

**Paper, Grondslagen van het Recht**

Universiteit Utrecht – Rechtsgeleerdheid – Bachelor 1 – Werkgroep - – Ewald Tienkamp (-)  
(Printversie van woensdag 14 januari 2009, 14:34:19, totaal aantal pagina's 9)

**Paper**

**Tweede versie**

Student: **Ewald Tienkamp**  
Studentnummer: -

Mailadres: -  
Mailadres privé: -

Vak: Grondslagen van het Recht  
Werkgroepdocent: -  
Werkgroepnummer: -

Thema van paper: **4.5, Privacy op de werkvloer**

Paper titel: Weten wat een werknemer wil van het wereldwijde web  
Subtitel: Een inventarisatie van de juridische mogelijkheden voor de werkgever wat betreft registratie en monitoring van het internetgebruik door werknemers

Aantal pagina's (incl. voorblad, literatuurlijst, excl. bijlage(n)): 9  
Printversie: 14 januari 2009, 14:34:19

Bijlage(n): Paper eerste versie, met correcties, inclusief Urkund bevestigingsmail

## **Weten wat een werknemer wil van het wereldwijde web**

*Een inventarisatie van de juridische mogelijkheden voor de werkgever wat betreft registratie en monitoring van het internetgebruik door werknemers*

Meerdere keren per jaar verschijnen onderzoeken over het percentage werknemers dat zich bezighoudt met privégebruik van het internet onder werktijd. Vaak zijn de gepubliceerde onderzoeken uitgevoerd in opdracht van vacaturesites als Monsterboard.nl<sup>1</sup> en ITJobBoard<sup>2</sup> of afkomstig van specifieke adviesbedrijven. Beide groepen voorzien het onderzoek van een persbericht en halen op die manier eenvoudig de publiciteit.

Een voorbeeld van een dergelijk adviesbedrijf is Ernst & Young. Jaarlijks verzorgen zij de ICT Barometer.<sup>3</sup> Een deel van deze barometer beschouwt het privé internetgebruik door werknemers. Zo bracht de ICT Barometer van 2006 ons het nieuws dat er een bescheiden afname plaatsvond van het privégebruik,<sup>4</sup> terwijl 2007 ons verraste met een 'schrikbarende toename'.<sup>5</sup>

Bovengenoemde publicaties van cijfers worden geregeld voorzien van commentaren. Hierin wordt uitgeweid over de schadelijkheid van het privégebruik van het internet of er worden ethische adviezen gegeven wanneer dergelijk gedrag mag worden berispt. Zo stelt FNV Bondgenoten al in het jaar 2000 dat 'privégebruik is toegestaan, mits het niet storend is voor het dagelijks werk'.<sup>6</sup>

Stijgingen en dalingen en wenselijkheid en schadelijkheid houden de gemoederen dus al enige tijd bezig. In dit artikel blijven deze ontwikkelingen en discussies buiten beschouwing. Ongeacht de wenselijkheid bestaat reeds sinds het begin van de kwestie de technische mogelijkheid voor werkgevers om het internetgebruik van werknemers te controleren. In hoeverre deze mogelijkheid ook een juridische mogelijkheid is, wordt hier onderzocht aan de hand van de vraag, wat precies het juridische kader is waar werkgevers rekening mee moeten houden, als zij de wens hebben het internet- en e-mailgebruik van werknemers te controleren en/of registreren.

Het juridische kader wordt achtereenvolgens op nationaal en internationaal vlak geschetst. Waar op internationaal niveau in het bijzonder de grondrechten rond privacy aan bod komen, wordt op nationaal niveau ook gekeken naar civiel recht en strafrecht. Op zowel nationaal als internationaal vlak wordt de beschikbare jurisprudentie bekeken.

Voordat we hiermee starten, is het verstandig om nader te duiden wat in deze context precies bedoeld wordt met het controleren en registreren van het gebruik van genoemde elektronische communicatiemiddelen. Met het controleren en registreren wordt bedoeld een methode om (digitale) logboeken bij te houden waarin te zien is welke werknemer, vanaf welke pc, wanneer en wat, heeft bezocht, ontvangen of verzonden. Een simpele zoektocht bij een populaire zoekmachine als Google wordt geflankeerd door vele advertenties voor commerciële pakketten die precies deze taak vervullen.<sup>7</sup> Kortom, de technische mogelijkheden zijn er.

### **Nationale juridische grenzen**

Hoe zit het echter met de juridische mogelijkheden? In het Wetboek van Strafrecht (Sr) bestaan verschillende bepalingen die duidelijk stellen dat bepaald gedrag expliciet verboden is.

