1-2, p. 145.
[85] Kamerstukken II, 29 362, nr. 4.

vastgelegd van bestuursorganen die zijn aangesloten bij de voorziening en wordt het gebruik van persoonsnummers voor de OTV bepaald."[86]

Inzake de eNIK merkt de minister van BZK in 2005 het volgende op:

"De opname van de elektronische functionaliteit in de Nederlandse identiteitskaart vergt een wijziging van de Paspoortwet. Deze wijziging is mijns inziens betrekkelijk technisch van aard. Voorts is niet uitgesloten dat enige andere wetten aangepast moeten worden, met name om (de rechtsgeldigheid van) het gebruik van de eNIK in het verkeer tussen overheid en burger te regelen."[87]

In 2006 vermeldt de minister van BZK dat wordt *"nagegaan (...) of DigiD geregeld dient te worden in een wet in formele zin"*.[88]

Sinds 2007 wordt niets meer vernomen omtrent wetgeving inzake DigiD en eNIK. Onduidelijk is of er ooit samenhang is geweest tussen de voorbereiding van de wetgeving terzake van DigiD enerzijds en eNIK anderzijds. Ook de relatie met de Wet elektronisch bestuurlijk verkeer[89] en de Wet elektronische handtekeningen[90] is (historisch) onduidelijk.

6.2 ICT en wetgeving: een moeizame relatie

Feitelijk is de eNIK tot nu toe in het geheel niet van de grond gekomen en is DigiD daartegenover, althans wat betreft aantal gebruikers, een doorslaand succes. Een wettelijke regeling ligt echter - deswege of desondanks? - bij mijn weten niet in het verschiet. Het is interessant om na te gaan, hoe deze situatie zich verhoudt tot de analyse en uitgangspunten in de nota *Wetgeving voor de elektronische snelweg*, die zich specifiek bezighield met het overheidsoptreden in de elektronische omgeving en de inzet van het "instrument" wetgeving daarbij.

In de nota *"Wetgeving voor de elektronische snelweg"*wordt onder andere geconstateerd dat de snelheid van de ICT-ontwikkelingen ("technologische turbulentie") gevolgen heeft voor de inzet van het instrument wetgeving:

[86] Nota van Toelichting, Stb. 2004, 584, p. 3.
[87] Kamerstukken II, 29 363, nr. 39, p. 2.
[88] Staatscourant 2006, 160, p. 7.
[89] Stb. 2004, 214.
[90] Stb. 2003, 199.

"• Technologie-afhankelijkheid: door de snelle opeenvolging en convergentie van technieken biedt regelgeving op basis van concrete media of technieken op langere termijn onvoldoende houvast(...).
• Flexibiliteit: het proces van formele wetgeving vergt zorgvuldige besluitvorming en kan daardoor te lang duren om de omloopsnelheid van problemen te kunnen bijbenen. Wetgeving dreigt reeds te verouderen voor zij het Staatsblad bereikt.
• Doeltreffendheid: het ontbreekt de wetgever vaak aan de technische expertise en het inzicht in de maatschappelijke toepassingen van de techniek om op voorhand terreinen te kunnen reguleren."[91]

Men zou zich op het standpunt kunnen stellen dat de nota *Wetgeving voor de elektronische snelweg*, gezien het tijdsverloop en de revolutionaire ICT-ontwikkelingen nadien, nog slechts van historische waarde is en niet als uitgangspunt kan dienen voor een actuele analyse van een instrument als DigiD. Dit zou echter miskennen dat de nota op onderdelen nog steeds hout snijdt. Dit geldt in elk geval voor de boven geciteerde constateringen ten aanzien van de verhouding tussen ICT en wetgeving. Prins heeft in dit verband recent op dezelfde pijnpunten gewezen en geconstateerd dat de rol van de politiek in relatie tot systeemontwikkeling marginaliseert: "Wetgeving fungeert [...] alleen nog als legitimerend voor een al ontwikkelde systeempraktijk in plaats van ex ante piketpaaltjes slaan."[92]

