Woord vooraf

In dit boek willen wij jou als professional meer bewustmaken van de verschillende risico's die onzorgvuldig gebruik van ICT met zich meebrengen en wat jij daaraan kan doen. ICT is vandaag de dag zo'n belangrijk onderdeel van ons dagelijks leven geworden dat er niet alleen sociale normen, maar ook steeds meer juridische normen zijn om te bepalen hoe wij hiermee om moeten gaan. Zo zal je ook als gebruiker van internetbankieren ook zelf zorgvuldig om moeten gaan met je gegevens door bijvoorbeeld je firewall up-to-date te houden en beveiligingssoftware te installeren. Wanneer je dat niet doet dan ben je in beginsel zelf verantwoordelijk voor geld dat van je rekening is verdwenen. Ook het onzorgvuldig omgaan met bijvoorbeeld bedrijfsgegevens of gegevens van patiënten kan grote gevolgen hebben voor zowel de organisatie waarvoor je werkt als voor zijn klanten. Van een professional mag dan ook worden verwacht dat hij zorgvuldig omgaat met ICT. Wat dat inhoudt bespreken wij verder in dit boek.

Dit boek is geschreven als inleidend studieboek met als doel je bewust te maken van de verschillende risico's die het dagelijkse gebruik van ICT met zich meebrengen. Wij richten ons op zorgvuldig ICT-gebruik door de gemiddelde professional die niet werkzaam is in de ICT-branche. Om je bewust te maken van de verschillende risico's hebben wij een poging gedaan om je op een eenvoudige wijze uit te leggen hoe zorgvuldig ICT-gebruik een juridische invulling krijgt en hoe een computer werkt en deze een verbinding maakt met een netwerk. Wij beperken ons hiertoe. Voor een antwoord op de vraag hoe je bijvoorbeeld wijzigingen in bepaalde instellingen aanbrengt verwijzen wij je graag naar daarvoor bedoelde internetfora of de helpdesk van je internetserviceprovider (KPN, XS4ALL, ZIGGO, etc.).

Bij het bespreken van de verschillende onderdelen nemen wij als uitgangspunt dat de ICT waarover wij spreken goed functioneert en richten ons vooral op zaken waarbij de gebruiker zelf een actieve rol kan spelen bij het zorgvuldig gebruik van ICT. Denk daarbij aan het instellen van sterke wachtwoorden of het gebruik van een beveiligde verbinding. Om die reden hebben wij het bijvoorbeeld niet over valse certificaten die het mogelijk maken dat derden zich ongevraagd via malware toegang verschaffen tot je computer. Het betreft hier immers een verantwoordelijkheid van de certificaatleverancier waar je als gebruiker niet veel aan kan doen. Ook de invloed van hackers en geheime diensten op het dagelijks gebruik van ICT zal om dezelfde reden beperkt worden besproken.

Het eerste hoofdstuk maakt je wegwijs: wat is zorgvuldig ICT-gebruik en wat betekent dat in termen van juridische aansprakelijkheid. In de volgende hoofdstukken wordt de relatie tussen een computer, software en netwerken, zoals het internet besproken. Hoofdstuk 5 vormt een samenvatting in de vorm van gedragsregels. In het laatste hoofdstuk nemen wij een kijkje achter de schermen van de

computer en gaan wij nader in op het verzamelen van data, surveillance en privacy. Waar de eerste vijf hoofdstukken gaan over gedragsregels gaat het laatste hoofdstuk ook over de vraag waarom die gedragsregels van belang zijn.

In dit boek wordt gebruikgemaakt van zogenoemde boxen. Deze boxen worden gebruikt om een thema of begrip nader toe te lichten. Voor specifieke en verder onbesproken begrippen is er achterin tevens een verklarende woordenlijst opgenomen. Bij het bespreken van bepaalde handelingen wordt soms gebruikgemaakt van rechterlijke uitspraken. Verwijzingen naar rechterlijke uitspraken (jurisprudentie) zijn zoveel mogelijk aangeduid met het ECLI-nummer zodat uitspraken eenvoudig zijn terug te vinden op internet (http://uitspraken.rechtspraak.nl/).

Tijdens het schrijven van dit boek hebben wij als auteurs veel gelezen en dus ook zelf veel geleerd over zorgvuldig ICT-gebruik. Ook wij kwamen er al schrijvend achter dat wij ook zeker niet alle normen die wij in dit boek beschrijven altijd hebben toegepast. De juridische normen die wij in dit boek bespreken vormen de ondergrens van zorgvuldig ICT-gebruik en zal je dan ook moeten volgen. Andere normen zijn bedoeld als een idee om eens over na te denken, zoals wij dat al schrijvend ook deden. Wij hopen dat jij, net als wij, na het lezen van dit boek bewust keuzes maakt ten aanzien van het dagelijkse gebruik van ICT. Wanneer je als lezer opmerkingen of suggesties hebt dan vernemen wij deze graag.

Bezoek ook onze website op www.zorgvuldigictgebruik.nl.