Het College Bescherming Persoonsgegevens stipt in haar rapport *Goed werken in netwerken*

<sup>1</sup> 'Nederlandse werknemers gebruiken massaal e-mail op werk voor privé-zaken', <[http://about.monsterboard.nl/9100\\_nl\\_p1.asp](http://about.monsterboard.nl/9100_nl_p1.asp)>

<sup>2</sup> *Werknemer regelt privé-zaken tijdens kantooruren*, <<http://www.managersonline.nl/nieuws/7559/werknemer-regelt-privzaken-tijdens-kantooruren.html>>

<sup>3</sup> *Ernst & Young ICT Barometer*, <[www.ict-barometer.nl](http://www.ict-barometer.nl)>

<sup>4</sup> *Werkgever neemt veelvuldig privé surfen en e-mailen voor lief*, <<http://www.ict-barometer.nl/persbericht.php?id=16>>

<sup>5</sup> *Schrikbarende toename privé mailen, bellen en surfen onder werktijd*, <<http://www.ict-barometer.nl/persbericht.php?id=33>>

<sup>6</sup> Titia Ketelaar, 'Privé-surfen: `tijd stelen van de baas'', *NRC Handelsblad* 8 september 2000, <[http://www.nrc.nl/dossiers/privacy/de\\_werknemer/article1558101.ece/Prive-surfen\\_%60tijd\\_stelen\\_van\\_de\\_baas](http://www.nrc.nl/dossiers/privacy/de_werknemer/article1558101.ece/Prive-surfen_%60tijd_stelen_van_de_baas)>

<sup>7</sup> Google zoekopdracht 'employee internet monitoring', <<http://www.google.nl/search?q=employee+internet+monitoring>>

### Paper, Grondslagen van het Recht

Universiteit Utrecht – Rechtsgeleerdheid – Bachelor 1 – Werkgroep - - Ewald Tienkamp (-)  
(Printversie van woensdag 14 januari 2009, 14:34:19, totaal aantal pagina's 9)

(over beide later meer) een aantal voor ons relevante strafbepalingen aan.<sup>8</sup> Zo kan men denken aan artikel 138a Sr, computervrederebreuk. In het eerste lid van dit artikel wordt (simpel gesteld) het opzettelijk en in strijd met de wet binnendringen in een computersysteem strafbaar gesteld. In de leden 2 en 3 van dit artikel worden verdere bewerkingen door de dader op de computer in kwestie strafbaar gesteld. In de artikelen 139b en 139c Sr is achtereenvolgens het af luisteren en aftappen van gesprekken buiten de woning en gesprekken over telecommunicatie buiten de woning strafbaar gesteld. Artikel 273d Sr,<sup>9</sup> enigszins in het verlengde van de twee voorgaande artikelen stelt de schending van het digitaal briefgeheim strafbaar. Met andere woorden, het inzien van bijvoorbeeld e-mailverkeer. Tot slot kan nog genoemd worden artikel 350a Sr. Dit artikel is gericht op het verbieden van het opzettelijk vernielen van computergegevens, waarvan bijvoorbeeld sprake is indien e-mail- of internetgegevens van werknemers vernietigd worden.

Alle bovenstaande wetsartikelen hebben met elkaar gemeen dat ze het bestanddeel wederrechtelijk expliciet in de delictomschrijving hebben staan. Met wederrechtelijkheid wordt bedoeld 'strijd met het recht'. Indien er dus geen rechtvaardigingsgrond aanwezig is voor de handeling zoals die in het wetsartikel staat, is de handeling pas strafbaar. Doordat de artikelen wederrechtelijkheid in het artikel zelf hebben staan, is bij aanwezigheid van een rechtvaardigingsgrond het delict niet gepleegd.<sup>10</sup>

Kijken naar het strafrecht is dan ook niet voldoende. Hiervoor dient het wettelijk kader uitgebreid te worden met de grenzen en bevoegdheden die bestaan op andere rechtsgebieden.