6.3 Legaliteitsbeginsel

Het legaliteitsbeginsel drukt uit dat de staat gebonden is aan het recht - ook wel: wetmatigheid van bestuur geheten - en is daarmee één van de pijlers van de rechtsstaat. Het legaliteitsbeginsel speelt onder andere een belangrijke rol bij de toelaatbaarheid van inperkingen op grondrechten.[93] Hieronder worden definitie, reikwijdte en de functies van het legaliteitsbeginsel beknopt besproken en wordt ingegaan op de vraag welke betekenis dit beginsel heeft in relatie tot DigiD.

6.3.1 Definitie en reikwijdte van het legaliteitsbeginsel

Het legaliteitsbeginsel is als algemeen beginsel niet gecodificeerd in de Grondwet. Wel bevatte de Grondwet 1815 reeds enige aspecten ervan, namelijk met betrekking tot eigendomsbeperking, strafoplegging (nulla poena) en belastingheffing[94]. In de Grondwet van 1848 werd het briefgeheim

[91] Kamerstukken II 1997/98 , 25 880, nrs. 1-2, p. 11.
[92] J.E.J. Prins, 'De eOverheid voorbij. Recht doen aan de digitale werkelijkheid' in *VAR-reeks 146*, Den Haag: Boom 2011, p. 90.
[93] EHRM 26 april 1979, NJ 1980, 146 (*Sunday Times).*
[94] Artikelen 164, 172 en 197 Grondwet 1815.

geïntroduceerd; schending ervan was slechts mogelijk indien bij wet geregeld.[95] In de loop van de twintigste eeuw zijn gaandeweg meer grondrechten in de Grondwet opgenomen[96], met steeds wettelijke beperkingsclausules. Maar ook los van de grondrechten werd het legaliteits*vereiste* steeds meer legaliteits*beginsel:* vanaf de Grondwet 1887 werden waterstaat, openbaar onderwijs en armbestuur (ouderenzorg) van zo groot belang geacht, dat regeling bij wet werd voorgeschreven.[97]

Inmiddels is de reikwijdte van het legaliteitsbeginsel veel breder. Niet alleen de straffende of belastingheffende overheid heeft een wettelijke grondslag nodig, maar deze eis geldt steeds als de overheid sturend optreedt. Voermans heeft het (staatsrechtelijk) legaliteitsbeginsel recent tegen het licht gehouden in het NJV preadvies 2011.[98] Voermans kwam in de literatuur een veelheid aan definities tegen.[99] Het voert te ver al deze definities hier (nogmaals) te behandelen. Er is niet één leidende definitie. De Staatscommissie voor de Grondwetsherziening 2009-2010 verwoordde het beginsel als volgt:

"Openbaar gezag wordt alleen uitgeoefend krachtens de Grondwet of de wet."[100]

Lastig in deze omschrijving is het begrip "openbaar gezag", dat niet nader wordt toegelicht en ook niet evident is vanuit de doctrine. Ik vermeld hier daarom eveneens- onder andere vanwege de eenvoud ervan- de definitie van Kortmann:

"alle overheidsoptreden moet berusten op en overeenstemmen met - kenbare en voldoende specifieke - algemene regels."[101]

"(A)lle overheidsoptreden" blijkt bij Kortmann echter minder ruim dan men op het eerste gezicht zou aannemen:

"Als stelregel mag (...) worden aangenomen, dat de overheid, waar zij eenzijdig lasten en verplichtingen aan de onderdaan oplegt, alsook sancties of dwang toepast, moet kunnen verwijzen naar een in de Grondwet of de wet vervatte algemene regel."[102]

[95] Artikel 154 Grondwet 1848.
[96] Uiteindelijk culminerend in Hoofstuk 1 Grondwet 1983.
[97] Artikelen 188, 192 en 193 Grondwet 1887.
[98] W.J.M. Voermans, 'Legaliteit als middel tot een doel' in *Controverses rondom legaliteit en legitimatie* (Handelingen NJV 2011-1), Deventer: Kluwer 2011.
[99] Voermans 2011, p. 7-10.
[100] Rapport Staatscommissie voor de Grondwetsherziening 2009-2010, p. 40.
[101] C.A.J.M. Kortmann, *Constitutioneel recht*, Deventer: Kluwer, 2008, p. 326.

