PRAKTIJK

Informatieverlies en de tikkende tijdbom 'WikiLeaks'

A.G. Wennekes

1 Inleiding

De wereld werd in de feestelijke decembermaand van 2010 opgeschrikt door onthullingen van de klokkenluiderssite[1] 'WikiLeaks'. Met name de Verenigde Staten waren woedend over het uitlekken van geheime informatie die onder andere ging over de oorlog in Irak, politici en ambassadeurs. De klokkenluiderssite plaatste bijna 400.000 militaire documenten over de oorlog in Irak. De onthulde documenten zouden de levens van Irakese informanten en van soldaten in gevaar kunnen brengen. Het Amerikaanse ministerie van Justitie onderzoekt of Julian Assange, de oprichter van WikiLeaks, naar aanleiding van de publicaties kan worden vervolgd.

De commotie rond WikiLeaks is ten tijde van het schrijven van deze bijdrage enigszins weggeëbd, maar regelmatig lezen we in de media nieuwe gevallen van uitlekken van geheime informatie. Recente berichten in de pers zijn onder andere: 'Geheime defensiedocumenten op straat in Utrecht' en 'Britse politie verliest usb met anti-terreur info'.[2] De media maken dankbaar gebruik/misbruik van de verkregen informatie en besteden hier veel aandacht aan.

Onlangs verrichtte KPMG een onderzoek dat liet zien dat de afgelopen drie jaar meer dan 500 miljoen mensen in de wereld zijn geraakt door het informatieverlies.[3] Het aantal incidenten lijkt af te nemen, maar in de eerste helft van 2010 werden toch nog 15 miljoen mensen getroffen. De mogelijke gevolgen zijn aanzienlijk en kunnen zich onder andere manifesteren in de vorm van financiële of bedrijfseconomische schade, of van (politieke) carrièreschade. Betrokkenen worden dikwijls geconfronteerd met vervelende gevolgen.

1 De naam klokkenluider is enigszins verwarrend omdat de gegevens die worden gepubliceerd niet als enige kenmerk hebben het aan het licht brengen van misstanden, maar ook inzage geven in vertrouwelijke informatie.

2 Respectievelijk de Volkskrant 28 januari 2011 en Webwereld 6 september 2010 (<www.webwereld.nl>).

3 De resultaten van het onderzoek zijn in november 2010 gepubliceerd. Zie <www.datalossbarometer.com/docs/KPMG_Data_Loss_Barometer_-_Issue_3_-_November_2010.pdf>. Van belang is op te merken dat het begrip 'informatieverlies' veel meer omvat dan het lekken van informatie. In deze bijdrage zal echter met name het uitlekken van vertrouwelijke informatie worden besproken. Informatieverlies als gevolg van 'hacking', dat onderdeel van het onderzoek van KPMG was, valt buiten het kader van deze bijdrage.

Het uitlekken van informatie gebeurt veelal op elektronische wijze, bijvoorbeeld via e-mails of het verlies van datadragers zoals een USB-stick. In toenemende mate gebeurt dit ook door het gebruik van sociale netwerken zoals Twitter, LinkedIn, Hyves en Facebook.

Veel bedrijven en hun werknemers zijn zich onvoldoende bewust van de risico's en de gevaren die het uitlekken van vertrouwelijke informatie met zich mee kunnen brengen. Met behulp van praktijkvoorbeelden zal in deze bijdrage in het kort worden uiteengezet op welke wijze er informatie wordt gelekt en hoe dit eenvoudig is te voorkomen. Tevens zullen de belangrijkste juridische aspecten van het uitlekken van informatie worden besproken. Daarbij wordt gekeken wat de juridische status is van een elektronisch bericht, een elektronische overeenkomst of een elektronische brief.

2 Vormen van informatieverlies

We kunnen het lekken van gevoelige informatie onderscheiden in bewust lekken en onbewust lekken. Dit is verder onder te verdelen in:
- onbewust lekken door de auteur of (legitieme) houder van de informatie (hierna: de houder) zelf;
- onbewust lekken door een ander;
- bewust lekken door de houder zelf; en
- bewust lekken door een ander.

