2014•2015
FACULTEIT RECHTEN
master in de rechten

Masterproef

Werkgeverscontrole op het internetgebruik van de werknemer in het social media tijdperk: een (Europese) update vereist?

Promotor :
Prof. dr. Petra FOUBERT

Joren Janssen
Proefschrift ingediend tot het behalen van de graad van master in de rechten

2014•2015
FACULTEIT RECHTEN
master in de rechten

Masterproef

Werkgeverscontrole op het internetgebruik van de werknemer in het social media tijdperk: een (Europese) update vereist?

Promotor :
Prof. dr. Petra FOUBERT

Joren Janssen
Proefschrift ingediend tot het behalen van de graad van master in de rechten

universiteit hasselt | KU LEUVEN | Maastricht University

Samenvatting

Sociale media hebben ertoe geleid dat het internetgebruik in het laatste decennium sterk veranderd is. Het internet vormt vandaag de dag een immense bron van informatie, entertainment en communicatie, waarbij interactiviteit centraal staat. Dit blijkt niet alleen een gevaar te zijn voor het recht op privacy op zich, maar ook voor de arbeidsverhouding tussen werkgevers en werknemers. Het internet kan onder andere een afleiding vormen voor werknemers, waardoor werkgevers de nood zullen voelen om hun prestaties te controleren. Om de rechten en belangen van beide partijen te vrijwaren is regulering van deze controle gewenst. De volgende vraag stelt zich: voldoet de momenteel geldende wet- en regelgeving betreffende werkgeverscontrole op internetgebruik van een werknemer aan de noden van een arbeidsrelatie in de hedendaagse technologische samenleving?

Het blijkt snel dat de wetgeving ter zake verouderd is. Daarnaast zijn de rechtsnormen wat betreft privacy op het werk erg beperkt in omvang. De Europese Unie heeft twee algemene richtlijnen inzake privacy gepubliceerd die door de Belgische wetgever in nationaal recht zijn omgezet.

Op Europees niveau zijn er momenteel geen bepalingen die van rechtstreeks belang zijn voor het Belgisch rechtsstelsel. Zij hebben als voornaamste waarde dat zij in het verleden een impuls hebben gegeven aan de nationale wetgever om actie te ondernemen. Met een toekomstige Algemene Verordening Gegevensbescherming lijkt een mogelijke stap naar verbetering gezet.

De meest relevante rechtsnormen op nationaal niveau zijn te vinden in een collectieve arbeidsovereenkomst, cao nr. 81 ter bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische communicatiegegevens. Deze cao bepaalt onder welke voorwaarden een werkgever toezicht mag uitoefenen op het internetgebruik van zijn werknemers. Ondanks de vele kritiek op deze cao heeft tot op heden geen andere bijzondere rechtsbepaling het daglicht gezien. Het is aan de rechterlijke macht om de bepalingen van de cao, alsook meer algemene wetgeving, zo goed mogelijk toe te passen in de moderne arbeidsrechtelijke context. Werkgevers worden aangeraden om een eigen beleid inzake internetgebruik op papier te zetten, maar dit is niet meer dan een lapmiddel voor het probleem dat zowel werkgevers als werknemers geen rechtszekerheid hebben. De wet is onvoldoende duidelijk om zeker te zijn van de eigen rechtspositie in geval van een conflict.

Nieuw wetgevend optreden is nodig, bij voorkeur op Europees niveau. Enkel zo zal rechtszekerheid geboden kunnen worden en kan de Europese interne markt verder worden uitgebouwd.

In de Verenigde Staten van Amerika heeft men een ander historisch parcours afgelegd, maar toch is de situatie zeer gelijkaardig aan die in de Europese Unie. De rechter wordt verwacht verouderde wetgeving zo goed mogelijk toe te passen. Voor beide rechtsstelsels wordt dan ook geconcludeerd dat nieuw wetgevend optreden gewenst is, waarbij naar elkaars principes gekeken zou moeten worden om zo een evenwicht te bekomen tussen de belangen van werkgevers en werknemers.

Dankwoord

Zowel de hiernavolgende masterscriptie als dit dankwoord worden openbaar gepubliceerd. Als er iets blijkt uit deze scriptie, is het wel dat hetgeen bewust openbaar wordt gepubliceerd, niet beschermd kan worden door enige privacyverwachting. Toch neem ik de gelegenheid om onomwonden diegenen te danken die me hebben bijgestaan gedurende mijn opleiding en het schrijven van dit eindwerk.

In de eerste plaats kan ik het aantal *likes* dat ik wil versturen naar mijn promotor, prof. dr. Petra Foubert, moeilijk in woorden uitdrukken. Vanaf de dag dat ik het onderwerp voor deze scriptie aan haar voorstelde tot de inzending van een afgewerkt tekstgeheel heb ik op haar doordachte en opbouwende kritiek kunnen rekenen. Ook daarvoor speelde zij al een aanzienlijke rol in mijn opleiding tot jurist en introduceerde ze mij met veel enthousiasme in de juridische wereld met de hoorcolleges "Beginselen van het recht". Ik wil haar dan ook bedanken: niet alleen voor de goede begeleiding bij deze scriptie, maar ook voor het aanwakkeren van mijn interesse voor het (arbeids)recht.

Daarnaast wil ik mijn ouders bedanken voor de steun en de aanmoedigingen doorheen mijn opleiding. Mijn Facebookberichten hebben ze misschien niet *geshared*, maar wel de vele goede en minder goede momenten.

Ook richt ik graag een *tweet* van dank tot mijn vriend, Niels: voor de morele steun en om het beste in mezelf naar boven te halen.

Ten slotte wil ik graag mijn vrienden bedanken die ik heb leren kennen gedurende mijn opleiding. Dankzij hen is deze studieperiode een onvergetelijke ervaring geworden en ik hoop nog lang met hen contact te kunnen houden. Zelfs via sociale media als het moet, na de werkuren natuurlijk.

Joren Janssen Hasselt, 4 januari 2015

Inhoudsopgave

Lijst van afkortingen

BuPo	Internationaal Verdrag inzake burgerrechten en politieke rechten
cao	Collectieve arbeidsovereenkomst
CBPL	Commissie ter bescherming van de persoonlijke levenssfeer
ECPA	Electronic Communications Privacy Act
EHRM	Europees Hof voor de Rechten van de Mens
EU	Europese Unie
EVRM	Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden
GW	Belgische Grondwet
IAO	Internationale Arbeidsorganisatie
IEPA	Internet Employment Privacy Act
NAR	Nationale Arbeidsraad
NLRA	National Labor Relations Act
OESO	Organisatie voor Economische Samenwerking en Ontwikkeling
SCA	Stored Communications Act
SNOPA	Social Networking Online Protection Act
SNS	Sociaalnetwerksite
UVRM	Universe Verklaring van de Rechten van de Mens
VN	Verenigde Naties
VS	Verenigde Staten van Amerika
WAO	Wet arbeidsovereenkomsten, wet 3 juli 1978 betreffende de arbeidsovereenkomsten
WEC	Wet Elektronische Communicatie, wet 13 juni 2005 betreffende de elektronische communicatie
WVP	Wet Verwerking Persoonsgegevens, wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens

Inleiding

1 Probleemschets

"Wat men op het internet zet, is publiek."

Dit was de reactie van prof. em. Roger Blanpain na een vonnis van de Leuvense arbeidsrechtbank, waarin een werknemer zijn ontslag om dringende reden bevestigd zag.[1] Het kaderlid van een technologiebedrijf had op sociaalnetwerksite Facebook neerbuigende berichten geplaatst over de economische resultaten van de onderneming, wat volgens de werkgever leidde tot financieel leed en imagoschade.[2]

De uitspraak van prof. em. Blanpain is op het eerste zicht weinig revolutionair en zowaar vanzelfsprekend. Bij de start van 2015 bleek dat vele Belgen zich voornamen om hun gebruik van sociale media te beperken, onder meer omwille van de gevaren voor hun privacy.[3] Toch zijn vele inwoners van de digitale communicatiewereld zich niet bewust van de risico's die deze met zich meebrengt.

Computers, smartphones, tablets,… Stuk voor stuk zijn deze toestellen niet meer weg te denken uit de moderne leefwereld. Ze worden gebruikt als bron van informatie of entertainment, maar vooral als communicatiemiddel. Elke persoon in het bezit van een dergelijk toestel is ongeacht zijn locatie, indien gewenst, vierentwintig uur op vierentwintig bereikbaar, zeven dagen op zeven.

In het bijzonder door de opkomst van sociaalnetwerksites blijft niets nog geheim, of een gebruiker dient al sterk aandacht te schenken aan de privacy-instellingen van het betrokken communicatieplatform. Via digitale omgevingen delen gebruikers eigen en vaak persoonlijke informatie met hun online *vrienden* of zelfs alle andere gebruikers. Ook daarbuiten kunnen gegevens, zonder medeweten van de oorspronkelijke gebruiker, verspreid worden.

De continue bereikbaarheid van een gebruiker impliceert de aanwezigheid van internet op de werkvloer. Werknemers kunnen communiceren door middel van eigen toestellen, alsook door middel van toestellen ter beschikking gesteld voor hun arbeid. Menig werkgever zal de nood voelen om een controle uit te voeren op het internetgebruik van zijn werknemer, aangezien dit gebruik een nadelige invloed kan hebben op diens werkprestaties. De werknemer kan afgeleid worden van zijn taken, hij kan al dan niet bewust gevoelige informatie van de onderneming verspreiden of gevaarlijke bestanden zoals virussen binnenhalen via het informaticanetwerk.