Deze stelregel lijkt weer enigszins terug te grijpen naar de historische context van het legaliteitsbeginsel, te weten eigendomsbeperking, straf en belastingheffing, met dien verstande dat "dwang" hierbinnen een buitencategorie vormt. In het Fluoridering-arrest[103] besliste de Hoge Raad dat de toevoeging van fluor aan het drinkwater een maatregel van zo ingrijpende aard is, is dat hij slechts geoorloofd is, indien de wetgever daarvoor (expliciet) de mogelijkheid heeft willen bieden. De Hoge Raad past hier het legaliteitsbeginsel dus toe op een maatregel van feitelijke aard. De door Kortmann bedoelde "dwang" kan dus ook feitelijk van aard zijn. Belangrijke overwegingen voor de Hoge Raad waren de monopoliepositie van het waterleidingbedrijf, het feit dat drinkwater een eerste levensbehoefte is en het feit dat de burgers praktisch gedwongen werden de fluor tot zich te nemen, ook als zij daartegen overwegende bezwaren hadden.

Overigens wordt vrij algemeen aangenomen dat het legaliteitsbeginsel niet perse een wet in formele zin vereist: het mag ook in een lagere regeling staan mits deze uiteraard wel zijn grondslag heeft in een wet in formele zin.

6.3.2 Functies van het legaliteitsbeginsel

Het legaliteitsbeginsel is een middel tot een doel. Een functionele benadering is dus op zijn plaats. In het NJV preadvies 2011 inventariseert Voermans de functies van het legaliteitsbeginsel.[104] Scheltema beperkt zich in zijn bespreking van het preadvies van Voermans[105] tot de functies[106] democratische legitimatie, rechtszekerheid en rechtsgelijkheid[107]. Het komt mij voor dat dit inderdaad de kernfuncties van het legaliteitsbeginsel zijn:

a. democratische legitimatie: de volksvertegenwoordiging stelt regels vast die bepalen of en in hoeverre de overheid op mag treden na een transparante afweging van verschillende argumenten en voorkeuren;
b. rechtszekerheid: het voorkomen van willekeur door overheidsbestuur te binden aan algemene, kenbare regels;
c. rechtsgelijkheid: abstract geformuleerde regels zorgen voor gelijke behandeling.

---

[102] Kortmann 2008, p. 328.
[103] HR 22 juni 1973, NJ 1973, 386.
[104] Voermans 2011, p. 10-14.
[105] M. Scheltema, 'Legaliteit als middel tot een doel', NJB 2011, p. 1433.
[106] Scheltema noemt deze functies liever doelstellingen (Scheltema 2011).
[107] Of hij hierbij het gelijk aan zijn kant heeft valt buiten het kader van dit artikel.

Schlössels/Zijlstra komen tot ongeveer dezelfde opsomming.[108]

Naast de hierboven benoemde functies kan ook de *ordenende* functie worden genoemd: de maatschappelijke of technologische ontwikkelingen worden in goede banen geleid[109], waardoor (eveneens) een voordeel in de sfeer van de effectiviteit en doelmatigheid wordt behaald (d).[110]

6.3.3 Het legaliteitsbeginsel toegepast op DigiD

De vraag of DigiD vanwege het legaliteitsbeginsel wettelijke regeling behoeft valt niet met een eenvoudig "ja" of "nee" te beantwoorden.

Er is niet één definitie van het legaliteitsbeginsel en de definities die er wel zijn laten ruimte voor interpretatie.