2.1 Onbewust lekken door de houder zelf

Het onbewust lekken van informatie kan op diverse manieren plaatsvinden. Enkele voorbeelden zijn: het onbeveiligd versturen van een e-mail, een e-mail verkeerd adresseren of een e-mail versturen die niet verstuurd had mogen worden. Zie bijvoorbeeld het persbericht van 12 november 2010 in het Financieele Dagblad met de kop: 'Blunder analist kost UBS beursgang GM'. Een analist van de zakenbank UBS had per abuis een e-mail gestuurd naar meer dan honderd investeerders met een mogelijke waardering van het aandeel GM. Dit is als begeleidende bank verboden. GM nam onmiddellijk afstand van de inhoud van deze e-mail en zette de zakenbank UBS aan de kant. Het foutje van de analist kostte UBS volgens Reuters $ 10 miljoen aan gemiste inkomsten.

Onbewust lekken kan ook worden veroorzaakt door onzorgvuldig gebruik van datadragers, zoals een USB-stick. Omdat veelal de gegevens op een USB-stick onbeveiligd zijn opgeslagen, kan het slordig omgaan met een dergelijke datadrager grote problemen veroorzaken. Op 28 mei 2011 kon men in de landelijke dagbladen lezen dat iemand op een rommelmarkt een USB-stick had gekocht voor € 1. Op deze datadrager stond vertrouwelijke informatie over de verkoop van F-16-gevechtsvliegtuigen aan Chili. Het ging hier om een contract van € 100 miljoen.

Wat langer geleden, op 17 december 2009, berichtte het dagblad Trouw dat een Rabobankmedewerker een USB-stick had verloren met gegevens van drieduizend particulieren en van kerken, scholen en ondernemingen. De gegevens stonden ook hier onbeveiligd op de datadrager.
Onjuist gebruik van een telefoon of een Blackberry kan ook informatieverlies veroorzaken. Zo kwam in maart 2011 breeduit in het nieuws dat de voicemails van klanten van Vodafone door onbevoegden eenvoudig konden worden afgeluisterd. Dit was mogelijk omdat de gebruikers de standaardcode voor het beluisteren van een voicemail vanaf een ander toestel niet hadden gewijzigd.

Een andere oorzaak van informatieverlies kan zijn het onbedachtzaam wegwerpen van papieren documenten in de prullenbak, terwijl deze in de papierversnipperaar thuishoren, het laten liggen van vertrouwelijke stukken bij de printer of het kopiëren van vertrouwelijke stukken. Op 1 juni 2011 konden we in de Volkskrant lezen dat een rechercheur een vertrouwelijk dossier kopieerde op een machine waarmee ook de dossiers voor de advocaten werden afgedrukt. Een deel van het geheime dossier kwam per abuis tussen de geprinte papieren terecht, die vervolgens naar 21 advocaten werden gestuurd.

Onbewust informatieverlies kan ook voorkomen wanneer er wordt gewerkt op een openbare computer, en dan met name wanneer er documenten worden geopend. Deze documenten worden namelijk tijdelijk op de lokale computer opgeslagen. Het is daarom van groot belang om, na gebruik, de internetgeschiedenis en tijdelijke bestanden te verwijderen. Dit is meestal via de internetbrowser eenvoudig te bewerkstelligen, maar kan bijvoorbeeld ook met een progamma zoals *CCleaner Portable*, indien geïnstalleerd op een USB-stick. Daarnaast zijn er vele andere situaties denkbaar waarin onbewust informatieverlies kan ontstaan. Te denken valt aan het plaatsen van data op een desktop of laptop in plaats van op het beveiligde netwerk, waardoor die data bij vervanging of verlies van de computer bereikbaar zijn voor derden, enzovoort. Een uitputtende opsomming is uiteraard niet te geven.

Daarnaast zijn de nieuwe sociale netwerken, zoals Twitter en Facebook, dikwijls een bron van vertrouwelijke informatie. Berichten en vertrouwelijke informatie worden door gebruikers (te) snel en (te) gemakkelijk met behulp van deze media naar buiten gebracht. De materiële en immateriële schade kan aanzienlijk zijn. Zo konden we in de Groene Amsterdammer op 14 februari 2009 lezen dat Maxime Verhagen op zijn vingers werd getikt door Balkenende vanwege een foto die hij op Twitter plaatste. Het uitlekken van vertrouwelijke informatie via deze sociale netwerken is voor diverse bedrijven een reden om de medewerkers het deelnemen aan blogs, Twitter enzovoort te verbieden, in ieder geval tijdens werktijd.