Rotterdam, juni 2018

M. van Dijk en S. Gellaerts

Inhoudsopgave

1 Zorgvuldig ICT-gebruik

1.1 Inleiding

Wij maken dagelijks gebruik van verschillende vormen van Informatie en Communicatie Technologie (ICT). Zo maken wij gebruik van computers, zoals een desktop, laptop, tablet of smartphone om toegang te krijgen tot verschillende systemen en netwerken. Dat gebruik is soms privé en soms zakelijk. Vaak loopt dat gebruik door elkaar doordat mensen steeds vaker hun privé-e-mail lezen op de smartphone van hun werkgever of andersom. De meeste gegevens zijn tegenwoordig digitaal opgeslagen in verschillende systemen. Denk daarbij aan systemen voor documentbeheer maar ook aan sociale netwerken zoals Facebook. Met de eerdergenoemde computers kunnen wij zowel toegang krijgen tot deze netwerken en daarmee tot heel veel informatie. De keerzijde daarvan is, dat als wij toegang kunnen krijgen tot deze computers en netwerken, het niet uitgesloten is dat anderen dat ook kunnen.

Om te voorkomen dat anderen ongewenst toegang krijgen tot onze persoonlijke en zakelijke computers en netwerken is het van belang om zorgvuldig om te gaan met deze ICT-middelen. Niet in de laatste plaats omdat onzorgvuldig gebruik van ICT-middelen nadelige gevolgen kan hebben voor jezelf als privépersoon of zakelijk voor je klanten. Je kan daarbij denken aan de situatie waarin je een filmpje post waarop je dronken aan het dansen bent en vergeet deze privé te maken, als gevolg waarvan je een nieuwe baan misloopt. Maar ook aan de aansprakelijkheid van je werkgever wanneer jij teksten of foto's van het internet hebt gebruikt om het zakelijke blog wat mooier te maken. Maar denk ook aan de situatie waarin jij een onbeveiligde verbinding gebruikt en bedrijfs- of patiëntgegevens op straat komen te liggen. Dat de gevolgen van onzorgvuldig gebruik van ICT-middelen door professionals voor de burger groot kunnen zijn laat zich makkelijk raden. Zo kan mede door de koppelingen van allerlei ICT-systemen één foutieve adreswijziging bij de gemeente worden overgenomen door andere instanties zoals de Belastingdienst waardoor iemand ten onrechte geen huurtoeslag, studiefinanciering, of uitkering meer krijgt.

Zorgvuldig gebruik van ICT-middelen heeft ook sterke raakvlakken met het voorkomen van cybercrime. Cybercrime wordt vaak mogelijk gemaakt door kwaadaardige software, zoals virussen. Er zijn twee oorzaken van besmetting door kwaadaardige software, ook wel aangeduid als malware. De eerste oorzaak betreft fouten in de software. Zo kan iemand bijvoorbeeld gebruikmaken van een fout in de beveiliging van de software die je gebruikt. De tweede oorzaak ligt bij jou als gebruiker zelf, bijvoorbeeld als je malware binnenhaalt tijdens het bezoeken van geïnfecteerde websites. Zo bevatten websites die gratis muziek of films ter download aanbieden regelmatig malware. Hoewel je zowel bij het ontdekken van fouten in de software als het detecteren van malware in beginsel van anderen

afhankelijk bent, hebben beide aspecten gemeen dat er bij de ontdekking ervan handelen van de gebruiker verwacht mag worden. Om te kunnen handelen moet je bewust zijn van de risico's en veiligheidsaspecten die samenvallen met de ICT-middelen die je dagelijks gebruikt. Met dit boek willen wij je meer bewustmaken van deze risico's.

In de komende paragrafen en hoofdstukken willen wij je veiligheidsbewustzijn verhogen door je te wijzen op de verschillende risico's die samenhangen met het dagelijkse gebruik van ICT. Bedenk hierbij altijd dat het gaat om een risico (dat kan intreden of niet). De keuze tijdens het zorgvuldig gebruik van ICT-middelen gaat eigenlijk voortdurend om een afweging ('trade-off') tussen gebruiksgemak aan de ene kant en aspecten van veiligheid en privacy aan de andere kant. Zo biedt een sterk wachtwoord en een tweestapsauthenticatie weliswaar de beste bescherming tegen onbevoegd gebruik van je account, maar vraagt wel een extra handeling van jou als gebruiker. De afweging tussen gebruiksgemak en veiligheid zal je als professional elke keer zelf moeten maken. De keuze die je maakt wordt in de praktijk mede beïnvloed door sociale, juridische en technische normen. Zo kunnen collega's onderling de (sociale) afspraak maken om hun wachtwoord om de negentig dagen te wijzigen. Daarnaast kan jouw werkgever je daartoe ook juridisch verplichten door dit op te nemen in een ICT-reglement. Tot slot kan ook de ICT-afdeling je (technisch) dwingen je wachtwoord te wijzigen door je pas weer toegang tot het systeem te geven als jij een nieuw wachtwoord hebt ingesteld. Je ziet bij deze voorbeelden direct dat er vier belangrijke actoren zijn bij zorgvuldig gebruik van ICT-middelen. De eerste is jouw werkgever die regels opstelt voor het zorgvuldig gebruik van ICT en een klimaat schept waarin medewerkers elkaar veilig kunnen aanspreken op onzorgvuldig gebruik van ICT-middelen. De tweede actor is de ICT-afdeling van jouw werkgever die verantwoordelijk is voor de inrichting van een veilige digitale werkomgeving waarbinnen zorgvuldig gebruik kan worden gemaakt van ICT-middelen. De derde actor zijn jouw collega's die als groep sociale normen creëert voor zorgvuldig ICT-gebruik. En tot slot de vierde actor, jijzelf. Je bent zelf uiteindelijk verantwoordelijk voor jouw handelen maar ook voor het aanspreken van de andere actoren op het gewenste gedrag. Wij richten ons in dit boek vooral op jou als professional en op de actieve rol die jij als gebruiker kan spelen in het kader van het zorgvuldig gebruik van ICT.