De privacy van de werknemer ten opzichte van zijn werkgever vormt al jaren een punt van discussie, zowel in de theorie als in de praktijk. Ondanks de onbetwistbare gezagsverhouding van een werkgever ten opzichte van zijn werknemer mag hij in België zijn ondergeschikte noch

[1] X, "Professor Blanpain: 'Flauwe kul dat Facebookpagina privé is'", *De Standaard*, 17 november 2011, http://www.standaard.be/cnt/dmf20111117_145.
[2] Arbrb. Leuven 17 november 2011 (*Option*).
[3] X, "Belg wil minder tijd spenderen aan sociale media", *De Standaard*, 1 januari 2015, http://www.standaard.be/cnt/dmf20150101_01453912.

verbieden contact te hebben met de buitenwereld tijdens zijn diensturen, noch zonder meer zichzelf inzage verlenen in diens correspondentie.

Het recht op privacy van de werknemer en het gezag van de werkgever creëren een spanningsveld in de belangen van beide partijen. Gedurende de jaren ’90 en aan het begin van dit millennium is er zowel op nationaal als supranationaal niveau aandacht besteed aan beleidsvorming omtrent privacy binnen de arbeidsrelatie. Voornamelijk de Belgische wetgever en de sociale partners hebben beleidsdocumenten opgesteld om het moeilijke evenwicht tussen privacy en werkgeverscontrole te vinden.

Sedertdien is met name de rechter aan zet geweest om te toetsen of in individuele gevallen werknemers niet benadeeld worden en of, aan de andere kant, werkgevers voldoende mogelijkheden hebben om hun werknemers te onderwerpen aan een zekere controle. De werkgever zelf kan, binnen de krijtlijnen van de wetgeving, een eigen privacybeleid uittekenen door middel van een arbeidsreglement.

De vraag of de recente ontwikkelingen in het digitale landschap een impact hebben op het conflict ter zake, namelijk de balans tussen de belangen van werkgever en werknemer inzake internetgebruik, is overgelaten aan het oordeel van de rechter. Met recente ontwikkelingen wordt in het bijzonder verwezen naar de dominantie van sociale media en het zogenaamde *web 2.0*. Dit laatste is het gevolg van een evolutie in het internet waarbij interactie tussen beheerder en gebruiker en gebruikers onderling een primair kenmerk is. De wetgever is de laatste jaren opvallend stil gebleven.

Deze scriptie heeft als doel te onderzoeken of de momenteel geldende wet- en regelgeving betreffende de werkgeverscontrole op het internetgebruik van de werknemer voldoet aan de noden van een arbeidsrelatie in de hedendaagse technologische samenleving. De manier waarop de digitale leefwereld vervlochten is met de corporele samenleving doet vermoeden dat het eenvoudigweg bannen van elektronische communicatie op de werkvloer geen optie is. Gezien de rechten van de werknemer is het belangrijk grenzen te stellen aan de mate waarin de werkgever zich kan mengen in de privacy van zijn werknemer. De werkgever mag daarentegen ook niet machteloos staan ten opzichte van onaanvaardbaar gedrag van zijn ondergeschikten.

Biedt de geldende wet- en regelgeving een afdoend arsenaal aan rechten en plichten voor zowel werknemer als werkgever? Of wordt voor de instandhouding van de precaire balans te veel vertrouwd op het oordeel van Vrouwe Justitia en haar rechters? Uit de conclusie van deze scriptie zal moeten blijken of een bijkomend optreden van de (Europese) wetgever gewenst is om de belangen van werkgever en werknemer met elkaar te verzoenen.

2 Methodologie

2.1 Onderzoeksvragen

Deze scriptie is opgebouwd rond volgende centrale onderzoeksvraag:

> Voldoet de momenteel geldende wet- en regelgeving betreffende werkgeverscontrole op internetgebruik van een werknemer aan de noden van een arbeidsrelatie in de hedendaagse technologische samenleving?

Met "noden" wordt verwezen naar het recht op privacy van een werknemer en zijn recht om te communiceren, alsook de nood van een werkgever aan gezag en controle.

Om de centrale onderzoeksvraag te beantwoorden dienen eerst enkele subvragen te worden gesteld en beantwoord. Volgende vragen, onderverdeeld per deel waar zij in hoofdorde zullen voorkomen, zullen behandeld worden.

Deel 1 Elektronische communicatie (binnen de arbeidsverhouding)

- Wat is de rol van internet en sociale media in de moderne samenleving?
- Hoe wordt de toegankelijkheid en openbaarheid van elektronische communicatie in juridisch opzicht afgewogen ten opzichte van het recht op privacy? Welke rechtsbronnen inzake de rechten van de mens zijn van belang?
- Hoe verhoudt het recht op privacy zich ten opzichte van de gezaghebbende positie van de werkgever? Welke belangen spelen een rol in de spanningsverhouding tussen de rechten van werkgever en werknemer?

Deel 2 Werkgeverscontrole van internetgebruik

- Welke supranationale, internationale en Belgische wet- en regelgeving is van toepassing op internetcontrole door de werkgever?
- Kan een werkgever het internetgebruik van zijn werknemers controleren? Welke voorwaarden dienen te worden vervuld opdat deze controle kan plaatsvinden? Op welke wijze kan een werkgever deze controle uitvoeren?
- Kan een werkgever gevolgen verbinden aan de ontdekking van ongeoorloofd internetgebruik? Zijn deze gevolgen proportioneel ten aanzien van de gestelde daden?
- Hoe wordt de wet- en regelgeving vandaag in de praktijk toegepast?
- Wat is de rol van de rechterlijke macht in de feitelijke beoordeling van internetcontrole?
- Is de geldende wet- en regelgeving voldoende om aan de redelijke wensen van werkgevers en werknemers tegemoet te komen?
- Indien de geldende wet- en regelgeving niet tegemoetkomt aan de redelijke wensen van werkgevers en werknemers, welke initiatieven kunnen ondernomen worden om de spanningsverhouding tussen werkgever en werknemer te verlichten?

Deel 3 Werkgeverscontrole van internetgebruik in de Verenigde Staten van Amerika

- Welke beginselen liggen aan de grondslag van de arbeidsrelatie in de Verenigde Staten van Amerika?
- Wordt het spanningsveld tussen werkgever en werknemer betreffende internetcontrole in de Verenigde Staten van Amerika op dezelfde wijze benaderd als in de Europese Unie en België?
- Indien de momenteel geldende wetgeving in België niet toereikend is, kan inspiratie worden gezocht in het rechtsstelsel van de Verenigde Staten van Amerika? Indien de momenteel geldende wetgeving wel toereikend is, kunnen ideeën uit het Amerikaanse stelsel geïmplementeerd worden om de werking van het Belgische stelsel te bevorderen?

2.2 Grenzen van het onderzoek

Deze scriptie zal enkel gaan over controle door een werkgever gericht op het analyseren van de prestaties of integriteit van zijn werknemers, niet over controle gericht op het ontdekken van medische of familiale informatie van de ondergeschikte.

Vanwege de aard van de wet- en regelgeving rond privacy binnen de arbeidsverhouding zal deze scriptie zich in eerste instantie focussen op de situatie in de sector van private ondernemingen. Met name door de uitvaardiging van cao's is de situatie in deze sector juridisch meer gereguleerd. Tenzij expliciet vermeld zal er geen rekening worden gehouden met overheidsbedrijven.

Gezien de eerder technische aard van het onderwerp internet en sociale media, zal de analyse in deze scriptie zich beperken tot een omschrijving van de broodnodige beginselen inzake internet en digitale ontwikkelingen om het geschetste conflict in het arbeidsrecht te kunnen kaderen. Hierbij zal de nadruk liggen op de evolutie van *web 1.0* naar *web 2.0*. Klassieke statische websites, e-mail en sociaalnetwerksites worden in acht genomen, gezien de juridische benadering van deze communicatievormen nagenoeg eenvormig is. Andere vormen van communicatie zoals telefonie vallen buiten het studiegebied van deze scriptie.

Wanneer een verwijzing volgt naar sociaalnetwerksites, zal behoudens uitzondering enkel verwezen worden naar Facebook of LinkedIn. Deze twee sociaalnetwerksites vormen schoolvoorbeelden van zowel privaat als professioneel gerichte sociale media en bieden de mogelijkheid om de meest relevante aspecten van sociaalnetwerksites te bespreken.

Ter inleiding zullen de basiskenmerken van het recht op privacy samengevat worden, alsook zal verwezen worden naar andere rechtsnormen die verder in het onderzoek relevant zullen zijn. De regelgeving van internetcontrole is immers geënt op algemene regelgeving, met name de regels betreffende de rechten van de mens en het arbeidsrecht. Deze informatie kan niet ontbreken, maar dient louter ter plaatsing van het onderwerp en zal slechts beknopt omschreven worden. Op bijzondere regelgeving met betrekking tot internetcontrole door een werkgever zal uiteraard uitgebreider worden ingegaan.

Indien zich problemen of gebreken in de regelgeving of in de praktijk inzake werkgeverscontrole op het internet blijken voor te doen, zullen mogelijke oplossingen geformuleerd worden. Dit echter zonder de pretentie deze zonder meer als voldoende te beschouwen.

2.3 Bronnen en onderzoeksmethode

2.3.1 Bronnenonderzoek

Zoals het een goed jurist betaamt, wordt bij het bronnenonderzoek voor deze scriptie vertrokken vanuit de wet. Na een supranationaal perspectief wordt het Belgisch recht uitgediept en worden richtlijnen, wetten, cao's en andere relevante bronnen van recht bestudeerd.

Na de analyse van de regelgeving wordt de rechtsleer bij het onderzoek betrokken, om een eerste blik op de praktische uitvoering van de regelgeving te krijgen. Er wordt gezocht naar een evenwicht tussen oude en nieuwe bronnen om een beeld te krijgen van de evolutie van het recht, alsook wordt er gestreefd naar een afwisseling van teksten van auteurs genesteld in de mensenrechten met werken van auteurs die zich in het arbeidsrecht verdiept hebben. Op deze manier kunnen verschillende visies vanuit verschillende achtergronden met elkaar vergeleken worden. Wat arbeidsrechtelijke literatuur betreft wordt het proefschrift van Hendrickx, *Privacy en arbeidsrecht*, als uitgangspunt genomen.[4] Dit werk dateert evenwel van 1999, voordat er sprake was van de nieuwe digitale ontwikkelingen waar deze scriptie over handelt. Hoewel de validiteit van deze bron zeker onderkend wordt, wordt deze met een kritisch oog voor nieuwe ontwikkelingen bekeken.