Er is nog niet veel jurisprudentie met betrekking tot het lekken van vertrouwelijke informatie. Redenen kunnen zijn dat men geen ruchtbaarheid wil geven aan het lekken van vertrouwelijke informatie of dat eventuele geschillen in der minne worden opgelost.

Een van de weinige geschillen die wel aan de rechter werden voorgelegd, was een ontslagzaak, die uiteindelijk bij het hof[4] kwam. De ontslagzaak betrof een werknemer van een bank die in strijd met de interne regels tot tweemaal toe vertrouwelijke informatie verspreidde. De regels bestonden uit een arbeidsvoorwaardenregeling en een algemene gedragscode. Laatstgenoemde ziet onder meer op de interne verspreiding van bedrijfsinformatie en het gebruik van e-mail en internet.

De eerste maal dat de werknemer vertrouwelijke informatie had verspreid, betrof een presentatie voor een boardmeeting. De werknemer had de presentatie naar een kleine groep collega's gestuurd, onder wie zijn leidinggevende. De tweede maal had de werknemer een presentatie naar een oud-collega gestuurd. Deze ex-collega werkte bij een andere financiële instelling. Vervolgens had de werknemer de presentatie met toestemming van zijn leidinggevende naar een externe journalist gestuurd. De leidinggevende zelf had een derde toegang gegeven tot het intranet waarop de presentatie te vinden was.

Omdat de werkgever niet goed kon onderbouwen dat het bedrijf als gevolg van de eerste verspreiding schade had geleden en in het tweede geval met medeweten van de werkgever de presentatie aan een journalist was gezonden, zag de rechter geen dringende reden voor ontslag.

2.2 Onbewust lekken door een ander

Het onachtzaam delen van kennis over zaken of personen met derden is een vorm van onbewust lekken van potentieel vertrouwelijke informatie. Dit gebeurt niet alleen in een gesprek, maar ook digitaal. Een veelgemaakte fout is bijvoorbeeld het klakkeloos doorsturen van een e-mail, zonder dat men eerdere berichten die in de e-mail staan, weghaalt. Ook kan het gebeuren dat iemand vertrouwelijke documenten in de prullenbak gooit die iemand heeft laten liggen bij de printer. Beide voorbeelden laten de mogelijkheid open dat vertrouwelijke informatie door derden wordt gelezen.

Daarnaast kan het onbewust lekken van gegevens plaatsvinden door het te vroeg vrijgeven van informatie. Zo werd bijvoorbeeld op 31 augustus 2010 door de Rechtbank Breda de schriftelijke uitspraak over een verkrachtingszaak in Ossendrecht op internet gepubliceerd, terwijl de mondelinge uitspraak pas in de middag zou worden gedaan. Toen deze fout werd ontdekt, is de uitspraak direct van internet verwijderd, maar het kwaad was al geschied.

2.3 Bewust lekken door de houder zelf

De voorbeelden die genoemd zijn onder onbewust lekken kunnen uiteraard ook allemaal *bewust* door de houder zelf of door een ander plaatsvinden. Uit het onderzoek van KPMG, dat genoemd is in paragraaf 1, blijkt dat 20 procent van het informatieverlies voor rekening komt van kwaadwillende werknemers. Dat deze 20 procent voor rekening komt van kwaadwillende insiders is verontrustend en kan men kwalificeren als diefstal.

4 Hof Amsterdam 12 juli 2007, LJN BB6127.

Informatieverlies varieert van relatief onschuldige e-mails tot gevoelige persoonlijke of bedrijfsinformatie. Daarnaast worden nogal eens bedrijfsgegevens, waaronder de knowhow, doorgespeeld naar een ander bedrijf. Ter illustratie: een ontslagzaak die bij de Rechtbank Amsterdam[5] diende met betrekking tot het bewust lekken van vertrouwelijke informatie. Een werknemer van een bank met als functie *senior financial professional* had vertrouwelijke bankinformatie van een klant, onder andere over creditvolumes en kredietfaciliteiten, verstrekt aan een bevriende relatie ten behoeve van een bedrijf dat de juistheid van die informatie wilde verifiëren. Hij is vervolgens op staande voet ontslagen. In de procedure stond vast dat de werknemer de vertrouwelijke informatie onder valse voorwendselen had opgevraagd bij collega's in binnen- en buitenland. Ook had de werknemer zonder medeweten van de werkgever een getuigenverklaring tegen de werkgever afgelegd ten behoeve van eerdergenoemd bedrijf, welke verklaring vervolgens is gebruikt in een procedure tegen de werkgever. De interne klokkenluidersregeling en de daarin voorgeschreven procedure had de werknemer niet gevolgd. De voorzieningenrechter vond dat de handelingen van de werknemer dermate in strijd waren met de eisen van goed werknemerschap, dat ontslag op staande voet in beginsel zonder meer gerechtvaardigd was.