Aan de hand van de geschiedenis van de ICT (par. 1.2) bieden wij je eerst een kort overzicht van de belangrijkste ontwikkelingen en de wijze waarop computers en netwerken zijn ontstaan. Daarna gaan wij in op de vraag wat zorgvuldig ICT-gebruik is en op welke normen dit gebruik gebaseerd is (par. 1.3). Vervolgens gaan wij nader in op de grenzen die het recht stelt aan het gebruik van ICT (par. 1.4). Tot slot staan wij stil bij een belangrijk thema in het domein van zorgvuldig ICT-gebruik: de wisselwerking tussen zakelijk en privégebruik van ICT (par. 1.5). De veiligheid van jouw computer en netwerk thuis zijn immers direct van belang voor veiligheid van het netwerk op je werk wanneer je thuis op je eigen computer nog even iets afmaakt voor morgen op je werk.

Tot slot nog een belangrijke nuancerende noot. De gemiddelde gebruiker zal zich, evenals de auteurs van dit boek, ook als hij zich houdt aan alle aanwijzingen

die wij hier geven, niet kunnen weren tegen de invloed van kwaadwillende hackers of geheime diensten. Het heersende idee is dat alles wat digitaal is in beginsel gekraakt kan worden. Wij richten ons niet op deze uitersten.

Box 1.1 De NSA kijkt altijd mee

In juni 2013 bracht voormalig medewerker van de Amerikaanse geheime dienst (NSA), Edward Snowden gegevens naar buiten dat deze dienst gegevens verzamelde van niet-verdachte burgers. Deze documenten maakten in één keer duidelijk dat de Amerikaanse geheime dienst, in samenwerking of met medeweten van andere geheime diensten heel veel gegevens opsporen en opslaan. Zo werd duidelijk dat de NSA destijds bijna 200 miljoen sms'jes per dag onderschepte. In 2015 werd door een beveiligingsbedrijf gesuggereerd dat een beveiligingslek bij routerfabrikant Juniper indirect veroorzaakt zou zijn doordat de NSA een beveiligingslek mogelijk zou hebben gemaakt. Deze berichten maken ook duidelijk dat de gemiddelde gebruiker zich hier niet tegen kan weren. Omdat er ook aanwijzingen zijn dat de NSA (en geheime diensten uit andere landen) zich ook bezighoudt met spionage van bedrijven blijft het debat over hun invloed wel actueel. Zo waren er in 2013 vanuit de Rijksuniversiteit Groningen bezwaren tegen het gebruik van Gmail om te voorkomen dat Amerikanen mee zouden kunnen kijken.

Na deze inleiding gaan wij in hoofdstuk 2 verder met een introductie van de werking van een computer en wordt in hoofdstuk 3 uitgelegd hoe een computer verbinding maakt met verschillende netwerken. In beide hoofdstukken zal worden stilgestaan bij de vraag wat jij kan doen om zorgvuldig met al deze middelen om te gaan. In hoofdstuk 4 wordt stilgestaan bij veelgebruikte applicaties en de veelvoorkomende risico's bij het gebruik ervan. Tot slot worden in hoofdstuk 5 aan de hand van de eerder besproken theorie een aantal basisregels voor zorgvuldig gebruik van ICT besproken.

1.2 Korte geschiedenis van de ontwikkelingen in ICT

Oorlog is voor veel innovaties het startpunt geweest van een enorme ontwikkeling. Dat is voor ICT eigenlijk niet anders. In 1936 beschreef en gebruikte de Britse wiskundige Alan Turing een denkbeeldige machine, de zogenaamde Turingmachine voor het bewijzen van een wiskundig model. Dat model geldt als het eerste theoretische model voor de computer. Door de Tweede Wereldoorlog ontstond er een grote behoefte aan krachtige rekenmachines. De drie basisautomaten van de computer bestonden op dat moment uit een geheugenautomaat, een besturingsautomaat en een rekenautomaat. De eerste rekenmachines stelden men in staat om geheime boodschappen te ontcijferen en berekeningen voor productie van bijvoorbeeld vliegtuigen en kernbommen te maken. Zo ontwikkelde men in het Verenigd Koninkrijk de eerste elektronische computer (Colossus) om onder meer de Duitse geheime codes van de Enigma te kraken. In 1948 werd in Manchester (VK) de eerste werkende computer gebouwd, waarbij ook Turing was betrokken.