Volgens de definitie van de Staatscommissie zou sprake moeten zijn van "openbaar gezag". Zoals eerder aangegeven kan echter niet worden aangegeven wat hier onder precies moet worden verstaan.

Binnen de definitie van Kortmann kwalificeert DigiD (uiteraard) wel als een vorm van overheidsoptreden, maar is daarbij ook sprake van lasten, verplichtingen, sancties of dwang? Het kan m.i. niet worden volgehouden dat de overheid hier in een uitsluitend begunstigende rol optreedt. Beweerd kan worden dat, voor zover inmiddels sprake is van "verdringing", de burger feitelijk wordt gedwongen DigiD te gebruiken. Overigens is het dan, zoals reeds eerder betoogd, aannemelijk dat in strijd zou worden gehandeld met artikel 2:14 lid 1 Awb, zodat reeds om die reden wetgeving aan de orde zou zijn (tenzij alsnog wordt teruggegrepen naar de nevenschikking-systematiek).

Vanuit de met het beginsel bediende functies valt wel het een en ander op te merken. Bij DigiD ontbreekt de *democratische legitimatie*: het parlement is - ondanks een verzoek daartoe bij motie - nooit betrokken geweest bij op de opzet van DigiD. De beleidskeuzes zijn niet in het openbaar gemaakt en het is niet bekend welke argumenten hierbij een rol hebben gespeeld. Gezien het grote aantal burgers dat gebruik maakt van DigiD, de principiële kwetsbaarheid van een voorziening als

[108] R.J.N. Schlössels en S.E. Zijlstra, *Bestuursrecht in de sociale rechtsstaat*, Deventer: Kluwer 2010, p. 138.
[109] G.J. Veerman, *Over wetgeving,* Den Haag: Sdu 2009, p. 126 -130.
[110] Schlössels/Zijlstra 2010, p. 138.

deze en de verdringingsproblematiek kan toch zeker worden gesproken van voor de burger belangrijke afwegingen en vereist de inrichting van DigiD derhalve parlementaire betrokkenheid.

De functies *rechtszekerheid* en *rechtsgelijkheid* lijken in het geval van DigiD minder relevant: van willekeur en ongelijke behandeling is (nog) geen sprake. Een risico met betrekking tot de rechtszekerheid is dat de tussen burger en DigiD geldende rechten en plichten vast liggen in contractuele gebruiksvoorwaarden. Dit is niet wat wordt bedoeld met algemene, kenbare regels. Inzake rechtsgelijkheid kan worden gewezen op de positie van de computerloze burger (de ernstigste vorm van digibetisme) en de emigrant: de eerste komt waarschijnlijk steeds meer in een achterstandspositie, de tweede kan op dit moment so wie so niet *inloggen.*

De *ordenende* functie, die beoogt de maatschappelijke of technologische ontwikkelingen in goede banen te leiden, komt volgens de Onderzoeksraad (zie par. 4.2) onvoldoende uit de verf. In de ontwikkeling van DigiD lijkt soms inderdaad sprake van een zekere stuurloosheid, zeker inzake de keuze om al dan niet een chipkaart te ontwikkelen danwel zo'n chip toe te voegen aan het paspoort of een andere chipkaart (bijvoorbeeld een bankpas) toe te laten als toegang tot (een deel van) de voorzieningen.
Het is goed denkbaar dat het ontbreken van een richtinggevende uitspraak van het parlement heeft bijgedragen aan deze stuurloosheid.

6.4 DigiD: (alsnog) wettelijk regelen?

Vanuit het legaliteitsbeginsel zijn dus wel aanknopingspunten te vinden om voor DigiD een wettelijke basis te creëren. Ook de eerder genoemde motie Van der Ham/Szabó en de toezeggingen van de minister van BZK (zie paragraaf 6.1) nopen hiertoe. Recent riep de Onderzoeksraad de rijksoverheid op actiever gebruik te maken van haar regelgevende bevoegdheid (zie par. 4.2). En voor zover sprake is van "verdringing" is wetgeving sowieso aan de orde.