Het doorspelen van informatie kan ook leiden tot overtreding van het zogenoemde 'mededelings- en tipverbod', zoals neergelegd in art. 5:57 Wet op het financieel toezicht (Wft), wanneer de informatie kwalificeert als voorwetenschap. Art. 5:57 Wft verbiedt – kort gezegd – eenieder informatie waarop zijn voorwetenschap ziet, mee te delen aan derden of een derde aan te zetten tot het verrichten of bewerkstelligen van transacties. Ondanks dit 'mededelings- en tipverbod' lezen we regelmatig in de landelijke dagbladen dat er sprake of een vermoeden is van handel met voorkennis waarbij door een insider vertrouwelijk informatie is doorgespeeld.

Een recent voorbeeld is de voorkenniszaak 'Grolsch'. Het betrof de overname van de Nederlandse brouwer Grolsch door SABMiller, eind 2007. Een secretaresse van een lid van de Raad van Bestuur van Grolsch had aan haar partner medegedeeld dat er sprake was van een voorgenomen overname van Grolsch, waarna die zijn vader hiervan op de hoogte bracht. Zijn vader kocht vervolgens aandelen Grolsch, waarvan de koers na de bekendmaking van het overnamebod fors de hoogte in ging. De Rechtbank Amsterdam oordeelde op 18 februari 2011 dat er sprake was van voorkennis en dat de verdachte (de secretaresse) deze kennis in strijd met art. 5:56 Wft had medegedeeld aan een derde.[6] De directiesecretaresse kwam ervan af met een voorwaardelijke boete omdat het gevaar voor herhaling verwaarloosbaar was. Zij was inmiddels al ontslagen en daar kwam bij dat zij het feit had gepleegd in de huiselijke sfeer en in feite het slachtoffer van het handelen van familie was geworden.

5 Rb. Amsterdam 21 januari 2010, JAR 2010/66.
6 Rb. Amsterdam 18 februari 2011, LJN BP5069.

Voorts is op dezelfde dag in een strafzaak tegen de schoonvader op grond van art. 36e van het Wetboek van Strafrecht (Sr) de winst uit de handel met voorkennis in certificaten als wederrechtelijk verkregen voordeel aangemerkt.[7]

Uit een op 2 mei 2011 gepubliceerd onderzoek van de Erasmus Universiteit, in samenwerking met PricewaterhouseCoopers (PWC), onder circa vierhonderd analisten en beleggers wereldwijd, blijkt dat institutionele beleggers in een-op-eengesprekken met ondernemingsbesturen vaak koersgevoelige informatie krijgen toegespeeld. Bijna de helft van de respondenten (47 procent) geeft aan dat er in deze gesprekken bewust of onbewust 'materiële', ofwel koersgevoelige informatie wordt verstrekt.

Het uitlekken van vertrouwelijke informatie, en het ongeoorloofd gebruik daarvan, komt overigens niet alleen voor bij het handelen met voorkennis in aandelen, maar ook bijvoorbeeld in aanbestedingszaken.

2.4 Bewust lekken door een ander

Bewust lekken van vertrouwelijke informatie door een ander dan de houder kan gebeuren door iemand die werkzaam is bij het gedupeerde bedrijf, maar ook door een derde. Het lekken van informatie door een derde komt in vele vormen voor. Gedragscodes en bedrijfsreglementen zijn op een derde niet van toepassing, tenzij de derde wordt ingehuurd om tijdelijke werkzaamheden te verrichten voor het bedrijf en de gedragscodes en bedrijfsreglementen heeft moeten aanvaarden en ondertekenen.

Hoewel in deze bijdrage het fenomeen hacking niet wordt behandeld, kan het informatieverlies door het onderscheppen van telefoonverkeer niet ontbreken. Ondanks strenge privacywetgeving wordt in Nederland telefoonverkeer regelmatig afgetapt en niet alleen door justitie. Voorheen was er vrij ingewikkelde en dure apparatuur nodig om het telefoonverkeer af te luisteren, maar volgens diverse bronnen[8] is het nu mogelijk om met name het gsm-verkeer eenvoudig af te luisteren met goedkope apparatuur.