Tijdens de Korea-oorlog werd er wederom een grote stap gemaakt met de ontwikkeling van ICT. IBM kreeg de opdracht om voor het Amerikaanse ministerie van Defensie een krachtige computer te bouwen die voorzag in een grotere rekencapaciteit. Ook in het bedrijfsleven bleek de behoefte hieraan groot. Grace Hopper bedacht in 1951 het concept van een programma dat berekeningen op gebroken getallen automatisch kon omzetten naar machine-instructies, de zogenaamde compiler. Hiermee konden ook opdrachten worden gegeven voor het aansturen van randapparatuur, zoals printers. Sinds John Backus tussen 1953 en 1957 de FORTRAN-compiler ontwikkelde, en daarmee het voor mensen eenvoudiger maakte de assemblers en machinetalen te begrijpen, bestaan er twee vormen van programma's: broncode programma's en objectcode programma's. De broncode fungeert als hogere programmeertaal en de objectcode fungeert als weergave van de machinetaal. De beschikbaarheid van deze programma's leidde tot de ontwikkeling van ondersteunende programma's zoals systeemprogrammatuur of bedrijfssystemen ook wel besturingssystemen of operating systems genoemd. Dergelijke besturingssystemen maken communicatie mogelijk tussen de centrale verwerkingseenheden en de randapparatuur.

In de jaren zestig kwamen er steeds meer bedrijfstoepassingen en ging de zoektocht naar werkwijzen om de capaciteit van computers zo efficiënt en effectief mogelijk te benutten onverminderd door. De computerchip zorgde vanaf 1963 voor verdere miniaturisering, capaciteitsvergroting en kostenverlaging van apparatuur.

Sinds deze periode werd het ook mogelijk om met de besturingssystemen meerdere gebruikers tegelijkertijd op één machine te laten werken, het zogenaamde timesharing. Gebruikers werden met ieder een eigen terminal (toetsenbord en monitor) aan een mainframe (computer) verbonden. Hieruit vloeide ook het idee van een computernetwerk voort. Bedrijven zoals de huidige telefoonaanbieders begonnen met het aanbieden van lijnen voor datatransmissie en het verbinden van terminals over grotere afstand door middel van telefonienetwerken. In deze tijd ontstonden ook applicaties zoals databases en andere analysetools.

Het Amerikaanse ministerie van Defensie startte in de jaren zestig ook met verschillende projecten om de bestaande netwerken van het Amerikaanse leger zo te koppelen dat, als er één netwerk weg zou vallen, de informatie nog steeds toegankelijk zou zijn via de andere gekoppelde netwerken. Dit netwerk van gekoppelde netwerken werd het ARPAnet (Advanced Research Projects Agency Network) genoemd en geldt als de voorloper van het huidige internet.

De eerste e-mail over een computernetwerk werd in 1971 verzonden door Ray Tomlinson, die ook het @-teken introduceerde om de naam van de persoon en de naam van de computer te scheiden. In deze tijd werden ook veel protocollen geschreven die tot op de dag van vandaag dienst doen en vanwege de complexiteit van het internet ook lastig te vervangen zijn.

In 1974 ontwikkelden Vinton Cerf en Robert Kahn het Transmission Control Protocol/Internet Protocol beter bekend onder afkorting TCP/IP. Dit protocol maakte het mogelijk om verschillende netwerken snel en makkelijk aan elkaar te

koppelen en vormt de standaard voor het huidige internet. In 1975 publiceerde Edgar (Ted) Codd zijn relationele model en dat de relationele database mogelijk maakte. Hij ontwikkelde ook de taal om informatie uit die database op te vragen, de zogenaamde Structured Query Language, beter bekend onder afkorting: SQL. Deze databases zijn de basis geworden voor bijna alle opslag van informatie, zoals bijvoorbeeld een productendatabank van een webwinkel.

