Informatiebeveiliging, e-handel en recht

Koops, E.J.; van der Hof, S.

Published in:
Recht en elektronische handel

Publication date:
2002

Koops, B.J., S. van der Hof (2002), 'Informatiebeveiliging, e-handel en recht'
Verschenen in: R.E. van Esch & J.E.J. Prins (red.), *Recht en elektronische handel*,
Deventer: Kluwer 2002, p. 387-409

18. Informatiebeveiliging, e-handel en recht

Bert-Jaap Koops & Simone van der Hof[1]

18.1 Inleiding

Onder informatiebeveiliging wordt verstaan het door middel van technische, organisatorische en juridische instrumenten beveiligen van informatie(systemen) en informatiestromen in en tussen organisaties. Het doel van informatiebeveiliging is – vanuit ondernemingsoogpunt – het waarborgen van de continuïteit van de bedrijfsvoering en het minimaliseren van schade voor bedrijven en organisaties door het trachten te voorkomen van beveiligingsincidenten en het minimaliseren van de eventuele gevolgen.[2] Daarnaast zullen ook particulieren maatregelen op gebied van informatiebeveiliging willen treffen om (directe of gevolg-)schade aan PC's en persoonlijke informatie(bestanden) te voorkomen.
Informatiebeveiliging maakt het mogelijk om informatie in groepen in en tussen organisaties te gebruiken zonder dat de integriteit van de informatie wordt aangetast

[1] Bert-Jaap Koops en Simone van der Hof zijn uhd respectievelijk senior-onderzoeker recht & informatisering bij het Centrum voor Recht, Bestuur en Informatisering van de Katholieke Universiteit Brabant. Dit hoofdstuk is afgerond op 1 januari 2002.
[2] Code voor Informatiebeveiliging 2000.

of op zijn minst de mogelijkheid van aantasting wordt verkleind. Met name de laatste jaren is de behoefte aan en het belang van informatiebeveiliging enorm toegenomen. Een van de redenen is dat bedrijven en particulieren gebruik maken van open netwerken als het Internet en blootstaan aan bedreigingen uit meerdere hoeken. De kwetsbaarheid van bedrijven is voorts toegenomen door decentralisatie van de gegevensverwerking en de grote afhankelijkheid van informatietechnologie. Bovendien worden bedreigingen geraffineerder en ontstaan er nieuwe schadeoorzaken, waartegen bedrijven en particulieren zich te weer moeten stellen.[3]

Bij informatiebeveiliging worden drie basisbeginselen onderscheiden, te weten (1) beschikbaarheid, (2) vertrouwelijkheid, en (3) deugdelijkheid.[4]

(1) *Beschikbaarheid* ziet op het garanderen dat gegevens en diensten op de juiste momenten beschikbaar zijn voor gebruikers.
(2) *Vertrouwelijkheid* betreft het beschermen van gegevens (bijvoorbeeld bedrijfsgeheimen of persoonsgegevens) tegen onbevoegde kennisname.
(3) *Deugdelijkheid* gaat over het waarborgen van de juistheid en volledigheid van gegevens (integriteit en authenticiteit) en de correcte werking van informatiesystemen (systeemintegriteit).

De instrumenten van informatiebeveiliging kunnen worden onderverdeeld in drie categorieën: (1) technische middelen, (2) organisatorische maatregelen en (3) juridische maatregelen.[5]

(1) Technische maatregelen komen neer op het inzetten van technische (hulp)middelen. Voorbeelden van technische hulpmiddelen zijn op encryptie gebaseerde technieken, zoals *Secure Socket Layer* (SSL) en digitale handtekeningen (en certificaten), maar ook *firewall*-technieken, het gebruik van PIN-codes en biometrische technieken.
(2) Bij organisatorische maatregelen gaat het om interne of externe maatregelen ten behoeve van de inrichting en het functioneren van organisaties. Gedacht kan worden aan het geven van voorlichting, het ontwikkelen van interne beveiligings- en autorisatieprocedures en het (laten) uitvoeren van EDP (*Electronic Data Processing*) *audits*, maar ook het gebruiken van een *Public Key Infrastructure* (PKI) en het certificeren van programmatuur.
(3) Bij juridische maatregelen gaat het vaak om afspraken tussen partijen, zoals overeenkomsten, *interchange agreements* en algemene voorwaarden, maar ook bijvoorbeeld mandaatregelingen, waarbij intern bevoegdheden worden toebedeeld. Ook is er sprake van juridische maatregelen bij (internationale) richtlijnen of voorbeeldwetgeving, zoals de UNCITRAL-*Model Law on Electronic Commerce*.

[3] Code voor Informatiebeveiliging 2000.
[4] Wij hanteren de term deugdelijkheid als koepelterm voor integriteit en authenticiteit. De BVD van informatiebeveiliging weerspiegelt aldus de in de literatuur gebruikelijke verwijzing naar de "CIA of information security": *confidentiality*, *integrity* en *availability*.
[5] Zie hierover nader Van Kralingen & Kolkman 1998, p. 209-211.

We behandelen eerst enkele centrale technieken en maatregelen voor informatiebeveiliging (18.3) en geven vervolgens een overzicht van wettelijke bepalingen over informatiebeveiliging (18.2). Daarna zullen aan de hand van de drie basisbeginselen van informatiebeveiliging – beschikbaarheid, vertrouwelijkheid en deugdelijkheid – de verschillende maatregelen in het licht van de verschillende juridische aspecten bij informatiebeveiliging worden behandeld.

18.2 Centrale technieken en maatregelen

Een van de centrale technieken voor informatiebeveiliging is cryptografie: het versleutelen van gegevens ten behoeve van vertrouwelijkheid. Cryptografie kan ook gebruikt worden voor een andere toepassing, de digitale handtekening, momenteel een van de belangrijkste methoden om deugdelijkheid te waarborgen. Voor deze laatste toepassing is niet alleen de techniek van cryptografie belangrijk, maar ook de organisatorische maatregel van een certificatieaanbieder (CA). Deze laatste is de bekendste verschijningsvorm van de Trusted Third Party (TTP), een figuur die in de literatuur over informatiebeveiliging veel voorkomt.
In deze paragraaf wordt een beschrijving gegeven van deze centrale technieken en maatregelen, die in de volgende paragrafen op diverse plaatsen aan bod zullen komen.

18.2.1 Cryptografie

Systemen voor het versleutelen van gegevens bestaan al sinds de Oudheid. Tot de jaren zeventig van de vorige eeuw waren al die systemen gebaseerd op een principe dat één en dezelfde, geheime sleutel moest worden uitgewisseld tussen communicatiepartners. Dat had als nadeel dat die sleutel dus op een betrouwbare manier moet worden overgebracht, bijvoorbeeld met de (slakken)post, een koerier of in persoon. Waar dat op kleine schaal goed mogelijk is, is zo'n systeem op grote schaal slecht toepasbaar, zeker voor een e-handelaar die met veel klanten veilig wil communiceren.
Om het probleem van sleuteluitwisseling op te lossen, is in de jaren zeventig een andere vorm van cryptografie uitgevonden: de asymmetrische cryptografie. Asymmetrische cryptografie gaat uit van het principe dat elke gebruiker twee sleutels heeft: een openbare of publieke[6] en een privésleutel[7]. Elke gebruiker verspreidt haar openbare sleutel onder potentiële communicatiepartners; de privésleutel houdt zij strikt geheim. De privésleutel wordt normaliter opgeslagen op een gegevensdrager (harde schijf of diskette), beveiligd met een (moeilijk te raden) wachtwoord. E-handelaar Erna en klant Karel kunnen nu als volgt veilig communiceren. Karel zoekt Erna's openbare sleutel op op haar weblocatie en versleutelt daarmee een bericht. Hij stuurt het bericht naar Erna, die het vervolgens ontcijfert met haar corresponderende

[6] Een publieke sleutel is de openbare helft van een encryptiesleutelpaar die verspreid wordt onder communicatiepartners. Hiermee kan een digitale handtekening gecontroleerd worden. Ook kan hiermee een bericht worden versleuteld om het voor onbevoegden onleesbaar te maken (alleen de houder van de bijbehorende privésleutel kan het ontsleutelen), Koops & Van der Wees 1998, p. 233-4.
[7] Een privésleutel is de helft van een encryptiesleutelpaar die door de bezitter strikt geheim gehouden moet worden. Hiermee kan een digitale handtekening gemaakt worden. Ook kan de sleutel gebruikt worden om versleutelde berichten leesbaar te maken, Koops & Van der Wees 1998, p. 233-4.