Rechtspraak vormt de derde en laatste stap in dit onderzoek, waarbij individuele gevallen op de voorgrond treden. Zowel internationale, supranationale als nationale rechtspraak komt aan bod, voor zover deze een impact heeft op het Belgische rechtsstelsel. Deze stap dient ter beoordeling van de toepassing van het wettelijk kader.

In een apart deel wordt het recht van de Verenigde Staten van Amerika geanalyseerd, dit met hetzelfde stappenplan in het achterhoofd.

2.3.2 Onderzoeksmethode

Het onderzoek gaat van start met een combinatie van beschrijvende, definiërende en verklarende vragen. Er wordt onderzocht waarover de spanningsverhouding tussen werkgever en werknemer gaat, welke belangen hier spelen, welke impact internet heeft op deze verhouding, welk recht van toepassing is en wat door dit recht bepaald wordt.

De toepassing van het recht in de praktijk wordt beoordeeld aan de hand van evaluerende vragen. Door middel van rechtspraak en hypotheses wordt onderzocht of het recht zoals het is voldoet aan de noden van de hedendaagse samenleving.

[4] F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, xxi+358 p.

De finale onderzoeksvraag van deel 2, namelijk welke initiatieven ondernomen kunnen worden om de situatie voor werkgever en werknemer te verbeteren, is een normatieve vraag. Er wordt onderzocht wat ondernomen kan worden om problemen op te lossen en hoe het recht zou moeten zijn.

Wat de onderzoeksvragen inzake de Verenigde Staten van Amerika betreft, gaat het vanzelfsprekend om vergelijkende vragen. Vooreerst zal een onderzoek moeten worden gevoerd naar de stand van zaken van het rechtsstelsel in de Verenigde Staten, maar het doel van dit deel is met name de aanpak in de Europese Unie en België te vergelijken met deze in de Verenigde Staten. Het gaat om functionele rechtsvergelijking.

De keuze voor de Verenigde Staten van Amerika valt te verdedigen door de grote verschillen in het arbeidsrecht in vergelijking met het Europees stelsel, wat een andere benadering impliceert. Zo zal blijken dat Amerikanen een andere waarde geven aan het recht op privacy dan Europeanen. De juridische notie *privacy* stamt ook uit het Amerikaanse recht.[5] Daarnaast vormen de Verenigde Staten de bakermat voor vele sociaalnetwerksites, wat het interessant maakt om hun visie te bestuderen. De Verenigde Staten hebben veel ervaring met controle van internetgebruik en de evolutie van het Amerikaans recht vormt dan ook een interessant vergelijkingspunt.

3 Structuur

Het onderzoek start met het kaderen van de begrippen elektronische communicatie, internet en sociaalnetwerksites. Hierop volgt een korte uiteenzetting van de regelgeving rond het grondrecht op privacy op basis van artikel 8 van het Europees Verdrag van de Rechten van de Mens. Deel 1 van deze scriptie wordt afgesloten met een afweging van de belangen van de werkgever tegen de belangen van de werknemer.

Deel 2 vormt de kern van het onderzoek en bestaat uit een analyse van de wet- en regelgeving betreffende werkgeverscontrole op het internetgebruik van de werknemer. Het onderwerp hiervan zijn de regels op supranationaal, internationaal en nationaal niveau zoals geldend in België. Ook wordt de aanpak in de praktijk bestudeerd door middel van een analyse van rechtsleer en rechtspraak. Deze informatie dient te leiden tot een voorlopige conclusie in verband met de vraag of de momenteel geldende regelgeving voldoet aan de actuele noden van de sociale partners.

Het derde deel dient een rechtsvergelijkende analyse van de Belgische aanpak met de regels van de Verenigde Staten van Amerika te bieden. Er wordt met name onderzocht of het Amerikaans rechtsstelsel een oplossing kan bieden voor de conflicten die bestaan in het in België geldende stelsel. Ook voor conflictvrije situaties kan het Amerikaans stelsel mogelijk legitieme alternatieven bieden.

Er wordt geëindigd met een besluit, waarbij wordt geconcludeerd of er al dan niet nieuw wetgevend optreden is vereist op internationaal en supranationaal, dan wel op nationaal niveau.

[5] F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, 5.

Deel 1 Elektronische communicatie (binnen de arbeidsverhouding)

1 Elektronische communicatie

De mens is een sociaal wezen. Hij wordt geboren binnen een familie en onderhoudt niet alleen relaties met de leden daarvan, maar ook met vrienden, collega's en andere kennissen. Sommige banden duren zelfs een leven lang. Onderlinge communicatie speelt binnen een dergelijke band een centrale rol. Hendrickx noemt communicatie "een primordiale voorwaarde voor sociaal gedrag".[6] Mensen converseren voortdurend met elkaar: ze wisselen ideeën uit, praten over belangrijke en minder belangrijke gebeurtenissen in het leven en zijn er voor elkaar in goede en slechte tijden.

Gedurende de laatste decennia is elektronische communicatie een steeds groter aandeel van deze communicatie beginnen accommoderen. Ook vanop een afstand, soms zelfs van aan de andere kant van de wereld, kunnen individuen contact met elkaar houden. Maar ook op korte afstand vormt het wereldwijde web een onmiskenbare bron van conversatie en informatie: er bestaan ontelbare internetfora om meningen uit te wisselen, webwinkels om alle mogelijke aankopen te doen, nieuwswebsites om continu op de hoogte te blijven van de actualiteit, enzovoort.

Afhankelijk van de context wordt via elektronische communicatie aldus een zekere hoeveelheid van persoonlijke gegevens overgedragen. Voor deze scriptie worden drie vormen van elektronische communicatie in acht genomen: internet in de klassieke betekenis, elektronisch postverkeer of e-mail en sociaalnetwerksites.

1.1 Internet in de klassieke betekenis

Internet in de klassieke betekenis van het woord, ook wel *web 1.0* genoemd, is de verzameling van statische webpagina's waarvan de ontwerper of beheerder de inhoud bepaalt.[7] Het voornaamste kenmerk hiervan vormt de principiële onmogelijkheid van bezoekers van de website om er zelf informatie aan toe te voegen.[8]

Hoewel zuivere vormen van *web 1.0* in het courante internetlandschap nog moeilijk te onderscheiden zijn, wordt de term van internet in de klassieke betekenis in het kader van deze scriptie gebruikt voor het aanduiden van nieuwswebsites, webshops, websites van bedrijven, enzovoort. De gebruiker bezoekt de website, maar heeft hierbij weinig tot geen input in de informatie die verschijnt op het scherm.

De benaming *web 1.0* doet vermoeden dat het hier gaat over een archaïsche vorm van internetgebruik. Deze websites zijn echter nog steeds van belang aangezien hier in vele gevallen persoonlijke informatie op kan worden achtergelaten. Zo kan men zich inschrijven voor een

[6] F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, 9.
[7] J. LORRÉ, "Facebook en arbeidsrecht: *mysterium tremendum et fascinans*", *RW* 2011, afl. 36, (1498) 1499 en C. PREUMONT, "Les médias sociaux à l'épreuve du droit du travail", *JTT* 2011, afl. 22, (353) 353.
[8] T. STRUBBE, "Is er plaats voor sociale media op de werkvloer?" in B. DE MEULENAERE (ed.), *Internet &/@ Recht*, Gent, Larcier, 2013, (45) 46 (hierna verkort T. STRUBBE, "Is er plaats voor sociale media op de werkvloer?").

nieuwsbrief door zijn of haar e-mailadres achter te laten of kan men een bankrekening openen of een aankoop verrichten door personalia en eventuele betaalgegevens in te vullen.

1.2 E-mail

E-mail kan omschreven worden als digitaal, elektronisch postverkeer.[9] Gebruikers maken een e-mailadres aan bij een online dienstverlener, meestal in de vorm van *(vrij te kiezen naam)@(naam dienstverlener).(extensie)*. Voorbeelden van populaire gratis dienstverleners zijn Outlook.com (voorheen Hotmail), Google Mail en Yahoo! Mail.

E-mails worden, net als fysieke post, gebruikt voor berichten van alle aard. Op veel vlakken vormt e-mail de vervanging van de klassieke briefwisseling: zowel private als professionele informatie wordt uitgewisseld via dit medium.

1.3 Sociaalnetwerksites

Sociaalnetwerksites (SNS) zijn online platformen waarop een gebruiker zich inschrijft en contact legt met andere gebruikers van dit platform.[10] De in juridische kringen algemeen aanvaarde definitie luidt als volgt: sociaalnetwerksites zijn "onlineplaatsen die mensen de gelegenheid bieden om zichzelf voor te stellen, hun sociale netwerken uit te bouwen, hun interesses te delen en verbonden te zijn met anderen."[11]

Via zijn *profiel* of persoonlijke pagina maakt de gebruiker deel uit van een online gemeenschap, waarop hij persoonlijke informatie, boodschappen, fotomateriaal, enzovoort kan delen.[12] De inhoud van het profiel wordt geleverd door de gebruiker zelf.[13]

Sociaalnetwerksites zijn een onderdeel van de ruimere noemer van sociale media, alsook van *web 2.0*. Bij deze opvolger van *web 1.0*, althans bij naam, ligt de nadruk op *user-generated content*. Dit wil zeggen dat de gebruikers van een website in interactie gaan met de ontwerper of beheerder van de website, of met andere gebruikers, en zodoende zelf inhoud voor de website creëren. Sociaalnetwerksites vormen hiervan het voorbeeld bij uitstek, maar ook weblogs, wiki's als Wikipedia en videosites als YouTube vallen onder de noemer *web 2.0*.