Deze ontwikkelingen maken het mogelijk om een groot netwerk van computers met elkaar te laten communiceren. Om alle computers onderling goed te laten communiceren zijn er afspraken gemaakt en beschreven in de Requests For Comments (RFC) die worden beheerd door de Internet Engineering Task Force (IETF). Een van de functies die het internet biedt is de mogelijkheid van het World Wide Web (WWW). Het WWW bevat een aantal technische afspraken waardoor wij overal ter wereld documenten en andere hulpmiddelen kunnen raadplegen met behulp van een URL, hyperlinks en het internet. Met WWW geef je eigenlijk aan dat je via het internet een website wilt gaan bezoeken (par. 3.2.4). Tim Berners-Lee ontwikkelde vanaf 1989 dit WWW-concept om informatie te kunnen delen tussen de wetenschappers die samenwerkten in projecten van zijn werkgever CERN. Hij ontwikkelde daarvoor een uniforme adresseringsmethode voor pagina's. Dit was eerst bekend onder de naam Universal Document Identifier (UDI). Dit staat nu onder meer bekend als de Uniform Resource Locator (URL) en Uniform Resource Identifier (URI). Naast deze uniforme adresseringsmethode ontwikkelde hij ook de opmaaktaal HTML, die onder meer tekst, afbeeldingen, video en hyperlinks ondersteunt. Om deze documenten ook te kunnen ophalen ontwikkelde hij ook het netwerkprotocol HTTP. Onder meer dankzij deze methoden kan jij nu eenvoudig websites bezoeken.

In de periode van de jaren tachtig werd het door steeds verdergaande miniaturisering van elektrische componenten mogelijk om een Personal Computer (PC) te maken. In dezelfde periode werd er onder meer om handel te drijven een standaardtaal gecreëerd voor het uitwisselen van gestructureerde berichten tussen onafhankelijke computers. De in deze periode ontwikkelde Electronic Data Interchange (EDI) is tegenwoordig vooral bekend in haar open variant E(lectronic)-commerce. In deze periode kwamen ook de – inmiddels grote – bedrijven als Microsoft (1975), Apple (1976) en Oracle (1977) op. IBM dat ook een grote rol speelt in de geschiedenis van ICT is in 1911 voortgekomen uit een fusie van drie bedrijven en opgericht als International Business Machines (IBM).

Vanaf 1995 werd het internet voor een groter publiek toegankelijk. Waar men in de jaren zeventig nog met grote terminals werkte en in de jaren tachtig met PC's met inbelverbindingen, zijn vanaf deze periode veel huishoudens via een kabel of draadloos verbonden met hun PC, laptop, smartphone of tablet. De mainframes van de jaren zeventig werden vervangen door servers die continue met elkaar in verbinding staan. Contact met één van deze servers geeft toegang tot het gehele netwerk waarin deze server is opgenomen. In deze periode werd ook een aantal functionaliteiten aan het internet toegevoegd, zoals FTP, e-mail, de taal HTML en grafische browsers. Het internet als digitale megabibliotheek werd evenals als gewone bibliotheken voorzien van zoeksystemen, onder meer via zoekmachines

zoals Altavista, Yahoo, Baidu, Bing en Google. In deze periode (1998) ontstond ook de term open source. De term verwijst ten aanzien van software naar het ontwikkelingsmodel waarbij aan gebruikers bepaalde rechten ten aanzien van het bestuderen, wijzigen en opnieuw distribueren van de broncode worden toegekend door middel van zogenoemde opensourcelicenties.

Vanaf 2000 deed de smartphone langzaam zijn intrede op de markt en werd deze voorzichtig omarmd door de consument. Eerst in Japan (1999), gevolgd door Amerika (2002). De grote introductie volgde pas rond 2006 met merken als Blackberry en Nokia, de iPhone van Apple in 2007 en de eerste op Android gebaseerde smartphone in 2008 door HTC. De introductie van de smartphone gaf het grote publiek altijd en overal toegang tot internet en het World Wide Web. Die ontwikkeling betekende ook gelijk de doorbraak voor het via internet zaken doen (E-commerce) en de doorbraak van de inmiddels grote e-commercebedrijven zoals Amazon (1994), e-Bay (1995) en de Alibaba group (1999). Ook Wikipedia (2001) brak in deze periode door als online encyclopedie. Deze eenvoudige toegang tot internet en het World Wide Web werd versterkt door introductie van de tablet. Hoewel er al vanaf de jaren tachtig tablets werden ontwikkeld, bracht Apple de tablet onder de aandacht van het grote publiek met de introductie van de iPad in 2010. Het idee voor een tablet is dus al veel ouder en kwam zelfs al voor in een film uit 1968 – de 2001: A Space Odyssey van Stanley Kubrick. Ook het met een stem bedienen van systemen, zoals Siri (Apple) of Cortana (Microsoft) kwam al voor in deze film.

Aan het begin van de 21e eeuw (2000) kwam Cloud computing op doordat grote spelers, zoals Amazon, Google, Microsoft en Yahoo, webdiensten gingen ontwikkelen. Cloud computing is het via een netwerk beschikbaar stellen van hardware, software en gegevens. In tegenstelling tot een fysieke server met data, brengt de Cloud met zich mee dat niet exact duidelijk is waar de gegevens zich bevinden. De data zweeft ergens in het netwerk. De mogelijkheid om een serveromgeving te virtualiseren (de softwarematige reproductie van een fysiek netwerk) bracht het gebruik van de 'Cloud' in een stroomversnelling. Je maakt zonder het waarschijnlijk zelf te weten, geregeld gebruik van de Cloud, bijvoorbeeld met programma's, zoals Dropbox, Icloud en Wetransfer die de gegevens opslaan of overdracht mogelijk maken via de Cloud. Het internet en cloudopslag zorgde aan het begin van de 21e eeuw voor veel (inmiddels grote) internetbedrijven, zoals Dropbox (2007), Airbnb (2008), Wetransfer(2009) en Uber (2009).

