



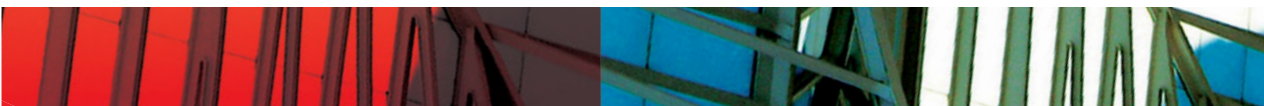
ICT-recht voor de praktijk



Noordhoff Uitgevers

Dr. mr. C.N.J. de Vey Mestdagh
Mr. dr. J.J. Dijkstra
Mr. dr. S.C. Huisjes

Eerste druk



ICT-recht voor de praktijk

ICT-recht voor de praktijk

Dr. mr. C.N.J. de Vey Mestdagh

Mr. dr. J.J. Dijkstra

Mr. dr. S.C. Huisjes

Ontwerp omslag: G2K Designers, Groningen/Amsterdam
Omslagillustratie: iStockphoto

Wolters-Noordhoff bv voert voor het hoger onderwijs de imprints Wolters-Noordhoff, Stenfert Kroese, Martinus Nijhoff en Vespucci.

Eventuele op- en aanmerkingen over deze of andere uitgaven kunt u richten aan:
Wolters-Noordhoff bv, Afdeling Hoger Onderwijs, Antwoordnummer 13, 9700 VB Groningen,
e-mail: info@wolters.nl

Met betrekking tot sommige teksten en/of illustratiemateriaal is het de uitgever, ondanks zorgvuldige inspanningen daartoe, niet gelukt eventuele rechthebbende(n) te achterhalen. Mocht u van mening zijn (auteurs)rechten te kunnen doen gelden op teksten en/of illustratiemateriaal in deze uitgave dan verzoeken wij u contact op te nemen met de uitgever.

0 1 2 3 4 5 / 12 11 10 09 08

© 2008 C.N.J. de Vey Mestdagh, J.J. Dijkstra, S.C. Huisjes

Behoudens de in of krachtens de Auteurswet van 1912 gestelde uitzonderingen mag niets uit deze uitgave worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever. Voor zover het maken van reprografische verveelvoudigingen uit deze uitgave is toegestaan op grond van artikel 16h Auteurswet 1912 dient men de daarvoor verschuldigde vergoedingen te voldoen aan Stichting Reprorecht (postbus 3060, 2130 KB Hoofddorp, www.cedar.nl/reprorecht). Voor het overnemen van gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (artikel 16 Auteurswet 1912) kan men zich wenden tot Stichting PRO (Stichting Publicatie- en Reproductierechten Organisatie, postbus 3060, 2130 KB Hoofddorp, www.cedar.nl/pro).

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.

ISBN (ebook) 978 90 01 84768 5
ISBN 978 90 01 98442 7
NUR 820

Woord vooraf

ICT-recht wordt steeds belangrijker voor praktijkjuristen. Niet alleen omdat het aantal zaken waarbij ICT-recht een rol speelt toeneemt, maar ook omdat ICT-recht binnen de juridische organisatie zelf een steeds grotere rol speelt. De praktijkjurist dient niet alleen zijn cliënten te kunnen adviseren over zaken van privacyrecht, domeinnamen- en auteursrecht, e-commerce en computer-criminaliteit. Hij maakt tevens deel uit van een organisatie die (deels geautomatiseerd) juridische informatie en kennis verwerkt en daarover intern en extern communiceert. Hoe zit het daarbij bijvoorbeeld met de bescherming van de privacy van de eigen cliënten? Welke juridische haken en ogen zitten er aan het geven van online adviezen? Wie kan er aansprakelijk worden gesteld voor via het internet aangeboden kennis? Wie is er 'eigenaar' van de informatie en kennis die binnen de organisatie wordt opgebouwd, wordt vastgelegd en bijvoorbeeld via een website wordt gecommuniceerd? Deze vragen moeten binnen elke overheidsorganisatie en binnen elk bedrijf door juristen worden beantwoord.