Maar zullen wetgeving en het politieke besluitvormingstraject in dit geval niet slechts keuzes legitimeren die in feite allang zijn gemaakt (mosterd na de maaltijd)?[111] En welke concrete voordelen heeft zo'n wetgevingstraject, bijvoorbeeld voor de burger? Wie zit te wachten op een "inhoudsloze hypertrofie van de wetgeving"?[112]

[111] Prins 2011, p. 90.
[112] E.M.H. Hirsch Ballin, *Vertrouwen op het recht* (oratie Tilburg), Alphen aan de Rijn: Samsom 1982, p. 38.

Reserves als deze kunnen altijd worden gemaakt als regulering aan de orde is. De vraag wat *in concreto* de toegevoegde waarde van regelgeving is, zou beantwoord moeten worden door een bestuurskundige of door een rechtseconoom, maar ik ben bang dat het antwoord altijd enigszins in de lucht zal blijven hangen. En voor wat betreft de mosterd na de maaltijd: de wet kan ook een codificerende functie hebben.

DigiD is onderdeel van de vitale ICT-overheidinfrastructuur en is een belangrijke, onmisbare schakel tussen burger en overheid aan het worden. De voorziening kent kwetsbaarheden en het gebruik heeft een directe impact op de positie van de burger. Door parlementaire betrokkenheid kunnen de belangen van de burgers beter worden behartigd, bijvoorbeeld als het gaat om transparantie, verantwoordelijkheid, beveiligingsniveau en kwaliteit van de dienstverlening. Zeker waar gebruik de facto is of zal worden voorgeschreven is het aan te bevelen de spiegelbeeldige (prestatie-)aanspraken van de burger, bijvoorbeeld op een hoogstaande beveiliging van zijn communicatie met de overheid alsmede een laagdrempelige ingang bij problemen die daarbij optreden, vast te leggen in een wet[113] [114].

Daarnaast dwingt wetgeving tot visie en brengt een zekere structuur waar deze thans nog ontbreekt (ordenende functie).

Een eventuele formeelwettelijke regeling van DigiD zou kunnen worden toegevoegd aan afdeling 2.3 van de Awb en zal tot op zekere hoogte een kaderwet zijn, die door lagere regelgeving kan worden ingekleurd. Voor wat betreft beveiliging kan eventueel worden verwezen naar de beveiligingsnorm NEN-ISO/IEC 27002.

7 Een kijkje over de grens

Op de website epractice.eu worden de vorderingen op het gebied van eGovernment en dus ook van *eID* bijgehouden. Een volledige bespreking van de status in alle EU-landen valt ver buiten het kader van dit artikel; de geïnteresseerde lezer wordt naar de genoemde website verwezen. Hieronder wordt de situatie in achtereenvolgens Duitsland, Frankrijk, UK, België en Finland in vogelvlucht besproken.

[113] Al dan niet in formele zin. Delegatie is uiteraard uitsluitend aan de orde indien een deugdelijke delegatiegrondslag aanwezig is.
[114] Voor wat betreft de elektronische handtekening opent artikel 2:16 Awb, laatste zin reeds de weg hiertoe. Hier gaat het overigens wel om een wet in formele zin.

In ***Duitsland*** geldt sinds 1 november 2010 de Bondswet *Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften* van 18 juni 2009[115]. Deze wet regelt het zogenaamde (elektronische) *neue Personalausweis* dat in de plaats komt van het traditionele paspoort. Het *neue Personalausweis* kan naar keuze van de houder ook worden gebruikt voor elektronische identificatie en voor het plaatsen van een elektronische handtekening. Eind 2011 waren op ongeveer 80 miljoen inwoners 9 miljoen *neue Personalausweise* uitgegeven.[116]
Op www.ccepa.de/onlineanwendungen is zichtbaar welke elektronische dienstverlening wordt aangeboden. Opvallend is dat dit ook commerciële partijen betreft. Het aanbod lijkt - op enkele uitzonderingen na[117] - nog beperkt.