In juni 2013 bracht voormalig medewerker van de Amerikaanse geheime dienst, the National Security Agency (NSA), Edward Snowden informatie naar buiten over de wijze waarop deze dienst gegevens verzamelde van burgers wereldwijd. Zijn onthullingen in interviews en documenten maakte voor de wereld duidelijk hoe ver de Amerikaanse geheime dienst ging om zeer grote hoeveelheden gegevens te verzamelen. Ook zijn er suggesties dat geheime diensten zelf actief zijn bij het ontstaan of in stand houden van zogenoemde beveiligingslekken en zich niet alleen bezighouden met terrorismebestrijding, maar ook met bedrijfsspionage. Deze onthullingen hebben de wereld nadrukkelijk gewezen op de invloed van geheime diensten en mogelijkheden die ICT zowel goed- als kwaadwillenden biedt. Een

reeks van gebeurtenissen leidde er in 2018 toe dat Facebook publiek schuld bekende over het beleid op het platform en de wijze waarop zij waren omgegaan met data van hun gebruikers in de afgelopen jaren. Dit maakte duidelijk welke invloed de grote platformen hebben en wat er met onze data gebeurt.

Voorgaande beschrijving rechtvaardigt de conclusie dat de ontwikkelingen op het gebied van ICT razendsnel gaan. Dat wat vandaag nog 'state of the art' is kan morgen achterhaald zijn. Zo werd er nog geen tachtig jaar geleden moeite gedaan om tijdens de Tweede Wereldoorlog met een reusachtige computer een relatief eenvoudige code te kraken en wordt nu gesproken over thema's zoals de quantumcomputer, blockchaintechnologie, en the Internet of Things en domotica (par. 2.5.1), waarbij hele netwerken allerlei systemen ook in de privésfeer met elkaar verbinden. Hierdoor wordt de rol van ICT op ons dagelijks leven onmiskenbaar groter en daarmee ook het belang van zorgvuldig gebruik ervan.

1.3 Wat is zorgvuldig gebruik van ICT?

Zorgvuldig gebruik van ICT gaat voornamelijk over de vraag wanneer jij als gebruiker zorgvuldig omgaat met Informatie en Communicatie Technologie (ICT). Het gaat in de kern dan ook over jouw gedrag. Bij zorgvuldig ICT-gebruik veronderstellen wij dat de technologie op orde is en het gebruik ervan veilig is. Wanneer je ergens in dienst bent ligt de verantwoordelijkheid dat de ICT goed functioneert en betrouwbaar is in beginsel bij je werkgever. Voor de veiligheid van je eigen persoonlijke ICT-middelen, zoals een (privé)computer of smartphone, ben je in beginsel zelf verantwoordelijk. Interessante vragen doen zich voor wanneer jij zonder overleg jouw zakelijke e-mail installeert op jouw eigen smartphone en deze smartphone niet voldoende beveiligd hebt. Bij wie ligt dan de verantwoordelijkheid als er daaruit schade ontstaat? Kan jouw werkgever dan de schade op jou verhalen?

De vraag of bepaald gedrag zorgvuldig is of niet, wordt bepaald door sociale en juridische normen. Zo bepalen sociale normen wat onder vrienden of collega's als normaal wordt gezien. Bijvoorbeeld over wat je wel of niet op Facebook zet of deelt via WhatsApp. Ook het overtreden van sociale normen kan consequenties hebben. Zo berichtte de BBC in 2015 dat drie Britse rechters werden ontslagen, omdat zij pornowebsites hadden bezocht via hun werkaccount. Zij werden niet ontslagen omdat het bezoeken van pornowebsites via hun werkaccount bij wet verboden was, maar omdat dit gedrag onacceptabel werd bevonden vanwege de positie die zij vervulden. Een ander voorbeeld komt uit de Verenigde Staten waarbij een rechter van de Pennsylvania Supreme Court in 2016 werd ontslagen naar aanleiding van het uitlekken van de inhoud van e-mails die hij naar bevriende juristen stuurde en de daaropvolgende publiekelijke verontwaardiging daarover.

Naast de sociale normen wordt de vraag wat zorgvuldig gebruik van ICT is, voor een belangrijk deel bepaald door de grenzen die het recht en uiteindelijk de rechter daaraan stelt. Zo kan bepaald gedrag in strijd zijn met de wet, een contract of een zorgvuldigheidsplicht. Denk daarbij bijvoorbeeld aan de Auteurswet die bepaalt dat jij een foto in beginsel niet zonder toestemming van de maker op je zakelijke blog

mag plaatsen. Maar bijvoorbeeld ook aan de vraag of jij in strijd met een afgesloten contract of zorgvuldigheidplicht handelt wanneer jij je computer onvoldoende beveiligt maar wel geld van de bank wilt omdat er geld van je bankrekening is verdwenen. Het is uiteindelijk de rechter die bepaalt of je in strijd hebt gehandeld met de wet, een contract of een zorgvuldigheidsplicht en daar consequenties aan kan verbinden.