privésleutel. Concurrent Coba kan het bericht niet ontcijferen als zij het zou onderscheppen, omdat zij Erna's privésleutel niet kent.
Een analogie kan dit verduidelijken. Erna gebruikt vertaling in het Koeterwaals als haar cryptosysteem. Ze heeft een publieke sleutel: het woordenboek Nederlands-Koeterwaals, en een privésleutel: het woordenboek Koeterwaals-Nederlands. Karel versleutelt een boodschap aan Erna door met het woordenboek Nederlands-Koeterwaals het bericht in het Koeterwaals te vertalen. Erna kan het vervolgens lezen door het terug te vertalen naar het Nederlands. Omdat zij de enige is met een woordenboek Koeterwaals-Nederlands, blijft de boodschap voor alle anderen Koeterwaals. Iemand kan weliswaar de moeite nemen om bij elk woord Koeterwaals het (openbare) woordenboek Nederlands-Koeterwaals te gebruiken om te kijken bij welk Nederlands woord dit hoort, maar dit is in de praktijk – zeker bij de Dikke Koeterwaals – praktisch onmogelijk.

De crux van het beveiligen met cryptografie berust op de volgende principes: een robuust systeem dat zijn veiligheid in de praktijk bewezen heeft (en liefst openbaar is zodat het geen verborgen achterdeuren kan bevatten), een sleutel van voldoende lengte, en een zorgvuldige omgang door de gebruikers met het wachtwoord dat de privésleutel beveiligt.[8]
Vooral dat laatste is een zwakke schakel bij de beveiliging. De privésleutel – de naam zegt het al – mag slechts bekend zijn aan de houder van het sleutelpaar dan wel andere bevoegde gebruikers. Voor een correcte en betrouwbare werking is het derhalve van belang dat de houder de sleutel niet toegankelijk voor anderen laat "rondslingeren". Vaak zal de sleutel zijn beveiligd met behulp van een wachtwoord of een PIN-code die slechts bekend hoort te zijn aan de houder van de sleutel of andere geautoriseerde gebruikers. Het is dan ook van belang een dergelijk wachtwoord niet te noteren of tegen onbevoegden te vermelden, terwijl ook niet een makkelijk te raden wachtwoord mag worden gekozen (zoals een woord uit het woordenboek). Ook is het aan te bevelen de apparatuur waarop de sleutel is opgeslagen, zoals een PC of een smartcard, te beveiligen of veilig op te bergen. De publieke sleutel moet in tegenstelling tot de private sleutel publiekelijk worden bekend gemaakt, waarbij een certificatenaanbieder (CA) behulpzaam kan zijn – een TTP.

Voor e-handel van specifiek belang zijn twee cryptoprotocollen die veel worden gebruikt. SET (Secure Electronic Transactions) verzorgt het veilig versturen van kredietkaartnummers.[9] SSL (Secure Sockets Layer) is een methode om gestandaardiseerd versleutelde en geauthenticeerde berichten over het Internet te versturen. Als de server van de e-handelaar SSL heeft geïmplementeerd, kan het bladerprogramma van de klant zorgen voor versleutelde communicatie met de e-handelaar (herkenbaar aan het voorvoegsel 'https', met de s van 'secure').[10]

[8] Zie verder over techniek en gebruik van cryptografie de standaardwerken Schneier 1996 en Menezes, Van Oorschot & Vanstone 2001, en meer inleidend Garfinkel 1997, deel IV.
[9] Zie <http://www.sans.org/infosecFAQ/covertchannels/SET.htm> en <http://www.setco.org/set.html>.
[10] Zie <http://developer.netscape.com/tech/security/ssl/protocol.html> en Garfinkel 1997, hfd. 12 over SSL.

18.2.2 Digitale handtekeningen

Asymmetrische encryptie kan ook worden gebruikt voor het creëren van een digitale handtekening. De wijze van toepassing is enigszins anders dan wanneer het wordt gebruikt voor vertrouwelijkheid van communicatie.
De digitale handtekening werkt eveneens met behulp van een publiek-privaat sleutelpaar. Karel – de sleutelhouder – kan nu met zijn privésleutel een uittreksel (*digest* of *hash*) van een bericht versleutelen. Dit versleutelde uittreksel voegt hij toe aan het bericht en hij verstuurt het geheel aan geadresseerde Erna. Zij kan vervolgens met behulp van de publieke sleutel van Karel controleren of het bericht inderdaad van hem afkomstig is: als Karels publieke sleutel werkt op het versleutelde uittreksel in combinatie met het ondertekende bericht, moet het zijn versleuteld met de privésleutel van Karel. Daarmee kan Erna tegelijk controleren of het bericht onderweg niet door concurrente Coba of fraudeur Frits is veranderd.

De digitale handtekening heeft aldus twee functies, te weten het waarborgen van de *integriteit* van elektronische berichten alsmede het garanderen van de *authenticiteit* in het communicatieverkeer. Met het eerste wordt bedoeld dat kan worden gecontroleerd of berichten tijdens het transport over het netwerk zijn gewijzigd (lees: gemanipuleerd). Het tweede betekent dat kan worden geverifieerd van wie een elektronisch bericht of document afkomstig is. Tevens zal hiermee vaak ook een authenticatie van de inhoud worden bewerkstelligd, maar dat hoeft niet per definitie het geval te zijn. Er zijn ook *blind signatures* waarbij de tekenende instantie niet op de hoogte is van de inhoud van het bericht. Blinde handtekeningen vinden bijvoorbeeld toepassing bij de uitgifte van elektronisch geld (*e-cash*), opdat de bank wel kan controleren dat een betaling correct is maar niet wie de betaler is.

Overigens kan een digitale handtekening ook in combinatie met encryptie voor vertrouwelijkheid worden gebruikt, door eerst de vertrouwelijkheid te garanderen (met de publieke sleutel van de ontvanger) en vervolgens het bericht te ondertekenen (met de privésleutel van de afzender).

18.2.3 Trusted Third Parties (TTP's)

Trusted Third Parties (TTP's) kunnen worden ingezet om de betrouwbaarheid van het communicatieverkeer te vergroten. De TTP kan verschillende verschijningsvormen aannemen en diverse functionaliteiten uitoefenen. Over het algemeen staat daarbij op een of andere manier het waarborgen van de integriteit van informatie centraal.

De momenteel belangrijkste TTP is de certificatenaanbieder of certification authority (CA). Een CA is een vertrouwde instantie die publieke sleutels certificeert en digitale certificaten[11] publiceert ten behoeve van digitale handtekeningen; indien gewenst kan de CA ook zelf de sleutelparen aanmaken.

[11] Een digitaal certificaat is een digitaal document dat de binding van een (natuurlijk of rechts-) persoon met een publieke encryptiesleutel garandeert, uitgegeven door een Certificatenaanbieder (CA). Het certificaat bevat tenminste de publieke sleutel van de persoon, de unieke naam van de persoon, een

Bij de digitale handtekening is het noodzakelijk om houder en publieke sleutel op een betrouwbare wijze aan elkaar te verbinden. Anders zou Frits immers een sleutelpaar kunnen aanmaken op naam van Karel en daarmee bij Erna digitale diensten afnemen op kosten van Karel. Het creëren van een band tussen houder en publieke sleutel gebeurt door middel van digitale certificaten die door een CA worden uitgegeven na controle van de identiteit en/of hoedanigheid van de houder en van diens bezit van de bijbehorende privésleutel.
Over het algemeen zal een CA ook een zogeheten *Revocation Service* aanbieden, oftewel een dienst waarbij certificaten worden ingetrokken bij de beëindiging van de overeenkomst, het aflopen van de geldigheidsduur van het certificaat, de constatering van fouten in het certificaat of bij het uitlekken van de privésleutel die hoort bij de in het certificaat opgenomen publieke sleutel. De ingetrokken certificaten worden opgenomen in een online databank, de *Certificate Revocation List*. Gebruikers van digitale handtekeningen behoren deze lijst te raadplegen alvorens op een digitale handtekening te vertrouwen.
CA's maken over het algemeen onderdeel uit van een *Public Key Infrastructure* (PKI). Een PKI is een hiërarchische of horizontale structuur van CA's waarbinnen architectuur, organisatie, gebruikte techniek, gebruiken en procedures op elkaar zijn afgestemd en waarbij CA's elkaar certificeren. Een PKI verstevigt aldus het vertrouwen in de CA en in de digitale handtekeningen binnen de infrastructuur.