Het boek *ICT-recht voor de praktijk* voorziet in een overeenstemmende behoefte aan kennis van twee doelgroepen. Er bleek enerzijds behoefte te bestaan aan inleidende leerstof op academisch niveau en leerstof op hbo-niveau en anderzijds aan een inleidend naslagwerk voor praktijkjuristen waarmee zij snel een overzicht kunnen krijgen van de regelgeving op de belangrijkste deelgebieden het ICT-recht.

De auteurs van dit boek hebben brede ervaring met het ICT-recht. Zij ontwikkelden onder andere de bachelors- en mastersopleidingen Recht & ICT bij de Rijksuniversiteit Groningen en zij zijn betrokken bij het ontwikkelen van ICT-recht onderwijs bij de Hogeschool van Amsterdam. Ook verrichtten zij wetenschappelijk onderzoek op dit gebied en waren zij als advocaat of extern adviseur betrokken bij ICT-recht zaken in de rechtspraak. De keuze van de behandelde onderwerpen en de wijze van behandelen ervan is gebaseerd op deze ervaring en op informatie van andere ICT-recht docenten en juristen uit de ICT-recht praktijk.

C.N.J. de Vey Mestdagh
Lector Recht & ICT HVA, manager sectie Recht & ICT RUG
Amsterdam/Groningen, oktober 2007

Inhoud

1 Recht in de digitale wereld 9

Dr. mr. C.N.J. de Vey Mestdagh

- 1.1 Trends in de digitale wereld 10
- 1.2 Internationalisering en digitalisering van rechtsbetrekkingen 11
- 1.3 Behandelde onderwerpen van ICT-recht en wijze van behandelen 15

2 Privacy en ICT 17

Dr. mr. C.N.J. de Vey Mestdagh

- 2.1 Bescherming van de persoonlijke levenssfeer 18
- 2.2 Wet bescherming persoonsgegevens 20
- 2.3 Op wie en waar is de wet van toepassing? 21
- 2.4 Op welke verwerkingen is de wet van toepassing? 23
- 2.5 Onder welke voorwaarden zijn verwerkingen toegestaan? 26
- 2.6 Verboden verwerkingen 30
- 2.7 Formele verplichtingen van de verantwoordelijke 31
- 2.8 Formele rechten van de betrokkene 35
- 2.9 Handhaving van de wet 37
- 2.10 Toezicht 38
 - Samenvatting 39
 - Literatuur en verdieping 40

3 Overheid en ICT 41

Mr. dr. S.C. Huisjes

- 3.1 Elektronische overheidsdienstverlening en de Algemene wet bestuursrecht 42
- 3.2 Openbaarheid van bestuur 45
- 3.3 De overheid en privacy: de Wet bescherming persoonsgegevens 47
- 3.4 De elektronische handtekening en de overheid 49
- 3.5 Elektronische communicatie en openbare orde 51
- 3.6 Geautomatiseerde overheidsbeslissingen 52
 - Samenvatting 53
 - Literatuur en verdieping 54

4 Rechten van intellectuele eigendom en ICT 55

Mr. dr. J.J. Dijkstra

- 4.1 Intellectuele eigendomsrechten 57
- 4.2 Auteursrecht 61
- 4.3 Databankenrecht 78
- 4.4 Merkenrecht 82
 - Samenvatting 87
 - Literatuur en verdieping 87

5 ICT-contracten 89

Mr. dr. J.J. Dijkstra

- 5.1 Automatisering 91
- 5.2 De juridische duiding van een computerprogramma 92
- 5.3 ICT-contracten en standaardsoftware 94
- 5.4 ICT-contracten en maatsoftware 99
- 5.5 Gemengde contracten 107
- 5.6 Application Service Providing 108
 - Samenvatting 110
 - Literatuur en verdieping 110