---

[9] C.J. MUHL, "Workplace e-mail and Internet use: employees and employers beware", *Monthly Labor Review* 2003, afl. 2, (36) 36 (hierna verkort C.J. MUHL, "Workplace e-mail and Internet use: employees and employers beware").

[10] V. BUELENS en P. STROOBANTS, *Is 'facebooken' een werkwoord?*, Mechelen, Kluwer, 2012, 10.

[11] E. DE PAUW, "Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?", *Orde van de dag* 2010, afl. 49, (5) 7. Zie ook J. LORRÉ, "Facebook en arbeidsrecht: *mysterium tremendum et fascinans*", *RW* 2011, afl. 36, (1498) 1498 en T. STRUBBE, "Is er plaats voor sociale media op de werkvloer?", *supra* noot 8, (45) 46.
Amerikaans auteur Whitfield onderscheidt drie doeleinden waarvoor sociaalnetwerksites worden gebruikt, namelijk (1) om een openbaar of semi-openbaar profiel te creëren, (2) een lijst van connecties op te maken en te behouden en (3) contact te houden met deze connecties, alsook met anderen die van de sociaalnetwerksite gebruik maken. Deze visie strookt aldus met de juridische benadering die in België wordt gevolgd. B.N. WHITFIELD, "Social media @ work: #policyneeded", *Arkansas Law Review* 2013, afl. 3, (843) 845.

[12] J. LORRÉ, "Facebook en arbeidsrecht: *mysterium tremendum et fascinans*", *RW* 2011, afl. 36, (1498) 1498 en R. RAYSMAN, "A practical look at social media policies", *Computer & Internet Lawyer* 2012, afl. 3, (10) 10.

[13] T. STRUBBE, "Is er plaats voor sociale media op de werkvloer?", *supra* noot 8, (45) 46-47.

Twee van de meest gebruikte sociaalnetwerksites zijn Facebook en LinkedIn.[14] Andere klinkende namen van SNS zijn Netlog, Google+ en Twitter. Facebook en LinkedIn zullen doorheen deze scriptie als typevoorbeeld gebruikt worden.

1.3.1 Facebook

Er zijn SNS in alle vormen en maten, met verschillende doeleinden. Sommigen situeren zich voornamelijk in de privésfeer, zoals Facebook, dat de nadruk legt op het contact houden met online *vrienden*. De gebruiker beschikt over een profiel, een persoonlijke pagina, waarop hij informatie kan plaatsen. Deze informatie varieert van personalia en informatie over werkervaring en hobby's tot foto's, video's en verwijzingen naar andere websites. Een belangrijk kenmerk van Facebook, dat ook bij vele andere SNS voorkomt, is *instant messaging*. Gebruikers hebben de mogelijkheid om rechtstreeks naar andere gebruikers private berichten te verzenden, die alleen door de geselecteerde ontvangers gelezen kunnen worden.[15] Ter vergelijking: sociaalnetwerksite Twitter bestaat enkel en alleen maar uit de *instant messaging*-functie en legt de nadruk op korte berichten.[16] Deze SNS komt verder evenwel niet aan bod.

1.3.2 LinkedIn

Andere sociale netwerksites hebben eerder het bewerkstelligen van professionele contacten tot doel, zoals LinkedIn. Het profiel van de gebruiker bestaat hier uit een digitaal curriculum vitae, dat bezocht kan worden door andere gebruikers die onder andere vaardigheden van de profielbeheerder kunnen onderschrijven.[17] De nadruk ligt op professioneel netwerken, waarbij potentiële werkgevers en werknemers kennis kunnen nemen van elkaars profiel.

1.4 Evolutie van *web 1.0* naar *web 2.0*

Door de ontwikkeling van *vindplaats van statische informatie* naar *interactief communicatiemedium* is het internet een plaats van actieve, massale gegevensuitwisseling geworden.[18] De algemene consensus is dat deze evolutie geleidelijk aan toenam aan het begin van het millennium.[19] Men spreekt nu ook wel van "participatief internet".[20] In 2013 maakte 69% van de Belgen gebruik van minstens één SNS.[21]

Ondanks het gebruiksgemak van het wereldwijde web kunnen er vele vraagtekens worden geplaatst bij het gebruik van SNS en het internet in de brede zin. In welke mate is privacy op het

[14] X, "Zeven op tien Belgen actief op sociale netwerken", algemeen persbericht IAB Belgium, 23 januari 2013, http://www.iab-belgium.be/wp-content/uploads/2013/01/Persbericht-IAB-Zeven-op-tien-Belgen-actief-op-sociale-netwerken.pdf.
[15] http://www.facebook.com (consultatie 24 december 2014).
[16] http://www.twitter.com (consultatie 24 december 2014).
[17] http://www.linkedin.com (consultatie 24 december 2014).
[18] T. STRUBBE, "Is er plaats voor sociale media op de werkvloer?", *supra* noot 8, (45) 46.
[19] Darcy DiNucci, een informaticaconsultant, was de eerste om de term *web 2.0* te gebruiken. In 1999 meende zij de eerste tekenen van een nieuwe evolutie op te merken. In 2004 werd de term opnieuw gebruikt door de stichter van mediabedrijf O'Reilly Media, waarna het beschouwd werd als een gevestigd concept. D. DINUCCI, "Fragmented Future", *Print* 1999, afl. 4, (32) 32 en T. O'REILLY, "What is Web 2.0", *O'Reilly.com*, 30 september 2004, http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html.
[20] C. PREUMONT, "Les médias sociaux à l'épreuve du droit du travail", *JTT* 2011, afl. 22, (353) 353.
[21] X, "Zeven op tien Belgen actief op sociale netwerken", algemeen persbericht IAB Belgium, 23 januari 2013, http://www.iab-belgium.be/wp-content/uploads/2013/01/Persbericht-IAB-Zeven-op-tien-Belgen-actief-op-sociale-netwerken.pdf.

wereldwijde web nog aanwezig? Beheerders van websites en zeker van SNS zijn zich bewust van de vraag naar privacy van hun gebruikers. Iemand hoeft evenwel geen informaticus te zijn om eenvoudige privacybeschermende maatregelen te omzeilen en zo toch aan de gewenste informatie te komen. Soms laten gebruikers zelf na zich voldoende te beschermen, met openbaarheid van hun informatie over de hele wereld tot gevolg.

Men wil de burger bewust maken van deze gevaren, wat onder andere heeft geleid tot een uiteenzetting van belangrijke principes door de Europese Unie en aanbevelingen van de Belgische Commissie ter bescherming van de persoonlijke levenssfeer (CBPL).[22] Reeds voor de opkomst van *web 2.0* vaardigde de CBPL een advies uit: toen bestonden er immers ook al andere digitale communicatievormen op de werkvloer, zoals statische websites en e-mail. Ondanks herhaalde pogingen om privacy-instellingen transparant voor en aanpasbaar door gebruikers te maken, hetgeen vooral wat Facebook betreft regelmatig in de media wordt gepubliceerd, blijft er toch kritiek komen op beheerders van SNS.[23] Zo wordt in de meer gespecialiseerde media al druk gespeculeerd over de proceduremogelijkheden die de nieuwe *rechtsvordering tot collectief herstel* teweeg zal brengen in de strijd tegen schendingen van de privacy door SNS.[24]

Vooraleer er wordt ingegaan op de conflictsituatie die ontstaat door het gebruik van elektronische communicatiemiddelen binnen de arbeidsverhouding, wordt er een blik geworpen op de rol van het grondrecht op privacy in de context van elektronische communicatie. Er wordt ook aandacht besteed aan de rechtsbronnen die van belang zijn voor het Belgische rechtsstelsel.

---

[22] Zie o.a. Richtl. Europees Parlement en Raad nr. 95/46/EG, 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb.L.* 23 november 1995, afl. 281, 31-50; Richtl. Europees Parlement en Raad nr. 2002/58/EG, 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, *Pb.L.* 31 juli 2002, afl. 201, 37-47 en COMMISSIE TER BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, advies nr. 10/2000 betreffende het toezicht door de werkgever op het gebruik van het informaticasysteem op de werkplaats, 3 april 2000, 8 p.

[23] Zie o.a. X, "Facebook zet dino in om privacy te controleren", *De Standaard*, 23 mei 2014, http://www.standaard.be/cnt/dmf20140522_01115386; X, "Oostenrijkse advocaat wil Europeanen mobiliseren tegen Facebook", *De Standaard*, 1 augustus 2014, http://www.standaard.be/cnt/dmf20140801_01200554 en X, "Ruim 20.000 deelnemers voor rechtszaak tegen Facebook", *De Standaard*, 6 augustus 2014, http://www.standaard.be/cnt/dmf20140806_01206581.

[24] N. PORTUGAELS, I. SAMYN, W. VANDENBUSSCHE en Y.S. VAN DER SYPE, "Sociale netwerksites en class actions", *Juristenkrant*, afl. 295, 8 oktober 2014, 16 en E. WAUTERS, E. LIEVENS en P. VALCKE, "Bescherming van gebruikers van sociale media. Juridisch perspectief op algemene voorwaarden van socialenetwerksites", *NJW*, afl. 312, 10 december 2014, (866) 880.

Art. XVII.35 en volgende Wetboek Economisch Recht maken het mogelijk voor een geheel van consumenten om een rechtsvordering in te stellen wanneer zij schade hebben geleden als gevolg van een gemeenschappelijke oorzaak. Schade voortvloeiend uit de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer valt hier ook onder (art. XVII.37, 10° Wetboek van economisch recht 28 februari 2013, *BS* 29 maart 2013.).