Voorts kan een TTP fungeren als sleutelbeheerder (*Key Escrow Agent*), dat wil zeggen een vertrouwde derde die (kopieën van) ecryptiesleutels in bewaring houdt. Een TTP kan ook een zogeheten gegevensherwinner (Data Recovery Organisation, DRO) zijn. Een DRO garandeert dat versleutelde gegevens toegankelijk blijven voor bevoegden, ook indien de ontcijfersleutel niet (meer) beschikbaar is. Een DRO kan sleuteldepot (*key escrow*) of sleutelherwinning (*key recovery*) gebruiken. Gegevensherwinning is een techniek waarbij per bericht de ontcijfersleutel toegankelijk is voor de TTP. In tegenstelling tot sleuteldepot is bij gegevensherwinning niet de privésleutel toegankelijk, maar de sessiesleutel. Een sessiesleutel is een symmetrische sleutel die één keer wordt gebruikt voor een berichtenuitwisseling of een telefoongesprek en nadat de sessie is afgelopen wordt weggegooid.[12]

Ten slotte kan een TTP ook tijdstempeldiensten (*time-stamping*) aanbieden, waarbij wordt gegarandeerd dat gegevens op een bepaalde datum en tijd zijn aangemaakt of verstuurd. Meer in het algemeen kan de TTP bewijs- en bewaardiensten aanbieden, zoals het bewaren van publieke sleutels en hun certificaten, ondertekende digitale documenten en reservekopieën.

geldigheidsdatum en gegevens over de CA. Het geheel is door de CA ondertekend met diens privésleutel, waardoor de gegevens niet manipuleerbaar zijn, Koops & Van der Wees 1998, p. 233-4.
[12] Zie alles Koops & Van der Wees 1998, p. 233-4.

18.3 Wettelijke bepalingen over informatiebeveiliging

In het algemeen bestaat er geen plicht tot informatiebeveiliging. Sommigen vinden dat de maatschappij zich inmiddels dusdanig heeft ontwikkeld, dat beveiligen "een op ieder rustende inspanningsverplichting" is, zodat onvoldoende beveiliging in principe een onrechtmatige daad oplevert.[13] Een dergelijke uitspraak gaat in zijn algemeenheid te ver. In bepaalde gevallen kan er zeker een maatschappelijke plicht op iemand rusten om te zorgen voor een goede beveiliging, zodat zij aansprakelijk kan worden gesteld als er iets mis gaat. Maar dat hangt dan wel van de omstandigheden af.[14] Niettemin zijn er bepaalde situaties waarvoor de wetgever al een zeker niveau van verplichte informatiebeveiliging heeft voorgeschreven. Het gaat dan vooral om de beveiliging van persoonsgegevens.

Artikel 13 van de Wet bescherming persoonsgegevens[15] legt een algemene beveiligingsplicht op aan de verantwoordelijke voor de verwerking van persoonsgegevens:

> De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Artikel 14 geeft aan dat de verantwoordelijke ook een beveiligingsplicht heeft als zij de gegevens laat verwerken door iemand anders:

1. Indien de verantwoordelijke persoonsgegevens te zijnen behoeve laat verwerken door een bewerker, draagt hij zorg dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De verantwoordelijke ziet toe op de naleving van die maatregelen.
2. De uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke.
3. De verantwoordelijke draagt zorg dat de bewerker […] b. de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13.
4. Is de bewerker gevestigd in een ander land van de Europese Unie, dan draagt de verantwoordelijke zorg dat de bewerker het recht van dat andere land nakomt, in afwijking van het derde lid, onder b.

(Zie par. 16.xxx wat precies onder de begrippen 'verantwoordelijke', 'bewerker', 'verwerken' en 'persoonsgegeven' moet worden verstaan.)

Deze beveiligingsplicht doet geen uitspraak over welk niveau van informatiebeveiliging precies nodig is – dat hangt af van bijvoorbeeld de soort persoonsgegevens, de risico's van aantasting en de draagkracht van het bedrijf. Het College Bescherming Persoonsgegevens heeft (toen het nog Registratiekamer heette) een rapport uitgebracht met een nadere aanduiding van welk niveau in welke situaties passend is.[16] Dergelijke uitwerkingen kunnen, evenals de Code voor

[13] Franken & Kaspersen 1997, p. 414-415.
[14] Zo zal een systeembeheerder die nalaat enige vorm van antivirusprogrammatuur te gebruiken op het systeem aansprakelijk kunnen zijn voor door virussen aangerichte schade.
[15] Wet van 6 juli 2000, Stb. 2000, 301, inwerkingtreding 1 september 2001 (Stb. 2001, 337).
[16] Van Blarkom & Borking 2001.

Informatiebeveiliging, bedrijven helpen met het bepalen van een beveiligingsbeleid voor de verwerking van persoonsgegevens.
Voor persoonsgegevens in de *telecommunicatiesector* geldt nog een specifieke verplichting, omdat de Europese regelgeving hiervoor een specifiek kader heeft gesteld. Artikel 11.3 van de Telecommunicatiewet legt een beveiligingsplicht op aanbieders van openbare telecommunicatienetwerken en -diensten, die overeenkomt met de plicht van art. 13 Wbp. Het tweede lid van art. 11.3 TW legt echter ook een informatieplicht op:

> De [telecommunicatie-]aanbieders dragen er zorg voor dat de abonnees worden geïnformeerd over
> a. bijzondere risico's voor de doorbreking van de veiligheid of de beveiliging van het aangeboden netwerk of de aangeboden dienst;
> b. de beschikbare middelen waarmee de onder a bedoelde risico's kunnen worden uitgesloten of verkleind en de kosten die daarmee gemoeid zijn.

Telecomaanbieders horen hun abonnees dus bijvoorbeeld te informeren over de risico's van hackers en virussen die op hun netwerken en diensten kunnen toeslaan. Daar zou bijvoorbeeld onder kunnen vallen het informeren over de bijzondere risico's van permanent openstaande Internetpoorten, bijvoorbeeld bij ADSL. Maar ook viruswaarschuwingen kunnen op basis van dit artikel worden verstuurd aan abonnees; de veelgehoorde klacht van telecomaanbieders "dat dat niet mag van de privacywetgeving" lijkt gezien de genoemde informatieplicht niet terecht. Voor de zekerheid zou men dit in het contract met de abonnee kunnen afspreken.

Naast deze beveiligingsplichten is er weinig in algemene zin geregeld over informatiebeveiliging. De enige overige relevante bepaling is art. 2:393 lid 4 van het Burgerlijk Wetboek. Dit verplicht de accountant om in zijn verslag aan de raad van commissarissen en aan het bestuur melding te maken van zijn "bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking". Hij moet dus melden wat hem is opgevallen over de informatiebeveiliging van het bedrijf, al hoeft hij niet zelfstandig op zoek te gaan naar mogelijke gaten in de beveiliging.
Voor het overige zijn er diverse wettelijke bepalingen die bepaalde onderdelen van informatiebeveiliging nader regelen. Deze komen in de volgende paragrafen aan de orde.

18.4 Beschikbaarheid

18.4.1 Beschikbaarheid van de weblocatie en het netwerk

Een bedrijf dat e-handel drijft, is voor een belangrijk deel afhankelijk van een goed beschikbare infrastructuur. Als een weblocatie tijdelijk uit de lucht is, kan dat klanten kosten, terwijl ook de bedrijfsvoering ernstig kan worden gestoord door het uitvallen van een netwerk.
De e-handelaar moet daarom afspraken maken met de netwerk- en Internet-dienstenaanbieders over de beschikbaarheid van het netwerk en de dienst. De telecomaanbieder zal vaak niet meer dan een inspanningsverplichting willen aangaan, maar de e-handelaar zal wel bepaalde minimumniveaus van bereikbaarheid

gegarandeerd willen zien. Een *Service Level Agreement* kan dan uitkomst bieden (vgl. daarover hfd. 8 [komt dit daarin aan de orde?]).

