

ELEKTRONIESE MONITERING IN DIE INDIENSNEMINGSKONTEKS

Anél Bezuidenhout

11927852

Skripsie voorgelê ter gedeeltelike nakoming vir die vereistes vir die
graad *Magister Legum* in Arbeidsreg aan die Noordwes-Universiteit
(Potchefstroom Kampus)

Studieleier: PH Myburgh

Modules suksesvol voltooi

LLMA 874;LLMA 875

LLMA 876;LLMA 878

Potchefstroom

November 2004

INHOUDSOPGAW

INLEIDING	3
HOOFSTUK 1 DIE REG OP PRIVAATHEID	6
1.1 Privaatheid in die Gemenereg.....	6
1.2 Die Grondwet van die Republiek van Suid-Afrika 108 van 1996.....	7
1.2.1 Omvang van die Reg op Privaatheid	9
1.2.2 Die Doel van die Reg op Privaatheid	11
1.2.3 Beperking van 'n Fundamentele Reg.....	14
HOOFSTUK 2 IN DIE INDIENSNEMINGSKONTEKS.....	16
2.1 Die Leerstuk van Regmatige Verwagting	16
2.2 Die Omvang van die Werknemer se Reg op Privaatheid	18
2.3 Definisie en Doel van Elektroniese Monitering.....	21
2.4 Gevolge van Monitering op die Werknemer	24
HOOFSTUK 3 WETGEWING VAN TOEPASSING	27
3.1 Suid-Afrikaanse Wetgewing.....	27
3.1.1 Wet op Beheer van die Onderskepping van Kommunikasie.....	27
3.1.1.1 Algemene Bepalings en Uitsluitings	27
3.1.1.2 In die Loop van die Uitvoer van Besigheid	29
3.1.1.3 Nie-Nakoming van die Bepalings	31
3.1.2 Wet op die Verbieding van Onderskepping en Monitering.....	34
3.1.3 Wet op Bevordering van Toegang tot Inligting.....	34
3.2 Die Internasionale Arbeidsorganisasie	35
3.3 Internasionale Wetgewing	36
3.3.1 Relevansie.....	36
3.3.2 Die Verenigde State van Amerika	36
3.3.3 Die Verenigde Koninkryk	40
3.3.4 Europese Unie.....	42
3.3.5 Kanada	43
HOOFSTUK 4 KONKLUSIE	46
4.1 Konklusie	46
4.2 Aanbevelings	48
BIBLIOGRAFIE	52

'...if you walked into a store, and the guard at the store recorded your name; if cameras tracked your every step, noting what items you looked at and what items you ignored; if an employee followed you around, calculating the time you spent in any given aisle; if before you could purchase an item you selected, the cashier demanded that you reveal who you were - if any or all of these things happened in real space, you would notice...

In cyberspace you would not.'

There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live - did live, from habit that became instinct - in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.

- George Orwell, 1984

New technologies are putting employees under constant surveillance, removing supervision from the hands of managers trained to observe and counsel employees and giving it to electronic gadgetry. Without some reasonable control, we risk turning workplaces into electronic sweatshops.

- Bruce Phillips, Privacy Commissioner

INLEIDING

In die laat negentiende eeu het privaatheid hoofsaaklik verwys na die onregmatige betreding van 'n persoon se eiendom, of persoonlike ruimte, soos 'n hotelkamer of skeepskajuit. Teen die middel van die twintigste eeu is die begrip uitgebrei om ook persoonlike en familie-aangeleenthede, soos gesondheid en gesinsbeplanning, in te sluit. Teen die einde van die twintigste eeu is die konsep, met die bekendstelling van die rekenaar, deelgemaak van die tegnologiese inligtingsera.¹

Die ontwikkeling van die Internet tot 'n alledaagse verskynsel, in onder andere huishoudings, besighede, maatskappye en die staat, het daartoe gelei dat die individu se reg op privaatheid beperk word. Tegnologiese vooruitgang het tot gevolg gehad dat die individu se vermoë om toegang tot sy of haar persoonlike inligting, sowel as elektroniese kommunikasie, te beheer min of geen is.

In die indiensnemingskonteks impliseer monitering dat die werkgever die werksverrigting van die werknemer monitor en beteken elektroniese monitering dat die elektroniese media waarvan die werknemer gebruik maak, insluitend e-pos en Internet, deur die werkgever gemonitor word.² Die werkgever het toegang tot die werknemer se elektroniese media en is instaat om werknemers te monitor sonder dat hul daarvan kennis dra.

Die reg op privaatheid het hoofsaaklik beskerming van 'n persoon se liggaam, persoonlike ruimtes en verhoudings ten doel. Die vraag is of die monitering van gestoorde inligting, e-pos boodskappe en ander kommunikasie binne die omvang van hierdie reg val.

¹ Bynum & Rogerson *Computer Ethics and Professional Responsibility* 2004 Blackwell Publishing Ltd.

² A. Rogers *You Got Mail But Your Employer Does Too: Electronic Communication and Privacy in the 21st Century Workplace* 5 J Tech L & POL'Y 1 (2000).

Verder moet in gedagte gehou word dat geen reg absoluut is nie en beperk kan word ingevolge die beperkingsklousule in die *Grondwet van die Republiek van Suid-Afrika*³. Sou die reg op privaatheid wel binne hierdie verhouding bestaan, is die vraag of monitering deur 'n werkgewer sodanig 'n regmatige beperking van hierdie reg is.

Die reg op privaatheid het verder ook 'n inherente beperking genaamd die leerstuk van regmatige verwagting. Volgens hierdie leerstuk vind die reg op privaatheid slegs toepassing in die mate waarin 'n persoon 'n redelike en regmatige verwagting tot privaatheid het. Die werkgewer voorsien in die loop van diens aan die werknemer die toepaslike toerusting en argumenteer dus dat dit wel 'n regmatige beperking van die reg op privaatheid impliseer. Die werknemer in die indiensnemingsverhouding het, volgens die werkgewer, nie redelikerwys die verwagting tot privaatheid nie. Die verwagting bestaan egter by werknemers dat hul elektroniese kommunikasie privaat is en beskou gevolglik monitering as 'n onaanvaarbare inbreukmaking op hul reg op privaatheid.⁴

Die bespreking wat volg sal die posisie van privaatheid in die Gemeenereg, die Grondwet en ander Suid-Afrikaanse wetgewing, sowel as relevante internasionale wetgewing, volledig uiteensit. Die werkgewer se posisie met betrekking tot die beskerming van sy of haar eiendom word van nader beskou. Daar is dus duidelik twee definitiewe en teenstrydige regte. Vir die werknemer is monitering 'n inbreukmaking op sy of haar privaatheid. Die werkgewer, as verskaffer en eienaar van die rekenaarnetwerk, is geregtig om elektroniese media van die werknemer, in die loop van diens, te monitor. Hierdie teenstrydige belang van die werknemer en die werkgewer het die potensiaal om wantroue in die werksverhouding te skep en 'n verlaging in moraal en produktiwiteit teweeg te bring.

³ 108 van 1996. Hierna na verwys as die Grondwet.

⁴ Han H Li *Electronic Mail Privacy in the Workplace* Mailto: hali@lynx.neu.edu.

Die vraag is tot watter mate die werknemer se reg op privaatheid, met betrekking tot die bogenoemde, beskerm word in die lig van die werkgewer se regmatige beperking daarvan, sowel as die mate waarin die leerstuk op regmatige verwagting 'n rol daarin speel.

Die Suid-Afrikaanse reg poog om beide hierdie regte te beskerm en word die belang van die werknemer en die werkgewer teen mekaar opgeweeg. Uit hoofde van internasionale wetgewing en regspraak is dit duidelik dat die omvang van die reg op privaatheid deur interpretasie bepaal word. Riglyne hieruit is vir interpretasie van die Suid-Afrikaanse reg op privaatheid van kardinale belang.

Ten slotte word die implementering van 'n duidelike en volledige beleid, ten aansien van die reg op privaatheid tussen werknemer en werkgewer, aanbeveel. Hierdie beleid sal die balansering van die werknemer en werkgewer se konflikterende belang, met minimale spanning en optimale produktiwiteit, moontlik maak.

HOOFSTUK 1 DIE REG OP PRIVAATHEID

1.1 Privaatheid in die Gemeenereg

Die Grondwet bepaal in artikel 8(3) dat 'n hof die gemeenereg moet toepas, of ontwikkel, in die mate waarin wetgewing nie aan daardie reg gevolg gee nie. Hierdie subartikel is van toepassing op regte vervat in die Handves en sluit dus die reg op privaatheid in.

Inbreukmaking op 'n persoon se privaatheid, ingevolge die gemeenereg, is 'n *iniuria*. Privaatheid word geag 'n onafhanklike persoonlikheidsreg te wees en 'n belangrike komponent van 'n persoon se waardigheid of *dignitas*.⁵ Ingevolge *Financial Mail v Sage Holdings*⁶ sluit dit die onregmatige betreding van 'n persoon se persoonlike privaatheid of die onregmatige openbaarmaking van persoonlike inligting in. Onregmatige openbaarmaking geskied wanneer 'n persoon van 'n ander se persoonlike aangeleenthede te wete kom of dit publiseer.⁷

Daar bestaan geen objektiewe toets aan die hand waarvan bepaal kan word watter persoonlike aangeleenthede beskerming geniet nie.⁸ Volgens die Konstitusionele Hof, in die *Financial Mail*-saak, word die onregmatigheid van inbreukmaking beoordeel aan die hand van *boni mores* en die gemeenskapsopvatting van geregtigheid. Laasgenoemde word bepaal deur die hof wat die betrokke aangeleentheid aanhoor. In *Bernstein v Bester NO*⁹ word die betreding van 'n privaatwoning, die lees van privaat dokumente, afluister van privaat gesprekke en die openbaarmaking van inligting, op onregmatige wyse verkry, ingesluit onder die gemeenereg as 'n skending van privaatheid. Volgens die

⁵ De Waal et al *Bill of Rights Handbook* 4th ed 2001 (Juta).

⁶ 1993 (2) SA 451 (A).

⁷ J Neethling et al *Neethling's Law of Personality* 1995.

⁸ J Hofman *E-commerce and Issues in the Law of Privacy* UCT April/June 2000.

⁹ 1996 (2) SA 751 (CC).

Konstitusionele Hof moet vasgestel word of die inbreukmaking onregmatig is en indien wel, of 'n regverdigingsgrond vir die inbreukmaking bestaan. Die Hof wend dus 'n tweeledige toets aan wat voorkeur geniet in terme van die Grondwet en waarsku teen die gebruik van gemeenregtelike beginsels om 'n fundamentele reg te interpreteer.¹⁰

Die skrywer is van mening dat die reg op privaatheid duidelik deur die Gemeenereg erken en beskerm word, hoewel die fundamentele reg hier ter sprake, nie aan die hand van gemeenregtelike beginsels geïnterpreteer moet word nie. Die rede hiervoor is dat geen objektiewe toets ingevolge die Gemeenereg bestaan, aan die hand waarvan inbreukmaking (of die mate waarin dit geskied), bepaal kan word nie.

1.2 Die Grondwet van die Republiek van Suid-Afrika 108 van 1996¹¹

Artikel 8(1) van die Grondwet bepaal dat die Handves van Regte van toepassing is op die totale reg. Die Handves bind wetgewende, uitvoerende en regsprekende gesag, sowel as alle staatsorgane. Artikel 8(2) bind 'n natuurlike of regspersoon, hoewel slegs in die mate waarin dit toepasbaar is met die aard van die betrokke reg en enige plig deur die reg opgelê. Dit is dus duidelik dat die reg op privaatheid vertikaal, sowel as horisontaal, toepassing vind en gevolglik die partye in die indiensnemingsverhouding, horisontaal, bind. Die werknemer kan dus aanspraak maak op 'n reg op privaatheid en die omvang van hierdie reg word gevolglik bespreek.

Artikel 14 van die Grondwet:

Elkeen het die reg op privaatheid, waarby inbegrepe is die reg dat –

- (a) hul persoon of woning nie deursoek word nie;
- (b) hul eiendom nie deursoek word nie;
- (c) daar nie op hul besittings beslag gelê word nie; of

¹⁰ Bernstein v Bester, verwys na par.1.2.

¹¹ Hierna genoem die Grondwet.

(d) daar nie op die privaatheid van hul kommunikasies inbreuk gemaak word nie.

Die eerste gedeelte van hierdie artikel waarborg 'n algemene reg op privaatheid, wat uitgebrei kan word na 'n persoon se persoonlike ruimtes in die algemeen. Die tweede gedeelte van die artikel bied beskerming teen spesifieke vorme van inbreukmaking op die reg. In die VSA word die algemene reg op privaatheid in die Grondwet se *Veertiende Wysiging* vervat, terwyl die *Vierde Wysiging* spesifieke areas beskerm. In Duitsland vervat artikel 2 van die *Basiese reg* die algemene klousule en artikel 10 waarborg uitdruklik die privaatheid van pos en telekommunikasie. In die Suid-Afrikaanse Grondwet vorm die spesifieke beskermingsareas deel van die algemene reg op privaatheid.¹² Die privaatheid van pos en telekommunikasie word dus onder die algemene reg op privaatheid tuisgebring. Ingevolge *Director of Public Prosecutions: Cape of Good Hope v Buthgate*¹³ is aangeleenthede, met betrekking tot die onderskepping van kommunikasie, gewoonlik 'n inbreukmaking op 'n persoon se privaatheid. Daar moet egter in gedagte gehou word dat die reg op privaatheid slegs inwerking tree, indien op die algemene reg (op privaatheid) inbreuk gemaak word en vind nie toepassing ten einde individue teen deursoeking, beslaglegging of die onderskepping van kommunikasie, te beskerm nie.