3 Juridische aspecten

3.1 Gelijkstelling geschrift met elektronische vorm

Onder invloed van Europese regelgeving zien we steeds meer dat het elektronische verkeer wettelijk wordt geregeld. Deze juridisering brengt met zich mee dat de gebruiker zich nog meer bewust moet zijn van de rechtskracht van een elektronisch bericht.

In Nederland bestaat er geen vormvereiste voor het tot stand komen van een geldige overeenkomst, behalve bij overeenkomsten waarvoor een schriftelijkheids-

7 Rb. Amsterdam 18 februari 2011, LJN BP5059. Over het handelen met voorkennis, zie o.a. C.W.M. Lieverse, Jurisprudentie effectenrecht, O&F 2005-69, p. 36-37.

8 Zie o.a. <http://webwereld.nl/nieuws/67198/aivd--massaal-afluisteren-gsm-dreigt.html>.

vorm is voorgeschreven door de wet, of als partijen dit zijn overeengekomen. Het te snel verzenden van een e-mail – al dan niet met bijlagen – of het invullen en verzenden van een aanmeldingsformulier via internet kan juridische gevolgen hebben.[9]

Sinds de Aanpassingswet richtlijn inzake elektronische handel,[10] die op 30 juni 2004 in werking is getreden, kunnen overeenkomsten die op grond van de wet in schriftelijke vorm tot stand moeten komen, ook langs de elektronische weg worden afgesloten. Hier zijn echter wel enkele voorwaarden aan verbonden en bepaalde overeenkomsten zijn uitgesloten.

Daarnaast is sinds enige tijd in meerdere wetten geregeld dat elektronisch verkeer dezelfde rechtskracht heeft als een geschrift. Zie bijvoorbeeld de 'Wet elektronisch bestuurlijk verkeer',[11] die op 1 juli 2004 in werking is getreden, en de Wet van 20 februari 2010 tot wijziging van enige bepalingen van het Wetboek van Burgerlijke Rechtsvordering en het Burgerlijk Wetboek teneinde naast het in deze bepalingen gestelde vereiste van schriftelijkheid ook ruimte te bieden aan de ontwikkelingen op het gebied van het elektronisch verkeer,[12] die op 1 juli 2010 in werking is getreden. Deze laatste regelt dat verzekeringspolissen via elektronische weg afgegeven kunnen worden en dat onder bepaalde omstandigheden ook onderhandse akten en algemene voorwaarden in elektronische vorm zijn toegestaan.

Tijdens de behandeling van het wetsvoorstel 'Wet elektronisch bestuurlijk verkeer' is in de Eerste Kamer de vraag gesteld of overhandiging van algemene voorwaarden niet uitsluitend hoeft te gebeuren in de vorm van een schriftelijk stuk, maar of dit ook kan door de overhandiging van een USB-stick, dvd of cd-rom.[13] De minister antwoordde dat onder de in art. 6:234 lid 2 Burgerlijk Wetboek (BW) geboden mogelijkheid om langs elektronische weg algemene voorwaarden ter beschikking te stellen, ook moet worden begrepen de overhandiging van een USB-stick, dvd of cd-rom met daarop de algemene voorwaarden in digitale vorm. Wel is vereist dat de wederpartij met deze wijze heeft ingestemd (art. 6:234 lid 3 BW).[14]

Een verdere ontwikkeling betreffende het wettelijk regelen van digitale informatie zien we bijvoorbeeld ook in het wetsvoorstel dat op 14 maart 2011 aan de Tweede Kamer[15] is aangeboden ten aanzien van de elektronische indiening van een dagvaarding.

9 Kanttekening hierbij is dat de overeenkomst moet voldoen aan art. 3:33 BW (wil en verklaring) en art. 6:217 BW (aanbod en aanvaarding). Stel dat er een concreet aanbod wordt gedaan op internet dat kan worden aanvaard door het aanklikken van een button, dan kan dat aanklikken worden gezien als een wilsverklaring.
10 Stb. 2004, 210. Deze wet dient ter uitvoering van Richtlijn 2000/31/EG.
11 Stb. 2004, 214.
12 Stb. 2010, 222.
13 Kamerstukken I 2008/09, 31 358, B, p. 6.
14 Kamerstukken I 2008/09, 31 358, C, p. 10.
15 Kamerstukken II 2010/11, 32 695.