18.4.2 Beschikbaarheid en aansprakelijkheid van tussenpersonen

Informatiestromen tussen bedrijven, organisaties en individuele personen lopen vaak via intermediairs die diensten op het gebied van het transport en/of de opslag van gegevens verstrekken aan bedrijven en particulieren. Verschillende tussenpersonen kunnen in het kader van de elektronische handel worden onderscheiden in de categorieën aanbieders van toegang tot het Internet, aanbieders van technische diensten en aanbieders van inhoudelijke diensten. In Richtlijn 2000/31/EG inzake elektronische handel wordt meer in het algemeen gesproken van diensten van de informatiemaatschappij, die zowel door natuurlijke als rechtspersonen kunnen worden aangeboden (artikel 2). Onder deze diensten wordt verstaan: "elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten verricht wordt".[17] Voorbeelden van dergelijke tussenpersonen zijn *Trusted Third Parties* (TTP's), telecommunicatieaanbieders en Internet-toegangs- en -dienstenaanbieders.
Veelal zal voor de beschikbaarheid van deze diensten het algemene aansprakelijkheidsregime van Boek 6 Burgerlijk Wetboek gelden (zie hoofdstuk 11). In de regel zal tussen tussenpersoon en afnemer een contractuele relatie bestaan, waardoor hier vooral de contractuele aansprakelijkheid en niet zozeer de aansprakelijkheid uit onrechtmatige daad relevant is. Met de opkomst van de elektronische handel zijn op Europees niveau bijzondere aansprakelijkheidsbepalingen geformuleerd voor bepaalde, voor de elektronische handel relevante tussenpersonen. In de nu volgende paragrafen wordt onderzocht in hoeverre deze bepalingen relevant zijn voor de beschikbaarheid van diensten van de informatiemaatschappij.

18.4.2.1 TTP's

Voor het waarborgen van de betrouwbaarheid van elektronisch gegevensverkeer en gegevensopslag kunnen de diensten van een *Trusted Third Party* – een vertrouwde onafhankelijke partij – worden ingeroepen. De TTP is daarmee niet een tussenpersoon die externe informatiestromen verzorgt, maar een aanbieder van diensten die de betrouwbaarheid van de communicatie tussen – mogelijk niet met elkaar bekende – partijen beogen te bevorderen (zie par. 18.2.3).

Voor de TTP in de functie van een certificatenaanbieder of *certification authority* (CA) heeft de Richtlijn elektronische handel in artikel 6 een bijzondere aansprakelijkheidsbepaling geformuleerd. Deze bepaling geldt voor CA's die zogeheten gekwalificeerde certificaten aan het publiek uitgeven.
De CA is aansprakelijk voor de juistheid van de in het gekwalificeerde certificaat opgenomen informatie en de correcte verbinding tussen houder van het certificaat en de bijbehorende publieke sleutel, tenzij hij aantoont niet nalatig te hebben gehandeld

[17] Artikel 1 onder 2 richtlijn 98/48/EG tot wijziging van richtlijn 98/34/EG inzake informatieprocedure op het gebied van normen en technische voorschriften, 5 augustus 1998, Pb EG L 217/18.

(lid 1). Tevens is de CA aansprakelijk voor schade geleden door derden ten gevolge van een niet-geregistreerde intrekking van het certificaat, tenzij de CA ook hier weer aantoont dat hij niet nalatig heeft gehandeld (lid 2). De CA is niet aansprakelijk voor schade ten gevolge van overschrijding van in een certificaat opgenomen beperkingen of maximale waarde van transacties waarvoor het certificaat kan worden gebruikt (lid 3 en 4).
Vanuit het oogpunt van beschikbaarheid zijn met name de eerste twee leden van artikel 6 relevant. Ten eerste dient de CA te zorgen voor beschikbaarheid van correcte informatie. Een derde moet kunnen vertrouwen op de juistheid van een certificaat, zowel inhoudelijk als in verbinding met de bijbehorende publieke sleutel. Dat betekent dat CA's procedures voor het vaststellen van de identiteit van certificaathouders en hun gegevens moeten ontwikkelen, die de juistheid van de data waarborgen. Certificaathouders kunnen bijvoorbeeld worden gevraagd om een kopie van hun legitimatiebewijs dan wel om in persoon voor de CA te verschijnen. De opslag van de gegevens dient adequaat te worden beveiligd, teneinde ongeoorloofde toegang en manipulatie te voorkomen. Voor zover het persoonsgegevens betreft, moet men ook voldoen aan de beveiligingsplicht van de Wbp (zie par. 18.3). Bovendien moet correcte informatie in een online databank toegankelijk zijn voor publiek, zodat een digitale handtekening aan de hand van het certificaat kan worden geverifieerd. De CA moet dus secuur bijhouden of certificaten nog geldig en niet reeds ingetrokken zijn en deze informatie binnen redelijke termijn verwerken in deze openbare lijsten. Voorts dient de online databank adequaat te worden beveiligd om illegale toegang en manipulatie te voorkomen. Tot slot zal toegang tot de online databank gegarandeerd moeten worden. Wanneer de server waarop de databank draait voortdurend plat ligt, hebben gebruikers niet of onvoldoende de gelegenheid om certificaten te controleren. Ter bevordering van de toegankelijkheid kunnen CA's dezelfde informatie bijvoorbeeld op verschillende servers aanbieden. Als er een server uitvalt hebben gebruikers of derden dan nog de mogelijkheid om via een andere server te controleren. Verder zouden CA's moeten zorgen voor toereikende, actuele reservekopieën. Wanneer de informatie in de databank niettemin wordt gemanipuleerd, kan er snel een reservekopie beschikbaar worden gesteld.
De leden 3 en 4 van artikel 6 zijn in het licht van het voorgaande in zoverre relevant, dat beperkingen in certificaten voor derden kenbaar moeten zijn. Er staat echter niet wie verantwoordelijk is voor deze kenbaarheid. Lidstaten kunnen in de implementatiewetgeving aangeven dat certificaten in dat verband aan bepaalde eisen moeten voldoen. CA's zouden deze vervolgens moeten meenemen bij de inrichting van hun procedures die beschikbaarheid van hun diensten moeten garanderen.

De in het kader van het TTP.NL project opgestelde randvoorwaarden bepalen dat een TTP, onder zekere – overigens niet nader aangeduide – voorwaarden, aansprakelijkheid voor de door haar geleverde diensten en verrichte transacties moet aanvaarden. Om aansprakelijkheidsvraagstukken te kunnen beantwoorden wordt een eenduidige en onweerlegbare vastlegging van uitgevoerde activiteiten door de TTP onmisbaar geacht.[18]

[18] Zie Beleidsnotitie Nationaal TTP-Project, Min. V&W, Min. EZ, maart 1999, p. 21.

18.4.2.2 Telecommunicatieaanbieders

Telecommunicatieaanbieders zijn bedrijven die diensten aan het publiek aanbieden die geheel of gedeeltelijk bestaan in de overdracht of routering van signalen over een telecommunicatienetwerk (artikel 1.1 onder e en f Telecommunicatiewet). Veel van het gegevenstransport in het kader van de elektronische handel loopt via telecommunicatienetwerken. De telecommunicatie-infrastructuur is daarmee een belangrijke schakel in de ontwikkeling en uitvoering van de online handel en kan bij een eventueel falen tot grote schadeposten leiden bij bedrijven die gebruik maken van telecommunicatiediensten voor het elektronisch communicatie- en handelsverkeer.