Op het gebied van privaatrecht is het interessant om te kijken naar de regels die de verhouding tussen werkgever en werknemer aankleden. De eerste twee artikelen die in dat geval worden aangehaald in de literatuur, zijn artikel 7:611 en 6:248 Burgerlijk Wetboek (BW).<sup>11</sup>

Artikel 7:611 BW schrijft voor dat de werkgever en de werknemer verplicht zijn om zich als een goed werkgever en een goed werknemer te gedragen. Dat klinkt mooi, maar is weinig concreet. Het zogeheten 'goed werkgeverschap' en het 'goed werknemerschap' wordt verder ingekleurd door artikel 6:248 BW. In laatstgenoemd artikel worden zaken als 'de wet', 'de gewoonte' en, belangrijkste, de 'redelijkheid en billijkheid' als onbedoelde rechtsgevolgen van een overeenkomst aangeduid. In combinatie met het goed werkgeverschap en goed werknemerschap kan er bij een *arbeidsovereenkomst* dus van beide kanten verwacht worden dat er geen buitensporig gedrag plaatsvindt. Kortom, de werkgever speelt niet 24 uur per dag voor Big Brother en de werknemer is niet uren lang pornosites aan het bezoeken.<sup>12</sup>

Deze twee wetsartikelen zorgen enkel voor impliciete grenzen en bieden derhalve in eerste instantie weinig houvast. Wij zullen dadelijk zien dat er in de jurisprudentie wel enige invulling aan deze artikelen is gegeven. Eerst wil ik wijzen op een ander artikel uit het burgerlijk wetboek, namelijk artikel 7:660 BW. Dit artikel stelt dat de 'werknemer verplicht is zich te houden aan de voorschriften omtrent het verrichten van de arbeid, alsmede aan die [voorschriften] welke strekken ter bevordering van de goede orde in de onderneming van de werkgever'. Het artikel geeft verder aan dat deze voorschriften niet per se onderdeel hoeven te zijn van de specifieke arbeidsovereenkomst in kwestie, maar ook onderdeel mogen zijn van algemeen verbindende voorwaarden. Op basis van dit wetsartikel alleen kan een werkgever dus een algemene regeling opstellen die het registreren en monitoren van al het internetgebruik regelt en waarmee werknemers als onderdeel van hun arbeidsovereenkomst instemmen. Het is echter wel raadzaam om bij het opstellen van dergelijke voorschriften de eerder aangehaalde artikelen 7:611 en 6:248 BW in het achterhoofd te houden, in de eerste plaats omdat dergelijke algemeen verbindende voorschriften door de ondernemingsraad goed gekeurd dienen te worden. In artikel 27 lid 1 onder k en l Wet op de ondernemingsraden (WOR) is gesteld dat alle regelingen die gericht zijn op het verwerken van persoonsgegevens (onder k) en regelingen inzake voorzieningen gericht op waarneming of controle van gedrag of prestaties (onder l) door de ondernemingsraad goedgekeurd dienen te worden.<sup>13</sup>

<sup>8</sup> Terstegge 2002, p. 20

<sup>9</sup> Niet in Terstegge 2002, wel in Engelfriet 2008

<sup>10</sup> Kronenberg & De Wilde 2007, p. 42

<sup>11</sup> Van der Ploeg 2007; Pauw 2007

<sup>12</sup> Pauw 2007, p. 169

<sup>13</sup> NB: de correspondentie en het internetgebruik van OR-leden mag niet worden ingezien door de werkgever, op basis

## Paper, Grondslagen van het Recht

Universiteit Utrecht – Rechtsgeleerdheid – Bachelor 1 – Werkgroep - – Ewald Tienkamp (-)  
(Printversie van woensdag 14 januari 2009, 14:34:19, totaal aantal pagina's 9)