6 E-commerce (elektronische handel) 111

Mr. dr. S.C. Huisjes

- 6.1 Regulering van e-commerce 112
- 6.2 Domeinnamen 114
- 6.3 Online contracteren; regulering van e-commerce 116
- 6.4 De elektronische handtekening 119
- 6.5 Bescherming van de e-consument 120
- 6.6 De aansprakelijkheid van de internetprovider 123
 - Samenvatting 125
 - Literatuur en verdieping 126

7 Computercriminaliteit 127

Mr. dr. J.J. Dijkstra

- 7.1 Strafbepalingen 129
- 7.2 Opsporingsbevoegdheden 136
- 7.3 Strafbaarstelling virtuele kinderpornografie 144
 - Samenvatting 153
 - Literatuur en verdieping 154

8 Telecommunicatierecht 155

Mr. dr. S.C. Huisjes

- 8.1 Registratie en vergunningen 157
- 8.2 Frequenties en nummers 158
- 8.3 Interconnectie en interoperabiliteit 160
- 8.4 Bescherming van de 'teleconsument' 161
- 8.5 Privacy en aftappen 163
- 8.6 De toezichthouder(s) 165
 - Samenvatting 166
 - Literatuur en verdieping 167

Over de auteurs 168

Register 169

1

Recht in de digitale wereld

Dr. mr. C.N.J. de Vey Mestdagh

- 1.1 Trends in de digitale wereld**
- 1.2 Internationalisering en digitalisering van rechtsbetrekkingen**
- 1.3 Behandelde onderwerpen van ICT-recht en wijze van behandelen**

De alomtegenwoordigheid van informatie en communicatietechnologie (ICT) is voor ons zo vanzelfsprekend geworden dat we ons niet langer realiseren hoe enorm verweven ons bestaan is geraakt met toepassingen van ICT. Dit is het gemakkelijkste in te zien als we ons de situatie voorstellen waarin alle ICT plotseling zou verdwijnen. Het openbaar vervoer en het verkeer over de weg zouden al snel stilstaan. Scholen, kantoren en fabrieken zouden moeten sluiten. De voedsel- en energievoorziening zouden haperen. Veel betalingen zouden niet langer kunnen worden gedaan en een groot deel van het geldverkeer zou komen stil te liggen. Telefoon, radio, televisie en internetverbindingen zouden uitvallen. Het is vanwege deze sterke verwevenheid van ICT met onze samenleving en vanwege het wereldwijde en digitale karakter van veel ICT-toepassingen dat er wel wordt gesproken van de *digitale wereld*. Het gaat hierbij niet om een hype maar om een onafgebroken doorzettende ontwikkeling. Er zijn op dit moment bijvoorbeeld wereldwijd meer dan een miljard internetaansluitingen en dit aantal groeit snel. Een steeds groter deel van onze dagelijkse communicatie, ons werk en onze vrijetijdsbesteding vinden plaats met behulp van meer en meer ICT. Dit maakt ons niet alleen steeds afhankelijker van ICT maar verandert ook onze onderlinge betrekkingen ingrijpend.

1.1 Trends in de digitale wereld

De belangrijkste kenmerken van de digitale wereld waardoor onze onderlinge betrekkingen veranderen komen al tot uitdrukking in de naam. Er is sprake van een *wereld* en deze wereld is *digitaal*. De trends die hiermee samenhangen zijn *internationalisering* en *digitalisering* van onze betrekkingen.

Internationalisering omdat onze onderlinge betrekkingen steeds minder eenduidig verbonden zijn met een bepaald deel van de fysieke wereld, dat wil zeggen met een bepaalde plaats binnen een bepaalde natie. Onze communicatie en onze onderlinge transacties hebben vaker een grensoverschrijdend karakter. De omgeving waarin deze communicatie en transacties plaatsvinden en de machten die deze omgeving beïnvloeden hebben een steeds globaler en minder lokaal karakter.