In ***Frankrijk*** wordt de eOverheid beheerst door *Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives*[118]. Een elektronische identiteitskaart wordt hierin echter niet geregeld.

In 2010 wordt wel het project *IDéNum* gelanceerd. Dit project beoogt te komen tot een digitale identiteitskaart. Deze kaart staat los van het reisdocument. In Frankrijk worden nog steeds uitsluitend traditionele reisdocumenten gebruikt.

De Franse publieke dienstverleningsportal www.service-public.fr is toegankelijk door middel van gebruikersnaam/wachtwoord, zoals bij het Nederlandse DigiD. Het aanbod lijkt nogal beperkt.

De ***UK*** heeft, behalve de implementatie van de Richtlijn elektronische handtekeningen (1999/93/EU) in de *Electronic Communications Act*[119], geen specifieke regelgeving op het gebied van de eOverheid.

De UK heeft op dit moment geen plannen voor een (nationale) elektronische identiteitskaart (en is daarmee een uitzondering in de EU).

Het aanbod op de publieke dienstverleningsportal www.direct.gov.uk lijkt vooral te bestaan uit - overigens veelal nuttige - informatie en formulieren; directe interactie door middel van de

[115] Bundesgesetzblatt Jahrgang 2009 Teil I Nr. 33, ausgegeben zu Bonn am 24. Juni 2009, p. 1346 v.
[116] Bij hoeveel hiervan de elektronische identificatie en -handtekeningfunctie werd geactiveerd is de auteur niet bekend.
[117] Zoals arbeitsagentur.de.
[118] Zie www.legifrance.gouv.fr.
[119] Zie www.legislation.gov.uk.

Government Gateway User ID (gebruikersnaam/wachtwoord) bestaat slechts voor enkele aanvraagprocedures, zoals het aanvragen van een *state pension.*

In ***België*** beschikt inmiddels nagenoeg elke burger over een eID[120]. De wettelijke basis hiervoor werd in 2003 gelegd.[121] De eID combineert een aantal functies: identiteitskaart[122], (sterke) authenticatie en - optioneel - een geavanceerde digitale handtekening.[123] Op my.belgium.be wordt een veelheid van eID-toepassingen aangeboden, waaronder aangifte bij de politie, belastingaangifte, het afsluiten van een woninghuurcontract en inzage in allerlei gegevens, onder andere in het domein van de sociale zekerheid.

De eID-functies en -toepassingen in ***Finland*** lijken zich ongeveer op hetzelfde niveau te bevinden als in België.[124] Een verschil is dat, afhankelijk van de dienst die wordt benaderd, ook de bankkaart kan worden gebruikt in plaats van de FINeID. In Finland geldt sinds 2009 een wet voor (sterke) elektronische identificatie en digitale handtekening.[125] Deze wet bevat specifieke bepalingen over privacybescherming en informatiebeveiliging.[126]

Op basis van deze beknopte inventarisatie kunnen geen dwingende conclusies worden getrokken. Wel kan worden geconstateerd dat België en Finland voorop lijken te lopen in de ontwikkeling van eID. Deze voorsprong betreft zowel de techniek als de regelgeving. In deze landen gaat de - min of meer - succesvolle introductie van eID gepaard met aandacht van de wetgever.[127] Duitsland lijkt dit spoor te volgen; UK en Frankrijk zijn vooralsnog achterblijvers in deze ontwikkeling. Nederland neemt een tussenpositie in: DigiD heeft enerzijds veel gebruikers en een flink aantal nuttige toepassingen maar ontbeert anderzijds adequate regulering; voorts is er geen concreet perspectief op een (geavanceerde) elektronische handtekening.