Deze bepalingen zijn er gekomen naar aanleiding van een aanbeveling van de Europese Commissie op 11 juni 2013, die de lidstaten vraagt ervoor te zorgen dat er gerechtelijke mechanismen zijn voor collectief verhaal. Dit om de toegang tot de rechter te verzekeren. Aanbeveling 2013/396/EU van de Europese Commissie, 11 juni 2013 over gemeenschappelijke beginselen voor mechanismen voor collectieve vorderingen tot staking en tot schadevergoeding in de lidstaten betreffende schendingen van aan het EU-recht ontleende rechten, *Pb.L.* 26 juni 2013, afl. 201, 60-65.

Eveneens op 11 juni 2013 diende de Commissie een voorstel tot richtlijn hieromtrent in. Deze richtlijn trad op 26 november 2014 in werking en dient omgezet te worden tegen 27 december 2016 (art. 21 Richtl. Europees Parlement en Raad nr. 2014/104/EU, 26 november 2014 betreffende bepaalde regels voor schadevorderingen volgens nationaal recht wegens inbreuken op de bepalingen van het mededingingsrecht van de lidstaten en van de Europese Unie, *Pb.L.* 5 december 2014, afl. 349, 1-19).

2 Recht op privacy

Privacy is een actueel voorwerp van discussie over de hele wereld. Het impliceert de bescherming van persoonlijke informatie, het recht van een individu om zijn informatie af te weren van de buitenwereld.[25] Eenieder is gesteld op de vertrouwelijkheid van zijn of haar gegevens, althans in de mate waarin men deze vertrouwelijkheid verwacht. Hendrickx vertrekt bij de definiëring van privacy vanuit de idee dat een persoon het recht heeft om met rust gelaten te worden.[26]

Het recht op privacy is een onvervreemdbaar burgerlijk recht, een mensenrecht van de eerste generatie.[27] Het is ook een persoonlijkheidsrecht, inherent aan het leven.[28] Toch komt het om de haverklap voor dat er een inmenging plaatsvindt in iemands privéleven, al dan niet rechtmatig.

Uit de regelgeving rond het recht op privacy blijkt dat het een mensenrecht is, eigen aan het mens zijn. Toch is de normering rond dit onderwerp beperkt. Er is geen algemeen omvattende wetgeving op de bescherming van de persoonlijke levenssfeer in België. Slechts enkele bepalingen voorzien in het recht op eerbiediging van het privéleven.[29] Naast deze algemene bepalingen is er wel bijzondere regelgeving voorzien voor privacy bij elektronisch communicatieverkeer.

2.1 Recht op eerbiediging van privéleven: principes en uitzonderingen

2.1.1 Uitgangspunt: artikel 8 EVRM

Artikel 8 van het Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM) bepaalt dat eenieder recht heeft op eerbiediging van zijn privéleven, zijn gezinsleven, zijn huis en zijn briefwisseling.[30]

Artikel 22 van de Belgische Grondwet (GW) waarborgt eveneens het recht op eerbiediging van het privéleven.[31] Artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten (BuPo) doet hetzelfde.[32] Deze normen hernemen de basis van hetgeen bepaald in art. 8 EVRM en volgen dezelfde principes.

In zijn rechtspraak geeft het Europees Hof voor de Rechten van de Mens (EHRM) een bijzonder ruime interpretatie aan de begrippen *privé-, familie- en gezinsleven*, waardoor art. 8 EVRM op een brede waaier van situaties van toepassing kan zijn.[33] Ook *correspondentie*, wat ten tijde van het opstellen van het EVRM nog tot letterlijke brievenpost was beperkt, wordt nu ook geacht communicatiemiddelen als telefonie, e-mail en internet te omvatten.[34]

---

[25] F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, 8.
[26] F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, 5.
[27] S. SMIS, C. JANSSENS, S. MIRGAUX en K. VAN LAETHEM, *Handboek Mensenrechten*, Antwerpen, Intersentia, 2011, 20 (hierna verkort S. SMIS, C. JANSSENS, S. MIRGAUX en K. VAN LAETHEM, *Handboek Mensenrechten*).
[28] J. VANTHOURNOUT, "Privacy, informatica en arbeidsverhouding: de catenaccio voorbij?", *TSR* 2002, afl. 4, (479) 484 (hierna verkort J. VANTHOURNOUT, "Privacy, informatica en arbeidsverhouding").
[29] D. HEYLEN en I. VERREYT, *Arbeidsrecht toegepast*, Antwerpen, Intersentia, 2014, 115.
[30] Verdrag 4 november 1950 tot bescherming van de rechten van de mens en de fundamentele vrijheden, *BS* 19 augustus 1955, *erratum BS* 29 juni 1961 (hierna EVRM).
[31] Belgische Grondwet 17 februari 1994, *BS* 17 februari 1994.
[32] Internationaal verdrag 19 december 1966 inzake burgerrechten en politieke rechten, *BS* 6 juli 1983.
[33] S. SMIS, C. JANSSENS, S. MIRGAUX en K. VAN LAETHEM, *Handboek Mensenrechten*, *supra* noot 27, 261.
[34] S. SMIS, C. JANSSENS, S. MIRGAUX en K. VAN LAETHEM, *Handboek Mensenrechten*, *supra* noot 27, 264.

Volgens de letter van het verdrag is er enkel sprake van bescherming van het privéleven tegen inmenging van openbaar gezag, maar in rechtspraak en rechtsleer is algemeen aanvaard dat het artikel ook van toepassing is op horizontale verhoudingen tussen burgers.[35]

Ondanks het belang van het recht op privacy voorziet artikel 8 EVRM in de mogelijkheid om in zekere mate beperkingen te stellen aan dit recht. Het recht op privacy is niet absoluut en kan beperkt worden.[36] Inmenging in de privacy is toegestaan wanneer drie beginselen worden gerespecteerd: het legaliteitsbeginsel, het finaliteitsbeginsel en het proportionaliteitsbeginsel.

2.1.1.1 Legaliteitsbeginsel

Wanneer een inmenging in het privéleven plaatsvindt dient dit bij wet te gebeuren. De burger moet weten wat hem te wachten staat. Men vereist geen wet in de formele zin als grondslag voor de inmenging. Elke duidelijk geformuleerde norm van intern recht, geschreven of ongeschreven, volstaat, zolang de betrokken personen er maar kennis van kunnen krijgen. Bijvoorbeeld een duidelijke en precieze regel in een arbeidsreglement is voldoende.[37]

2.1.1.2 Finaliteitsbeginsel

Art. 8, tweede lid EVRM voorziet limitatief in enkele situaties waarin een inmenging in het privéleven gerechtvaardigd kan zijn. De inmenging dient in een democratische samenleving nodig te zijn "in het belang van 's lands veiligheid, de openbare veiligheid, of het economisch welzijn van het land, de bescherming van de openbare orde en het voorkomen van strafbare feiten, de bescherming van de gezondheid of de goede zeden, of voor de bescherming van de rechten en vrijheden van anderen."[38]

Wat het toezicht op elektronische communicatie betreft dient vooral aandacht te worden besteed aan de grond "handelingen ter bescherming van de rechten en vrijheden van anderen." Later zal blijken dat de concrete toepassing van controlemechanismen door de werkgever gerechtvaardigd wordt met deze reden, voornamelijk verwijzend naar de economische belangen van de onderneming.[39]

2.1.1.3 Proportionaliteitsbeginsel

Ten slotte mag een inmenging in het privéleven enkel gebeuren in de mate dat deze nodig is om het streefdoel, dat men beoogt met de inmenging, te bereiken. Hier wordt een tweeledige toets uitgevoerd: ten eerste wordt bekeken of de maatregelen relevant zijn, ten tweede of deze evenredig zijn aan het gestelde doel.[40] Uit meer bijzondere wetgeving zal bijvoorbeeld blijken dat

[35] T. CLAEYS en D. DEJONGHE, "Gebruik van e-mail en internet op de werkplaats en controle door de werkgever", *JTT* 2001, afl. 792, (121) 122; S. COCKX, "Sociale media in de arbeidsrelatie: 'vriend' of vijand?", *Or.* 2012, afl. 1, (12) 12-13. Deze zienswijze wordt eveneens bevestigd door het Europees Hof voor de Rechten van de Mens: EHRM, *Niemietz t. Duitsland*, 16 december 1992 en EHRM, *Halford t. Verenigd Koninkrijk*, 25 juni 1997. Zie *infra* deel 2, 2.2.2.
[36] C. PREUMONT, "Les médias sociaux à l'épreuve du droit du travail", *JTT* 2011, afl. 22, (353) 354.
[37] T. CLAEYS en D. DEJONGHE, "Gebruik van e-mail en internet op de werkplaats en controle door de werkgever", *JTT* 2001, afl. 792, (121) 123.
[38] Art. 8, tweede lid EVRM, *supra* noot 30.
[39] Zie *infra* deel 1, 3.2 en deel 2, 3.1.2.
[40] D. HEYLEN en I. VERREYT, *Arbeidsrecht toegepast*, Antwerpen, Intersentia, 2014, 116.

de inhoud van e-mails niet gecontroleerd mag worden wanneer de nodige informatie reeds kan bekomen worden door loutere verzendinformatie als de identiteit van de ontvanger en het tijdstip van verzending te verzamelen.[41]

2.1.2 Afstand van het recht op eerbiediging van het privéleven?

Het is algemeen aanvaard dat het recht op privacy geen absoluut recht is, maar kan een individu ook afstand doen van dit recht?

In principe luidt het antwoord "neen". Dit vloeit voort uit het feit dat het gaat om een persoonlijkheidsrecht.[42] Er kunnen evenwel modaliteiten op het recht op privacy bedongen worden. De grenzen van privacy zijn immers relatief en subjectief, het ene individu zal al meer tolerant zijn ten opzichte van controle dan het ander. Denk bijvoorbeeld aan de controversiële controle van de inhoud van handtassen van klanten in een grootwarenhuis.[43] Terwijl de ene klant er geen bezwaar tegen zal hebben om even haar handtas te openen voor de winkelier, zal de ander dit zien als een inbreuk op haar privacy en zal zij weigeren haar handtas boven te halen.