Digitalisering omdat onze identiteit, ons handelen en de voorwerpen van ons handelen worden gedigitaliseerd. Ook dit heeft ingrijpende gevolgen. Digitalisering van onze identiteit brengt met zich mee dat de mogelijkheden om anoniem te blijven, maar ook de mogelijkheden om elektronisch gegevens over ons te verzamelen en te bewerken enorm zijn toegenomen. We kunnen ons bijvoorbeeld verschuilen achter het IP-nummer van een computer, door de computer van een ander of een computer in een internetcafé te gebruiken of door gebruik te maken van anonimiseringsdiensten. Daar tegenover staat dat de overheid, bedrijven en anderen persoonsgegevens die aan onze digitale identiteit zijn gekoppeld gemakkelijker kunnen verwerken. Digitalisering van ons handelen brengt met zich mee dat we niet alleen internationaal, dat wil zeggen grensoverschrijdend, kunnen handelen, maar ook ons handelen letterlijk kunnen verplaatsen over de wereld door computers elders onze opdrachten te laten uitvoeren. Zo kunnen we private en zakelijke transacties naar wens in het buitenland laten plaatsvinden en kunnen we ons daarmee onttrekken aan de invloed van onze lokale omgeving. Digitalisering van ons handelen brengt ook met zich mee dat de reikwijdte en de invloed van ons handelen in technisch opzicht enorm worden vergroot. Denk maar eens aan de mogelijkheden om niet slechts een beperkt aantal personen mondeling of per brief of per telefoon, maar een veel groter aantal personen per e-mail, via een weblog, een forum of een website met informatie of diensten te benaderen zonder dat dit veel extra moeite of geld kost. Deze toegenomen invloed uit zich ook in de mogelijkheden om onszelf en onze digitale omgeving te beschermen door gebruik te maken van anonimisering, cryptografie, virusscanners en filteringsoftware. Ten slotte krijgen we ook steeds meer software tot onze beschikking waarmee we zelf informatie kunnen verwerken en publiceren op een manier die in de fysieke wereld voorbehouden was aan organisaties als de overheid, de pers en uitgevers. Wij krijgen hierdoor meer invloed op de informatie die we ontvangen en op de informatie die we verspreiden.

Naast digitalisering van onze identiteit en ons handelen speelt ten slotte ook de digitalisering van de voorwerpen van ons handelen (berichten, documenten,

websites, muziek- en filmbestanden) een grote rol omdat die digitale voorwerpen veel gemakkelijker manipuleerbaar zijn dan fysieke voorwerpen met name doordat zij door een ieder die er eenmaal over beschikt oneindig kunnen worden gekopieerd en verspreid.

1.2 Internationalisering en digitalisering van rechtsbetrekkingen

De hiervoor beschreven gevolgen van internationalisering en digitalisering hebben ook een grote invloed op de juridische kant van onze onderlinge betrekkingen, onze *rechtsbetrekkingen*. Deze invloed is driedelig:

- 1 De digitale wereld stelt nieuwe inhoudelijke eisen aan het recht, waardoor nieuwe regelgeving nodig is.
- 2 De digitale wereld is grensoverschrijdend waardoor het internationale recht een grotere rol speelt.
- 3 De handhaving van het recht in de digitale wereld is problematisch.

1.2.1 Internationalisering van rechtsbetrekkingen

Internationalisering betekent voor onze rechtsbetrekkingen dat zij steeds vaker geregeld worden door het internationale recht. Want welk recht is er van toepassing als wij vanuit verschillende landen grensoverschrijdend met elkaar communiceren en transacties sluiten? Welke rechtsbescherming geniet ik als consument of ondernemer als mijn wederpartij vanuit een ander land handelt? Welk recht is van toepassing als iemand in de digitale wereld een misdrijf pleegt?