Box 1.2 ICT-vaardigheden van de gemiddelde Nederlander

Het Centraal Bureau voor de Statistiek (CBS) doet regelmatig onderzoek naar de computer- en internetvaardigheden van Nederlanders. In 2016 had 17% van de Nederlanders weinig ICT-vaardigheden. 64% van de jongeren in de leeftijd van 12-25 en 57% van de volwassenen in de leeftijd van 25-45 hadden meer dan basisvaardigheden in het gebruik van ICT. Overigens hoef je daarvoor niet over bijzondere vaardigheden te beschikken. Bij computergebruik hoef je geen computerprogramma te kunnen schrijven met een programmeertaal, de instellingen van software te kunnen wijzigen of een nieuw besturingssysteem te kunnen installeren om toch een gebruiker te zijn met meer dan basisvaardigheden. Bij internetvaardigheden geldt ook dat je niet over bijzondere vaardigheden hoeft te beschikken. Zo kan je ook een gebruiker zijn met meer dan basisvaardigheden zonder dat je een webpagina kan ontwerpen of de veiligheidsinstellingen van je internetbrowser kan veranderen. In 2016 heeft 75% van de Nederlanders persoonlijke informatie op internet gedeeld, zoals adresgegevens, telefoonnummers en e-mailadressen. Met gegevens over locatie, gezondheid, werk of inkomen zijn wij terughoudender. De meeste mensen die treffen maatregelen om te voorkomen dat anderen toegang hebben tot hun gegevens. Zie daarover ook hoofdstuk 6.

Bron: CBS, ICT, kennis en economie 2017

Een ander thema, dat wij verder niet zullen behandelen, betreft de vraag welke invloed onzorgvuldig ICT-gebruik heeft op je persoonlijke welzijn. Het gaat dan om sociale thema's zoals geluk en verslaving (aan een smartphone of sociale media). Zo toont onderzoek (E. Kross e.a., 'Facebook Use Predicts Declines in Subjective Well-Being in Young Adults', 2013; PLOS one 0069841) kort gezegd aan dat jongeren ongelukkig worden als ze veel op Facebook zitten en dat de activiteit een indicatie is voor de mate waarin zij later op de dag tevreden zijn. Ook dergelijke onderzoeken kunnen een factor zijn bij het beslissen hoe je omgaat met ICT-middelen.

Wij richten ons nu verder op wat jij als professional kan en juridisch misschien ook wel moet doen: zorgvuldig omgaan met ICT-middelen. Ons doel is om je bewust te maken van de meest voor de hand liggende risico's waar je als (niet-ICT-)professional in je dagelijkse werk mee geconfronteerd wordt. Het gaat ons er dus niet om je tegen iedereen te beschermen (want dat lukt niet), maar om het kwaadwillenden zo moeilijk mogelijk te maken door de meest voor de hand liggende beschermingsmogelijkheden te benutten. Vergelijk dat met het installeren van een alarminstal-

latie en goede sloten op de deur. Wanneer iemand echt wil, dan komt hij binnen. Je houdt een inbreker of een hacker die echt binnen wil komen niet tegen. Je kan het hem echter wel zo lastig en onaantrekkelijk mogelijk maken. Het beschermen van je computer en je verbinding moet uiteindelijk net zo gewoon worden als het op slot doen van je huisdeur. In beide gevallen kan je een poort open laten staan, maar dan loop je ook het risico dat er iemand binnenkomt.

Zorgvuldig ICT-gebruik gaat in de kern vaak om een keuze tussen veiligheid en privacy aan de ene kant en gebruiksgemak aan de andere kant. Je zal dan ook per geval een afweging moeten maken welke van de twee volgens jou in dat geval de voorkeur moet krijgen.

1.4 Zorgvuldig ICT-gebruik en recht

ICT is vandaag de dag zo'n belangrijk onderdeel geworden van ons dagelijks leven dat er steeds meer juridische normen zijn en worden ontwikkeld om te bepalen hoe wij met ICT om moeten gaan. De vraag wat zorgvuldig gebruik van ICT is wordt naast sociale normen dan ook voor een belangrijk deel bepaald door de grenzen die het recht en uiteindelijk de rechter daaraan stelt. Het recht stelt grenzen aan het verrichten van bepaalde handelingen. Dat geldt voor handelingen die jij als professional verricht naar of voor derden, maar ook voor handelingen die derden verrichten tegenover jou als professional maar ook als privépersoon. Hoe het recht aankijkt tegen zorgvuldig gebruik van ICT is alleen om die reden al van belang. Daarbij komt dat iedereen geacht wordt de wet te kennen en zeker als professional mag van jou worden verwacht dat je enige kennis hebt van wat er juridisch wel en niet mag. Wij hebben niet als doel om een jurist van je te maken. Wel willen wij jou enige basiskennis bijbrengen die verwacht mag worden van een (aankomende) professional. Dit vervangt vanzelfsprekend geen professioneel juridisch advies, maar je zult versteld staan hoe ver je zelf kan komen.