Volgens de leer van de afstand van grondrechten kan iemand onder bepaalde voorwaarden een beperking toestaan op zijn eigen privacy.[44] De inbreuk op het privéleven vereist een individuele, welingelichte en vrije toestemming die de inbreuk voorafgaat. De persoon die toestemming geeft moet met voldoende kennis, zonder invloed van buitenaf, kunnen beslissen. De toestemming dient ook bijzonder voor de specifieke inmenging en herroepbaar te zijn. Elke nieuwe inmenging in de privacy vereist een nieuwe toestemming.[45]

Verder dient er steeds rekening te worden gehouden met de redelijke privacyverwachtingen van de persoon jegens wie een inmenging van zijn privéleven plaatsvindt. Zo zal later in deze scriptie blijken dat bijzonder belang wordt gehecht aan afspraken tussen partijen vooraleer een overeenkomst wordt aangegaan, in het bijzonder een arbeidsovereenkomst.[46] Zijn er geen dergelijke afspraken, dan durft de rechter al eens bijzonder streng optreden voor de werknemer. Zo oordeelde het arbeidshof van Gent dat wanneer de werknemer een mobiele telefoon krijgt van zijn werkgever voor de uitvoering van zijn werk, het niet voorbij de redelijke verwachtingen gaat dat deze een gedetailleerd overzicht zal verkrijgen van het verbruik van de telefoon.[47] De rechter zal snel vertrouwen op het redelijk denkvermogen van de werknemer. Deze wordt verwacht een beroep te doen op zijn gezond verstand.

---

[41] Zie art. 6 cao nr. 81 van 26 april 2002 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische communicatiegegevens, *BS* 29 juni 2002 (hierna verkort cao nr. 81). Zie *infra* deel 2, 3.2.1, ii.
[42] F. HENDRICKX, *Elektronisch toezicht op het werk*, Mechelen, Kluwer, 2005, 34.
[43] X, "Aldi Genk controleert alle handtassen ondanks gewijzigd beleid directie", *Het Belang van Limburg*, 12 augustus 2014, http://www.hbvl.be/cnt/dmf20140811_01213853/aldi-genk-controleert-alle-handtassen-ondanks-gewijzigd-beleid-directie.
[44] F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, 57.
[45] F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, 57.
[46] Zie *infra* deel 2, 4.1.
[47] Arbh. Gent 12 mei 2014, *JTT* 2014, afl. 20, 320-312. Zie ook *infra* noot 292.

2.2 Privacy en elektronische communicatie

Een veel bediscussieerde bedreiging voor privacy is het gebruik van elektronische communicatie en, in het bijzonder, SNS. Voornamelijk jongeren, maar steeds meer mensen van alle generaties, maken gebruik van dit soort communicatieplatform om gebeurtenissen, ideeën en andere hersenspinsels te delen met andere gebruikers.

Een risico bij sociale media is dat een zeer ruime groep van gebruikers van een dergelijk medium vrije toegang heeft tot een groot aantal persoonlijke gegevens van andere gebruikers. Mensen denken vaak niet meer na bij wat ze online plaatsen. Sociale media zijn zo ingebed in de hedendaagse samenleving dat het delen van informatie een dagdagelijks feit is geworden.[48]

Hendrickx verdeelt het begrip *privacy* in verschillende bestanddelen: informationele, communicatieve, fysische en psychische privacy en zelfbepaling.[49] In het bijzonder de eerste twee aspecten zijn van belang wanneer men spreekt van privacy bij elektronische communicatie.

- Informationele privacy wordt omschreven als het recht dat men heeft om persoonlijke informatie te beschermen en controle hierover te hebben.[50] Een voor de hand liggend voorbeeld is de registratie van de frequentie van het gebruik van elektronische communicatiemiddelen en de websites die men bezoekt op de werkvloer.[51]

- Communicatieve privacy bestaat uit de vrijheid om al dan niet communicatie aan te gaan en de toegang tot communicatiemiddelen, alsook de vertrouwelijkheid van communicatie.[52] Zo heeft een werkgever het recht om, zelfs tijdens de werkuren, te communiceren met familieleden.[53]

- Fysische en psychische privacy slaan op de idee dat een persoon zelf bepaalt in welke mate iemand aan hem mag komen, hij verwacht de eerbiediging van zijn integriteit.[54] Zo is er een principieel verbod om een werknemer verplichtend te onderwerpen aan een HIV-test.[55]

- Zelfbepaling, ten slotte, houdt in dat een individu vrij is eigen beslissingen te nemen, zonder druk van de buitenwereld.[56] In arbeidsrechtelijke context is een voorbeeld hiervan de beslissing van een persoon om een geslachtsoperatie te ondergaan. In principe is deze

[48] J. ROUSSEAU en I. PLETS, "Sociale media en arbeidsrecht. Een praktische leidraad voor sociale-mediarichtlijnen" in P. VALCKE, P.J. VALGAEREN en E. LIEVENS (eds.), *Sociale media: actuele juridische aspecten*, Antwerpen, Intersentia, 2013, (119) 121 (hierna verkort J. ROUSSEAU en I. PLETS, "Sociale media en arbeidsrecht").
[49] F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, 7-14.
[50] J. VANTHOURNOUT, "Privacy, informatica en arbeidsverhouding", *supra* noot 28, (479) 488.
[51] Arbh. Gent 12 mei 2014, *JTT* 2014, afl. 20, 320-312.
[52] F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, 181-182.
[53] Dit belet de werkgever echter niet om bepaalde communicatiemiddelen af te sluiten. Het is zijn prerogatief om werknemers toegang te geven tot elektronische communicatiemiddelen of niet. Zie *infra* deel 2, 3.1.2.
[54] F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, 11.
[55] F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, 244.
[56] F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, 12.

beslissing aan zichzelf om te nemen en kan de werkgever dit niet aangrijpen als reden voor ontslag.[57]

Hoewel deze opdeling verhelderend kan zijn, blijkt in de realiteit dat een afbakening tussen deze aspecten moeilijk is geworden. Zo zal, in het kader van elektronische communicatie, nagenoeg nooit een onderscheid kunnen worden gemaakt tussen informationele en communicatieve privacy. De informatie die onrechtmatig ter kennis wordt genomen kan daarnaast ook een impact hebben op de fysische of psychische privacy, of de zelfbepaling, van de communicerende persoon. Deze indeling wordt dan ook ter illustratie van mogelijke schendingen van privacy opgenomen, maar voor een analyse van de praktijk biedt deze verder weinig waarde.

Zowel op Europees als op nationaal niveau zijn er enkele belangrijke bepalingen voorzien om het conflict tussen het recht op privacy en de openbaarheid van elektronische communicatie op te lossen.

2.2.1 EU-richtlijnen

De Europese Unie (EU) hanteert twee, zij het wat oudere, richtlijnen die relevant zijn voor de verwerking van persoonsgegevens en de controle op elektronische communicatie.

Richtlijn 95/46/EG, ook gekend als de privacyrichtlijn, beschermt persoonsgegevens bij de verwerking ervan.[58] Deze richtlijn werd in België geïmplementeerd met de Wet Verwerking Persoonsgegevens.[59]

Richtlijn 2002/58/EG is de opvolger van richtlijn 97/66/EG en handelt in het bijzonder over de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in elektronische communicatie.[60] Deze richtlijn werd in Belgisch recht omgezet door middel van de Wet Elektronische Communicatie (WEC).[61]

Lidstaten moeten via hun nationale wetgeving het vertrouwelijke karakter van elektronische communicatie en de daarmee verband houdende verkeersgegevens garanderen. Richtlijn 2002/58/EG verbiedt het afluisteren of controleren van communicatie wanneer toestemming van de gecontroleerde personen ontbreekt, tenzij overeenkomstig de bepalingen van richtlijn 95/46/EG dergelijke controle geoorloofd is. Ook hierbij wordt verwezen naar de beginselen van art. 8 EVRM.[62]

---

[57] HvJ C-13/94, *P v S en Cornwall County Council*, 30 april 1996.
[58] Richtl. Europees Parlement en Raad nr. 95/46/EG, 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb.L.* 23 november 1995, afl. 281, 31-50 (hierna verkort RL 95/46/EG).
[59] Wet 11 december 1998 tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *BS* 3 februari 1999.
[60] Richtl. Europees Parlement en Raad nr. 2002/58/EG, 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, *Pb.L.* 31 juli 2002, afl. 201, 37-47 (hierna verkort RL 2002/58/EG).
[61] art. 1 wet 13 juni 2005 betreffende de elektronische communicatie, *BS* 20 juni 2005 (hierna verkort WEC).
[62] Art. 5, eerste lid *jo.* art. 15, eerste lid RL 2002/58/EG, *supra* noot 60.

2.2.2 Belgische wetgeving

2.2.2.1 Wet Verwerking Persoonsgegevens

De Wet Verwerking Persoonsgegevens (WVP) van 8 december 1992, ook de privacywet genoemd, beschermt de persoonsgegevens van het individu.

De wet definieert *persoonsgegevens* als "iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon". Deze identificatie dient te gebeuren aan de hand van een identificatienummer of een kenmerkend element van de fysieke, fysiologische, psychische, economische, culturele of sociale identiteit van de natuurlijke persoon.[63]

Wat kan worden gekwalificeerd als *verwerking* van deze persoonsgegevens, wordt ruim geïnterpreteerd. Elke bewerking of elk geheel van bewerking met betrekking tot gegevens die aan een individu worden gekoppeld, op eender welke wijze uitgevoerd, valt onder het toepassingsgebied van de WVP.[64] Elke al dan niet geautomatiseerde verwerking komt in aanmerking.[65]

Uit deze definities blijkt dat het doel van de WVP bestaat uit het verzekeren van bescherming van de persoonlijke levenssfeer van iedere natuurlijke persoon.