Als mensen in toenemende mate grensoverschrijdend rechtsbetrekkingen aangaan dan worden daarover veelal internationale afspraken gemaakt. Het recht van de Europese Gemeenschap (EG) speelt hierbij een belangrijke rol. Veel van de nationale regelgeving van de landen van de EG is gebaseerd op richtlijnen waarover binnen de EG overeenstemming is bereikt, zodat burgers van de EG ook bij grensoverschrijdend handelen steeds dezelfde rechtsbescherming genieten. We zullen in dit boek zien dat internationaal recht en met name Europees recht op de meeste van de behandelde onderwerpen een grote invloed heeft. Zo is bijvoorbeeld de bescherming van persoonsgegevens in de EG gebaseerd op een richtlijn die ons in de gehele EG dezelfde rechtsbescherming garandeert en zelfs beschermt tegen export van onze gegevens naar landen buiten de EU met een geringere rechtsbescherming (zie hoofdstuk 2). Op langere termijn zal deze trend van internationalisering waarschijnlijk uitmonden in een proces van *globalisering* waarbij individuele staten, maar ook organisaties van staten zoals de EG een kleinere en private organisaties een steeds grotere rol gaan spelen. We zien deze ontwikkeling bijvoorbeeld al optreden bij de wereldwijde regulering van domeinnamen, waarin de private organisatie ICANN een centrale rol speelt (zie hoofdstukken 4 en 6).

1.2.2 Digitalisering van rechtsbetrekkingen

De digitalisering van onze onderlinge betrekkingen heeft een nog grotere invloed op onze rechtsbetrekkingen en roept veel vragen op. Hoe identificeren wij de handelende personen? Wie is de eigenaar van digitale informatie? Wie is er verantwoordelijk voor digitale informatie? Hoe bewijs je dingen in de digitale wereld? Hoe handhaaf je het recht in een wereld waarin anonimiteit, cryptografie en de mogelijkheden tot kopiëren en publiceren binnen ieders bereik liggen en ook massaal worden gebruikt?

Het *digitaliseren van onze identiteit* heeft een veelheid aan gevolgen voor het recht. Een digitale identiteit kan gemakkelijker worden verborgen en gemanipuleerd. Dit heeft zowel voordelen als nadelen. Gewone burgers kunnen zichzelf hierdoor beter beschermen tegen ongewenste inbreuken op hun persoonlijke levenssfeer. Er zijn echter veel gevallen waarin zij zich juist wel digitaal willen identificeren, bijvoorbeeld bij de overheid, in het economische verkeer of in de privésfeer. De manipuleerbaarheid van de digitale identiteit en daaraan gekoppelde persoonsgegevens stelt dan juist weer hoge eisen aan de betrouwbaarheid van de identificatie en aan de verdere verwerking van de persoonsgegevens. Bedrijven hebben daarbij niet alleen te maken met de betrouwbaarheid van de digitale identificatie van hun klanten en handelspartners en met de zorgvuldigheid van verwerking van persoonsgegevens, maar ook met de wens om zichzelf digitaal herkenbaar te maken voor consumenten en handelspartners via domeinnamen en digitale merken. Ten slotte kunnen kwaadwillenden natuurlijk ook juist misbruik maken van de mogelijkheden tot anonimiseren en manipuleren die de digitale identiteit biedt. Personen kunnen anderen anoniem schade toebrengen door het verspreiden van negatieve informatie via het internet. Computercriminelen kunnen anoniem virussen verspreiden en inbreken in andermans computer. Personen en bedrijven kunnen op onrechtmatige wijze persoonsgegevens verwerken, bijvoorbeeld voor het anoniem versturen van reclame (spam). Ook kunnen zij zich de identiteit (het IP-nummer, de domeinnaam of het digitale merk) van een ander toe-eigenen.

Dit alles heeft geleid tot nieuwe regelgeving op het gebied van de digitale handtekening (zie hoofdstukken 3 en 6) en op het gebied van de rechtmatige verwerking van persoonsgegevens (zie hoofdstuk 2). Maar ook op het gebied van de aansprakelijkheid van de internetprovider voor het afgeven van identiteitsgegevens en het afsluiten van gebruikers (zie hoofdstuk 6) en op het gebied van domeinnamen (zie hoofdstukken 4 en 6). En ten slotte op het gebied van de bestrijding van computercriminaliteit (zie hoofdstuk 7) en van spam (hoofdstuk 8).