Die Konstitusionele Hof se tweeledige toets in *Bernstein v Bester*¹⁴, soos na verwys, moet toegepas word ten einde te bepaal of inbreukmaking plaasgevind het. Ten eerste moet die omvang van die reg op privaatheid oorweeg word en indien wel, of die inbreukmaking regverdigbaar is ooreenkomstig die beperkingsklousule.

¹² De Waal et al *Bill of Rights Handbook* 4th ed 2001 (Juta).

¹³ 2000 (2) SA 535 (C).

¹⁴ NNO 1996 (4) BCLR 449 (CC); 1996 (2) SA 751 (CC).

1.2.1 Omvang van die Reg op Privaatheid

Die Konstitusionele Hof verklaar in die *Bernstein*-saak¹⁵ dat die reg op privaatheid toepassing vind in die verhouding tussen werkgewer en werknemer, maar soos enige ander fundamentele reg, nie absoluut is nie. Die rede daarvoor is dat die interpretasie van een persoon se reg beperk word deur die reg van 'n ander persoon. Ten aansien van privaatheid, beteken dit dat die binnekring van 'n persoon, soos familielewe, seksuele voorkeur en huisomgewing beskerm word teen konflikterende regte van die gemeenskap. Die gemeenskapsbelang bedreig die individu se reg op privaatheid, ten einde sosiale aktiwiteite en ekonomiese belang van die gemeenskap te bevorder. Privaatheid in die persoonlike sfeer word dus erken en beskerm, maar na mate 'n persoon betrokke raak in die gemeenskap se aktiwiteite, soos die besigheids- en sosiale sfeer, word die omvang van die persoonlike sfeer ooreenkomstig beperk.

In *Mistry v Interim Medical and Dental Council of South Africa*¹⁶ beslis die Konstitusionele Hof, in verband met ondernemings, hoe meer openbaar 'n onderneming is en hoe strenger gereguleer, hoe minder ernstig enige moontlike inbreukmaking. Die Hof voeg by dat, met betrekking tot die perseël, toerusting, material en dokumente, 'n persoon se verwagting tot privaatheid aangepas moet word by die nakoming van redelike regulasies en die verdra van administratiewe inspeksies, wat 'n onlosmaaklike komponent is van die effektiewe regulasiesisteem van enige besigheid. Die Konstitusionele Hof verwys ook na 'n Kanadese Uitspraak, *Thompson Newspapers Ltd v Canada (Director of Investigation and Research, Restrictive Trade Practises Commission)*.¹⁷ Volgens die Hof kan die verwagte mate van privaatheid aansienlik varieer, afhangend van die individu se betrokkenheid by die staat. Dit

¹⁵ Supra vn 14.

¹⁶ 1998 (4) SA 1127 (CC).

¹⁷ (1990) 47 CRR 1.

word algemeen aanvaar dat die individu se aktiwiteite tot 'n mindere of meerdere mate deur die staat gereguleer word en sodoende verseker dat die individu se belang, met die gesamentlike doelwitte van die gemeenskap, versoenbaar is. Dit kan die inspeksie van praatpersele en dokumente tot gevolg hê.

In *Shelton v Commissioner for the South African Revenue Stamps*¹⁸ beslis die Landdroshof dat die reg op privaatheid nie toepassing vind in die besigheidsfeer nie. Die uitspraak is, opgeweeg teen uitsprake van die Konstitusionele Hof nie korrek nie en vind, soos reeds bespreek in paragraaf 1.2, in enige horisontale verhouding toepassing.

Die Constitutional Hof noem *obiter dicta* in *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors*¹⁹ dat die reg op privaatheid inwerking tree waar 'n persoon die vermoë het om te besluit wat hy of sy aan die publiek wil openbaar en die redelike verwagting het dat die besluit gerespekteer sal word. Die omvang van hierdie reg strek dus egter slegs sover 'n regmatige verwagting tot privaatheid bestaan.²⁰ Hierdie is dan die leerstuk van regmatige verwagting en word later in die hoofstuk bespreek.

Met verwysing na die *Mistry*-saak²¹ word regulering van 'n onderneming en 'n vermindering van 'n persoon se verwagting tot privaatheid, verkry vanuit 'n gesagsposisie tussen die staat en sy burgers. Die reg op privaatheid, in die vertikale verhouding, word beperk vir 'n gemeenskaplike doel. Die Handves van Regte bind, ingevolge artikel 8(2), individue in die vertikale, sowel as die horisontale, verhouding. Die gevolgtrekking kan dus gemaak word dat die werkgewer, vanuit die

¹⁸ 2000 (2) SA 106 (E).

¹⁹ 2000 (10) BCLR 1079 (CC).

²⁰ 'n Regmatige verwagting volgens die hof, ingevolge die *Bernstein*-saak, beteken dat 'n persoon 'n subjektiewe verwagting moet hê, ten aansien van privaatheid, wat deur die gemeenskap as objektief redelik erken word.

²¹ *Supra* vn 16.

horisontale verhouding, op die uitvoer van soortgelyke inspeksies geregtig is ten einde effektiewe regulering, ook in sy of haar onderneming, te bewerkstellig.

1.2.2 *Die Doel van die Reg op Privaatheid*

Die reg op privaatheid het 'n drieledige doel. Daar moet in gedagte gehou word dat die individu se subjektiewe verwagting van privaatheid beoordeel word aan die hand van wat die gemeenskap, objektief as redelik beskou.

Die eerste oogmerk van die reg op privaatheid is die beskerming van 'n persoon se liggaam, persoonlike ruimtes en verhoudings. Ten tweede is die beskerming van die geleentheid tot ontwikkeling van 'n persoon se persoonlikheid, met betrekking tot self-realisasie en vervulling. Laastens om die vermoë van die individu, met betrekking tot die beheer en gebruik van persoonlike inligting, te beskerm.

Ten einde die eerste oogmerk te illustreer, word na die *Bernstein-saak*²² verwys. Die grondwetlikheid van artikel 417 en 418 van die *Wet op Maatskappye*²³ is in hierdie aangeleentheid oorweeg. Die Konstitusionele Hof beslis dat inligting in 'n individu se besit nie beskerm word teen openbaarmaking daarvan, indien openbaarmaking deur die Wet vereis word nie. Verder word ook vereis dat die openbaarmaking van sodanige inligting tot finansiële voordeel en behoorlike likwidasië van die maatskappy sal lei.²⁴ Die beperking van 'n persoon se reg op privaatheid word dus, volgens die skrywer, nie ten koste van reg en geregtigheid beskerm nie en word dit in hierdie betrokke aangeleentheid deur die Hof beskou as 'n regmatige beperking van die reg op privaatheid.

²² Supra vn 14.

²³ 69 van 1973.

²⁴ De Waal et al *Bill of Rights Handbook* 4th ed 2001 (Juta).

Die tweede oogmerk word uitdruklik deur die Duitse Grondwet, as 'n algemene reg op privaatheid, beskerm. Die geleentheid tot die ontwikkeling van 'n persoon se persoonlikheid verleen aan individue die bevoegdheid om te handel soos dit hul behaag, sonder inmenging. Die geleentheid tot ontwikkeling van 'n persoon se persoonlikheid word nie deur die Suid-Afrikaanse Grondwet, tot so 'n mate erken nie.²⁵ Volgens die *Bernstein*-uitspraak, met verwysing na die Europese reg, word slegs die individu se reg om verhoudings met ander individue te vestig en instand te hou ter vervulling van die individu se persoonlikheid, onder die privaatheidskonsep ingesluit. Die uitspraak in *National Coalition for Gay and Lesbian Equality v Minister of Justice*²⁶ van die Konstitusionele Hof bevestig bogenoemde uitspraak en verklaar dat elke individu die reg het tot 'n private persoonlike sfeer. Dit beteken dat elke individu in SA die reg het om verhoudings te vestig en instand te hou, sonder inmenging van die gemeenskap. Die werknemer se gebruik van elektroniese en ander kommunikasiemediums van die werkgever kan onder hierdie oogmerk tuisgebring word. Die opweeg van belange, soos na verwys, is hier van toepassing. Die doel van die werknemer in die besigheid van die werkgever is hier ter sprake en is dit nie die vestiging en instandhouding van verhoudings nie, maar wel die lewering van 'n diens.

Die waarborg rakende beheer oor persoonlike inligting, as derde oogmerk van die reg op privaatheid, hou verband met die beskerming van die inherente reg op menswaardigheid, soos verkry uit die Gemeenereg en vervat in die Grondwet.²⁷ Die waarborg word egter beskerm ongeag of die moontlikheid bestaan dat inligting, indien openbaar gemaak, die individu se menswaardigheid kan skend. Monitering van 'n werknemer se kommunikasie, van watter aard ook al,

²⁵ *Ferreira v Levin* 1996 (1) SA 984 (CC).

²⁶ 1999 (1) SA 6 (CC).

²⁷ Artikel 10.

impliseer dat die werknemer minder beheer ten aansien van persoonlike inligting het. Hierdie oogmerk is egter eerder op die vertikale verhouding gerig en sal die fokus vir doeleindes van die bespreking op die eerste en tweede oogmerke rus. Die vraag is dan of die monitering van gestoorde inligting, e-pos boodskappe en ander kommunikasie inbreukmaak op 'n werknemer se persoonlike ruimtes en verhoudings.

Met betrekking tot siviele aangeleenthede, argumenteer die respondent in *Protea Technology & another v Wainer & others*²⁸ dat telefoongesprekke wat onregmatig onderskep is, nie toelaatbare getuienis is nie. Die respondent argumenteer dat dit instryd is met die bepalings van die *Verbod op Monitering en Onderskepping*²⁹ omdat geen persoon geregtig is op die opsetlike onderskepping van 'n telefoongesprek tensy 'n hofbevel daartoe uitgereik is of enige van die partye tot die gesprek daarvan kennis dra en toestemming daartoe verleen het nie. Die Hof bevind dat die Wet nie uitdruklik of by implikasie aandui dat onderskepping, teenstrydig met die Wet, ontoelaatbare getuienis is nie en dus nie alleenlik op grond daarvan uitgesluit kan word nie.³⁰

Tweedens argumenteer die respondent dat die onderskepping van 'n telefoongesprek inbreukmaak op sy fundamentele reg op privaatheid.³¹ Die Hof bevind dat die werknemer, binne die indiensnemingskonteks, daarop geregtig is om privaat telefoonoproepe te ontvang en te maak en

²⁸ 1997 (9) BCLR 1225 (W).

²⁹ Interception and Monitoring Prohibition Act 127 of 1992. Hiema na verwys as IMPA.

³⁰ Volgens *Karuma v R* 1955 AC 197, 1955 1 All ER 236, met betrekking tot die strafproses, huldig die Engelse reg die standpunt dat die onregmatige of onbehoorlike bekom van getuienis, nie toelaatbaarheid affekteer nie. Die toets wat aangewend word om vas te stel of getuienis toelaatbaar is, is die relevantheid daarvan gesien in die lig van die aangeleentheid. Sou hierdie getuienis dus toelaatbaar wees, word geen oorweging geskenk aan die wyse waarop dit verkry is nie. Hierdie uitgangspunt is bevestig in *R v Sang* 1979 2 All ER 1222 (HL).

³¹ Artikel 14(d).

dat 'n regmatige verwagting tot privaatheid wel met betrekking daartoe bestaan. Die Hof noem verder dat, in so 'n mate as wat dit aangeleenthede van werkgewer raak, die werkgewer geregtig is op volledige rekenskap van die werknemer. Dus verloor die werknemer sy of haar reg op privaatheid sodra hy/sy oorgaan van die persoonlike sfeer na die werkgewer se besigheidsfeer. Die werkgewer is daarop geregtig om kennis te dra van die wyse waarop (en die werk waarmee) die werknemer hom- of haarself besig hou, ongeag van die metode waarop inligting in hierdie verband ingewin word. Hierdie beperking van die individu se reg op privaatheid moet egter onder die beperkingsklousule, in artikel 36 van die Grondwet, tuisgebring word alvorens dit as regmatig beskou kan word.

1.2.3 Beperking van 'n Fundamentele Reg

Geen reg, soos reeds gesien, is absoluut nie. Hierdie beperking, ingevolge artikel 36 van die Grondwet, moet redelik en regverdigbaar wees in 'n oop en demokratiese samelewing gebasseer op menswaardigheid, gelykheid en vryheid. Behalwe hierdie vereiste, word ook vereis dat die beperking algemeen toegepas word. Daar kan dus op grond van artikel 36 op 'n fundamentele reg inbreuk gemaak word mits die rede vir die inbreukmaking deur die konstitusionele demokrasie as regmatig beskou word. Volgens artikel 36 word vyf faktore oorweeg om te bepaal of 'n inbreukmaking regmatig is: (a) die aard van die reg; (b) die belangrikheid van die doel van die beperking; (c) die aard en omvang van die beperking; (d) die verband tussen die beperking en die doel; en (e) of minder beperkende alternatiewe dieselfde doel sou bereik.