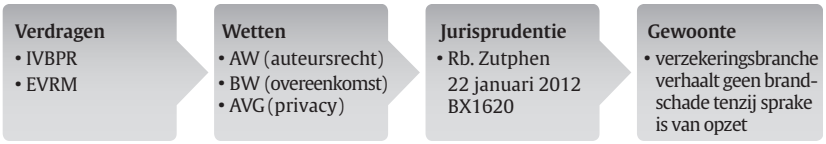
De vraag die zich voordoet is welke grenzen het recht stelt aan zorgvuldig gebruik van ICT. Die vraag is in zijn algemeenheid lastig te beantwoorden. Dat komt omdat de wet weinig zegt over zorgvuldig ICT-gebruik en rechters alleen uitspraak doen in een specifiek geval waarin specifieke omstandigheden binnen een bepaalde periode en in een bepaalde context bij de beoordeling een rol hebben gespeeld. Om dit boek overzichtelijk te houden en niet te juridisch te maken zullen wij in de volgende subparagrafen vooral de grenzen van het recht verkennen door de stappen door te nemen die elke jurist maakt wanneer hij de vraag moet beantwoorden of een bepaalde onzorgvuldige handeling aan iemand kan worden toegerekend. Bijvoorbeeld bij de vraag naar de toerekening van het risico voor onzorgvuldig gebruik van een elektronische handtekening.

In deze paragraaf kijken wij eerst naar de bronnen van het recht (par. 1.4.1), waardoor je zicht krijgt op het antwoord op de vraag op welke bronnen het recht gebaseerd is en welke bronnen jij dus zelf kan raadplegen als een ander of jijzelf een recht inroept. In de praktijk zal het antwoord op de vraag wanneer er sprake is van (on)zorgvuldig gebruik van ICT voornamelijk worden bepaald door de wet of

een tussen partijen gesloten overeenkomst (par. 1.4.2) en door uitspraken van rechters, ook wel aangeduid als jurisprudentie (par. 1.4.3).

1.4.1 Juridische bronnen van zorgvuldig ICT-gebruik

Het recht kent traditioneel vier zogenoemde rechtsbronnen: het verdrag; de wet; jurisprudentie; en de gewoonte.



Wanneer de rechter een vraag voorgelegd krijgt of een bepaalde handeling (doen of nalaten) zorgvuldig is of niet, dan begint hij met het raadplegen van de verdragen of wetten die van toepassing zijn op de zaak die voor hem dient. Bij zorgvuldig ICT-gebruik kan je denken aan zaken die of spelen in het domein van het strafrecht, zoals kinderporno (art. 240b Sr) en computervredebreuk (art. 138ab Sr) of aan zaken in het domein van het privaatrecht (regelt de wettelijke verhouding tussen burgers onderling). Denk daarbij aan de vraag of een WhatsAppbericht ook als een 'schriftelijke aanzegging' van de werkgever ex art. 7:668 BW moet worden gezien. Het antwoord op die vraag bepaald namelijk mede of een werknemer via dat bericht rechtsgeldig kan worden ontslagen of niet.

Box 1.3 Zoeken naar wetsartikelen en jurisprudentie

In dit boek worden verwijzingen gemaakt naar wetsartikelen en uitspraken van rechters (jurisprudentie). Wanneer het wetsartikelen betreft uit het BW (Burgerlijk Wetboek) dan wordt eerst het boek genoemd gevolgd door het wetsartikel. Zo is art. 6:213 lid 1 BW, een afkorting van art. 236, lid 1 uit boek 6 van het Burgerlijk wetboek. Deze wetten zijn terug te vinden op http://wetten.overheid.nl, waar je op de website de naam van de wet in kan tikken die je zoekt.

Verwijzingen naar rechtspraak vinden plaats door middel van het ECLI-nummer, dat is een Europese standaard voor het uniek nummeren van rechterlijke uitspraken. In Nederland vind je deze via de website http://uitspraken.rechtspraak.nl. Bedenk bij het zoeken dat in Nederland de Hoge Raad (HR) het hoogste gerecht vormt, gevolgd door het Gerechtshof (Hof) en de Rechtbank (Rb.). Zie verder paragraaf 1.4.3.

Wanneer de tekst van de wet zelf niet direct uitsluitsel geeft, dan zal de rechter kijken naar de wijze waarop de wet tot stand is gekomen (wetsgeschiedenis) of de toelichting die de wetgever op deze wet heeft gegeven (Memorie van Toelichting of MvT). Uit deze toelichting kan bijvoorbeeld blijken welk idee of doel de wetgever had bij het invoeren van een wet of een bepaald artikel. Vanuit die gedachte kan de rechter soms bepalen hoe een bepaald wetsartikel zou moeten worden