Het burgerlijk recht lijkt al met al een prima basis voor het opstellen van een gedragscode binnen een bedrijf om daarmee het registreren van het internetgedrag van werknemers te rechtvaardigen (mits instemming van de ondernemingsraad is gegeven). Dit is echter niet zomaar mogelijk: aan een directe invoering staan grondrechten in de weg. Grondrechten komen in een nationale variant (de Grondwet) en een internationale variant (verdragen). Hoewel daarbuiten ook ongeschreven grondrechten bestaan blijven die hier buiten beschouwing. De internationale behandelen we later. Eerst behandel ik onze eigen Grondwet. In artikel 10 en 13 Grondwet (Gw) staan enkele bepalingen die de mogelijkheid om communicatie te onderscheppen en/of registreren in algemene zin beperken. Let op dat het hier gaat om veel algemenere rechten dan waar we naar op zoek zijn. Op nationaal niveau is het recht van privacy van werknemers namelijk niet expliciet vastgelegd.<sup>14</sup> Artikel 10 Gw draait om de bescherming van de persoonlijke levenssfeer, terwijl artikel 13 Gw het brief- en telefoongeheim waarborgt.<sup>15</sup> Beide artikelen geven aan dat deze grondrechten gelden, behoudens bij de wet te stellen beperkingen. Het belangrijkste in deze zin is artikel 10 lid 2 Gw, waar staat dat de wet regels opstelt ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. De wet die deze regels bevat is de Wet bescherming persoonsgegevens (Wbp). In de Wbp staan meerdere artikelen die voor ons relevant zijn. Deze artikelen stellen uitgebreide voorwaarden aan de verwerking van persoonsgegevens en zullen hier in samenstellingen worden behandeld. Artikel 6 en 7 Wbp geven de eerste beperkingen aan voor de verwerking van gegevens. Artikel 6 schrijft voor dat persoonsgegevens op behoorlijke en zorgvuldige wijze moeten worden verwerkt, waarbij artikel 7 voorschrijft dat verwerking van persoonsgegevens enkel is toegestaan voor 'welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden'. Dit betekent voor ons onderzoek naar de registratie en controle van het internetgebruik van werknemers, dat de werkgever zorg dient te dragen voor waarborgen inzake de zorgvuldigheid waarmee deze gegevens worden verwerkt en dat de werkgever deze gegevens enkel mag opslaan ingeval er een duidelijk omschreven en gerechtvaardigd doel mee is gediend. Onder geldig doel wordt in de literatuur onder andere verstaan bewijs en archivering van berichten, systeem- en netwerkbeveiliging en kosten- en capaciteitsbeheersing.<sup>16</sup> Artikel 8 en 9 Wbp scherpen de voorwaarden voor de verwerking van persoonsgegevens verder aan. Naast vele kortere vereisten, zoals de ondubbelzinnige toestemming van de betrokkene, wordt in literatuur en jurisprudentie uit deze artikelen als belangrijkste de vereisten van proportionaliteit en subsidiariteit gehaald. Het proportionaliteitsvereiste vraagt om evenredigheid tussen het doel van de gegevensverwerking en de inbreuk die de gegevensverwerking maakt op de privacy (in dit geval de privacy van de werknemer). Het subsidiariteitsvereiste verlangt noodzakelijkheid voor het verzamelen van de persoonsgegevens, dus dat er geen enkel ander, beter, goedkoper en met name minder indringend middel voorhanden is om hetzelfde doel te bereiken als ten grondslag ligt aan de wens tot verwerking van persoonsgegevens. De laatste artikelen van de Wbp die we behandelen zijn de artikelen 34 tot en met 36 en artikel 40 van de Wbp. Deze artikelen bevatten regelingen die kunnen worden samengevat onder de noemer van het transparantiebeginsel (met name artikel 35 Wbp).<sup>17</sup> Het transparantiebeginsel behelst het principe dat voor de werknemers duidelijk dient te zijn wat precies wordt geregistreerd en dat de betrokken werknemers bovendien inzicht kunnen krijgen in de over hen verzamelde gegevens. Artikel 36 en 40 geven de werknemer ook het recht om bij of na inzage in de gegevens een verzoek in te dienen ter correctie van deze informatie.

van artikel 17 WOR en het feit dat er geen gezagsrelatie bestaat tussen werkgever en OR-lid (zie ook Meursing, Nugteren & Schumacher 2003, p. 23)

<sup>14</sup> Pauw 2007, p. 169

<sup>15</sup> Aangehaalde literatuur stelt dat artikel 13 ook betrekking heeft op e-mail en overige elektronische communicatie, zo interpreteert ook een kantonrechter te Utrecht (Kantonrechter Utrecht, 16 september 1998, NJ-kort 1998, nr. 83). *Rapport Commissie grondrechten in het digitale tijdperk* stelt echter dat dit niet zonder meer het geval is en beargumenteert dat een herschrijving van artikel 7, 10 en 13 wenselijk is

<sup>16</sup> Pauw 2007, p. 169, als bron aldaar genoemd: C.J. Loonstra en W.A. Zondag, *Arbeidsrechtelijke thema's*, Den Haag: Boom Juridische uitgevers 2004, p. 215

<sup>17</sup> Pauw 2007, p. 170; Terstegge 2002, p. 23

De Wbp scherpt de mogelijkheden aan die 7:660 BW de werkgever biedt en nuanceert de door 6:248 BW vereiste redelijkheid en billijkheid. Een algemeen verbindende bepaling waarin de werkgever het controleren en registreren van het internetgebruik van werknemers vastlegt dient dus te voldoen aan de eisen van zorgvuldigheid (artikel 6 Wbp), doelmatigheid (artikel 7 Wbp), proportionaliteit en subsidiariteit (artikelen 8 en 9 Wbp) en de vereisten van het transparantiebeginsel (artikelen 34-36 en 40 Wbp).