3.2 Regels voor het notariaat en de advocatuur

De koepelorganisatie van Europese balies, de 'CCBE', heeft op 19 november 2005 een richtlijn vastgesteld voor Europese advocaten inzake de omgang met e-mailverkeer en webtechnologie. Deze richtlijn is ook op Nederlandse advocaten van toepassing. Onderwerpen zijn onder meer: de inhoud van e-mail en internetsites, advocaat-cliëntcorrespondentie, databescherming, copyrightaangelegenheden en archivering van e-mails en documenten.

De beroeps- en gedragsregels van de Nederlandse Orde van Advocaten schrijven tevens voor dat bij het beroep van de advocaat vertrouwelijkheid en geheimhouding horen over alles wat met cliënten en kantoor te maken heeft. Deze geheimhouding zal dan ook in de arbeidsovereenkomst van medewerkers moeten worden bedongen. De geheimhoudingsplicht stelt ook eisen aan de zorgvuldigheid van de keuze, het gebruik en de beveiliging van ICT-voorzieningen, met name internet en e-mail.

Binnen het notariaat zijn onder andere de Wet op het notarisambt en de Verordening beroeps- en gedragsregels van toepassing. Richtlijnen zoals voorgeschreven door de Nederlandse Orde van Advocaten met betrekking tot het gebruik van e-mailverkeer en webtechnologie en dergelijke zijn door de Koninklijke Notariële Beroepsorganisatie niet gepubliceerd.

3.3 Goed werknemerschap, bedrijfspolicy en aansprakelijkheid

Een werknemer dient zich als goed werknemer te gedragen (art. 7:611 BW). In de wet is echter geen definitie te vinden van het begrip goed werknemerschap. Er moet worden uitgegaan van de eisen van redelijkheid en billijkheid en wat een goed werknemer behoort te doen en na te laten. Een werknemer behoort in ieder geval goed om te gaan met de belangen van de werkgever. Hieronder kunnen we verstaan: het zorgvuldig omgaan met e-mails en andere informatie, zoals de knowhow van het kantoor, de privacy van cliënten en de informatie met betrekking tot zaken en transacties die door het bedrijf worden verricht. Deze geheimhoudingsplicht kan in de arbeidsovereenkomst worden geregeld in een geheimhoudingsbeding. Ongeacht of er een geheimhoudingsbeding is opgenomen, kan schending van geheimen een gegronde reden voor ontslag op staande voet opleveren.[16]

Een voorbeeld waarin het fout ging, ondanks dat er een geheimhoudingsbeding was overeengekomen, zien we bij de directeur van een fabrikant van verwarmingsapparatuur die op staande voet werd ontslagen omdat hij diverse malen, in strijd met een geheimhoudingsbeding, e-mails met vertrouwelijke informatie aan derden buiten het bedrijf had verzonden. Zo had de directeur in de aanhef van zijn e-mails de teksten gebruikt als: 'private', 'I owe you a inside information', 'private talking' en 'Jeff, what I am going to tell you is confidential, very confidential.'[17]

16 Art. 7:678 lid 2 onder i BW.

17 Hof Leeuwarden 6 augustus 2008, JAR 2008, 242.

Naast geheimhouding wordt vaak in de arbeidsovereenkomst geregeld dat het de werknemer verboden is op welke wijze dan ook documenten en/of correspondentie en/of andere informatiedragers en/of kopieën hiervan, die aan de werkgever toebehoren, in zijn bezit te houden en dat de werknemer verplicht is om deze documenten, data enzovoort aan het einde van de arbeidsovereenkomst aan de werkgever te overhandigen.

Veel bedrijven hebben ook moeite met het omgaan met sociale media. Zo is er meestal geen beleid over het publiceren van bedrijfsinformatie op blogs, YouTube of sociale websites zoals Twitter, LinkedIn, Hyves en Facebook. Hierdoor kan het bedrijf uiteraard schade ondervinden, maar het kan ook voor zowel het bedrijf als de werknemer vervelende juridische consequenties met zich meebrengen. Hierbij kunnen we denken aan een onrechtmatige daad, schending van het auteursrecht of schending van het portretrecht.