Op grond van de Wet op de telecommunicatievoorzieningen (Wtv) bestond er voor telecomaanbieders een beperking van de aansprakelijkheid voor het niet of niet goed functioneren van de telecommunicatie-infrastructuur en tekortkomingen van de aan de houder van de concessie opgedragen diensten en van de zorg voor de vaste verbindingen (artikel 12). Bij de totstandkoming van de nieuwe Telecommunicatiewet (TW) is deze aansprakelijkheidsregeling komen te vervallen, zodat de aansprakelijkheid van telecomaanbieders sinds de inwerkingtreding van de TW wordt overgelaten aan het gemene recht. Telecomaanbieders staan nog wel de normale contractuele mogelijkheden – zoals een exoneratiebeding – ter hand om aansprakelijkheid te beperken.
Daarbij dient overigens wel in acht te worden genomen dat een dergelijke clausule opgenomen in een overeenkomst met een *consument* ex artikel 6:237 sub f BW als onredelijk bezwarend wordt beschouwd. De telecomaanbieder zal dus moeten aantonen dat het beding – de concrete omstandigheden van het geval in aanmerking genomen – niet onredelijk bezwarend is (omkering van de bewijslast ten voordele van de consument). Hoge schadeposten voortvloeiende uit wanprestatie met betrekking tot een consumentenovereenkomst zijn voor de telecomaanbieder echter niet snel te verwachten.
Bij *zakelijke* overeenkomsten kan strijdigheid met de redelijkheid en billijkheid de werking van een exoneratiebeding doorkruisen. Hiermee kan mogelijk een groter financieel risico voor de telecomaanbieder gepaard gaan, indien zakelijke klanten schade lijden door een falen van de infrastructuur of door de telecomaanbieder geboden diensten. Bij de behandeling van de wet is evenwel in aanmerking genomen dat de risico's voor de telecomaanbieder – mogelijke beperkingen in voorwaarden en verzekerde bedragen alsmede een te verwachten substantieel eigen risico in aanmerking genomen – in beginsel verzekerbaar zijn. Een wettelijk limitering van de aansprakelijkheid ex artikel 6:110 BW werd door de wetgever dan ook niet noodzakelijk bevonden.[19]

[19] Zie alles Tweede Kamer 1996-1997, 25 533, nr. 3, p. 43 e.v.

18.4.2.3 Internetaanbieders

Behalve door falen van de telecomaanbieder, kan een weblocatie ook tijdelijk uit de lucht worden gehaald door verstikkingsaanvallen (*denial-of-service attacks*). In februari 2000 werden hierdoor vele weblocaties, waaronder die van Amazon, Yahoo! en eBay, urenlang uit de lucht gehouden. Hoewel deze aanvallen in de publiciteit vaak als hacken worden aangeduid, vallen ze niet onder de strafbaarstelling van hacken (art. 138a Sr), omdat bij dit soort aanvallen nergens binnengedrongen wordt. De aanval blokkeert alleen de toegang tot de weblocatie door het automatisch genereren van een enorme hoeveelheid verzoeken aan de netwerkcomputer. Dergelijke aanvallen zijn relatief simpel te plegen met op het Internet beschikbare programma's. Ook op andere, relatief eenvoudige, manieren kan de toegang tot een netwerk worden geblokkeerd, zoals door wormen (programmaatjes die zichzelf eindeloos vermenigvuldigen) of door e-bommen (een enorme hoeveelheid gegevens in de e-postbus). Beveiliging tegen dit soort aanvallen is daarom een belangrijk aandachtspunt in de afspraken met de Internet-aanbieder, waarbij ook de aansprakelijkheid voor mogelijke schade geregeld kan worden. Bij gebreke van contractuele afspraken, wordt de contractuele aansprakelijkheid van de Internet-aanbieder bestreken door het gemene recht (zie hoofdstuk 11). De aansprakelijkheidsregeling van de Richtlijn Elektronische Handel is voor deze functie van de Internet-aanbieder niet relevant.

18.4.3 Beschikbaarheid van bewijsmateriaal

Binnen e-handel moet extra aandacht worden geschonken aan bewijsmateriaal. Elektronische transacties zijn immers vluchtiger dan papieren transacties. Aangezien ook elektronische bronnen geldig bewijs kunnen opleveren (Nederland kent immers een vrije bewijsleer), kan een e-handelaar informatie over gepleegde transacties opslaan op elektronische dragers.[20] Het is dan echter wel de vraag of zij deze na verloop van tijd – als het ooit tot een geschil komt – nog kan lezen.
Voor de fiscus moet de administratie ten minste zeven jaar beschikbaar zijn (art. 2:10 lid 1 BW voor rechtspersonen, art. 3:15a lid 2 BW voor zelfstandigen). Sommige rechtsvorderingen verjaren al na twee jaar (zoals een koopovereenkomst, art. 7:23 lid 2 BW), maar andere vorderingen kunnen langer meegaan: een vordering tot nakoming van een overeenkomst of tot schadevergoeding verjaart na vijf jaar (art. 3:307 en 310 BW); de algemene verjaringstermijn is twintig jaar (art. 3:306 BW). Wil de e-handelaar gedurende deze periode bewijs kunnen blijven aandragen, dan moet zij ervoor zorgen dat de opgeslagen gegevens ook daadwerkelijk toegankelijk blijven. Gegevens op informatiedragers moeten periodiek worden gecontroleerd of overgezet op nieuwe dragers (wie heeft er nog een station voor 5¼-duims floppen?), terwijl ook bestandsformaten geactualiseerd moeten worden (wie kan er nog WP4.2 voor DOS lezen?). In verband met de bewijskracht kunnen dergelijke overzettingen het beste volgens strikte, expliciet vastgelegde procedures plaatsvinden.
Voor de overheid gelden overigens veel langere termijnen op grond van de Archiefwet. Daarom is de overheid ook een voortrekker op het gebied van digitale

[20] Zie in algemene zin over e-bewijzen en e-bewaren: Kemna 2000.

duurzaamheid. Mogelijk kunnen e-handelaars aansluiten bij de inzichten die in het gelijknamige overheidsprogramma worden ontwikkeld.[21]
Een belangrijk hulpmiddel voor beschikbaarheid van bewijsmateriaal is de TTP (zie par. 18.2.3). Deze kan digitale documenten bewaren, zoals contracten, maar ook netberichten uit de precontractuele fase die voor de interpretatie van een contract relevant kunnen zijn. Daarnaast kan men andere TTP-diensten gebruiken die de bewijspositie ten goede komen, zoals het tijdstempelen van berichten en documenten.

18.4.4 Beschikbaarheid bij medewerkingsplichten

Het is ook belangrijk om informatie beschikbaar te hebben als de overheid plotseling op de stoep staat. De fiscus kan inzage vorderen in de administratie (art. 47 en 49 AWR), en de boekhouding dient daarbij in een goede en toegankelijke staat te zijn, zodat "te allen tijde de rechten en verplichtingen van de rechtspersoon kunnen worden gekend" (art. 2:10 lid 1 BW). Elektronisch vastgelegde gegevens moeten ook binnen redelijke tijd leesbaar kunnen worden gemaakt (art. 2:10 lid 4 BW).
In meer algemene zin hebben toezichthouders ook controlebevoegdheden waarbij de medewerking van het bedrijf kan worden gevorderd. Toezichthouders kunnen inzage vorderen in zakelijke gegevens en bescheiden (art. 5:17 Awb), en de geadresseerde is verplicht om alle medewerking te verlenen die redelijkerwijs kan worden gevorderd (art. 5:20 Awb). Soortgelijke bevoegdheden zijn ook van toepassing bij verdenking van economische delicten op grond van de WED (zie art. 18, 19 lid 1 en 24a).
En mocht men te maken krijgen met een strafvorderlijke doorzoeking, dan kan de politie vorderen om toegang te verlenen tot beveiligde computers (de wachtwoorden moeten dan beschikbaar zijn), maar ook om versleutelde bestanden te ontsleutelen (art. 125k Sv) (hetgeen overigens niet aan verdachten mag worden gevraagd, art. 125m lid 1 Sv).
Wil men kunnen voldoen aan deze medewerkingsplichten, dan zal de informatiehuishouding dusdanig op orde moeten zijn dat de gevorderde gegevens tijdig en in een leesbare vorm beschikbaar zijn. Men loopt anders het risico van een fiscale of bestuurlijke boete, of in het uiterste geval drie maanden gevangenisstraf wegens het niet voldoen aan een ambtelijk bevel (art. 184 Sr).