Artikel 28 van de Europese Privacyrichtlijn 95/46/EG voorziet in het bestaan van een onafhankelijke autoriteit die toeziet op de naleving van de privacywetgeving.<sup>18</sup> In Nederland ziet de bedoelde autoriteit toe op de Wbp en is in het leven geroepen onder de naam College bescherming persoonsgegevens (CBP). Het CBP heeft in 2002 een tweede versie uitgebracht van hun rapport *Goed werken in netwerken*.<sup>19</sup> In deze publicatie worden enkele technische zaken uitgelegd die komen kijken bij het controleren van internet- en e-mailgebruik, worden een aantal vuistregels gegeven waar op gelet kan worden bij de genoemde controle en wordt een juridisch kader geschetst.

Naast veel van de bovengenoemde juridische kaders behandelt het rapport ook de reeds aanwezige jurisprudentie. Aangezien het een van de oudere documenten is die voor dit stuk is geraadpleegd, is het een aardige start voor een inventarisatie van de relevante jurisprudentie. Iets meer dan tien uitspraken worden aangehaald, alle van kantonrechters, uit de periode 1998 tot en met 2001. Een algemene lijn valt uit die uitspraken niet te halen.<sup>20</sup> Zo vindt een kantonrechter te Haarlem dat 'in het huidige tijdsgewricht is aanvaard dat er een zekere 'privétisering' van de werkplek optreedt. Dat heeft tot gevolg dat ook een werkgever binnen zekere grenzen heeft te aanvaarden dat er onder werktijd privé-contacten worden onderhouden. Een werkgever behoort de privacy van die contacten te waarborgen'.<sup>21</sup> Ook een uitspraak van een kantonrechter in Utrecht was noemenswaardig, waar de rechter stelde dat artikel 13 Gw (brief- en telefoongeheim) ook betrekking heeft op elektronische communicatie.<sup>22</sup> De meeste uitspraken richten zich echter minder op een eventuele privacyschending van de werkgever, en meer op de vraag of het gedrag van de werknemer wel of niet een ontslag rechtvaardigt. Veelal wordt het ontslag voor bijvoorbeeld veelvuldig pornosites bezoeken gerechtvaardigd geacht door de kantonrechters. Hierbij wordt ook meegewogen of er een gedragscode aanwezig is, maar afwezigheid ervan is niet per definitie reden voor ongeldigheid van het ontslag.<sup>23</sup>

Ook in latere teksten wordt nationale jurisprudentie geanalyseerd. In *Richtlijnen e-mail en internetgebruik door werknemers*, een artikel uit 2003, wordt iets recentere jurisprudentie bekeken, voornamelijk uit de jaren 2001 tot en met 2003.<sup>24</sup> Ook hier enkel uitspraken van kantonrechters en voornamelijk afwegingen over de proportionaliteit van het ontslag van de werknemer ten opzichte van zijn gedrag.

Een derde tekst, waar nog recentere uitspraken zijn bekeken, is *De werkvloer; het 'thuis' van de werknemer?* uit 2007.<sup>25</sup> De daarin geanalyseerde uitspraken komen uit 2004, 2005 en 2007 en zijn opnieuw enkel afkomstig van kantonrechters. Evenals in het artikel *De verslaafde werknemer* uit 2007,<sup>26</sup> wordt de conclusie getrokken dat een vraag over een eventuele privacyschending buiten beschouwing blijft en dat de zaken zich concentreren op de vraag of het gedrag van de werknemer een ontslag rechtvaardigt.<sup>27</sup> Zoals Van der Ploeg opmerkt: '[in] Nederland hebben rechters de neiging om schending van de privacy over het hoofd te zien indien de werkgever bewijs heeft dat de werknemer fout is geweest'.<sup>28</sup>

<sup>18</sup> College bescherming persoonsgegevens, *Over het CBP*, <[http://www.cbprecht.nl/indexen/ind\\_cbp.stm](http://www.cbprecht.nl/indexen/ind_cbp.stm)> (laatst geraadpleegd: 14 december 2008)

<sup>19</sup> Terstegge 2002

<sup>20</sup> Terstegge 2002, p. 29

<sup>21</sup> Kantonrechter Haarlem, 16 juni 2000, Jurisprudentie Arbeidsrecht 2000, 170

<sup>22</sup> Eerder aangehaald in voetnoot: Kantonrechter Utrecht, 16 september 1998, NJ-kort 1998, nr. 83