Op grond van zijn 'instructierecht' uit art. 7:660 BW kan de werkgever gedragsregels opstellen voor het gebruik van e-mail, informatiedragers, internetverkeer en het gebruik van sociale media. Wanneer de werknemer zich niet houdt aan de regels kan de werkgever de werknemer een boete opleggen (art. 7:650 BW), mits dit schriftelijk is overeengekomen.

Ondanks dat er gedragsregels zijn vastgesteld, blijkt het toch wel eens fout te gaan. Dit komt ten dele omdat niet alles is geregeld, maar ook omdat gebruikers zich niet bewust zijn van de valkuilen bij verkeerd gebruik van elektronische informatie. Neem bijvoorbeeld het schenden van informatiebarrières – ook wel aangeduid als Chinese Walls – binnen een bedrijf. Onder Chinese Walls kunnen we verstaan het geheel van beleid, procedures en regelingen dat gericht is op het beheersen van eventuele belangenconflicten en op de juiste manier omgaan met vertrouwelijke informatie en koersgevoelige informatie.[18]

Al geruime tijd ligt bij de Tweede Kamer een wetsvoorstel met een regeling ter bescherming van klokkenluiders, ook wel *whistleblowers* genoemd.[19] In dit wetsvoorstel wordt als uitgangspunt genomen dat een werknemer vertrouwelijke zaken die de onderneming betreffen, vertrouwelijk behandelt. Dit is alleen anders wanneer een werknemer in redelijkheid van mening kan menen dat het algemeen belang openbaarmaking van gedachten of gevoelens of de bekendmaking van bijzonderheden noodzakelijk maakt. In dat geval kan de werknemer niet worden ontslagen. Op grond van het wetsvoorstel zou de werkgever dus niet een algemene geheimhoudingsplicht aan zijn werknemers kunnen opleggen. De bescherming van de klokkenluider druist in feite in tegen de geheimhoudingsplicht van de werknemer, maar wordt gerechtvaardigd wanneer hij de gemeenschap wil waarschuwen voor een specifieke, acute of dreigende misstand.

18 Zie bijv. het Besluit marktmisbruik Wft, hoofdstuk 6.

19 Kamerstukken II 2002/03, 28 990. Op dit moment is niet zeker of dit wetsvoorstel voortgezet zal worden of dat het ingetrokken wordt. De Stichting van de Arbeid heeft ook gedragsregels gepubliceerd voor het omgaan met vermoedens van misstanden bij het bedrijf (24 juni 2003, Publicatienr. 6/03). Deze gedragsregels kunnen bij cao worden geïmplementeerd.

3.4 Schending briefgeheim

De vraag is of het briefgeheim wordt geschonden wanneer een e-mail wordt geopend door een onbevoegde. In lid 1 van art. 13 van de Grondwet is het briefgeheim geregeld en in lid 2 het telefoon- en telegraafgeheim.
De 'Staatscommissie Grondwet' heeft in haar rapport ten aanzien van de aanpassing van de Grondwet het volgende opgemerkt:

> 'Artikel 13 Grondwet beschermt het briefgeheim en het telefoon- en telegraafgeheim. De tekst van deze bepaling is niet in overeenstemming met nieuwe ontwikkelingen. Zo is de telegraaf in onbruik geraakt en zijn naast de brief allerlei andere communicatiemiddelen, zoals e-mail, ontstaan. De Staatscommissie stelt daarom voor artikel 13 Grondwet aldus te formuleren dat ieder recht heeft op vertrouwelijke communicatie. Mensen moeten erop kunnen rekenen dat zij vertrouwelijk met elkaar kunnen communiceren zonder dat de overheid meeleest of -luistert, van welke middelen zij ook gebruik maken.'[20]

Hieruit kunnen we concluderen dat het e-mailverkeer vooralsnog niet onder het briefgeheim valt. Wel kan men een beroep doen op art. 8 van het Europees Verdrag ter bescherming van de rechten van de mens en de fundamentele vrijheden, waar in lid 1 is bepaald dat privécorrespondentie, waaronder e-mailverkeer kan worden gerekend, moet worden geëerbiedigd.

4 Technische hulpmiddelen

Hoewel deze bijdrage niet gaat over de technische aspecten met betrekking tot informatieverlies, worden enkele technische hulpmiddelen besproken die informatieverlies kunnen voorkomen of beperken.