In *Moonsamy v The Mailhouse*³² bevind die CCMA dat beleid, praktyk en regmatige regulasies binne 'n besigheid, die verwagting ten aansien van privaatheid kan verminder in persoonlike spasies soos kantore,

³² (1999) 20 ILJ 464 (CCMA).

lessenaars en liaseerkabinette. Verder is dit duidelik dat privaat kommunikasie van werknemers groter beskerming geniet as kommunikasie ten bate van 'n besigheid. In die laasgenoemde geval het die werkgewer, as eienaar van die besigheid, 'n reg op toegang tot die kommunikasie van die werknemer.

Die mate waarin privaatheid beperk kan word is egter onseker en behalwe die beperkingsklousule bevat die reg ook 'n inherente beperking, soos uit die bogenoemde blyk. Dit staan bekend as die leerstuk van regmatige verwagting. Volgens hierdie leerstuk vind die reg op privaatheid slegs toepassing in die mate waarin 'n persoon 'n redelike en regmatige verwagting daartoe het. Dus, hoe minder privaatheid 'n werknemer, in 'n betrokke indiensnemingverhouding, regmatig kan verwag, hoe minder aanspraak kan op privaatheid gemaak word. Hierdie leerstuk word in die volgende hoofstuk in meer besonderheid bepreek.

HOOFSTUK 2 IN DIE INDIENSNEMINGSKONTEKS

2.1 Die Leerstuk van Regmatige Verwagting

Die werknemer se uitsluitlike doel is die bevordering van die werkgewer se belang. Ten einde die werknemer hierin by te staan verskaf die werkgewer die toerusting wat die werknemer benodig. In die huidige konteks is dit, normaalweg, onder andere 'n rekenaar en toegang tot die Internet. Die bedoeling van die werkgewer is duidelik. Die toerusting word verskaf sodat die werknemer dit in die loop van besigheid kan gebruik en is die werkgewer gevolglik geregtig om die gebruik van hierdie toerusting te beperk, so ook die wyse waarop hierdie toerusting gebruik word, te gebied en te kontroleer.³³

Die verwagting bestaan wel by die werknemer dat toerusting soos die rekenaar, telefoon en selfs ander kantoortoerusting privaat is. Hierdie persepsie bestaan omdat die werknemer dit as sy/haar persoonlike (private) ruimte en belange ag.

Volgens *Neethling*³⁴ geniet elektroniese kommunikasie, soos e-pos, teoreties dieselfde beskerming as 'n poskaart. Dus dat die boodskap gelees kan word deur enige individu wat tydens die versendingproses daartoe toegang het. Dit strook egter nie met die bedoeling van die sender of die ontvanger nie. In *Protea Technology & Another v Weiner & Others*³⁵ beslis die Arbeidshof dat 'n werknemer sy reg op privaatheid prysgee, sodra hy betrokke raak in die werkgewer se besigheid. Die Hof verwys in die uitspraak ook na die *Huundai*-saak³⁶ wat bepaal dat die reg

³³ www.mlaw.co.za. *The Law Regarding Privacy*.

³⁴ Voetnoot 7.

³⁵ 1997 (9) BCLR 1225 (W).

³⁶ Supra 18.

op privaatheid slegs toepassing vind in die mate waarin 'n regmatige verwagting daartoe bestaan. Sou 'n reg op privaatheid nie in terme van e-pos of die Internet erken word nie, moet 'n redelike verwagting tot privaatheid ten minste erken word. Ter bevestiging is onlangs in Kanada³⁷ beslis dat 'n redelike verwagting tot privaatheid, met betrekking tot e-pos, wel bestaan. Die uitspraak kan op enige kommunikasiemedium van toepassing gemaak word.

Dit is duidelik dat die werkgever, met inagneming van die werknemer se fundamentele reg op privaatheid, moet waak teen onregmatige onderskepping en monitering van elektroniese media en telefoongesprekke. Indien die werkgever wel die verwagting van privaatheid geskep het, is dit onvermydelik dat artikel 14³⁸ toepassing sal vind en is die beperking daarvan nie regverdigbaar ingevolge artikel 36 nie.

Elke aangeleentheid word agter steeds op eie meriete, na gelang van diskresie bepaal. In die *Protea*-uitspraak word hierna verwys as die balansering van belange. Aan die een kant is die belang van die werkgever om sy of haar eiendom te beskerm en die bestuur daarvan te reguleer en aan die ander kant, die beskerming en afdwinging van die werknemer se fundamentele reg.

Die Konstitusionele Hof bevestig, in die *Bernstein*-saak, dat die reg op privaatheid slegs toepassing vind in die mate waarin 'n regmatige verwagting daartoe bestaan. Dit is dan ook die toets wat aangewend word om te bepaal of inbreukmaking van die betrokke reg plaasgeving het en bestaan ingevolge die *Protea-Technology*-saak uit subjektiewe en objektiewe faktore. Eerstens moet die werknemer 'n subjektiewe verwagting tot privaatheid hê en tweedens moet die subjektiewe verwagting objektief deur die gemeenskap as billik beskou word.

³⁷ *R v Weir* (1998) AJ No 155.

³⁸ Van die Grondwet.

Volgens Mischke³⁹ is dit onmoontlik om 'n regmatige verwagting ten aansien van privaatheid aan elektroniese kommunikasie te heg. Vanuit 'n tegnologiese oogpunt verskil e-pos kommunikasie aansienlik van die telefoon, wat direk met 'n geslote lyn verbind word. E-pos word opgebreek in ongeveer 1500 karakters en elke karakter word individueel versend. Gedeeltes van 'n boodskap kan dus binne 'n netwerk verlore raak of onderskep word op enige stadium tydens versending. 'n Derde persoon kan met behulp van toepaslike sagteware toegang verkry tot alle e-pos wat deur 'n netwerk gaan. Werknemers is nie bewus van hierdie proses nie.

2.2 Die Omvang van die Werknemer se Reg op Privaatheid

Elektroniese kommunikasie is 'n effektiewe, doeltreffende en lae koste besigheidshulpmiddel wat ontwerp is om kommunikasie te bevorder. Kommunikasie is 'n kardinale komponent van bemarking. Daar word van werknemers vereis om goeie verhoudings met kliënte te bou en sluit dit dus 'n mate van sosialisering in. Elektroniese kommunikasie is 'n effektiewe kanaal waardeur kliënte op informele basis bereik word. Privaat telefoonoproepe of e-pos word binne redelike perke as algemene praktyk aanvaar⁴⁰ en gee aan die werknemer die geleentheid om verhoudings met ander individue te vestig en instand te hou.⁴¹ Die tweede oogmerk van die reg op privaatheid word hierdeur aangespreek.

Die mees relevante en regmatige besigheidsredes, op grond waarvan 'n werkgever toegang tot privaat elektroniese kommunikasie en persoonlike inligting van 'n werknemer kan vereis, is die volgende:

³⁹ C Mischke *Workplace Privacy, e-mail interception and the law: Does new legislation limit employers' rights to read e-mail?* Contemporary Labour Law Vol 12, No 8, Mrt 2003.

⁴⁰ www.deneysreitz.co.za. *Insurance Seminar – Aug/Sept 2001: The Internet – An Employees Right to Privacy* News 2001.

⁴¹ Verwys na par. 1.2.2.

(a) wangedrag wat dissiplinêre optrede vereis; (b) verlening van bystand ten aansien van prestasie of bevoegdheid; (c) Moniteringsisteme wat die werknemer se aktiwiteite monitor; (d) belastingdoeleindes; (e) sosiale sekerheid; (f) opleiding; en (g) kollektiewe bedinging.⁴²

Hierdie aantal wyses van inbreukmaking op 'n persoon se privaatheid is meer subtiel as: (a) die fisiese deursoeking van 'n werknemer se liggaam wanneer hy of sy die kantoor verlaat, (b) die installering van observasiekameras, (c) die deursoeking van 'n werknemer se kantoorspasie ensomeer, maar verskil nie in essensie nie. Die misbruik van e-pos en Internet-fasiliteite wat deur die werkgever verskaf word, word beskou as wangedrag en hou gevolge in vir die werknemer wat gemonitor word. Gevolge soos dissiplinêre optrede en selfs ontslag. Dit sal uit die bespreking blyk dat howe in die VSA die rekenaar beskou as deel van die werksarea⁴³ en inbreukmaking op die werknemer se reg op privaatheid regmatig is ongeag die aard daarvan. Die doel hiervan is om die belang van die werkgever te beskerm.

In 2000 is 'n ondersoek gedoen deur die Amerikaanse Bestuursassosiasie en is gevind dat algemene observasie van die werknemer, deur middel van monitering, deur 74% van maatskappye in die VSA gedoen word.⁴⁴ McEvoy waarsku dat e-pos kommunikasie in die sisteem gestoor word en steeds aan monitering onderworpe is, selfs al is die boodskap van die werknemer se rekenaar verwyder. Maatskappye beweer dat hul die reg het om 'n beperking te plaas op die persoonlike gebruik van kantoorrekenaars en e-pos wat nie behoorlik en gepas is vir die werkplek nie. Volgens howe is werkgewers, as verskaffers en

⁴² Supra vn 35.

⁴³ Voetnoot 76.

⁴⁴ S McEvoy *E-Mail and Internet Monitoring and the Workplace: Do Employees Have a Right to Privacy* Fairfield University CT.

eienaars van die toerusting, geregtig om beleid te ontwikkel en te implementeer wat die gebruik van kantoortoerusting en e-pos reguleer.⁴⁵

In Texas is 'n aangeleentheid voor die Hof gebring⁴⁶ waar 'n werknemer se sluitkassie, met 'n kombinasieslot gesluit was en deur K-Mart oopgemaak is in 'n ondersoek. Die Hof bevind dat indien die werknemer sy of haar eie slot koop en die sluitkassie daarmee sluit, die verwagting tot privaatheid by beide partye bestaan. In *Dausen v State*⁴⁷ is 'n danser se eis op grond van inbreukmaking op haar privaatheid toegestaan nadat die werkgever haar gedwing het om haar sluitkassie oop te maak en dwelms daarin gevind is. Die Texas Appèlhof beslis in 1999 in 'n ongerapporteerde beslissing⁴⁸ dat 'n persoonlike e-pos- of rekenaarkode nie op dieselfde beginsel as die sluitkassies gegrond is nie. Die rede daarvoor is dat sluitkassies 'n diskrete fisiese plek is waarin die werknemer persoonlike eiendom stoor, terwyl e-pos op die rekenaar in die sisteem gestoor word en op 'n stadium in elk geval deur ander persone gelees sou word. Die Hof noem ook dat die gebruik van 'n maatskappy se elektroniese toerusting geen privaatheid waarborg nie, selfs nie met die gebruik van geheime kodes nie. Die posisie in Suid-Afrika na aanleiding van die *Moonsamy*-beslissing⁴⁹ blyk te wees dat privaatheid ten aansien van beide fisiese en elektroniese toerusting beperk is in die besigheidsfeer.

Die Hof beslis soortgelyk in *Smyth v Pillsbury Company*⁵⁰ en noem dat die werknemer geen regmatige verwagting tot privaatheid het, indien e-pos deur middel van die maatskappysisteem gestuur word nie. Hierdie beginsel is van toepassing selfs al bestaan daar nie 'n beleid ten

⁴⁵ MJ McCarthy *Your Manager's Policy on Employees' E-mail May Have a Weak Spot*, WALL ST J Apr 25, 2000.

⁴⁶ *K Mart Corp v Trotti* 667 SW 2d 632 (Tex App 1984).

⁴⁷ 868 SW 2d 363 (Tex App 1993).

⁴⁸ McLaren-beslissing, voetnoot 82.

⁴⁹ Supra vn 32.

⁵⁰ 914 F Supp 97 (ED) Pa 1996.

aansien van privaatheid in die maatskappy nie. Die Hof noem verder dat die maatskappy belang daarin het om ontoepaslike en onbehoorlike kommentaar, asook onwettige e-pos aktiwiteite, te voorkom en dat dit swaarder weeg as die werknemer se belang ten aansien van privaatheid.

In *Tiberino v Spokane County*⁵¹ is 'n sekretaresse ontslaan weens onbevredigende werksverrigting. Tiberino is voorsien van 'n rekenaar vir werksdoeleindes en in kennis gestel dat dit nie vir persoonlike doeleindes gebruik mag word nie. Sy is 'n maand later ontslaan omdat haar kollegas haar opdragte uitgevoer het, terwyl sy besig was met persoonlike e-pos. Die Washington Appèlhof bevind dat die ontslag billik was, hoewel die openbaarmaking van die e-pos inhoud wel 'n skending van haar privaatheid was.

2.3 Definisie en Doel van Elektroniese Monitering

Elektroniese monitering bestaan uit drie komponente. Eerstens sluit dit die gebruik van elektroniese uitvindings in waarmee die werkgever die algemene werksverrigting van die werknemer kan nagaan en bepaal.⁵² Tweedens sluit dit elektroniese observasie in. Dit monitor die werknemer se gebruik van elektroniese media om vas te stel of die werknemer laasgenoemde vir enige ander doel, as die uitvoering van werksverpligtinge, gebruik.⁵³ Derdens stel dit die werkgever instaat om elektroniese data te herwin of te herroep nadat dit uitgewis of verseël is, of die werknemer gepoog het om die inligting te vernietig.⁵⁴

⁵¹ 13 P 3d 1104 (Wash Ct App 2000).