18.5 Vertrouwelijkheid

E-handel gaat vaak gepaard met vertrouwelijke gegevens, zoals kredietkaartnummers en persoonsgegevens. Wil een e-handelaar het vertrouwen van de klant verkrijgen en behouden, dan zal zij moeten verzekeren dat dergelijke gegevens vertrouwelijk blijven. Ook voor de bescherming van bedrijfsgeheimen en het correct omgaan met auteursrechtelijk beschermde gegevens is vertrouwelijkheid van groot belang.
De belangrijkste techniek om vertrouwelijkheid van gegevens te verzekeren is cryptografie: systemen die gegevens versleutelen zodat ze onleesbaar zijn voor onbevoegden. In deze paragraaf gaan we nader in op de techniek en de juridische context van cryptografie, omdat dit van oudsher een belangrijk reguleringsonderwerp is geweest (zie 18.4.2). Dit betekent overigens niet dat cryptografie het algehele wondermiddel is – vertrouwelijkheid moet worden verzekerd door een doordacht

[21] Zie <http://www.archief.nl/DigiDuur/>.

samenstel van beveiligingsmaatregelen, waarin naast cryptografie ook andere technische maatregelen (zoals vuurmuren) en organisatorische maatregelen (zoals functiescheiding en autorisatieprocedures) nodig zijn.

18.5.1 Cryptografie – de juridische context

Cryptografie is een noodzakelijk onderdeel van informatiebeveiliging. Het kan echter ook worden gebruikt voor minder nobele doelen, bijvoorbeeld door misdadigers om de politie dwars te zitten. Van oudsher hebben overheden beperkingen opgelegd aan de export van cryptografie, en over regulering van het verhandelen en gebruik van cryptografie wordt nog druk nagedacht.[22]

18.5.1.1 Exportbeperkingen

Sinds de Koude Oorlog bestaan er wereldwijde afspraken over de export van cryptografie. Het huidige Wassenaar Akkoord is een overeenkomst tussen 33 landen die de export van wapens aan banden legt; cryptografie wordt beschouwd als een goed voor tweeërlei gebruik (militair en civiel) en wordt ook beperkt.[23] Dit geldt overigens alleen voor de export van cryptografiesystemen zelf; men mag wel vrijelijk versleutelde berichten 'exporteren'. De meeste Westerse landen hebben de afspraken omgezet in hun nationale wetgeving.
Hoewel de exportbeperkingen geleidelijk aan worden versoepeld, is er voor export van sterke cryptografie in het algemeen nog steeds een vergunning nodig. Binnen de EU is de export echter vrij.[24] Internationaal opererende bedrijven die met verschillende vestigingen of zusterbedrijven vertrouwelijk willen communiceren, moeten aandacht besteden aan de voorwaarden waaronder cryptografie vanuit die landen mag worden geëxporteerd.
Exportbeperkingen betekenen niet een verbod op export. In de meeste gevallen is het wel mogelijk cryptografie te exporteren, mits men daarvoor een vergunning heeft. Dergelijke vergunningen moet men aanvragen bij de nationale bevoegde instanties. Voor Nederland is dat de Afdeling Exportcontrole en Sanctiebeleid van het Ministerie van EZ.[25]

Overigens is *import* van cryptografie in het algemeen geen probleem; slechts enkele landen, waaronder vooralsnog ook Frankrijk, leggen daarvoor beperkingen op.

18.5.1.2 TTP's voor vertrouwelijkheid en ontsleutelplicht

Voor het waarborgen van de betrouwbaarheid van gegevensverkeer kan men een beroep doen op een Trusted Third Party (TTP, zie par. 18.2.3). Diverse beleidsmakers denken dat er ook TTP's voor vertrouwelijkheid (DRO's) op de markt zullen komen, die bijvoorbeeld privésleutels aanmaken en beheren voor gebruikers. Hoewel

[22] Zie Koops 2001 voor een overzicht. De bronnen voor de informatie in deze paragraaf zijn alle te vinden op deze weblocatie.
[23] Zie <www.wassenaar.org>.
[24] Council Regulation (EC) No 1334/2000 setting up a Community regime for the control of exports of dual-use items and technology, *OJ* L159, 30 January 2000.
[25] Zie <http://cwis.kub.nl/~frw/people/koops/cls-addr.htm> voor een overzicht van adressen van exportinstanties.

dergelijke TTP's nog niet op de markt zijn gesignaleerd, is de Nederlandse overheid wel druk doende om voor hen een beleid te ontwikkelen.
De beleidsnotitie Nationaal TTP-project heeft randvoorwaarden gesteld voor TTP's.[26] Vertrouwelijkheids-TTP's moeten desgevraagd sleutels ter beschikking stellen aan de overheid, maar zij hebben geen plicht om privésleutels ook daadwerkelijk te bewaren. In het project 'Rechtmatige toegang', waarin overheid en bedrijfsleven in 2000-2001 participeerden, is vervolgens bekeken of nadere voorwaarden kunnen worden gesteld. Daarbinnen is overwogen om vertrouwelijkheids-TTP's te verplichten hun diensten zodanig in te richten dat zij door hun gefaciliteerde versleutelde berichten altijd kunnen (laten) ontsleutelen.[27] Of een dergelijke verplichting wordt ingevoerd, hangt mede af van een economische effectrapportage, die vermoedelijk negatief zal uitvallen voor een wettelijke verplichting.
Voor gebruikers geldt in beginsel wel een ontsleutelplicht als zij worden geconfronteerd met een onderzoek door de overheid. Art. 125k lid 2 Sv geeft justitie de bevoegdheid om ontsleuteling te vorderen tijdens een doorzoeking, terwijl ook een ontsleutelplicht bij versleutelde telecommunicatie wordt voorgesteld[28]. Omdat deze bevelen niet aan verdachten mogen worden gegeven (vanwege het beginsel dat die niet hoeven mee te werken aan hun eigen veroordeling), zijn ze in de praktijk nauwelijks bruikbaar, maar daar valt weinig aan te doen.[29] Ook de nieuwe inlichtingen- en veiligheidsdiensten worden door de wetgever toebedacht met een bevoegdheid om ontsleuteling te bevelen.[30]

18.5.2 Cryptografie – de organisatorische context

E-handelaars die cryptografie gebruiken voor vertrouwelijkheid, beveiligen hun gegevens tegen onbevoegde kennisname. Als dat goed gebeurt, lopen zij evenwel een risico. Indien de rechtmatige gebruiker de sleutel kwijtraakt of het wachtwoord vergeet, of als een werknemer die de vertrouwelijke gegevens versleuteld heeft opgeslagen plotseling verdwijnt, kan het bedrijf zelf ook niet meer ontsleutelen – de gegevens zijn dan onherroepelijk verloren.
Om aan dit risico tegemoet te komen, zijn systemen ontwikkeld voor gegevensherwinning (*data recovery*). Door een kopie van de privésleutel op te slaan op een vertrouwde, beveiligde plaats, of door systemen te gebruiken waarbij sessiesleutels kunnen worden achterhaald, kan de rechtmatige gebruiker dan alsnog bij de gegevens, ook al is zij de benodigde sleutel kwijt. Dergelijke systemen hebben zich echter in de praktijk nog niet echt bewezen, en ze brengen ook extra veiligheidsrisico's met zich mee. Men moet daarom een afweging maken tussen het risico versleutelde gegevens kwijt te raken en het risico van extra veiligheidslekken.[31]
Mocht het nog onverhoopt misgaan, dan zijn er nog gespecialiseerde bedrijfjes[32] om versleutelde gegevens weer toegankelijk te maken (maar als die slagen, dan zaten er kennelijk zwaktes in de beveiliging!).

[26] TK 1998-1999, 26 581, nr. 1, p. 21-24.
[27] Zie <http://www.bof.nl/tappen/TTPnotulenmaart2001.pdf>.
[28] Voorgesteld art. 126m lid 5-8 Sv. TK 1998-1999, 26 671, nrs. 1-3.
[29] Koops 2000.
[30] Voorgesteld art. 24 lid 2 en art. 25 lid 7 WIV, EK 2000-2001, 25 877, nr. 337.
[31] Zie nader Koops & De Jong 1998.
[32] Zoals <http://www.accessdata.com/>.