De wet bepaalt aan welke voorwaarden voldaan moet zijn opdat persoonsgegevens rechtmatig verwerkt mogen worden. Zo heeft de persoon op wie de controle wordt uitgevoerd recht op een nazicht van de gegevens, heeft hij recht op toegang tot en verbetering van deze gegevens en dienen geautomatiseerde verwerkingen van informatie te worden gemeld bij de CBPL.[66]

Een grondige analyse van deze wet valt buiten het studiegebied van deze masterscriptie. Door de introductie van cao nr. 81 tot bescherming van de persoonlijke levenssfeer van werknemers ten opzichte van de controle op de elektronische onlinecommunicatiegegevens wordt de Wet Verwerking Persoonsgegevens nog maar zelden toegepast in een arbeidsrechtelijke context.[67] Indien toch relevant zal bij de bespreking van de cao een verwijzing worden gemaakt naar de bepalingen van de Wet Verwerking Persoonsgegevens.

2.2.2.2 Overige wetgeving inzake controle op elektronische communicatie

Naast de Wet Verwerking Persoonsgegevens kunnen nog twee bepalingen specifiek voor controle van informaticagebruik genoemd worden, namelijk artikel 124 WEC en artikel 314bis Strafwetboek.

[63] Art. 1, §1 wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS* 18 maart 1993 (hierna verkort WVP).
[64] Art. 1, §2 WVP, *supra* noot 63.
[65] V. OSAER en S. NAYAERT, "Privacy in de werksfeer" in G. VERMEULEN (ed.), *Privacy en strafrecht: nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu, 2007, (513) 544 (hierna verkort V. OSAER en S. NAYAERT, "Privacy in de werksfeer").
[66] Art. 12 en 17 WVP, *supra* noot 63.
[67] Zie cao nr. 81, *supra* noot 41.

De kern van deze artikelen is dat er sprake is van een onrechtmatige handeling wanneer kennis wordt genomen van communicatie zonder toestemming van de deelnemer of deelnemers. Het begrip *kennisname* wordt, net zoals *verwerking* in de WVP, breed geïnterpreteerd.

Art. 124 WEC verbiedt eenieder met opzet kennis te nemen van gegevens inzake elektronische communicatie met betrekking tot een andere persoon zonder diens voorafgaande toestemming.[68] Dit slaat op kennisname van gegevens over de deelnemende partijen of *omstandigheden* van de communicatie die heeft plaatsgevonden.

Art. 314bis Sw. beschermt daarentegen de *inhoud* van elektronische communicatie.[69] In bepaalde rechtsleer wordt geopperd dat dit artikel niet van toepassing is in de arbeidsrechtelijke sfeer, gezien het artikel vereist dat informatie wordt onderschept tijdens de overbrenging ervan. In feite dient er sprake te zijn van afluisteren, hetgeen niet snel voorkomt op de werkvloer. Werkgevers zullen veeleer een *ex post* controle uitvoeren op de communicatie van de werknemers.[70]

2.2.3 Belang van doelpubliek en redelijke verwachtingen

Een algemene regel is dat hetgeen men plaatst op SNS en, *mutatis mutandis*, op het internet, *in se* als publieke informatie wordt beschouwd en geen vertrouwelijkheid geniet die beschermd is door de wet. Dit geldt in arbeidsrechtelijke context zeker wanneer de berichten rechtstreeks te bekijken zijn door andere personeelsleden van de onderneming waar de auteur werkt.[71]

De toegang tot deze publieke informatie kan echter beperkt worden tot voor een selecte groep mensen.[72] Concreet wat Facebook betreft: wanneer *vrienden van vrienden* toegang hebben tot de informatie, kan de informatie niet als privé worden beschouwd. Is de toegang beperkt tot *vrienden*, dan kan men wel voor een bescherming pleiten.[73]

Er dient ten slotte te worden opgelet voor de leer van redelijke privacyverwachtingen.[74] De rechter kan een redenering volgen waarbij hij oordeelt of het redelijk was van de werknemer de mate van privacy te verwachten die hij op het oog had. Het Hof van Cassatie oordeelde dat dit criterium betrekking heeft op de inhoud en de omstandigheden waarin het gesprek *in casu* plaatsvindt.[75] Zoals in de inleiding reeds aangehaald, staat Blanpain hier minder voor open en ontkent hij dat enige redelijke privacyverwachting mogelijk is bij het gebruik van internet, in het bijzonder Facebook.[76]

---

[68] Art. 124 WEC, *supra* noot 61.
[69] Art. 314bis Strafwetboek 8 juni 1867, *BS* 9 juni 1867.
[70] S. COCKX, "Sociale media in de arbeidsrelatie: 'vriend' of vijand?', *Or.* 2012, afl. 1, (12) 14 en P. WATERSCHOOT, "Bespreking van enkele arresten van het Arbeidshof te Gent in verband met het gebruik en misbruik van e-mail en internet op de werkplaats en het controlerecht van de werkgever daarop", *RW* 2009, afl. 18, (730) 740.
[71] Arbrb. Namen 10 januari 2011, *JTT* 2011, afl. 28, 462-463.
[72] V. BUELENS en P. STROOBANTS, *Is 'facebooken' een werkwoord?*, Mechelen, Kluwer, 2012, 16-17.
[73] V. BUELENS en P. STROOBANTS, *Is 'facebooken' een werkwoord?*, Mechelen, Kluwer, 2012, 16-17.
[74] Arbh. Gent 12 mei 2014, *JTT* 2014, afl. 20, 320-312.
[75] K. VAN KILDONCK, "Privacy werknemers: onrechtmatig verkregen bewijs op het werk", *NJW* 2010, afl. 218, (180) 180.
[76] X, "Professor Blanpain: 'Flauwe kul dat Facebookpagina privé is'", *De Standaard*, 17 november 2011, http://www.standaard.be/cnt/dmf20111117_145.

Hoe meer publiciteit een individu aan zijn opvattingen geeft, hoe meer hij kan verwachting dat anderen er kennis van nemen en hoe minder hij zich bijgevolg zal kunnen beroepen op zijn recht op privacy.[77] Rechtspraak en rechtsleer zijn wel nog verdeeld over de stelling dat een persoon zich onbetwistbaar bewust moet zijn van de mate waarin hij beperkingen erkent van zijn recht op privacy. Zo ook het arbeidshof te Brussel, dat oordeelde dat het potentieel toegankelijk zijn van een niet-beveiligd discussieforum voor *elke* gebruiker voldoende is om te spreken over openbaarheid.[78]

[77] S. COCKX, "Sociale media in de arbeidsrelatie: 'vriend' of vijand?', *Or.* 2012, afl. 1, 14-15.
[78] Arbh. Brussel 4 maart 2010, A.R. 2010/AG/00014, onuitg. en S. COCKX, "Sociale media in de arbeidsrelatie: 'vriend' of vijand?', *Or.* 2012, afl. 1, (12) 15.

3 Tegengestelde belangen op de werkvloer

Een werknemer heeft als natuurlijke persoon het recht op respect voor zijn of haar privéleven en correspondentie. Dit recht op privacy mag niet zomaar met de voeten getreden worden.

Toch betreden we binnen het arbeidsrecht een bijzonder gebied, dit blijkt reeds uit enkele beginselen van de arbeidsverhouding uit de wet arbeidsovereenkomsten (WAO). Werkgever en werknemer zijn elkander eerbied en achting verschuldigd en zij zullen bij de uitvoering van de overeenkomst de welvoeglijkheid en goede zeden in acht moeten nemen.[79] Daarnaast is de werknemer verplicht zijn werk zorgvuldig en nauwkeurig te verrichten op tijd, plaats en wijze zoals is overeengekomen. Hij moet de bevelen en instructies van zijn werkgever volgen, zich onthouden van al hetgeen schade kan berokkenen aan zijn eigen veiligheid of die van zijn werkgever, alsook onthouden van het bekendmaken van geheimen van de onderneming of het verrichten van oneerlijke concurrentie.[80]

De werkgever beschikt in de arbeidsrelatie dus over een gezaghebbende positie waarbij hij een grote impact kan en zal hebben op de tijdsbesteding van *zijn* werknemer gedurende de uren dat deze onder zijn gezag staat.[81] Hij heeft immers het recht om zijn werknemer *niet* met rust te laten.[82]

Waar verbale of fysieke communicatie, door middel van een gesprek op de werkvloer of het verzenden van brieven, nog eenvoudig door de werkgever in het oog gehouden kon worden, is elektronische communicatie veel sneller en eenvoudiger toegankelijk voor de werknemer. Zo zal deze sneller in de verleiding komen om even het werk links te laten liggen om bijvoorbeeld een e-mail te sturen naar zijn vrienden of zijn mening te uiten op een online nieuwsbericht. Dit terwijl de werknemer bij het aangaan van een arbeidsovereenkomst nochtans in zekere mate afstand doet van zijn individuele vrijheid.[83]

Om zich ervan te verzekeren dat de werknemer zich aan de in de arbeidsovereenkomst gestelde regels houdt en zijn werk naar behoren uitvoert, kan een controle van diens activiteiten dus opportuun lijken. In talloze arbeidsrelaties wordt informatica-apparatuur voorzien om de werknemer bij te staan in het uitvoeren van zijn werkzaamheden, maar dit impliceert niet dat deze hem eveneens ter beschikking wordt gesteld om op regelmatige wijze privécommunicatie te voeren.

Dit creëert een spanningsveld tussen onder andere het recht op eerbiediging van de persoonlijke levenssfeer van de werknemer en het werkgeversgezag.