<sup>23</sup> Terstegge 2002, p. 29

<sup>24</sup> Meursing, Nugteren & Schumacher 2003

<sup>25</sup> Pauw 2007

<sup>26</sup> Van der Ploeg 2007

<sup>27</sup> Pauw 2007, p. 170

<sup>28</sup> Van der Ploeg 2007, p. 16

Een uitspraak van de Hoge Raad, en dan in het speciaal een uitspraak die zich richt op de eventuele rechtmatigheid van de controle en registratie van internetgebruik en e-mailgebruik van werknemers, is er helaas nog niet.<sup>29</sup>

Wat we tot nu toe op nationaal vlak hebben gezien is dat er voor werkgevers de mogelijkheid bestaat om onder de strenge voorwaarden van onder andere de Wbp een gedragscode op te stellen op basis van 7:660 BW, waarin staat dat, hoe en waarom het internetgebruik van werknemers wordt geregistreerd en gecontroleerd.

### **Internationale juridische grenzen**

Om deze nationale regelgeving verder in perspectief te kunnen plaatsen moet nog gekeken worden naar internationale verdragen. Grondrechten als eenieder verbindende bepalingen in internationale verdragen hebben op basis van artikel 93 Gw rechtskracht indien de verdragen door Nederland zijn goedgekeurd (artikel 91 Gw). Artikel 94 Gw bepaalt dat zojuist genoemde bepalingen de nationale bepalingen buiten spel zetten indien ze in strijd met elkaar zijn.

Het belang van dergelijke bepalingen is dan ook groot. Als het gaat om de privacy zijn er twee artikelen van verdragen die ook (gezaghebbende) rechtskracht genieten binnen Nederland, namelijk artikel 8 van het Europees verdrag tot bescherming van de rechten van de mens en fundamentele vrijheden (EVRM) en artikel 17 van het Internationaal verdrag inzake burgerrechten en politieke rechten (IVBPR).

Artikel 8 EVRM bepaalt in het eerste lid dat iedereen recht heeft op 'respect voor zijn privé leven (...) en zijn correspondentie.' Artikel 17 IVBPR op zijn beurt stelt in het eerste lid dat niemand mag worden onderworpen aan 'willekeurige of onwettige inmenging in zijn privé leven (...) en zijn briefwisseling'.

In artikel 8 lid 2 EVRM is aangegeven onder welke voorwaarden een eventuele inperking van de in het eerste lid genoemde rechten is toegelaten. Zo dient een inbreuk op het gegeven respect voor het privéleven 'noodzakelijk in een democratische samenleving' te zijn, 'in het belang van (...) het economisch welzijn van het land, het voorkomen van (...) strafbare feiten, [of ter] bescherming van (...) de goede zeden'.

Dat deze bepalingen van toepassing zijn op de relatie tussen werkgever en werknemer blijkt uit jurisprudentie. In 1992 kwam het Europese Hof voor de Rechten van de Mens (EHRM) met een uitspraak in de zaak Niemitz tegen Duitsland, waar de vraag centraal stond of artikel 8 EVRM ook bescherming bood op de werkplek.<sup>30</sup> Het EHRM bepaalde in deze zaak dat werknemers een 'gerechtvaardigd belang hebben om ook gedurende het uitvoeren van bedrijfsmatige activiteiten relaties met andere mensen aan te kunnen gaan. Een zekere mate van vrijheid om met anderen al dan niet persoonlijk te kunnen communiceren zonder inmenging door de werkgever is in dat kader onontbeerlijk'.<sup>31</sup>

Na het Niemitz arrest was het duidelijk dat werknemers ook op de werkvloer tot op zekere hoogte bescherming genoten van artikel 8 EVRM. Het arrest Halford, waar het EHRM in 1997 uitspraak in deed, bouwde voort op het eerdere arrest van Niemitz. In het Halford arrest draaide het om het opnemen van telefoongesprekken van een werknemer door de werkgever, zonder medeweten van de werknemer in kwestie.<sup>32</sup> Het Europese hof bepaalde hier dat de werknemer een zeker niveau van privacy kon en mocht verwachten, en sprak van een 'reasonable expectation of privacy'. Hier was niet alleen artikel 8 van toepassing op de verhouding tussen werkgever en werknemer, maar ook op privételefoongesprekken die de werknemer met de werktelefoon voert.