Het *digitaliseren van ons handelen* heeft eveneens een veelheid aan gevolgen voor het recht. Wat wij digitale communicatie noemen omvat tegenwoordig vele informatietransacties die voorheen voornamelijk in de fysieke wereld voltrokken werden. Op het internet vindt een groot deel van onze private com-

municatie plaats (via e-mail, voip, chatrooms, forums, etc.). Ook spelen wij er, komen wij er samen om onze hobby's te bedrijven en onze politieke opvattingen te bespreken en tonen wij er de producten van onze creativiteit of (al dan niet met toestemming) die van anderen, bijvoorbeeld via peer-to-peer netwerken zoals Morpheus en Limewire, waarmee wij muziek en films uitwisselen en via websites als Tucows, Download en YouTube, waarmee we software en films uitwisselen. Sommigen plegen ook misdrijven op het internet, zoals inbreken in onze computer. Maar niet alleen particulieren, ook bedrijven en de overheid maken steeds meer gebruik van de mogelijkheden die digitalisering biedt. Wij drijven handel via webwinkels en veilingssites zoals eBay en de overheid biedt in toenemende mate diensten via het internet aan. Een groeiend deel van ons handelen en dat van bedrijven en de overheid wordt gedigitaliseerd. Het recht wordt daarom uitgebreid met nieuwe regels die betrekking hebben op deze digitale handelingsalternatieven. Naast de bestaande regels die gelden voor het handelen in de fysieke wereld zijn er speciale regels ingevoerd die gelden voor de elektronische overheid (hoofdstuk 3), elektronische handel (hoofdstuk 6), computercriminaliteit (hoofdstuk 7) en telecommunicatie (hoofdstuk 8).

Digitalisering heeft echter niet alleen nieuwe digitale handelingsalternatieven, maar ook een groot aantal nieuwe (technische) handelingsmogelijkheden toegankelijk gemaakt. Wij kunnen onze communicatie met behulp van anonimeringstechnieken en cryptografie onzichtbaar maken voor derden en wij kunnen onszelf via firewalls, virusscanners, filters en dergelijke afschermen van en beschermen tegen de buitenwereld. Wij kunnen echter ook moeiteloos handelingen verrichten die voorheen waren voorbehouden aan organisaties zoals overheden en bedrijven. Al deze vormen van wat wel user empowerment wordt genoemd brengen met zich mee dat organisaties en personen in de digitale wereld een rolwisseling (hebben) ondergaan. Het recht verandert met deze rolwisseling mee. We zagen hiervoor al een voorbeeld van die rolwisseling waar het proces van internationalisering overgaat in globalisering en private organisaties taken van overheden overnemen. Een ander voorbeeld van rolwisseling vinden we in het privacyrecht. In het verleden was dit voornamelijk gericht op bescherming van de burger tegen de overheid in haar rol van verzamelaar en verwerker van persoonsgegevens van burgers. In de nieuwe regelgeving komt ook expliciet bescherming tegen bedrijven en particulieren in hun rol van (zakelijke) verwerker van persoonsgegevens van klanten tot uitdrukking (zie hoofdstuk 2). Bij het introduceren van onze digitale identiteit zien we dat niet alleen de overheid haar traditionele rol vervult bij het introduceren van de elektronische handtekening (zie hoofdstuk 3), maar ook het bedrijfsleven een belangrijke rol speelt (zie hoofdstuk 6). Ook in de toerekening van verantwoordelijkheid voor uitingen zien we een verschuiving. Digitale informatie-uitwisseling via het internet heeft de mogelijkheid tot het openbaar maken van informatie (meningen, feiten, creatieve uitingen) voor iedereen toegankelijk gemaakt. Vroeger was dit grotendeels voorbehouden aan schrijvers, journalisten, programmamakers en wetenschappers. Deze beperkte groep van personen publiceerde veelal met behulp van uitgevers en drukkers van kranten,