18.6 Deugdelijkheid

Deugdelijkheid omvat twee aspecten, namelijk het waarborgen van de juistheid en volledigheid van gegevens (integriteit en authenticiteit van gegevens) en de correcte werking van informatiesystemen (systeemintegriteit). Het bewaren van de integriteit van informatie(systemen) heeft duidelijke raakvlakken met het in voorgaande paragraaf behandelde onderwerp van vertrouwelijkheid. Personen of bedrijven kunnen schade lijden, indien gevoelige gegevens – bijvoorbeeld ten gevolge van manipulatie door kwaadwillenden – op zichzelf niet volledig, juist of consistent meer zijn; schade kan ook ontstaan als de systemen waarmee deze gegevens worden verwerkt niet correct werken en daardoor leiden tot manipulatie of inbreuk op het gebruik van de gegevens door ongeautoriseerde derden. Ook wanneer gegevens geen gevoelig karakter hebben, kan belang worden gehecht aan de deugdelijkheid ervan of de integriteit van systemen die de informatie verwerken. Bedrijven die online met elkaar contracteren, moeten bijvoorbeeld kunnen vertrouwen op de juistheid van over en weer gecommuniceerde informatie, waaronder productinformatie, leveringsinformatie, algemene voorwaarden en meer in het algemeen partijverklaringen. Veelal speelt tevens een rol dat partijen erop moeten kunnen vertrouwen dat zij in werkelijkheid ook communiceren met de persoon met wie zij denken te communiceren. Hiermee samenhangend zijn eisen van deugdelijkheid mede relevant voor bewijsdoeleinden.
In deze paragraaf wordt ingegaan op enkele technieken die de deugdelijkheid van het elektronische gegevensverkeer alsmede de elektronische gegevensopslag kunnen bevorderen. Daarbij worden de behandelde technieken tevens in een juridische context geplaatst.

18.6.1 Digitale handtekening

Onder 'elektronische handtekeningen' worden verstaan de informatietechnologische alternatieven voor een handmatige handtekening in het algemeen. Voorbeelden van elektronische handtekeningen zijn de PIN-code, de gescande handtekening en op biometrie of encryptie gebaseerde technologieën. Een speciale vorm van de elektronische handtekening is het laatstgenoemde voorbeeld, namelijk de op encryptie gebaseerde methode. Deze methode wordt aangeduid met de term 'digitale handtekening' en is momenteel de belangrijkste techniek voor het gebruiken van elektronische handtekeningen (zie par. 18.2.2).

De digitale handtekening is sinds jaren onderwerp van veel regulering wereldwijd om ervoor te zorgen dat de techniek toelaatbaar is als bewijs en kan worden gebruikt voor het rechtsgeldig ondertekenen van elektronische overeenkomsten.[33] In de Europese lidstaten wordt de richtlijn 1999/93/EG inzake elektronische handtekeningen geïmplementeerd. Deze richtlijn ziet op de toelaatbaarheid van digitale handtekeningen als bewijs en niet op het rechtsgeldig ondertekenen van elektronische

[33] Zie Van der Hof 2001 voor een overzicht van regulering en Aalberts & Van der Hof 2000 voor verschillende benadering in digitalehandtekeningenregulering.

overeenkomsten (artikel 1). De rechtsgeldigheid van elektronische contracten wordt bestreken door artikel 9 richtlijn 2000/31/EG inzake elektronische handel.
Richtlijn 1999/93/EG is op het eerste gezicht gericht op elektronische handtekeningen meer in het algemeen en beoogt een juridische gelijkstelling te bereiken met handmatige handtekeningen. De regeling maakt onderscheid tussen gewone elektronische handtekeningen en geavanceerde elektronische handtekeningen. Onder 'elektronische handtekening' worden begrepen: "elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authentificatie"[34] (artikel 2 onder 1). Een geavanceerde elektronische handtekening is "een elektronische handtekening die voldoet aan de volgende eisen: a) zij is op unieke wijze aan de ondertekenaar verbonden; b) zij maakt het mogelijk de ondertekenaar te identificeren; c) zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; en d) zij is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord" (artikel 2 onder 2). De digitale handtekening zal over het algemeen voldoen aan de eisen van een geavanceerde e-handtekening.
De geavanceerde e-handtekening ofwel digitale handtekening die is gebaseerd op een gekwalificeerd certificaat[35] en door een veilig middel is aangemaakt, wordt in de richtlijn gelijkgesteld aan de handmatige handtekening. De gewone elektronische handtekening kent een zwakkere status en mag noch rechtsgeldigheid worden ontzegd noch worden geweigerd als bewijsmiddel voor de rechter op het grond van het enkele feit dat de handtekening in elektronische vorm is gesteld, niet is gebaseerd op een gekwalificeerd certificaat, niet is gebaseerd op een door een geaccrediteerde CA afgegeven certificaat of niet met een veilig middel is aangemaakt (alles artikel 5).
In het kader van het TTP.NL project zijn randvoorwaarden voor onder andere TTP's die CA-functies uitoefenen opgesteld. De randvoorwaarden hebben voornamelijk betrekking op de betrouwbaarheid van CA's en omvatten factoren als beveiliging, bedrijfscontinuïteit, rechtmatig handelen, betrouwbare technologie, functiescheiding, toezicht en transparantie.[36]

18.6.2 Biometrie[37]

Biometrie is zowel een herkennings- als een beveiligingsmethode. Als herkenningsmiddel kent het verschillende functies, waaronder verificatie van de identiteit van een persoon en daarmee samenhangend authenticatie en autorisatie. Biometrie kan ook worden gebruikt voor beveiliging *zonder* identificatie, door de toegang tot een systeem te beperken tot degene van wie het biometrische kenmerk overeenkomt met het kenmerk dat in het systeem of op een *smart card* is opgeslagen.

[34] 'Authentificatie' is de term in de officiële Nederlandse vertaling maar is geen bestaand Nederlands woord. Wij gebruiken liever het reeds bestaande 'authenticatie'.
[35] Een gekwalificeerd certificaat is een digitaal certificaat dat voldoet aan specifieke, door de richtlijn gestelde eisen en is uitgegeven door een CA die tevens aan door de richtlijn gestelde criteria van betrouwbaarheid, veiligheid en deskundigheid voldoet (artikel 2 onder 10).
[36] Beleidsnotitie Nationaal TTP-Project, Min. V&W, Min. EZ, maart 1999, p. 17-22.
[37] Grotendeels gebaseerd op Van Kralingen, Prins & Grijpink 1997.

18.6.2.1 De techniek

Biometrie is een techniek die gebruik maakt van persoonskenmerken, zoals fysieke of gedragskenmerken. Op fysieke kenmerken gebaseerde biometrische methoden zijn onder meer identificatie door middel van iris- of gezichtsherkenning, het gebruik van vingerafdrukken en handgeometrie. Van gedragskenmerken wordt gebruik gemaakt bij de digitale pen. Bij deze methode worden druk en snelheid tijdens het tekenen gemeten en getoetst aan de voor de desbetreffende persoon in een database opgeslagen waarden. Het bijzondere aan biometrie is dat de gebruikte persoonskenmerken – naast het feit dat ze uniek zijn – niet kunnen worden vergeten, verloren of overgedragen.[38]

Een biometrisch kenmerk wordt (meermaals) ingelezen door een sensor. Vervolgens worden de onderscheidende gegevens van het biometrisch kenmerk gedigitaliseerd en omgezet in een reeks cijfers. Deze reeks wordt opgeslagen in een *template* dat vervolgens wordt gebruikt in het herkenningssysteem of de *smart card*. Tijdens de verificatie met behulp van het herkenningssysteem of de *smart card* wordt het proces van inlezen en digitaliseren herhaald en wordt het resultaat vergeleken met de in het systeem of op de *smart card* opgeslagen *template*. Aangezien het biometrische kenmerk niet altijd exact overeen zal komen met het *template*, wordt een zekere afwijking toegestaan. Deze afwijking mag niet te groot zijn, omdat het dan geen betrouwbaar herkenningsmiddel meer is, maar ook niet te klein, omdat anders gebruikers ten onrechte kunnen worden afgewezen.