⁵² 'n Voorbeeld daarvan sou wees dat die werkgever die werknemer se e-pos aan en van kliënte monitor ten einde te bepaal of die werknemer sy pligte na wense uitvoer.

⁵³ 'n Voorbeeld hiervan is waar die werkgever die werknemer se e-pos boodskappe monitor, in 'n ondersoek rakende 'n klagte, met betrekking tot seksuele teistering.

⁵⁴ 'n Voorbeeld is in gevalle waar die werkgever gespesialiseerde sagteware gebruik om e-pos boodskappe, op die hardeskyf gestoor, van 'n werknemer te herroep of terug

Die redes waarom werkgewers dit noodsaaklik ag om werknemers te monitor is die volgende:⁵⁵

- (a) Die moontlikheid dat werknemers handelsgeheime of vertroulike inligting sal versend; (b) Te voorkom dat werknemers die tegnologie, deur die werkgewer voorsien, sal gebruik om 'n eie besigheid te vestig; (c) Werkgewers kan aanspreeklik gehou word vir Internet of e-pos aktiwiteite van hul werknemers, indien dit in die werkgewer se naam of handelsmerk geskied; (d) Godsdienstige of politiese verklarings deur werknemers, wat naamskending tot gevolg het, word aan die werkgewer se naam gekoppel; (e) Die werkgewer is verplig om 'n werksatmosfeer te skep wat vry is van teistering en diskriminasie. Versending van onbehoorlike materiaal moet gevolglik voorkom of vernietig word, ten einde te verhoed dat die werkgewer hiervoor aanspreeklik is;⁵⁶ (f) Dit is noodsaaklik dat werkgewers toesien dat werknemers nie werksure gebruik vir persoonlike doeleindes nie. 'n Werkgewer kan finansieel daaronder ly; en (g) die risiko bestaan dat aanhegtings, foto's en virusse die netwerk se funksionering aansienlik kan vertraag of selfs tot stilstand bring.⁵⁷

Die werkgewer se aanspreeklikheid vir die ontvangs en versending van onbehoorlike materiaal deur die werknemer staan bekend as die leerstuk van middelike aanspreeklikheid. Dit kan spruit uit rasgebaseerde of seksuele teistering, naamskending, verspreiding van rekenaar-virusse, lae produktiwiteit, 'n besigheid se swak reputasie en die integriteit van die netwerk.⁵⁸

te kry, wat verband hou met 'n ondersoek rakende handelsgeheime, ens. www.dataforensics.com/litigation- Computer Forensics for Civil Litigation.

⁵⁵ A Gahtan *Monitoring Employee Communications*. URL www.gahtan.com/cyberlaw .

⁵⁶ Han H Li *Electronic Mail Privacy in the Workplace* Mailto: hali@lynx.neu.edu .

⁵⁷ D Carew *Your Boss can't Monitor your Email* Independent Online 07/11/03.

⁵⁸ S Hinde 2001: *A Privacy Odyssey* 2001 Computers&Security 21.

Die misbruik van Internet-fasiliteite deur werknemers in Suid-Afrika is aan die orde van die dag. Volgens statistiek ondervind 68,63% van maatskappye probleme met werknemers wat hul werkstyd vir die Internet verruil, 69,93% rapporteer dat hul werknemers seksueel teisterende e-pos boodskappe, grappe of beelde versend, ontvang of aflaai van die Internet en 64,71% van maatskappye ondervind probleme met degradering van hul netwerke, weens die misbruik van die Internet.⁵⁹

Die verskillende wyses waarop werknemers gemonitor kan word is: (a) die gebruik van die sleutelbord van die rekenaar. Hierdeur word bepaal hoe lank dit neem om 'n gegewe opdrag te voltooi, asook die lengte van enige breuke tussenin geneem; (b) die gebruik van die telefoon. Rekenaar bepaal die aantal en tipe oproepe, hoe lank 'n inbeller moes aanhou en hoeveel keer die telefoon gelui het voor dit beantwoord is, die lengte van elke oproep en die tyd tussenin; (c) die opstel van dokumente. Hoeveel keer die dokument opgestel is en die aantal verbeterings wat per reël gedoen is; en (d) die gebruik van die Internet. Sagteware stel die werkgever in staat om op enige geselekteerde tydstip, die beeld van 'n werknemer se rekenaarskerm vas te vang en dit te kompakteer, sodat die werkgever dokumentasie van al die werknemer se rekenaarwerk het.⁶⁰ Die werknemer se besoeke aan webblaaie word ook gemonitor, die tydsduur van die besoeke en of dit produktief was of nie. Werknemers se lêers, speletjies, e-pos ontvang of gestuur en toegang tot pornografie word gemonitor⁶¹ en (e) die forensiese tegnieke deur die werkgever gebruik om elektroniese kommunikasie te herroep nadat dit gestuur, ontvang of op die hardeskyf gestoor is.⁶²

⁵⁹ L. Dancaister *Internet Abuse: A survey of South African Companies* (2001) 22 ILJ 862.

⁶⁰ D. Towns *Legal Issues Involved in Monitoring Employees' Internet and E-mail Usage*, GIGALAW.COM 2 (2002).

⁶¹ M. Anderson *Identifying Internet Activity, Computer Forensics Goes to Cyberspace*. www.dataforensics.com/litigation- Computer Forensics for Civil Litigation.

⁶² M. Leahy *Recovery and Reconstruction of Electronic Mail as Evidence* 41 AM JUR. PROOF OF FACTS 3D 1 (2002).

In sommige gevalle word volgens Blackwell⁶³ selfs *Hygiene Guard Monitors* en *Global Positioning Satellite* onderskeidelik gebruik om werknemers se kleedkamergewoontes asook die gebruik van maatskappymotors deur werknemers te monitor.

Die voordele verbonde aan die monitering van werknemers is duidelik uit die bogenoemde, maar dit kan die vertrouensverhouding tussen die werknemer en die werkgever skade berokken en lei tot ongemotiveerde werknemers.⁶⁴

2.4 Gevolge van Monitering op die Werknemer

Goeie trou word geïmpliseer deur die dienskontrak en is die werknemer⁶⁵ onder verpligting om dienooreenkomstig teenoor die werkgever op te tree. Vertroue is die basis van die werksverhouding. Die Appèlhof bevestig in *Council for Scientific & Industrial Research v Fijen*⁶⁶ dat die basis van die indiensnemingsverhouding vertroue is en dat, soos in die Engelse reg, die verpligting op beide partye rus om nie die vertrouensverhouding skade te berokken nie. Daar word gevolglik van die werknemer vereis om die werkgever se belang bo sy of haar eie te stel. Ingevolge die Engelse Gemenereg word gehoorsaamheid, samewerking en sorg tydens werkverrigting as geïmpliseerde kontraktuele terme van die dienskontrak geag.⁶⁷

Dit het tot gevolg dat die werknemer, skuldig aan misbruik van die rekenaar gedurende werksure, die kontraktuele verpligting van goeie trou ingevolge die Gemenereg, verbreek. Indien 'n beleid ten aansien hiervan

⁶³ AH Blackwell *Don't Expect any Privacy in the Workplace* amyblackwell@wwwiz.com.

⁶⁴ D Carew *Your Boss can't Monitor your Email* Independent Online 07/11/03.

⁶⁵ Ingevolge *Sappi Novoboard (Pty) Ltd v Bolleurs* (1998) ILJ 784 (LAC).

⁶⁶ (1996) 12 ILJ 18 (A).

⁶⁷ S Deaken et al *Labour Law* 3rd ed (2001) 326.

bestaan, is die werknemer ook skuldig aan ongehoorsaamheid en handel uiteraard nie tot bevordering van die werkgever se belang nie.⁶⁸

Die WAV⁶⁹ bepaal dat ontslag van 'n werknemer nie onbillik is indien die werkgever kan bewys dat dit verband hou met die werknemer se gedrag of bevoegdheid, of met die werkgever se operasionele vereistes, nie.⁷⁰

Ten aansien van die gebruik van elektroniese media moet die standaard gestel billik wees en die werknemer moet daarvan kennis dra. Sou die werknemer nie aan die standaard voldoen nie, moet hy of sy ooreenkomstig normale prosedure daarvan ingelig word en voldoende geleentheid of opleiding ontvang om wel aan die standaard te voldoen. Indien die werknemer steeds nie aan die standaard voldoen nie, is ontslag op grond van onbekwaamheid die toepaslike remedie.

Indien die werknemer versuim om gehoor te gee aan regulasies of beleid ten aansien van die gebruik van elektroniese media, is die werkgever geregtig om die werknemer op grond van wangedrag te ontslaan.⁷¹ Die voorvereiste is egter dat die beleid of regulasie van toepassing billik moet

⁶⁸ C Morgan *Employer Monitoring of Employee Electronic Mail and Internet Use* (1999) 44 McGill LJ 849.

⁶⁹ Artikel 188(1)(a).

⁷⁰ Die ontslag moet egter steeds ingevolge subartikel 1(b) prosedureel billik wees.

⁷¹ PAK Le Roux *Employment Practices in the Age of the Internet* 2003 Centre for Business Law UNISA.

wees,⁷² die werknemer daarvan moet kennis dra⁷³ en dat ontslag die gepaste⁷⁴ sanksie is.

⁷² Billikheid vereis dat die werkgever die regulasie of beleid op grond van die besigheid se belange en behoeftes kan regverdig en die werkgever sodoende sy of haar eiendom, die doeltreffende en effektiewe bestuur daarvan en die versekering van 'n veilige en gesonde werksatmosfeer beskerm.

⁷³ 'n Werknemer kan slegs aanspreeklik gehou word vir die nie-nakoming van 'n beleid waarvan hy of sy kennis dra.

⁷⁴ Die begrip 'toepaslik' vereis dat faktore soos die werknemer se diensrekord, dienstydperk, redes vir oortreding, die mate waarin oortree is en of die werkgever se beleid deurgaans konsekwent toepassing gevind het, oorweeg moet word.

HOOFSTUK 3 WETGEWING VAN TOEPASSING

3.1 Suid-Afrikaanse Wetgewing

3.1.1 Wet op Beheer van die Onderskepping van Kommunikasie

3.1.1.1 Algemene Bepalings en Uitsluitings

Ingevolge artikel 2 van die *Wet op Beheer van die Onderskepping van Kommunikasie*⁷⁵ mag geen persoon opsetlik kommunikasie onderskep⁷⁶, poog om te onderskep of enige persoon tot onderskepping magtig, tydens die versending of ontvangs van kommunikasie, nie.

Die bogenoemde bepaling moet saam met die *Wet op Elektroniese Kommunikasie en Transaksies*⁷⁷ gelees word.⁷⁸ Artikel 86(1) van die ECTA bepaal, onderhewig aan die RICA, dat 'n persoon wat toegang verkry tot enige inligting of dit met opset onderskep, sonder die nodige toestemming, skuldig is aan 'n misdaad. Artikel 89(1) bepaal dat dit strafbaar is met 'n boete of gevangenisstraf van tot twaalf maande. Dit beteken nie dat werkgewers verbied word om aktiwiteite van werknemers te monitor nie, maar slegs dat aan spesifieke voorwaardes voldoen moet

⁷⁵ Regulation of Interception of Communications and Provision of Communication-related Information Act 70 van 2002. Hierna genoem die RICA.

⁷⁶ Die definisie van onderskep volgens artikel 1, is die verkryging van die inhoud van enige kommunikasie deur middel van enige onderskeppingstoestel, asook die openbaarmaking daarvan, insluitend (a) die monitering van kommunikasie deur middel van 'n moniteringstoestel; (b) die besigtiging, bestudering of inspeksie van die inhoud van indirekte kommunikasie; en (c) die geleiding van enige indirekte kommunikasie na enige ander bestemming as die oorspronklike.

⁷⁷ Electronic Communications and Transactions Act 25 of 2002. Hierna genoem die ECTA.

⁷⁸ T Bortz *The Regulation of Interception of Communications and the Provision of Communication-related Information Act 70 of 2002* Tech Werks Mrt 2003.

word, ten einde billik en wettig te wees.⁷⁹

RICA erken drie gevalle van onderskepping van kommunikasie as regmatig⁸⁰: (a) enige persoon mag kommunikasie onderskep indien hul 'n party tot die kommunikasie is; (b) enige persoon mag kommunikasie onderskep indien een van die partye daartoe, vooraf toestemming tot die onderskepping daarvan verleen het en is op beide direkte en indirekte kommunikasie van toepassing;⁸¹ en (c) enige persoon mag indirekte kommunikasie onderskep in die loop van die uitvoering van enige besigheid⁸² mits aan die volgende vereistes voldoen word:⁸³ (i) indirekte kommunikasie die middel is waardeur transaksies in die loop van die uitvoer van besigheid aangeteken word; (ii) die kommunikasie vir 'n regmatige oogmerk onderskep word, soos vir die vasstelling van feite, 'n ondersoek na of die vasstel van onregmatige gebruik van die telekommunikasiesisteem en die effektiewe gebruik van die fasiliteit deur die werknemer te verseker; (iii) kommunikasie wat onderskep word, tydens versending of ontvangs daarvan, in geheel of gedeeltelik verband hou met die besigheid van die werkgewer; en (iv) alle redelike pogings aangewend is om individue, wat die sisteem gebruik, vroegtydig in kennis te stel dat indirekte kommunikasie wel onderskep word en dat, as voorvereiste, die eienaar en verskaffer daarvan, toestemming tot onderskepping verleen het.