Het meest recente en relevante arrest van het EHRM is uit 2007 en draaide om een geschil tussen Copland en het Verenigd Koninkrijk.<sup>33</sup> In deze zaak ging het naast het afluisteren van het telefoonverkeer ook om het controleren van het gebruik van internet en e-mail. Net als in het arrest Halford was de werknemer niet op de hoogte dat ze onderwerp van onderzoek van de werkgever was. Dit heeft het EHRM dan ook meegewogen in haar oordeel. Het EHRM heeft

<sup>29</sup> Pauw 2007, p. 170

<sup>30</sup> EHRM 16 december 1992, NJ 1993, 400

<sup>31</sup> Asscher & Steenbruggen 2001

<sup>32</sup> EHRM, 25 juni 1997, NJ 1998, 506

<sup>33</sup> EHRM, 3 april 2007, JAR 2007, 233

## Paper, Grondslagen van het Recht

Universiteit Utrecht – Rechtsgeleerdheid – Bachelor 1 – Werkgroep - – Ewald Tienkamp (-)  
(Printversie van woensdag 14 januari 2009, 14:34:19, totaal aantal pagina's 9)

geoordeeld dat de telefoongesprekken, e-mails en het internetgebruik vallen onder de begrippen 'privé leven' en 'correspondentie', zoals bedoeld in artikel 8 EVRM. Doordat de werknemer niet op de hoogte was van de controle had ze, evenals de werknemer in het Halford arrest, een redelijke verwachting dat dit gebruik privé zou zijn. Het EHRM beschouwt de inbreuk op het privéleven niet volgens de wet en niet noodzakelijk in een democratische samenleving. De arresten Niemitz, Halford en Copland laten zien dat de privécommunicatie van een werknemer onder werktijd valt onder de bescherming van artikel 8 EVRM. Wat deze zaken echter gemeen hebben is dat bij alle personen de inbreuk op de privacy plaatsvond buiten het medeweten van de werknemer om. Doordat voor de constatering dat er sprake was van een inbreuk het EHRM het niet verwittigen van de werknemer zwaar laat meewegen, kan dan ook gesteld worden dat vanuit de internationale vrijheidsrechten het registreren van internetgebruik niet zomaar verboden is.

### De juridische grenzen

Hierboven is geprobeerd een antwoord te krijgen op de vraag met welk juridisch kader een werkgever te maken heeft, indien hij wenst het internet- en e-mailgebruik van zijn werknemers te registreren en/of controleren. Teneinde hierop een antwoord te geven is gekeken naar het totaal van nationale en internationale juridische beperkingen en voorwaarden.

Op nationaal vlak is allereerst gekeken naar het strafrecht. Hier is geconstateerd dat er verschillende bepalingen bestaan die bijvoorbeeld het 'inbreken op een computer' (computervredebreuk, art. 138a Sr.), het afluisteren van communicatie (artt. 139b en 139c Sr.) en het schenden van het digitaal briefgeheim (art. 273d Sr.) strafbaar stellen. Deze bepalingen geven expliciet aan dat wederrechtelijkheid is vereist voor strafbaarheid. Rechtvaardiging voor het 'schenden' van het digitale briefgeheim wordt ontleend aan het privaatrecht.

Het Burgerlijk Wetboek biedt op basis van artikel 7:660 BW de werkgever de mogelijkheid om algemene regels op te stellen voor het gebruik en de registratie van e-mail- en internetverkeer binnen de organisatie. Deze regels dienen te blijven binnen de grenzen zoals gesteld door het goed werkgeverschap en het goed werknemerschap (art. 7:611 BW) en de redelijkheid en billijkheid (art. 6:248 BW). Ook is voor de rechtskracht van dergelijke algemene regels instemming van de ondernemingsraad nodig (artikel 27 lid 1 onder k en l WOR).

Deze door het civiele recht toegekende mogelijkheden voor de werkgever worden ingeperkt door de in de Grondwet in artikel 10 en 13 neergelegde privacyrechten. Artikel 10 en 13 Gw gelden onder voorbehoud van regels, bij wet gesteld. Deze regels zijn vastgelegd in de Wet bescherming persoonsgegevens. Een algemeen verbindende bepaling waarin de werkgever het controleren en registreren van het internetgebruik van werknemers vastlegt dient op grond van de Wbp te voldoen aan de eisen van zorgvuldigheid (artikel 6 Wbp), doelmatigheid (artikel 7 Wbp), proportionaliteit en subsidiariteit (artikelen 8 en 9 Wbp) en de vereisten van het transparantiebeginsel (artikelen 34-36 en 40 Wbp).