Zoals besproken kan het verlies van een datadrager, bijvoorbeeld een USB-stick, veel problemen opleveren, zelfs wanneer schijnbaar alle gegevens van de USB-stick zijn gewist. Immers, met behulp van software, veelal via internet te downloaden, is het mogelijk om verwijderde bestanden moeiteloos terug te halen van de harde schijf, floppydisk, USB-stick, of welke datadrager dan ook. Het is dus zaak een datadrager goed te beveiligen. Het beveiligen van bijvoorbeeld een USB-stick is niet duur of ingewikkeld. TrueCrypt en FreeOTFE zijn gratis programma's die gebruikt kunnen worden om een USB-stick te versleutelen, ook wel cryptografie genoemd. Men krijgt dan alleen toegang als het juiste wachtwoord is ingevuld. Daarnaast zijn er USB-sticks te koop die zichzelf versleutelen, bijvoorbeeld de IronKey en de Kingston DataTraveler Vault. Hierbij zij opgemerkt dat een aantal landen beperkende wet- en regelgeving oplegt voor het bezit en de toepassing van cryptografie. In bijvoorbeeld China en diverse voormalige Sovjetrepublieken geldt

20 Rapport Staatscommissie Grondwet, p. 11. Het lid Overkleeft-Verburg is weliswaar ook voorstander van herziening van art. 13 Grondwet, maar stelt een andere bepaling voor: zie par. 8.6.6. van het rapport.

dat eigenlijk alle vormen van cryptografie verboden zijn, tenzij de autoriteiten expliciet toestemming hebben gegeven voor het gebruik ervan.[21]

Ook informatieverlies via het e-mailverkeer kan worden voorkomen wanneer een e-mail beveiligd wordt verstuurd met encryptieprotocollen zoals SSL/TLS. De meeste providers die het e-mailverkeer verzorgen, ondersteunen deze protocollen. Daarnaast is het mogelijk om een e-mail veilig te versturen door deze van tevoren te versleutelen en te beveiligen met een wachtwoord. Een e-mail die op een dergelijke manier is versleuteld en wordt onderschept, kan niet zomaar worden geopend.

Als laatste nog iets over het gebruik van tekstverwerkers. In de meeste tekstverwerkers is het mogelijk om te zien wie de oorspronkelijke auteur is van het document en bij welk bedrijf het document is aangemaakt. Bovendien is het soms mogelijk eerdere schijnbaar gewiste gegevens terug te halen, zoals de revisietekens van bijgehouden wijzigingen, opmerkingen, aantekeningen, enzovoort. Daarom is het noodzakelijk dat dergelijke informatie, al dan niet automatisch, wordt verwijderd voordat een document elektronisch wordt verzonden.

5 Samenvatting en conclusie

Zowel het onbewust als het bewust lekken van vertrouwelijke informatie is voor veel bedrijven een groot probleem. Behalve dat de klokkenluiderssite 'WikiLeaks' regelmatig met onthullingen in het nieuws komt, kunnen we ook met grote regelmaat in de landelijke dagbladen lezen dat vertrouwelijke informatie op straat komt te liggen.

Het is voorzienbaar dat het elektronische verkeer nog aanzienlijk zal toenemen, hetgeen vooral wordt mogelijk gemaakt en gestimuleerd door Europese regelgeving. In steeds meer wetten zien we dat een elektronisch bericht, verklaring of een elektronische handtekening gelijkstaat aan het geschrift. Dit betekent dat bijvoorbeeld een verklaring of een elektronische handtekening een juridische status heeft gekregen die zij eerder niet had.

We kunnen constateren dat naarmate digitalisering van communicatie toeneemt, het risico dat vertrouwelijke informatie uitlekt, stijgt. Het is daarom van belang dat bedrijven protocollen en reglementen opstellen met betrekking tot het elektronisch verkeer en het gebruik van het internet en dat deze steeds worden geactualiseerd en worden nageleefd. Hier ligt een belangrijke taak voor de risk & compliance officer van het bedrijf, zodat de tikkende tijdbom 'WikiLeaks' niet onverwachts afgaat.

21 Via de site van GOVCERT.NL, het Cyber Security en Incident Response Team van de Nederlandse overheid, is een brochure te downloaden met uitgebreide informatie (<www.govcert.nl/>, zoek op cryptogebruik).