Elektroniese kommunikasie, soos e-pos en die Internet, kan dus onder die definisie van indirekte kommunikasie tuisgebring word. Of boodskappe gestoor op die netwerk onder die definisie van indirekte

⁷⁹ D Carew *Your Boss can't Monitor your Email* Independent Online 07/11/03.

⁸⁰ Artikel 5.

⁸¹ Volgens artikel 1(2) van RICA beteken indirekte kommunikasie die stuur of ontvang van 'n boodskap, of enige gedeelte van 'n boodskap, via telekommunikasie of die posdiens en direkte kommunikasie geskied verbaal tussen twee of meer persone.

⁸² Die definisie van 'n besigheid ingevolge artikel 1 van die RICA, is enige besighedsaktiwiteit van enige persoon, insluitende privaat en publieke liggame.

⁸³ Artikel 6 van die RICA.

kommunikasie tuisgebring kan word is onseker. Riglyne word vanuit die Internasionale reg verkry en wel hieronder bespreek.

3.1.1.2 *In die Loop van die Uitvoer van Besigheid*

Dit is onseker wat die bedoeling van die wetgewer met hierdie frase was. Volgens die Britse Regulasie⁸⁴ is kommunikasie in die loop van besigheid in die Verenigde Koninkryk enige kommunikasie wat verband hou met die besigheid.⁸⁵

Die Britse Regulasie wettig nie die monitering van persoonlike indirekte kommunikasie sonder die werknemer se toestemming nie, maar wettig wel die onderskepping van indirekte kommunikasie om te bepaal of dit met die besigheid van die werkgewer verband hou. Volgens RICA is slegs die onderskepping van indirekte kommunikasie, wat met die besigheid verband hou, toelaatbaar en mag indirekte kommunikasie egter nie onderskep word om vas te stel of die kommunikasie met die besigheid verband hou nie. 'n Regmatige oogmerk, volgens RICA, balanseer die werknemer se reg op privaatheid en die noodsaaklikheid daarvan dat die misbruik van die besigheid se telefone, e-pos en Internet voorkom word en die sisteem teen bedreigings, soos virusse, beskerm word.

Dit is dus duidelik dat RICA die monitering van indirekte kommunikasie slegs as regmatig beskou indien dit as 'n uitsluiting, soos genoem in paragraaf 3.1.1.1, weergegee is en word die werknemer se toestemming in enige ander geval vooraf vereis.

⁸⁴ United Kingdom Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 No 2699.

⁸⁵ T Bortz *The Regulation of Interception of Communications and the Provision of Communication-related Information Act 70 of 2002* Tech Werks Mrt 2003.

Toestemming van die werknemer word op skrif vereis in artikel 5, maar volgens Michalson⁸⁶ is slegs artikel 6 direk van toepassing op die besigheid. Die straf of boete, in geval van nie-nakoming, verwys slegs na artikel 6. Sou 'n werkgever dus elektroniese kommunikasie van werknemers monitor in die loop van die uitvoering van besigheid, soos in RICA vervat, is die enigste vereiste dat redelike pogings vooraf aangewend moet word om werknemers hiervan in kennis te stel of alternatiewelik, dat die toestemming van die werknemer verkry moet word, hetsy uitdruklik of geïmpliseerd.

Beech⁸⁷ is ook van mening dat toestemming nie vereis word nie. Indien die werkgever, as persoon in beheer van die netwerk, alle redelike pogings aangewend het om die werknemers vooraf in kennis te stel van die onderskepping van indirekte kommunikasie, is voldoen aan die vereiste gestel in artikel 6(2).

Vir volledigheid kan genoem word dat dit volgens ECTA⁸⁸ voldoende is om toestemming met die druk van 'n sleutel te verleen, indien vereis word dat 'n dokument op skrif moet wees en die werknemer op 'n rekenaarskerm toegang tot die dokument het. Artikel 13 maak voorsiening vir 'n gevorderde elektroniese handtekening sou die Wet 'n handtekening vereis.

Die presiese betekenis van toestemming is onduidelik. Toestemming opsigself regverdig nie 'n inbreukmaking op privaatheid nie. Verder is toestemming binne hierdie konteks slegs van toepassing op e-pos boodskappe wat deur werknemers versend word en sluit nie boodskappe wat van buite ontvang word in nie. Volgens die Europese en Verenigde

⁸⁶ www.legalbrief.co.za. L Michalson *Office E-Mail: Consent doesn't have to be in writing* 6 Okt 2003.

⁸⁷ W Beech of Leppen Beech Attorneys *The Right of an Employer to Monitor an Employee's Electronic Mail, Telephone calls and Internet Usage* News Brief No 14 January 2003.

⁸⁸ Artikel 12.

State se wetgewing en regspraak blyk dit asof die werkgewer meer sal moet doen, as selfs skriftelike toestemming van werknemers verkry, indien hul voldoende beskerming van siviele en kriminele aanspreeklikheid wil geniet.⁸⁹ Hiermee word bedoel dat 'n volledige beleid opgestel, onderteken en geïmplimenteer moet word.

3.1.1.3 *Nie-Nakoming van die Bepalings*

Werkgewers wat werknemers se elektroniese kommunikasie sonder die nodige toestemming monitor is skuldig aan 'n kriminele oortreding⁹⁰ en kan 'n boete van tot R2 miljoen of tronkstraf van 10 jaar opgelê word. 'n Regspersoon kan 'n boete van tot R5 miljoen opgelê word en die werknemer self 'n boete van R2 miljoen of 10 jaar tronkstraf.⁹¹

Ingevolge *Cronje v Toyota Manufacturing*⁹² is 'n werknemer ontslaan weens 'n e-pos ontvang en versend. Die e-pos het die Eerste Minister van Zimbabwe, Mugabe, as 'n gorilla uitgebeeld en 'n rassistiese slagpreek aangeheg. Die werkgewer was gevolglik verplig om streng teen rassisme en die misbruik van e-pos in die werkplek op te tree. Getuienis het aangedui dat die werkgewer wel 'n beleid daarteen gehad het, die beleid konsekwent toegepas is en die werknemer wel daarvan kennis gedra het. Die Hof oorweeg ook die *Kode vir Goeie Praktyk: Ontslag*⁹³ en bevind dat die werknemer se oortreding die vertrouensverhouding tussen die partye onherstelbaar beskadig het en voortsetting daarvan onmoontlik gemaak is. Die rede vir die werknemer se ontslag was gevolglik billik.

⁸⁹ D Carew *Your Boss can't Monitor your Email* Independent Online 07/11/03.

⁹⁰ Artikel 49 van die RICA.

⁹¹ Artikel 51 van die RICA.

⁹² (2001) 3 BALR 213 (CCMA).

⁹³ Item 7 van Skedule 8 van die WAV.

In *Bamford & Others v Energizer (SA) Ltd*⁹⁴ is 5 werknemers ontslaan nadat die werkgever duisende pornografiese, rassistiese en seksistiese e-pos boodskappe, wat deur die werknemers op die sisteem gestoor is, gevind het. Die werkgever het geargumenteer dat die misbruik van die maatskappy se rekenaarsisteem die doeltreffendheid daarvan belemmer en die betrokke materiaal die potensiaal het om die maatskappy se handelsnaam op internasionale vlak skade te berokken. Die werknemers se verweer was dat daar geen beleid bestaan het ten aansien van die ontvangs of versend van die betrokke materiaal nie. Kennisgewings is egter deur die werkgever uitgereik, waaruit dit duidelik geblyk het dat die rekenaars slegs vir besigheidsdoeleindes gebruik mag word.

Die ontslane werknemers se argument dat op hul privaatheid inbreuk gemaak is, is deur die Arbiter verwerp omdat die e-pos boodskappe van die maatskappy se eie e-pos sisteem verhaal is en dus deur enigeen gelees kon word. Die Arbiter noem verder dat geen individu daarop geregtig is om privaatmateriaal op 'n werkgever se fasiliteite te stoor en die werkgever dan te verhoed om dit na te gaan nie. Die werkgever is egter geregtig om te bepaal of die stoor van hierdie materiaal enige doel het. Die fasiliteite is steeds die eiendom van die werkgever ongeag of 'n beleid ten aansien daarvan bestaan. Die werknemers se ontslag was gevolglik billik.

Dit blyk uit die bogenoemde dat die werkgever se kennisgewing ten aansien van fasiliteite wat vir privaat doeleindes gebruik word, as voldoende toestemming van die werknemer geag word.

In *Grieve v Denel (Pty) Ltd*⁹⁵ het 'n werknemer pornografiese webtuistes besoek en die rekenaars en netwerke, deur die werkgever voorsien, daarvoor gebruik. Die *ratio* stem ooreen met die van die *Bamford*-saak.

⁹⁴ (2001) 12 BALR 1251 (P).

⁹⁵ C7/2003, ongerapporteer.

In *Smuts v Backup Storage Facilities & Others*⁹⁶ is die feite soortgelyk en bevind die CCMA dat die werknemer die eiendom van die werkgewer misbruik het en werksure vir 'n ander doel aangewend is as vir die bevordering van die werkgewer se besigheid.

Werknemers wat weier om tot monitering toe te stem, kan nie ontslaan word op grond van hul weiering nie. Soos blyk uit die bogenoemde bespreking erken die WAV slegs drie billike gronde vir ontslag. Die weiering van toestemming is nie wangedrag nie. Dit kan geargumenteer word dat die werknemer onbevoeg is om die werk, soos ooreengekom, te verrig, indien die werkgewer die werknemer verbied om die fasiliteit te gebruik weens sy of haar weiering om toestemming tot monitering te verleen. Sou die werkgewer kan aandui waarom geen alternatiewe oplossing bestaan nie, monitering en onderskepping noodsaaklik is en die werknemer se redes vir weiering oorweeg is, het 'n argument dat operasionele vereistes die ontslag regverdig, redelikerwys ook 'n kans op sukses.⁹⁷ Volgens *Mischke* moet die werknemer se posisie in die besigheid oorweeg word, of 'n alternatief bestaan wat prakties uitvoerbaar is en of dit verband hou met die werkgewer se operasionele vereistes.

RICA het juis beskerming van werknemers se reg op privaatheid ten doel.⁹⁸ Die werkgewer sal dus 'n behoorlike beleid moet saamstel en die toestemming van die werknemers verkry alvorens die moniteringsproses geïmplimenteer kan word.

⁹⁶ WE2628-02, ongerapporteer.

⁹⁷ Billike prosedure is steeds van toepassing, soos vervat in artikel 41 van die BCEA. PAK Le Roux *Employment Practices in the Age of the Internet* 2003 Centre for Business Law UNISA.

⁹⁸ www.suntimes.co.za. P Sukhraj *New Law Stops Bosses Spying on E-mail* 2003/02/02.

3.1.2 **Wet op die Verbieding van Onderskepping en Monitering**⁹⁹

Hierdie Wet het inwerking getree in 1993 en die Internet was op daardie stadium nog nie 'n bekende konsep in SA nie. Die Wet is die voorloper van RICA en daardeur vervang.

In artikel 2(1)(a) word bepaal dat geen persoon met opset en sonder die toestemming van die sender enige kommunikasie mag onderskep wat deur middel van 'n telefoon of 'n telekommunikasielyn geskied nie. Artikel 2(1)(b) verbied die monitering deur enige moniteringstoerusting waarmee konfidentiële inligting rakende 'n persoon, 'n liggaam of 'n organisasie verkry word. Hierdie Wet het egter geen bepaling rakende die nagaan van inligting wat gestoor is op die rekenaar nie en is die enigste relevansie die telekommunikasielyn wat in definisie uitgebrei kan word om e-pos in te sluit.¹⁰⁰

3.1.3 **Wet op Bevordering van Toegang tot Inligting**¹⁰¹

Die Grondwet¹⁰² verleen 'n reg op toegang tot inligting, gehou deur die Staat of enige ander persoon, indien die inligting vereis word vir die uitoefening of beskerming van enige regte. Die bogenoemde Wet tree daarna in werking om effek te gee aan hierdie grondwetlike reg en kwalifiseer dieselfde reg op toegang tot inligting met dieselfde bewoording in artikel 50(1)(a). Die omvang van die regte wat beskerm of uitgeoefen word is onduidelik. Die Wet sal slegs relevant wees vir die bespreking indien die beperking van die reg op privaatheid, van die werknemer, hieronder tuisgebring kan word en die werkgewer geregtig

⁹⁹ Interception and Monitoring Prohibition Act 127 of 1992. Hierna genoem die IMPA.

¹⁰⁰ www.deneysreitz.co.za. B Patterson *Insurance Seminar Aug/Sept 2001: The Internet – An Employee's Right to Privacy* News 2001.

¹⁰¹ 2 van 2000. Hierna genoem PAIA.

¹⁰² Artikel 32.

is op inligting gehou deur die werknemer, met die beskerming of uitoefening van die werkgewer se regte ten doel.