Biometrische herkenningsmethoden worden veelal gebruikt in combinatie met een *smart card*. Dit gebeurt niet alleen uit doelmatigheid (de controle kan sneller plaatsvinden als geen contact hoeft te worden gezocht met een centrale databank), maar is ook uit privacyoverwegingen belangrijk (bij decentrale opslag is het risico van koppeling van persoonsgegevens en bestanden kleiner). Ook kan de combinatie van bezit (de *smart card*) en het persoonskenmerk de betrouwbaarheid en veiligheid van de herkenningsmethode vergroten. De kans dat een ongeautoriseerde gebruiker én de *smart card* heeft én een correct biometrisch kenmerk heeft dan wel weet te reproduceren is namelijk kleiner dan dat slechts een van beide vereist is voor herkenning of autorisatie.

18.6.2.2 De organisatorische context

Het proces van ontwikkeling van *templates* zal met waarborgen moeten worden omkleed en beveiligd. Ook dienen de *templates* dusdanig te worden opgeslagen dat eventuele manipulatie zo goed als uitgesloten is. Daartoe kan gebruik worden gemaakt van media die slechts eenmaal beschreven kunnen worden en niet te manipuleren zijn.

[38] Wel kan een persoon onder bedreiging gedwongen worden haar persoonskenmerk te gebruiken, zodat misbruik niet volledig is uitgesloten. De in de literatuur met zekere wellustigheid genoemde voorbeelden van afgehakte vingers laten wij hier buiten beschouwing: een goed biometrisch product reageert niet op dode lichaamsdelen.

De opgeslagen *templates* moeten vervolgens toegankelijk zijn voor geautoriseerden teneinde een vergelijking met voor verificatie gemaakte *templates* mogelijk en het proces van herkenning uitvoerbaar te maken. Naast opslag op *smart cards* (zie boven), kunnen templates ook in een centrale databank worden opgeslagen en online toegankelijk zijn voor geautoriseerden. Dat betekent dat er autorisatie- en beveiligingsprocedures dienen te worden opgesteld om adequate beveiliging van de gegevens te waarborgen en ongeautoriseerde toegang uit te sluiten. De opslag kan ook gedistribueerd over verschillende databanken worden opgeslagen, zodat bij corruptie van één databank de overige databanken als reservekopie fungeren en beschikbaarheid garanderen. Door middel van *remote copy*-technieken kan ervoor worden gezorgd dat dezelfde *templates* in verschillende databanken wordt opgeslagen. Voorts kan een TTP worden ingeschakeld om betrouwbare en veilige opslag van en toegang tot *templates* te realiseren. Tevens kan in het licht van beveiliging worden gedacht aan certificering van opslag- en toegangssystemen.

18.6.2.3 De juridische context

Bij de juridische context moet onderscheid worden gemaakt tussen juridische aspecten rondom het gebruik van biometrie als zodanig en de juridische status van biometrie als elektronische handtekening.

In het eerste geval kan een verplichting tot het gebruik van biometrie een wettelijke basis vereisen, omdat de toepassing een inbreuk op het grondrecht van lichamelijke integriteit (artikel 11 Gw) of van eerbiediging van de persoonlijke levenssfeer (artikel 10 Gw) kan vormen. Hierbij kan onder meer meespelen of er aan burgers andere opties openstaan dan alleen herkenning door biometrie. Indien het gebruik van biometrie op basis van vrijwilligheid gebeurt, zal men kunnen aannemen dat de persoon in kwestie instemt, en is er geen sprake van een inbreuk op een grondrecht. Dit kan overigens weer anders liggen wanneer sprake is van gevoelige gegevens, zoals het gebruik van gegevens omtrent iemands ras. Hiervan kan sprake zijn bij biometrische herkenning. De Wbp stelt zwaardere eisen aan het gebruik van gevoelige persoonsgegevens bij biometrische herkenning. In beginsel geldt een verbod (artikel 16), maar een uitzondering kan onder meer worden gemaakt met het oog op identificatie van een persoon voor zover dit voor dit doel onvermijdelijk is (artikel 18). De voor het biometrische herkenningsproces gebruikte *templates* kunnen voorts ook meer in het algemeen persoonsgegevens in de zin van de Wbp zijn, zodat de verplichting om te zorgen voor een passend beveiligingsniveau (artikel 13 Wbp, zie paragraaf 18.3) van toepassing is.

Biometrie kan evenals de digitale handtekening worden toegepast als elektronische handtekening. Het kan handtekeningfuncties als het verifiëren van iemands identiteit, het authenticeren van verklaringen en autoriseren van handelingen vervullen. Op grond van richtlijn 1999/93/EG inzake elektronische handtekeningen mogen biometrische herkenningsmethoden geen juridische geldigheid worden ontzegd. In de regel zal bij biometrische herkenningsmethoden geen sprake zijn van een door een CA uitgegeven gekwalificeerd digitaal certificaat, zodat geen sprake zal zijn van een

volledige gelijkstelling met de handmatige handtekening op grond van artikel 5 lid 1 van de richtlijn (zie paragraaf 18.6.1.3).

Afkortingen

Awb Algemene wet bestuursrecht
AWR Algemene wet inzake rijksbelastingen
BW Burgerlijk Wetboek
Sr Wetboek van Strafrecht
Sv Wetboek van Strafvordering
Wbp Wet bescherming persoonsgegevens
WED Wet op de economische delicten
WIV Wet op de inlichtingen- en veiligheidsdiensten 19.. (wetsvoorstel)

Literatuur

Aalberts & Van der Hof 2000
Babette Aalberts, Simone van der Hof, Digital Signature Blindness, ITeR-deel 32, Deventer: Kluwer 2000.

Van Blarkom & Borking 2001
G.W. van Blarkom & J.J. Borking, *Beveiliging van persoonsgegevens*, Achtergrondstudies & Verkenningen 23, Den Haag: Registratiekamer 2001, <http://www.registratiekamer.nl/download/002510_Binn_Regkamer_nr_23.pdf>.

Code voor Informatiebeveiliging 2000
Nederlands Normalisatie-instituut, Code voor Informatiebeveiliging, Delft 2000.

Franken & Kaspersen 2001
H. Franken & H.W.K. Kaspersen, 'Misbruik van informatie', in: Franken, Kaspersen & De Wild, *Recht en computer*, vierde druk, Deventer: Kluwer 2001.

Garfinkel 1997
Simson Garfinkel, *Web Security & Commerce*, Cambridge etc.: O'Reilly 1997.

Van der Hof 2001
Simone van der Hof, Digital Signature Law Survey, <http://rechten.kub.nl/simone/ds-lawsu.htm>.

Kemna 2000
Annemarie Kemna, 'Bewijzen en bewaren in het privaatrecht', in: J.E.J. Prins e.a. (red.), *Recht en informatietechnologie*, Den Haag: Sdu (losdelig), par. 7.4.

Koops & De Jong 1998
Bert-Jaap Koops & Huub de Jong, 'De risico's van data recovery voor overheid en gebruikers', *Computerrecht* 1998/5, p. 222-227.

Koops & Van der Wees 1998
Bert-Jaap Koops, Leo van der Wees, 'Woordenlijst dossier Trusted Third Parties', Computerrecht 1998/5, p. 233-234.

Koops 2000

Bert-Jaap Koops, *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?*, ITeR-deel 31, Deventer: Kluwer 2000.

Koops 2001

Bert-Jaap Koops, *Crypto Law Survey*, versie 19.0, juli 2001, <http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm>.

Kolkman & Van Kralingen 1998

Pascal Kolkman & Robert van Kralingen, *Verschuivend vertrouwen. Methoden voor het waarborgen van betrouwbaarheid in het elektronisch rechtsverkeer*, ITeR-deel 12, Deventer: Kluwer 1998.

Van Kralingen, Prins & Grijpink 1997

Robert van Kralingen, Corien Prins & Jan Grijpink, *Het lichaam als sleutel*, ITeR-deel 8, Alphen aan den Rijn: Samsom BedrijfsInformatie 1997, p. 3-66.

Menezes, Van Oorschot & Vanstone 2001

Alfred J. Menezes, Paul C. van Oorschot & Scott A. Vanstone, *Handbook of Applied Cryptography*, 5th printing, CRC Press 2001 (de eerste druk uit 1996 is beschikbaar op <http://www.cacr.math.uwaterloo.ca/hac/>).

Schneier 1996

Bruce Schneier, *Applied Cryptography. Protocols, Algorithms, and Source Code in C*, 2nd edition, New York etc.: John Wiley & Sons 1996.