[120] Zie eid.belgium.be.
[121] Wet van 25 maart 2003 (Belgisch Staatsblad 28 maart 2003) tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en van de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen.
[122] Vergelijkbaar met de Nederlandse identiteitskaart: ter identificatie binnenlands en als reisdocument binnen de EU (en enige andere landen).
[123] Conform Richtlijn 1999/93/EG.
[124] Op basis van eGovernment in Finland, Europese Unie januari 2012 (te vinden op http://epractice.eu/files/eGovernmentFinland.pdf) (eGovernment in Finland 2012).
[125] Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 7.8.2009/617.
[126] eGovernment in Finland 2012 p. 14.
[127] Hiermee is een oorzakelijk verband overigens niet bewezen.

8 Conclusie

In het voorgaande zagen we dat DigiD geen specifieke wettelijke regeling kent. De vraag is of dit voor deze verwerking wel een vereiste is.

De issues rond DigiD zijn het persoonsnummergebruik, de beveiliging, de verantwoordelijkheid en het eventueel (feitelijk) verplichtend karakter ervan ("verdringing"). Het element persoonsnummergebruik blijkt te voldoen aan de eisen van artikel 24 Wbp en behoeft derhalve geen nadere regulering. De overige issues geven echter wel reden tot zorg. De eNIK is nog steeds niet gerealiseerd. Dit betekent dat het hoogste beveiligingsniveau niet beschikbaar is. Dit heeft onder andere tot gevolg dat bepaalde categorieën persoonsgegevens niet via DigiD ontsloten kunnen worden[128] en wekt bovendien de indruk dat de beveiliging van DigiD geen topprioriteit is. DigiD kende in de loop der tijd meerdere majeure beveiligingsincidenten. Soms hadden deze incidenten (ook) te maken met andere partijen in de keten zoals de afnemers of de certificaatdienstverlener (DigiNotar). Dit laatste vrijwaart echter niet vanzelfsprekend de voor DigiD verantwoordelijke: de burger die via DigiD met de overheid communiceert, kan niet van het kastje naar de muur worden gestuurd. Dit geldt temeer nu het gebruik van DigiD langzaam maar zeker een kritisch punt bereikt: zo alternatieven (via formulieren of menselijk contact) al niet feitelijk reeds nu zijn uitgesloten[129], zal het gebruik van zulke alternatieven in vlot tempo marginaliseren.

Als deze "verdringing" doorzet, dient DigiD, zowel vanwege het beginsel van nevenschikking in de Awb als vanuit het (staatsrechtelijk) legaliteitsbeginsel, alsnog van een wettelijke basis te worden voorzien. Zo'n wettelijke basis is belangrijk, omdat daarmee de noodzakelijke betrokkenheid van het parlement bij de verdere uitbouw van DigiD wordt gerealiseerd (democratische legitimatie). Een wettelijke regeling dwingt bovendien tot een bezinning op hoofdlijnen en het maken van principiële keuzes (ordenende functie). Dit belang is in het verleden ook door regering en parlement erkend en recent door de Onderzoeksraad bevestigd. In België en Finland zagen we dan ook dat de - min of meer - succesvolle introductie van eID gepaard ging met aandacht van de wetgever.

Alles overziend moet worden geconcludeerd dat tot dusver gemak heeft geprevaleerd boven veiligheid. Dit gemak diende zowel de overheid (deregulering, geen zelfbinding, minder kosten) als de burger (geen gedoe met pasjes, card readers, geen kosten). Met deze pragmatische houding heeft de Nederlandse overheid in zekere zin echter in zijn eigen staart gebeten: cruciale keuzes met

[128] Zie ook noot 30.

[129] Zoals bij studiegerelateerde voorzieningen ten behoeve van een - in het algemeen - jonge doelgroep.

betrekking tot de eNIK en het paspoort kunnen moeilijk nog langer worden uitgesteld zonder dat de Nederlandse eGovernment ontwikkeling stagneert. Het lijkt aannemelijk dat deze keuzes niet meer buiten de wetgever om kunnen worden gemaakt.