3.2 Die Internasionale Arbeidsorganisasie

Die *Wet op Arbeidsverhoudinge*¹⁰³ bepaal in artikel 3(b) en (c) dat interpretasie daarvan moet geskied in ooreenstemming met die bepalinge van die Grondwet en in ooreenstemming met die openbare internasionale verpligtinge van die RSA.

Die WAV se oogmerk, soos bepaal in artikel 1(b), is die bevordering van ekonomiese ontwikkeling, sosiale geregtigheid, vreedsaamheid en demokrasie in die werkplek, deur middel van die primêre oormerke van die WAV. Een van hierdie primêre oogmerke is om uitvoering te gee aan die verpligtinge, wat ingevolge die Internasionale Arbeidsorganisasie,¹⁰⁴ aan die RSA as lidstaat opgelê is. Die beginsels van die ILO moet gevolglik binne die indiensnemingskonteks oorweeg word.

Die ILO het 'n praktykskode in 1996 aangeneem om werknemers se persoonlike inligting te beskerm. Die ILO kode word geag as die standaard met betrekking tot die beskerming van werknemers se reg op privaatheid. 'n Aantal beginsels is geïdentifiseer ten einde billikheid te verseker: (a) die inligting moet verkry word vir 'n regmatige en billike besigheidsoogmerk; (b) die inligting moet direk van die werknemer verkry word of met toestemming van die werknemer, van 'n eksterne bron; (c) die inligting moet gebruik word vir die doel waarvoor dit verkry is en mag nie openbaar gemaak word sonder die werknemer se toestemming nie; (d) die werknemer moet ingelig word van die aard van die inligting verkry, die wyse waarop dit verkry gaan word asook die doel waarvoor dit benodig word; (e) die werkgewer moet laastens slegs die

¹⁰³ 66 van 1995. Hierna genoem die WAV.

¹⁰⁴ Hierna genoem die ILO.

noodsaaklikste inligting verkry en van die minste beperkende metode gebruik maak om die oogmerk van die monitering te bereik.¹⁰⁵

Die Suid-Afrikaanse reg reflekteer die ILO beginsels voldoende. Ingevolge RICA word egter slegs toestemming vir monitering of onderskepping vereis, hoewel die werknemer ingevolge die ILO van die aard, wyse en doel daarvan ingelig moet word.

3.3 Internasionale Wetgewing

3.3.1 Relevansie

Die Grondwet¹⁰⁶ bepaal dat by die uitleg van die Handves van Regte 'n hof, tribunaal of forum die volkereg inag moet neem en buitelandse reg inag mag neem. Let veral op die woordspeling in die voorafgaande. Die reg op privaatheid is vervat in die Handves van Regte en is dit gevolglik van uiterste belang om die toepassing van hierdie reg in ander stelsels te ondersoek. Verder is die opweging van die werkgewer en werknemer se belang, ten aansien van privaatheid en die monitering van elektroniese media, 'n nuwe konsep in Suid-Afrikaanse reg en kan die onduidelikheid wat tans bestaan helderheid teen 'n internasionale agtergrond verkry.

3.3.2 Die Verenigde State van Amerika

Die *Electronic Communications Privacy Act*¹⁰⁷ is die belangrikste Amerikaanse wetgewing rakende privaatheid ten aansien van elektroniese media. Ingevolge hierdie Wet is die onderskepping of openbaarmaking van privaat kommunikasie onwettig. Enige individu,

¹⁰⁵ <http://www.epic.org/privacy/workplace/default.html> Workplace Privacy 26/11/2003.

¹⁰⁶ Artikel 39.

¹⁰⁷ 18 USC 1988. Hiema na verwys as ECPA.

privaat agentskap of die staat wat elektroniese kommunikasie met opset onderskep, handel instryd met die Wet.

Die Handves van Regte, soos vervat in die Grondwet van die Verenigde State, verleen nie eksplisiet 'n reg op privaatheid nie. Verskeie elemente van hierdie reg word in verskillende gedeeltes van die Grondwet gevind. Die Vierdie Wysiging vervat die relevante bepaling en bepaal dat elke burger die reg het om sy of haar persoon, woning, dokumente en besittings teen onbillike deursoeking en beslaglegging te beskerm. Die individu se reg op privaatheid ten aansien van elektroniese kommunikasie word egter nie uitdruklik in enige wetgewing gewaarborg nie.

In *O'Connor v Ortega*¹⁰⁸ bevind die Hof dat 'n dokter van 'n staatshospitaal 'n regmatige verwagting tot privaatheid ten aansien van sy lessenaar en liseerkabinette het. Die vraag is dus of hierdie verwagting dieselfde toepassing vind met betrekking tot persoonlike elektroniese lêers op die hardeskyf van sy rekenaar gestoor. Die Hof verklaar in verskeie aangeleenthede¹⁰⁹ dat die verwagting ten aansien van fisiese, diskrete plekke nie van toepassing is op gestoorde inligting op 'n sisteem nie.

In *Pratt & Whitney*¹¹⁰ verklaar die Nasionale Raad vir Arbeidsverhoudinge dat 'n maatskappy se rekenaarnetwerk deel is van die werksarea. Die Raad noem verder dat monitering deur die werkgewer, wat vakbond-aktiwiteite oor elektroniese kommunikasie verbied, instryd is met die ECPA. Vakbond-aktiwiteite is egter deel van 'n gesonde werksverhouding en geen duidelikheid is gegee rakende privaat aangeleenthede nie.

¹⁰⁸ 480 US 709, 716 (1987).

¹⁰⁹ Voetnoot 42 tot 46.

¹¹⁰ 26 AMR 36322 12-CA-18446 (Feb. 23, 1998)

In *Konop v Hawaiian Airlines Inc*¹¹¹ bevind die Hof dat Titel 1 van die ECPA slegs die onderskepping van elektroniese kommunikasie verbied wat in die proses van versending of ontvangs is. Die Hof noem verder dat ingevolge Titel 2 van die ECPA ongemagtigde toegang tot gestoorde elektroniese kommunikasie slegs verbied word voor die versending van die kommunikasie. Die Hof bevestig in *Fraser v Nationwide Mut Ins Co*¹¹² dat toegang tot gestoorde elektroniese kommunikasie, nadat dit ontvang of versend is, nie verbied word nie. Titel 1 en 2 verbied dus nie 'n werkgever om die werknemer se gestoorde e-pos, telefoonboodskappe en Internet kommunikasies te monitor nie.

Die ECPA verbied egter in Artikel 2511¹¹³ die onderskepping van gestoorde elektroniese kommunikasie, maar sluit nie onderskepping deur die voorsiener van die fasiliteit of enigeen wat toegang daartoe verkry het met die nodige toestemming, onder die verbod in nie. Die werkgever mag slegs kommunikasie wat met die besigheid verband hou onderskep. Hoewel die Wet ook die reg verleen om kommunikasie te onderskep om vas te stel of dit persoonlik van aard is. In Titel 3 word die onderskepping van elektroniese kommunikasie in die proses van ontvangs of versending verbied. Toestemming van die werknemer, hetsy uitdruklik of geïmpliseerd, vervat in die indiensnemingsooreenkoms of beleid is 'n uitsondering op die verbod mits die onderskepping in die loop van diens geskied.¹¹⁴ Sou die werkgever dus bloot kennis gee van die monitering aan die werknemer is dit voldoende ingevolge die Wet.¹¹⁵

Die reg erken dus die eiendomsreg van die werkgever, soos bevestig in die *Pillsbury*-beslissing en verleen aan werkgewers die reg tot

¹¹¹ 2002 WL 1941431.

¹¹² 135F Supp 2d 623 (ED Pa 2001).

¹¹³ Titel 2. Interception and disclosure of wire, oral, or electronic communications prohibited.

¹¹⁴ B Trout *Internet Laws Affecting Iowa Companies: Online Security* 2nd ed 2003.

¹¹⁵ <http://www.epic.org/privacy/workplace/default.html> *Workplace Privacy* 26/11/2003.

monitering van werknemers se elektroniese media,¹¹⁶ mits dit ter beskerming van hierdie eiendomsreg is. Verdere vereistes is dat dit in die loop van besigheid of noodsaaklik in die lewering van 'n betrokke diens is.

Die Hof bevind in *Simmons v Southwestern Bell Telephone Co*¹¹⁷ dat die monitering van telefoonlyn deur 'n werkgewer, om seker te maak 'n kwaliteit diens word gelewer, nie onwettig is nie. Die rede daarvoor is dat die werkgewer, as voorsiener van die diens en in die loop van besigheid, onder die uitsluiting in artikel 2511 van titel 2, tuisgebring kan word. Die maatskappy het aparte telefoonlyn vir privaatgebruik beskikbaar gestel.

Volgens die Hof in *Watkins v L.M. Berry & Co*¹¹⁸ is die monitering van privaat oproepe slegs toelaatbaar om die aard van 'n oproep te bepaal.

In *Deal v Spears*¹¹⁹ bevind die Hof dat die hoeveelheid privaatoprope wat deur die werkgewer gemonitor word buitensporig is en word dit nie meer beskou as 'in die loop van besigheid' nie. In so 'n geval weeg die werkgewer se ekonomiese verlies en reg om die besigheid te beskerm nie swaarder as die werknemer se reg op privaatheid nie.

Verder is bevind in *United States v Harpel*¹²⁰ dat die versuim om kennis van die monitering aan werknemers te gee, monitering van hul kommunikasie ontoelaatbaar maak.¹²¹

In *McLaren v Microsoft Corporation*¹²² is 'n werknemer ontslaan nadat die werkgewer gestoorde e-pos boodskappe onder die werknemer se

¹¹⁶ Han H Li *Electronic Mail Privacy in the Workplace* Mailto: hali@lynx.neu.edu.

¹¹⁷ 452 F Supp 392 (WD Okla 1978).

¹¹⁸ 704 F 2d 577 (11th Cir 1983).

¹¹⁹ 980 F 2d 1153 (8th Cir 1983).

¹²⁰ 423 F Supp 192, 196-97 (DSC 1976).

¹²¹ BJ Allen *Privacy in the Workplace: Responses to the Electronic Monitoring of Employees in the Private Sector* Des 1996.

persoonlike, geheime kode nagegaan het. Die rede vir die ondersoek, deur die werkgewer, was 'n klag van seksuele teistering. Die Hof bevind ten aansien van boodskappe gestoor op die kantoorrekenaar, dat die werknemer geen regmatige verwagting tot privaatheid het nie. Die Hof noem verder dat dit nie deur die redelike persoon as 'n ernstige inbreukmaking beskou sal word nie, selfs al het die werknemer 'n verwagting tot privaatheid gehad.

Opsommenderwys word die inbreukmaking op privaatheid, in die VSA, oorweeg deur die regmatige verwagting van die werknemer op te weeg teenoor die belang van die werkgewers. Dit impiseer die beskerming van werkgewers se rekenaarnetwerke en die minimalisering van werkgewers se aanspreeklikheid.¹²³ ECTA beskerm tot 'n groot mate die werkgewer se eiendomsreg en belang, mits monitering binne die perke van billikheid geskied, en weeg dit deurgaans swaarder as die werknemer se reg op privaatheid.

Hoewel dit blyk dat werknemers se reg op privaatheid nie swaarder weeg as die werkgewer se eiendomsreg en belang nie, word werkgewers tog geadviseer om beleid te ontwikkel en te implimenteer.

3.3.3 Die Verenigde Koninkryk

In die Verenigde Koninkryk¹²⁴ is daar tans geen beskerming van die reg op privaatheid nie en pogings om hierdie reg in wetgewing in te sluit, was nie suksesvol nie.¹²⁵ As deel van die Europese Unie vind die *Europese Konvensie vir die Beskerming van Menseregte en Fundamentele Vryheid*¹²⁶ toepassing en waarborg aan elke individu 'n

¹²² 1999 WL 229015 (TEX App 1999) (ongerapporteer).

¹²³ J Rothman *CIO Magazine* 15/03/01 CXO Media Inc.

¹²⁴ Hierna na verwys as die VK.

¹²⁵ E Shorts et al *Human Rights Law in the United Kingdom* 531 (Sweet&Maxwell ed 2001).

¹²⁶ Nov 4 1950 213 UNTS 221. Hierna genoem Konvensie.

algemene reg op privaatheid. Met die inwerkingtreding van die *Wet op Menseregte*¹²⁷ in 2001 is die genoemde Konvensie in wetgewing van die VK ingekorporeer en direk afdwingbaar. Artikel 8 van die HRA bind howe om 'n burger se reg op privaatlewe, familielewe, woning en korrespondensie te respekteer.