tijdschriften en boeken en van uitzendorganisaties voor radio en televisie. Veel van onze regelgeving was en is gericht op deze personen en organisaties. Het gegeven dat vrijwel iedere deelnemer aan de digitale wereld tegenwoordig over de mogelijkheden beschikt die voorheen aan deze personen en organisaties waren voorbehouden betekent dat deze regelgeving inhoudelijk zal worden gewijzigd. De (mede)verantwoordelijkheid voor uitingen op het internet verschuift bijvoorbeeld naar de internetproviders hoewel deze inhoudelijk geen enkele betrokkenheid bij deze uitingen hebben. In het verleden was het uitgesloten dat dergelijke intermediairs aangesproken konden worden op uitingen waar ze niet bij betrokken waren. Zo konden telefoonmaatschappijen niet aansprakelijk worden gesteld voor de inhoud van het telefoonverkeer, maar kunnen internetproviders zowel privaatrechtelijk (zie hoofdstuk 6) als strafrechtelijk (zie hoofdstuk 7) aansprakelijk zijn voor door hen gehoste websites van hun klanten.

De *digitalisering van de voorwerpen van ons handelen* ten slotte heeft vooral grote gevolgen voor de manipuleerbaarheid, vooral voor de kopieerbaarheid en verspreidbaarheid, van deze voorwerpen. De digitalisering van muziek, films en software heeft een grote invloed gehad op ons recht. Het gemak waarmee muziek en filmbestanden en software gekopieerd en gedeeld kunnen worden en waarmee de handelende personen zichzelf en hun handelen en de voorwerpen daarvan met behulp van anonimisering en cryptografie onzichtbaar kunnen maken heeft een revolutie veroorzaakt in de wereld van het auteursrecht. Particulieren hebben op het internet, via websites en peer-to-peer-netwerken beschikking gekregen over een medium waarmee zij digitale bestanden kunnen verspreiden met een gemak en op een schaal die de bestaande mogelijkheden van muziek- en filmuitgevers in grote mate overtrof. Muziekmaatschappijen zijn daarom sinds de jaren negentig van de vorige eeuw steeds meer omzettegeraakt. Meer dan tien jaar later is het nog steeds niet goed gelukt om het tij te keren, noch juridisch noch technisch. De digitalisering van gegevens heeft ook een revolutie veroorzaakt in de toegankelijkheid van gestructureerde gegevensverzamelingen (databanken). Het gaat hierbij niet alleen om de beschikbaarheid van telefoongidsen, programmagidsen, tijdtabelen voor het openbaar vervoer en dergelijke maar ook om het doorzichtig maken van gehele markten met behulp van (web)databanken. De huizenmarkt was bijvoorbeeld voor de digitalisering van het aanbod slechts voor een deel van de marktpartijen (de makelaars) doorzichtig. Wij kunnen nu echter ook als verkoper en koper doorzicht krijgen via websites die een groot deel van de huizenmarkt omvatten. Het gemak waarmee op het internet digitale verwijzingen (links) kunnen worden aangebracht biedt hier zowel voordelen voor verkopers, intermediairs (makelaars) als kopers. Alle partijen krijgen toegang tot een grotere en doorzichtige marktplaats. Dat geldt echter ook voor de concurrenten, die via een eenvoudige verwijzing naar (elementen uit) de databank van een ander hun aanbod kunnen vergroten.

Het recht heeft in de afgelopen jaren ook als gevolg van de digitalisering van de voorwerpen van ons handelen, zoals muziek, films, software en databanken ingrijpende veranderingen ondergaan (zie hoofdstuk 3).

1.3 Behandelde onderwerpen van ICT-recht en wijze van behandelen

Zoals we hiervoor hebben gezien roept de digitale wereld een veelheid van nieuwe rechtsvragen op. In dit boek zullen we de meeste van die rechtsvragen behandelen. Het criterium voor behandeling hebben we vooral gezocht in de praktische betekenis. Het gaat om de rechtsvragen die in de juridische praktijk het meest door cliënten zullen worden gesteld en om rechtsvragen die de praktijkjurist in elk geval ten aanzien van de informatieverwerking in zijn eigen juridische organisatie zal moeten beantwoorden, zoals de vraag naar de bescherming van persoonsgegevens van zijn cliënten en de vraag naar de eigendom van en aansprakelijkheid voor de door zijn organisatie via het internet verspreide juridische informatie of geleverde diensten.