Helaas heeft de Hoge Raad zich nog niet uitgesproken over een eventuele schending van de privacy bij controle van internetgebruik door een werkgever. Lagere rechters lijken tot nu toe vooral te kijken naar de proportionaliteit van een ontslag bij geconstateerd misbruik van de e-mail- of internetfaciliteiten door een werknemer. Een duidelijke uitspraak over de toepassing van de Grondwetsartikelen op de verhouding tussen werknemer en werkgever is (nog) niet te geven.

De internationale verdragen zijn, in ieder geval als het gaat om artikel 8 EVRM (respect voor het privéleven), wel zonder meer van toepassing zijn op de verhouding tussen werknemer en werkgever. Zo blijkt uit het Copland-arrest dat een inbreuk op de privacy van een werknemer door e-mail- en internetgebruik te controleren enkel mogelijk is indien dit noodzakelijk wordt geacht (in een democratische samenleving), volgens de wet plaatsvindt en indien de werknemer op de hoogte is van het (mogelijke) meekijken door de werkgever.

### **Paper, Grondslagen van het Recht**

Universiteit Utrecht – Rechtsgeleerdheid – Bachelor 1 – Werkgroep - – Ewald Tienkamp (-)  
(Printversie van woensdag 14 januari 2009, 14:34:19, totaal aantal pagina's 9)

Per saldo kan gesteld worden dat het door het EHRM geschetste kader overeen komt met het kader dat de Wbp heeft geschetst voor de in de grondwet neergelegde vrijheidsrechten. De in de Wbp gestelde eisen lopen grotendeels parallel met de eisen zoals die voortvloeien uit artikel 8 lid 2 EVRM en de uitspraken van het EHRM in de arresten van Niemitz en Copland. Er kan dan ook geconcludeerd worden dat zowel uit nationaal als internationaal juridisch kader de juridische mogelijkheid is toegekend aan een werkgever om het internet- en e-mailgebruik van de werknemer te controleren en registreren, maar dat hiervoor in het bijzonder rekening moet worden gehouden met de grenzen van het nationale privaatrecht, de uit onze Grondwet voortgekomen Wet bescherming persoonsgegevens en de internationale grondrechten, in het speciaal artikel 8 EVRM.

Ewald Tienkamp  
ewald@tienkamp.nl  
<http://ewald.tienkamp.info>

Ewald Tienkamp  
ewald@tienkamp.nl  
<http://ewald.tienk>

Ewald Tienkamp  
ewald@tienkamp.nl  
<http://ewald.tienkamp.info>

Ewald Tienkamp  
ewald@tienkamp.nl  
<http://ewald.tienk>

Ewald Tienkamp  
ewald@tienkamp.nl  
<http://ewald.tienkamp.info>

Ewald Tienkamp  
ewald@tienkamp.nl  
<http://ewald.tienk>

## Literatuurlijst

- **Ascher & Steenbruggen 2001**  
L.F. Asscher & W.A.M. Steenbruggen, 'Het Emailgeheim op de werkplek', *NJB* 2001-37, p. 1787-1794
- **Costa Baiôa 2008**  
Fleur Costa Baiôa, *Privacy en email op de werkvloer*, 8 september 2008, <http://www.wieringa-advocaten.nl/nlblawg.php?id=1340> (laatst geraadpleegd 19 november 2008)
- **Engelfriet 2008**  
Arnoud Engelfriet, *Internetten en mailen op het werk*, 21 april 2008, <http://www.iusmentis.com/internetten/prive-ophetwerk/> (laatst geraadpleegd op 19 november 2008)
- **Kronenberg & De Wilde 2007**  
M.J. Kronenberg & B. de Wilde, *Grondtrekken van het Nederlandse strafrecht*, Deventer: Kluwer 2007, p. 42
- **Meursing, Nugteren & Schumacher 2003**  
M. Meursing, E. Nugteren & K.I.M. Schumacher, 'Richtlijnen e-mail en internetgebruik door werknemers', *Rechtshulp*, nr. 10, 2003, p. 23-28
- **Pauw 2007**  
D.E. Pauw, 'De werkvloer; het "thuis" van de werknemer?', *Praktisch procederen*, nr. 6, dec. 2007, p. 168-171
- **Van der Ploeg 2007**  
A. van der Ploeg, 'De verslaafde werknemer', *Arbeid Integraal*, nr. 4, 2007, p. 5-25
- **Terstegge 2002**  
J.H.J. Terstegge, *Goed werken in netwerken*, Den Haag: College bescherming persoonsgegevens 2002
- **Zwenne e.a. 2007**  
Gerrit-Jan Zwenne e.a., *Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek en knelpuntenanalyse*, WODC/Ministerie van Justitie 2007