Aanvanklik is die reg op privaatheid slegs vertikaal toegepas en het die Gemeenereg tussen individue met betrekking tot die skending van die vertrouensverhouding, horisontaal, toepassing gevind. Dit is duidelik uit gesag¹²⁸ dat die VK 'n punt bereik het waar die reg op persoonlike privaatheid erken en ooreenkomstig beskerm word. Die klem in die VK was op die beskerming van eiendomsregte en nie op persoonlike regte soos in die VSA¹²⁹ nie.¹³⁰

Die *Wet op Onderskepping van Kommunikasie*¹³¹ het nie die onderskepping van kommunikasie verbied nie en die Europese Hof vir Menseregte verklaar in *Alison Halford v UK Merceyside Police*¹³² dat artikel 8 van die Konvensie wel toepassing vind en aan werknemers 'n regmatige verwagting tot privaatheid verleen. Die *Wet op Regulering van Ondersoekbevoegdheid*¹³³ vervang die OIC en verseker privaatheid van netwerkkommunikasie, soos e-pos, ook ten opsigte van 'n kantoorstelsel. Onder die RIPA is die *Telecommunications (Lawful Business Practice) (Interception Communications) Regulations*¹³⁴ uitgevaardig en bepaal dat werkgewer, kommunikasie in die werkplek

¹²⁷ 1998 c 42. Hierna genoem HRA.

¹²⁸ *Douglas v Hello! Ltd* (2001) QB 967,997 (Eng CA).

¹²⁹ Verenigde State van Amerika.

¹³⁰ L Cardonsky *Towards a Meaningful Right to Privacy in the United Kingdom* Boston Univ Int Law J 20 no 2 Fall 2002.

¹³¹ Interception of Communications Act 1985. Hierna na verwys as die IOC.

¹³² 73/1996/693/884. Verwys na voetnoot 35 en 36.

¹³³ The Regulation of Investigatory Powers Act (Communications Data) Order 2003 Statutory Instrument 2003 No 3172. Hierna na verwys as die RIPA.

¹³⁴ 2000 No 2699.

kan onderskep en monitor sonder toestemming. Die rede hiervoor is die opsporing van virusse, onbehoorlike e-pos boodskappe en lang private telefoonoproepe. Werkgewers moet egter steeds redelike pogings aanwend om werknemers hiervan in kennis te stel, maar dit word nie vereis nie.¹³⁵

Werkgewers wat egter op elke telefoongesprek inluister, gestoorde e-pos boodskappe en privaat en konfidentiële pos oopmaak, skep die moontlikheid van konflik tussen die RIPA en die HRA. Die RIPA maak in alle waarskynlikheid ook inbreuk op die *EU Directives* rakende privaatheid.¹³⁶ Hierdie *Data Protection Directive* is geformuleer deur die EU omdat lidstate van die Europese Unie, se wetgewing, met die vrylike beweging en verwerking van inligting ingemeng het.¹³⁷

3.3.4 Europese Unie

Die reg op privaatheid is vervat in die 1995 *Data Privacy Directive*¹³⁸ en die Konvensie¹³⁹ soos reeds bespreek. Artikel 1 van die *Directive* bepaal dat lidstate die fundamentele regte en vryhede van natuurlike persone moet beskerm en in besonder hul reg op privaatheid ten aansien van persoonlike data.

Die EU erken 'n algemene beginsel van proporsionaliteit.¹⁴⁰ Volgens hierdie beginsel word slegs beperkte inbreukmaking op persoonlike privaatheid in die besigheidsfeer toegelaat. Hierdie beginsel word ook in

¹³⁵ www.legalbrief.co.za. *Civil Liberties: Snoopers' Charter not a One-way Street* 6 Okt 2003.

¹³⁶ A Farrington 'The E-Corporation' and the Law Datawatch Iss 47 Jan/March 2001.

¹³⁷ BJ Allen *Privacy in the Workplace: Responses to the Electronic Monitoring of Employees in the Private Sector* Des 1996.

¹³⁸ 95/46/EC.

¹³⁹ Supra vn 120.

¹⁴⁰ M Huie et al *The Right to Privacy in Personal Data: The EU Prods the US and Controversy Continues* TULSA J Comp & Int'l L.

Duitsland toegepas. In essensie beteken dit dat die inbreukmaking nie groter moet wees as wat in die belang van die gemeenskap (en dus die werkgewer) noodsaaklik is om die doel te bereik nie.¹⁴¹ Die beginsel is deur die Hof erken as deel van die reg in *Stauder v City of Ulm*.¹⁴²

3.3.5 *Kanada*

Wetgewing ten aansien van die beskerming van privaatheid is grootliks beperk tot die openbare sektor. Die *Wet op Privaatheid*¹⁴³ het in 1982 inwerking getree. Die doel van die *Wet op Privaatheid* is om inligting deur die staat gehou te beskerm en is gebaseer op die *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, soos aangeneem deur die *Council of the Organization for Economic Co-operation and Development* in September, 1980.¹⁴⁴

In die *Canadian Charter of Rights and Freedoms*¹⁴⁵ bepaal artikel 7 dat elkeen die reg het op lewe, vryheid, sekuriteit van die persoon, so ook word die reg verleen om nie daarvan ontnem te word, tensy in belang van geregtigheid, nie. Elke persoon word dus die reg op sekuriteit verleen. Artikel 8 bepaal dat elkeen die reg het om beskerm te word teen onbillike deursoekking of beslaglegging. Elektroniese monitering word ingevolge *Hunter v Southam Inc.*¹⁴⁶ onder artikel 8 ingesluit, maar vind slegs toepassing waar 'n regmatige verwagting daartoe bestaan.

Artikel 26 bepaal dat alle wetgewing rakende privaatheid steeds bly voortbestaan.

¹⁴¹ TC Hartley *The Foundation of European Community Law* 137.

¹⁴² 1969 ECR 419.

¹⁴³ RS 1985 c P21.

¹⁴⁴ BJ Allen *Privacy in the Workplace: Responses to the Electronic Monitoring of Employees in the Private Sector* Des 1996.

¹⁴⁵ Schedule B of the Constitution Act 79 of 1982.

¹⁴⁶ (1984) 1 SCR 21.

Die *Canadian Criminal Code*¹⁴⁷ bepaal in hoofstuk 4 dat elkeen wat by wyse van elektromagnetiese, akoestiese, meganiese of ander toestel, privaat kommunikasie met opset onderskep, skuldig is aan 'n misdryf en tot 5 jaar gevangenisstraf opgelê kan word.¹⁴⁸ Privaat kommunikasie sluit enige verbale kommunikasie of telekommunikasie in, waar die partye daartoe 'n regmatige verwagting het dat die kommunikasie privaat is.¹⁴⁹ Die werkgewer handel instryd met artikel 184 indien elektroniese kommunikasie onder die begrip kommunikasie ingevolge artikel 183 tuisgebring kan word.

'n Aantal uitsonderings bestaan egter wel en is ingevolge artikel 184(2): (a) toestemming deur een van die partye tot die kommunikasie, (b) in geval van 'n noodsituasie en (c) die noodsaaklike onderskepping deur 'n openbare diensleweraar.

Die werkgewer het dus, ingevolge artikel 184(2)(a), slegs die werknemer se toestemming nodig om onder andere elektroniese kommunikasie van die werknemer te monitor.¹⁵⁰

Die *Personal Information Protection and Electronic Documents Act*¹⁵¹ vind toepassing indien 'n werkgewer persoonlike inligting van 'n werknemer in die loop van besigheid verkry, gebruik of openbaar maak. Die werkgewer mag slegs hierdie inligting verkry, gebruik of openbaar maak, sonder die werknemer se toestemming, om die nienakoming van beleid of ooreenkoms, bedrog of enige ander verbeking van die reg, te ondersoek.¹⁵²

¹⁴⁷ RS 1985 c C46.

¹⁴⁸ Artikel 184(1).

¹⁴⁹ Artikel 183.

¹⁵⁰ BJ Allen *Privacy in the Workplace: Responses to the Electronic Monitoring of Employees in the Private Sector* Des 1996.

¹⁵¹ 2000 c 5. Hierna genoem die PIPEDA.

¹⁵² J Rothman *CIO Magazine* 15/03/01 CXO Media Inc.

Navorsing ten aansien van privaatheid is gedoen deur Urs Gattiker en Linda Janz¹⁵³ en dui aan dat ongeveer 90% van maatskappye, in Kanada, 'n e-posnetwerk het. Die gemiddelde werknemer ontvang en versend 50 e-pos boodskappe per week en spandeer 200 minute daaraan, waarvan 30 minute vir persoonlike e-pos is. Dit beteken dat 'n werknemer ongeveer 3 werksure per week spandeer om e-pos te lees.¹⁵⁴ Vir die werkgever beteken dit ekonomiese verlies.

¹⁵³ PPS, A Privacy Project Survey (PPS) that was studied by Urs Gattiker and Linda Janz (both from University of Lethbridge, Canada), Martina Schollmeyer (Texas A&M University-Corpus Christi, USA), and Helen Kelly (University of Western Ontario, Canada).] Gattiker et al *Privacy and Security on the Internet/Information Highway* URL

¹⁵⁴ Han H Li *Electronic Mail Privacy in the Workplace* Mailto: hali@lynx.neu.edu.

HOOFSTUK 4 KONKLUSIE

4.1 Konklusie

Vir die werknemer is elektroniese monitering 'n inbreukmaking op sy of haar privaatheid. Aan die ander kant is die werkgever as voorsiener en eienaar van die rekenaarnetwerk geregtig om elektroniese media te monitor wat deur die werknemer, in die loop van diens, gebruik word. Die teenstrydige belang van die werknemer en die werkgever het die potensiaal om wantroue in die werksverhouding te skep en sal 'n verlaging in moraal en produktiwiteit teweeg bring.

Uit wetgewing en regspraak van die VSA, die EU en Kanada is dit duidelik dat die omvang van die reg op privaatheid deur interpretasie bepaal word. In Kanada is wetgewing wat privaatheid beskerm hoofsaaklik beperk tot die openbare sektor en word die staat verbied om persoonlike inligting, ongemagtig, te verkry en te gebruik, maar dieselfde beskerming word nie op horisontale vlak verleen nie. Die VSA verbied ongemagtigde monitering en onderskepping van elektroniese kommunikasie deur die staat, privaat agentskappe en individue voor versending daarvan en sluit die voorsiener van die fasiliteit van die verbod uit. Dit bied dus nie voldoende beskerming aan die individu in die loop van diens, indien die werkgever die voorsiener van die fasiliteit is nie. Wetgewing in die VSA verleen aan die werkgever die bevoegdheid om elektroniese kommunikasie te monitor ten einde vas te stel of die kommunikasie privaat van aard is. Dit is 'n leemte in SA. Die VSA erken en beskerm verder die werkgever se eiendomsreg en vereis nie toestemming rakende monitering nie. In SA word toestemming, uitdruklik of geïmpliseerd, vereis en bied gevolglik beter beskerming aan die werkgever ten aansien van aanspreeklikheid, hoewel nie voldoende nie.

Die EU erken 'n algemene beginsel van proporsionaliteit en word beperkte inbreukmaking op persoonlike privaatheid toegelaat, indien dit nie groter is as wat redelikerwys noodsaaklik is om die oogmerk te

bereik nie. Die beginsel word ook in Duitsland toegepas en is soortgelyk aan die opweeg van belange in die SA reg.

Suid-Afrikaanse wetgewing bied beskerming aan die individu sowel as die werknemer in die loop van diens en word vereis dat die werknemer se toestemming verkry word alvorens enige elektroniese monitering deur die werkgever gedoen kan word. Daar is egter geen duidelike indikasie ten aansien van wat bedoel word met in die loop van diens nie en wat bedoel word met toestemming is ook onduidelik. Riglyne ten aansien hiervan is van die internasionale reg verkry. Volgens die VK word enige kommunikasie ingesluit wat met die besigheid verband hou. Rakende toestemming blyk dit vanuit die internasionale reg dat dit voldoende is om redelike pogings aan te wend om werknemers van die monitering in te lig, hoewel outeurs van bykans elke bron die opstel en implementeer van 'n behoorlike beleid voorstel.

Die reg op privaatheid in alle regstelsels fokus primêr op diskrete fisiese plekke en eiendom. Volgens Mr JJ Sopinka, regter in die Kanadese Hooggeregshof, is dit nodig om die konsep van privaatheid te hersien indien ons ten volle voordeel wil trek uit moderne tegnologie en vooruitgang.¹⁵⁵

Die implementering van 'n duidelike en volledige beleid ten aansien van die reg op privaatheid, in die verhouding tussen die werkgever en die werknemer, sal tot gevolg hê dat die konflikterende belange van werkgever en werknemer hanteer kan word met die minimale spanning en optimale produktiwiteit.

¹⁵⁵ SM Entwistle *E-mail and Privacy in the Workplace* sementwis@acs.ucalgary.ca.

4.2 Aanbevelings

Werkgewers moet beleid ten aansien van privaatheid ontwerp, op skrif stel, deur werknemers laat onderteken en implementeer. Basiese riglyne vir die beleid sluit die volgende in:¹⁵⁶

Die beleid moet duidelik aandui of die elektroniese media, deur die werkgever voorsien, gebruik kan word vir persoonlike doeleindes of slegs vir besigheid. Verder, indien persoonlike e-pos gestuur mag word, of inligting aangaande die besigheid toelaatbare inhoud is. Of die werkgever die inhoud van elektroniese boodskappe sal monitor en tot watter mate. 'n Duidelike aanduiding dat die werkgever die eienaar van die e-posnetwerk is en dus toegang daartoe het moet verkieslik ingesluit word.

Die beleid moet die versending van pornografiese materiaal verbied om aanspreeklikheid vir seksuele teistering te voorkom. Opinies rakende ras, afkoms, geslag, seksuele oriëntasie, ouderdom, godsdiens, geloofsoortuiging en politieke oortuiging moet aangespreek en verbied word om aanspreeklikheid op grond van diskriminasie te voorkom. Die prosedure wat gevolg gaan word indien die beleid oortree word moet ook duidelik uiteengesit word.