In hoofdstuk 2 wordt het recht op bescherming van persoonsgegevens behandeld. Het gaat hierbij in de eerste plaats om de verplichtingen van de overheid en van bedrijven om onze persoonsgegevens op een rechtmatige en zorgvuldige manier te verwerken, maar ook om verplichtingen van particulieren om zorgvuldig om te gaan met de persoonsgegevens van anderen en deze bijvoorbeeld niet zomaar op het internet te zetten.

In hoofdstuk 3 wordt de relatie overheid – ICT behandeld. Het gaat hierbij om elektronische overheidscommunicatie met de burger, digitale openbaarheid van bestuur, geautomatiseerde verwerking van persoonsgegevens door de overheid, de rol van de overheid bij de invoering van de elektronische handtekening en het handhaven van de openbare orde met behulp van digitale middelen.

In hoofdstuk 4 worden de rechten van intellectuele eigendom in relatie tot ICT behandeld. Het gaat hierbij in het bijzonder om het auteursrecht op digitale bestanden, om de rechten van de maker van een databank en om de rechten van bedrijven op hun merken. Bij de behandeling van het auteursrecht wordt ondermeer aandacht besteed aan het kopiëren en verspreiden van muziek- en filmbestanden en van software. Bij het databankenrecht wordt onder andere de vraag behandeld of een concurrent zomaar links mag opnemen naar een via het internet beschikbaar gestelde databank, bijvoorbeeld van huizen. Bij het merkenrecht wordt aandacht besteed aan een voor het internet relevant onderdeel daarvan: het domeinnamenrecht.

In hoofdstuk 5 wordt ingegaan op ICT-contracten. Het gaat hierbij om de contracten die worden afgesloten voor het ontwikkelen, invoeren en onderhou-

den van software voor bedrijven en overheden. In dit hoofdstuk komen onder andere het vastleggen van de eisen waar de software aan moet voldoen, de aansprakelijkheid van partijen voor niet goed functionerende software en de eigendom van en gebruiksrechten (licenties) op de software aan de orde.

In hoofdstuk 6 wordt de regulering van e-commerce behandeld. Het gaat hierbij om vragen betreffende de identificatie van partijen (domeinnamen, elektronische handtekening), de totstandkoming van overeenkomsten en de bescherming van de e-consument. Ook wordt op de aansprakelijkheid van de internetprovider onder andere voor onrechtmatig handelen van zijn klanten ingegaan.

In hoofdstuk 7 wordt computercriminaliteit behandeld. Het toenemende gebruik van ICT biedt zowel nieuwe mogelijkheden voor criminelen tot misbruik als voor de overheid om misbruik op te sporen. In dit hoofdstuk komen nieuwe delicten zoals computervrederebreuk (hacken) en het verspreiden van virussen en nieuwe bevoegdheden van de overheid zoals het laten vastleggen en onderzoeken van verkeersgegevens door internetproviders en het aftappen van telefoon- en computernetwerken aan de orde.

In hoofdstuk 8 komt ten slotte het telecommunicatierecht aan de orde. Dit recht regelt de telecommunicatiemarkt en heeft onder andere betrekking op de eerlijke mededinging op die markt, de verdeling van schaarse (radio en televisie) frequenties en de bescherming van de consument tegen onredelijke tariefverhogingen en spam.

Elk hoofdstuk opent met een voorbeeldcasus. Deze casus worden in de hoofdstukken waar nodig gebruikt om de behandeling van de regelgeving toe te lichten. Elk hoofdstuk wordt afgesloten met verwijzingen naar relevante literatuur en websites, die kunnen worden gebruikt voor verdere verdieping en het naslaan van regelgeving en jurisprudentie.