Die werknemer en die werkgever sal baat vind by 'n beleid wat duidelik en behoorlik uiteengesit is. Onbeperkte monitering kan vermy word deur werknemers, langer as 5 jaar in diens, van monitering kwyt te stel, ander werknemers vir 'n beperkte tyd van 2 ure per week te monitor met of sonder kennisgewing. Slegs nuwe werknemers word dan vir 'n tydperk van 60 dae onbeperk gemonitor.

Die druk op die werknemers is gevolglik minder en produktiwiteit kan verhoog. Die teendeel van kennis aan die werknemer gee moet egter

¹⁵⁶ Han H Li *Electronic Mail Privacy in the Workplace* Mailto: hali@lynx.neu.edu.

oorweeg word. Indien werknemers kennis dra van presies wanneer hul gemonitor gaan word, is dit moontlik dat die werknemer vir daardie 2 ure uitstekend presteer en die res van die tyd nie. Die werknemer ontvang dan nie die nodige opleiding en bystand indien dit benodig word nie en is dit nie in die werkgewer se beste belang nie. Beperkte monitering sonder kennisgewing is dus ideaal.

Vir die effektiewe regulering van elektroniese monitering in die werkplek het Allen¹⁵⁷ die volgende kode voorgestel:

(1) Kennisgewing

- (a) 'n algemene kennisgewing moet aan werknemers gegee word dat hul gemonitor mag word, die aard van die monitering en die omvang daarvan;
- (b) daar moet aangedui word dat geen beperking op die omvang van die monitering is nie, hoewel dit billik en proporsioneel tot die oogmerk sal wees;
- (c) werknemers moet 'n indikasie ontvang van die legitieme verwagting, ten aansien van privaatheid, wat verwag kan word.

(2) Oogmerk

- (a) Monitering moet 'n billike besigheidsdoel dien;
- (b) Monitering sal plaasvind ten einde:
 - (i) 'n kwaliteit diens, produktiwiteit of opleiding waar nodig, te verseker om die verwagte standaard te handhaaf; en
 - (ii) nakoming van die beleid deur werknemers, in belang van die werkgewer, te verseker.

¹⁵⁷ BJ Allen *Privacy in the Workplace: Responses to the Electronic Monitoring of Employees in the Private Sector* Des 1996.

(3) Billikheid

- (a) monitering kan nie onder dwang geskied nie;
- (b) monitering moet billik wees ooreenkomstig die werk waarvoor die werknemer verantwoordelik is; en
- (c) evaluering van werknemers moet verkieslik nie alleenlik op grond van elektroniese monitering geskied nie, tensy geen alternatiewe metodes bestaan nie.

(4) Privaatheid

- (a) Elektroniese inligting mag slegs ten aansien van die besigheid verkry word;
- (b) Geen monitering in kleedkamers, sluitkassies en verkleekamers sal toegelaat word nie;
- (c) Indien die besigheid se telefone gemonitor word, moet telefone beskikbaar gestel word, vir privaat gebruik, wat nie aan monitering onderhewig is nie;
- (d) Indien werknemers se e-pos gemonitor word, kan 'n aparte e-pos adres vir privaat gebruik geskep word en kan die werkgever steeds die hoeveelheid tyd bepaal wat daaraan spandeer word, sonder om die inhoud daarvan na te gaan.¹⁵⁸

(5) Toegang

- (a) Werknemers moet toegelaat word om gestoorde inligting te hersien, foute te herstel en seker te maak dit is korrek;
- (b) Gestoorde inligting moet beskerm word en mag aan geen derde persoon openbaar word sonder die werknemer se toestemming nie.

(6) Uitsluitings

- (a) 'n Uitsluiting mag ten aansien van enige van die bogenoemde bepalinge gemaak word as die werkgever redelikerwys vermoed dat die werknemer:

¹⁵⁸ D Carew *Your Boss can't Monitor your Email* Independent Online 07/11/03.

- (i) siviele of kriminele wetgewing oortree, of
- (ii) die belang van die werkgewer of 'n werknemer wesenlik benadeel word.

Die voorgestelde kode balanseer die belange en regte van die werkgewer en die werknemer op so 'n wyse dat beide beskerming geniet. Die beskerming aan werknemers verseker dat werkgewers nie buite hul mag optree nie en verleen aan werkgewers voldoende ruimte om werknemers te monitor. Die vertrouensverhouding tussen werkgewer en werknemer bly dus sodoende behoue.

BIBLIOGRAFIE

ARTIKELS

A

BJ Allen *Privacy in the Workplace: Responses to the Electronic Monitoring of Employees in the Private Sector* Des 1996

B

W Beech of Leppen Beech Attorneys *The Right of an Employer to Monitor an Employee's Electronic Mail, Telephone calls and Internet Usage* News Brief No 14 January 2003

T Bortz *The Regulation of Interception of Communications and the Provision of Communication-related Information Act 70 of 2002* Tech Werks Mrt 2003

C

L Cardonsky *Towards a Meaningful Right to Privacy in the United Kingdom* Boston Univ Int Law J 20 no 2 Fall 2002

D

L Dancaster *Internet Abuse: A survey of South African Companies* (2001) 22 ILJ 862

F

A Farrington *'The E-Corporation' and the Law* Datawatch Iss 47 Jan/March 2001

H

S Hinde *2001: A Privacy Odyssey* 2001 Computers&Security 21

J Hofman *E-commerce and Issues in the Law of Privacy* UCT April/June 2000

M Huie et al *The Right to Privacy in Personal Data: The EU Prods the US and Controversy Continues* TULSA J Comp & Int'L L

L

M Leahy *Recovery and Reconstruction of Electronic Mail as Evidence* 41 AM JUR PROOF OF FACTS 3D 1 (2002)

PAK Le Roux *Employment Practices in the Age of the Internet* 2003
Centre for Business Law UNISA

M

MJ McCarthy *Your Manager's Policy on Employees' E-mail May Have a Weak Spot* WALL ST J Apr 25 2000

S McEvoy *E-Mail and Internet Monitoring and the Workplace: Do Employees Have a Right to Privacy* Fairfield University CT

C Mischke *Workplace Privacy, e-mail interception and the law: Does new legislation limit employers' rights to read e-mail?* Contemporary Labour Law Vol 12, No 8, Mrt 2003

C Morgan *Employer Monitoring of Employee Electronic Mail and Internet Use* (1999) 44 McGill LJ 849

R

A Rogers *You Got Mail But Your Employer Does Too: Electronic Communication and Privacy in the 21st Century Workplace* 5 J Tech L & POL'Y 1 (2000)

J Rothman *CIO Magazine* 15/03/01 CXO Media Inc

T

D Towns *Legal Issues Involved in Monitoring Employees' Internet and E-mail Usage* GIGALAW COM 2 (2002)

BOEKE

B

Bynum & Rogerson *Computer Ethics and Professional Responsibility* 2004 Blackwell Publishing Ltd

D

S Deaken et al *Labour Law* 3rd ed (2001) 326

De Waal et al *Bill of Rights Handbook* 4th ed 2001 (Juta)

G

Gattiker et al *Privacy and Security on the Internet / Information Highway*

URL

H

TC Hartley *The Foundation of European Community Law* 137

N

J Neethling et al *Neethling's Law of Personality* 1995

S

E Shorts et al *Human Rights Law in the United Kingdom* 531
(Sweet&Maxwell ed 2001)

T

B Trout *Internet Laws Affecting Iowa Companies: Online Security* 2nd ed
2003

INTERNET

A Blackwell *Don't expect any Privacy in the Workplace*
amyblackwell@wwwiz.com.

www.dataforensics.com/litigation Computer Forensics for Civil Litigation
-D Carew *Your Boss can't Monitor your Email* Independent Online
07/11/03

www.dataforensics.com/litigation- Computer Forensics for Civil Litigation
M Anderson *Identifying Internet Activity, Computer Forensics Goes to
Cyberspace*

www.deneysreitz.co.za. B Patterson *Insurance Seminar Aug/Sept 2001:
The Internet – An Employee's Right to Privacy* News 2001

www.ebiz.co.zaR Buys *When is E-mail blocking illegal?* Technews

www.epic.org/privacy/workplace/default.html Workplace Privacy
26/11/2003

SM Entwistle *E-mail and Privacy in the Workplace*
sementwis@acs.ucalgary.ca

Han H Li *Electronic Mail Privacy in the Workplace* Mailto:
hali@lynx.neu.edu

www.legalbrief.co.za *Civil Liberties: Snoopers' Charter not a One-way*
Street 6 Okt 2003

www.legalbrief.co.za. L Michalson *Office E-Mail: Consent doesn't have*
to be in writing 6 Okt 2003

www.legalbrief.co.za *Civil Liberties: Snoopers' Charter not a One-way*
Street 6 Okt 2003

www.mlaw.co.za. *The Law Regarding Privacy.*

www.suntimes.co.za. P Sukhraj *New Law Stops Bosses Spying on E-*
mail 2003/02/02

REGSPRAAK

A

Alison Halford v UK Merceyside Police 73/1996/693/884

B

Bamford & others v Energizer (SA) Ltd (2001) 12 BALR 1251 (P)

Bernstein v Bester NNO 1996 (4) BCLR 449 (CC); NO 1996 (2) SA 751
(CC)

C

Council for Scientific & Industrial Research v Fijen (1996) 12 ILJ 18 (A)

Cronje v Toyota Manufacturing (2001) 3 BALR 213 (CCMA)

D

Dausen v State 868 SW 2d 363 (Tex App 1993)

Deal v Spears 980 F 2d 1153 (8th Cir 1983)

Director of Public Prosecutions: Cape of Good Hope v Buthgate 2000 (2) SA 535 (C)

Douglas v Hello! Ltd (2001) QB 967,997 (Eng CA)

F

Ferreira v Levin 1996 (1) SA 984 (CC)

Financial Mail v Sage Holdings 1993 (2) SA 451 (A)

Fraser v Nationwide Mut Ins Co 135F Supp 2d 623 (ED Pa 2001).

G

Grieve v Denel (Pty) Ltd C7/2003, ongerapporteur

H

Hunter v Southam Inc (1984) 1 SCR 21

I

Investigating Directorate: Serious Economic Offences v Huyndai Motor Distributors 2000 (10) BCLR 1079 (CC)

K

K Mart Corp v Trotti 667 SW 2d 632 (Tex App 1984)

Konop v Hawaiian Airlines Inc 2002 WL 1941431

M

McLaren v Microsoft Corporation 1999 WL 229015 (TEX App 1999)
ongerapporteur

Mistry v Interim Medical and Dental Council of South Africa 1998 (4) SA 1127 (CC)

Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA)

N

National Coalition for Gay and Lesbian Equality v Minister of Justice 1999 (1) SA 6 (CC)

O

O'Connor v Ortega 480 US 709, 716 (1987)

P

Pratt & Whitney 26 AMR 36322 12-CA-18446 (Feb 23, 1998)

Protea Technology & another v Wainer & others 1997 (9) BCLR 1225
(W)

R

R v Weir (1998) AJ No 155

S

Sappi Novoboard (Pty) Ltd v Bolleurs (1998) ILJ 784 (LAC)

Shelton v Commissioner for the South African Revenue Stamps 2000 (2)
SA 106 (E)

Simmons v Southwestern Bell Telephone Co 254 F Supp 392 (WD Okla
1987)

Smyth v Pillsbury Company 914 F Supp 97 (ED) Pa 1996

Stauder v City of Ulm 1969 ECR 419

Smuts v Backup Storage Facilities & Others WE 2628-02,
ongerapporteur

T

Thompson Newspapers Ltd v Canada (Director of Investigations and
Research, Restrictive Trade Practises Commission) (1990) 47 CRR 1

Tiberino v Spokane County 13 P 3d 1104 (Wash Ct App 2000)

U

United States v Harpel 423 F Supp 192, 196-97 (DSC 1976)

W

Watkins v LM Berry & Co 704 F 2d 577 (11th Cir 1983)

WETGEWING

Canadian Charter of Rights and Freedoms, Constitution Act 79 of 1982

Canadian Criminal Code RS 1985 c C46

Data Privacy Directive 95/46 EC

Electronic Communications Privacy Act 18 USC 1988

Electronic Communications and Transactions Act 25 of 2002

Europese Konvensie vir die Beskerming van Menseregte en
Fundamentele Vryheid Nov 4 1950 213 UNTS 221

Grondwet van die Republiek van Suid-Afrika 108 van 1996

Human Rights Act 1998 c 42

Interception and Monitoring Prohibition Act 127 of 1992

Interception of Communications Act 1985

Privacy Act RS 1985 c P21

Regulation of Investigatory Powers Act (Communications Data) Order
2003 Statutory Instrument 2003 No 3172

Regulation of Interception of Communications and Provision of
Communication-related Information Act 70 van 2002

United Kingdom Telecommunications (Lawful Business Practice)
(Interception of Communications) Regulations 2000 No 2699

Wet op Arbeidsverhoudinge 66 van 1995

Wet op Bevordering van Toegang tot Inligting 2 van 2000

Wet op Maatskappye 69 van 1973