---

[79] Art. 16 wet 3 juli 1978 betreffende de arbeidsovereenkomsten, *BS* 22 augustus 1978, *erratum BS* 30 augustus 1978 (hierna verkort WAO).
[80] Art. 17 WAO, *supra* noot 79.
[81] Art. 17, 1° en 2° WAO, *supra* noot 79.
[82] F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, 32. Dit in tegenstelling tot het uit het recht op privacy afgeleide recht van de werknemer om met rust gelaten te worden, zie *supra* noot 26.
[83] D. HEYLEN en I. VERREYT, *Arbeidsrecht toegepast*, Antwerpen, Intersentia, 2014, 114.

In het *human resources management* zijn er verschillende strekkingen over het omgaan met werknemers. Aanhangers van de *agency theory* zullen een doorgedreven controle bepleiten, aangezien werkgever en werknemer conflicterende doelen hebben. Zonder controle zullen werknemers hun eigen doelstellingen nastreven, ten nadele van de werkgever. De *stewardship theory* daarentegen stelt voor te vertrouwen in de werknemer, aangezien het niet zeker is dat hij zijn divergerende doelstellingen zal nastreven ten nadele van de werkgever.[84]

Zelfs al wordt uitgegaan van een vertrouwensband tussen werkgever en werknemer, nog steeds zal de werkgever in vele gevallen willen overgaan tot een toetsing van de naleving van zijn werknemer aan voornoemde plichten.[85] Daarnaast hoeft controle niet te stammen uit wantrouwen van de werkgever, maar kan het ook gaan over een onderzoek nadat het onder de aandacht van de werkgever is gekomen dat er verdachte handelingen plaatsvinden op het netwerk van het bedrijf, of wil hij gewoon een routinecontrole uitvoeren om informatie te verzamelen over het nut van zijn informaticanetwerk.

Toch kan een onbeheerste controle vele negatieve gevolgen hebben voor de arbeidsrelatie. Werknemers zullen eerder stiekem op het internet gaan surfen via hun eigen elektronische toestellen, hetgeen nog steeds een bedreiging vormt voor de productiviteit. Ze zullen zich minder goed voelen op de werkvloer, waardoor de onvrede stijgt.[86] Zo lijden zowel werknemer als werkgever onder de gebeurtenissen.

Vooraleer in te gaan op de mogelijkheden van werkgeverscontrole op het internetgebruik van zijn werknemers, is het belangrijk een beeld te krijgen van de conflicterende rechten en belangen die spelen tussen beide partijen. Hieruit zal blijken dat het al dan niet gedogen van internetcontrole op de werkvloer geen eenvoudige kwestie van *wel* of *niet* is.

3.1 Belangen van de werknemer

3.1.1 Recht op privacy

Het recht op privacy geldt net zoals in het dagdagelijkse leven ook op de werkvloer. Dit recht is evenwel niet absoluut en kan worden ingeperkt. Om dit te kunnen doen moet er wel voldaan worden aan de eerder vermelde legaliteits-, finaliteits- en proportionaliteitstoets.[87] De arbeidsrelatie kan zo aanzienlijke beperkingen leggen op de draagwijdte van het recht op privacy.

Een grondrecht van de werknemer kan op twee manieren bekeken worden: ofwel als een recht waaraan *geknabbeld* wordt door het gezag van de werkgever, ofwel als een begrenzing van dat gezag. De zienswijze bepaalt veel voor de verdere opiniëring rond dit onderwerp.[88] Het uitgangspunt van deze scriptie is vooralsnog dat het recht op privacy als grondrecht in principe voorrang heeft, met het werkgeversgezag als beperking op dit recht.

[84] R. CAERS, *Human Resource Management in essentie*, Antwerpen, Intersentia, 2013, 8-9.
[85] Zie *supra* noot 79-81.
[86] C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 357.
[87] Zie *supra* deel 1, 2.1.1.
[88] F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, 35.

De minister van Justitie bevestigde in 2000, als reactie op een parlementaire vraag van Geert Bourgeois, dat de werknemer op de werkvloer wel degelijk over communicatievrijheid beschikt. De werkgever mag enkel controleren met als doel te bepalen of de werkzaamheden hierdoor worden verhinderd of niet.[89]

In het arrest *Niemietz* besliste het EHRM dat er geen onderscheid mag gemaakt worden tussen gesprekken met privé en met zakelijk karakter, aangezien beide beschermd worden door art. 8 EVRM.[90]

3.1.2 Recht op vrijheid van meningsuiting

Hoewel het recht op privacy het voornaamste belang van de werknemer is in onderhavig conflict, kan ook zijn recht op vrijheid van meningsuiting in het gedrang komen. Eenieder heeft op grond van art. 10 EVRM en art. 19 GW immers het recht een vrije mening te koesteren en hierover inlichtingen of denkbeelden te ontvangen of te verstrekken, zonder inmenging van enig gezag.[91]

Dit is echter ook geen absoluut recht, er zijn grenzen aan wat men mag verkondigen. Zo zal de werkgever wel degelijk kunnen ingrijpen wanneer een werknemer bijvoorbeeld onrust veroorzaakt op de werkvloer door ruzie te stoken of de onderneming in een slecht daglicht plaatst bij de buitenwereld.[92]

3.2 Belangen van de werkgever

Vroeger bestond internetgebruik voornamelijk uit eenrichtingsverkeer, waarbij de bezoeker slechts gebruik maakte van hetgeen de beheerder ter beschikking stelde: niet meer, niet minder. Door de evolutie naar *web 2.0* is daar verandering in gekomen. Zeker sociale media spelen sterk in op interactieve aspecten, waardoor de gevaren op de werkplaats ook zijn toegenomen. Een sociale mediabeleid is geen overbodige luxe, zoals ook Ikea moest vaststellen in 2012 toen werknemers een gespreksgroep op Facebook wijdden aan "domme vragen van klanten".[93]

Er zijn verscheidene redenen waarom werkgevers niet enthousiast zouden zijn over de aanwezigheid van elektronische communicatie op de werkvloer. De belangen van de werkgever in het conflict betreffende internetcontrole kunnen in vier begrippen worden samengevat: gezag, eigendomsrecht, loyauteit en vertrouwelijkheid.

3.2.1 Gezag

Bij het invoeren van de wet op de arbeidsovereenkomst van 10 maart 1900 was het fundamenteel beginsel van de arbeidsrelatie dat er een absoluut gezag was van de werkgever ten opzichte van de werknemer.[94] Van zodra de werknemer de fabriek binnenstapte, verloor hij zijn eigenheid en

[89] Vr. en Antw. Kamer 1999-00, 28 april 2000, 3816 (Vr. Nr. 93 Bourgeois).
[90] EHRM *Niemietz t. Duitsland*, 16 december 1992.
[91] Art. 10 EVRM, *supra* noot 30 en art. 19 Belgische Grondwet 17 februari 1994, *BS* 17 februari 1994.
[92] J. LORRÉ, "Facebook en arbeidsrecht: *mysterium tremendum et fascinans*", *RW* 2011, afl. 36, (1498) 1507.
[93] X, "Personeel van Ikea lacht met 'domme klanten'. Meubelketen werkt aan richtlijnen voor gedrag op Facebook", *De Standaard*, 16 februari 2012, http://www.standaard.be/cnt/gvb3m9age.
[94] Wet 10 maart 1900 op de arbeidsovereenkomst, *BS* 14 maart 1900.

stond hij onder patronaal gezag en toezicht.[95] Er bestond een ondoordringbare scheidingsmuur tussen het privéleven en het arbeidsleven. De werknemer had binnen de onderneming geen enkel recht op privacy, buiten de deuren was hij vrij te doen en te laten wat hij wilde.[96]

Deze visie is sindsdien sterk getemperd, maar nog steeds is de gezagsuitoefening een grondbeginsel van de arbeidsverhouding en wordt een zekere band van ondergeschiktheid gecreëerd binnen de horizontale rechtsrelatie.[97]

Het gevaar voor "virtueel absenteïsme" is groot: werknemers zijn *fysiek* aanwezig op de werkvloer, maar *virtueel* afwezig vanwege de afleiding.[98] Dit leidt tot een gebrek aan naleving van de instructies van de werkgever, wat zijn gezag ondermijnt.

3.2.2 Eigendomsrecht

De werkgever heeft de plicht de nodige materialen te voorzien opdat de werknemer zijn werk zoals overeengekomen kan uitvoeren.[99] De werkgever is eigenaar van deze materialen, zoals computers, het draadloos netwerk, enzovoort.

Art. 20, 1° WAO bepaalt uitdrukkelijk dat deze materialen ter beschikking worden gesteld voor de uitvoering van het werk. De werkgever kan zich dan ook beroepen op zijn eigendomsrecht wanneer de materialen misbruikt worden voor privégebruik of verkeerd (schadelijk) gebruik.[100]

3.2.3 Loyauteit

Werkgever en werknemer zijn elkaar eerbied en achting verschuldigd.[101] Dit houdt in dat zij elkaar niet zullen zwartmaken bij anderen door bijvoorbeeld op het internet kwaadsprekende berichten te verspreiden. In dat geval spreekt men mogelijk van laster en eerroof.[102]

Zoals Rousseau en Plets omschrijven, elke werknemer is in de hedendaagse maatschappij een potentiële woordvoerder van de onderneming geworden.[103] De werkgever mag dan ook redelijkerwijs van de werknemer verwachten dat deze zich behoorlijk gedraagt buiten de onderneming, eveneens op het internet. Een kaderfunctie of gelijkaardige posities kunnen bij de beoordeling van kwalijke handelingen door de werknemer als verzwarende omstandigheid in rekening worden gebracht.[104]

---

[95] J. LORRÉ, *Sociale media en werkgeverscontrole*, Mechelen, Kluwer, 2012, 105.
[96] V. OSAER en S. NAYAERT, "Privacy in de werksfeer", *supra* noot 65, (513) 513.
[97] Art. 2, 3, 4, 5 en art. 19, 1° *jo*. 17, 2° WAO, *supra* noot 79.
[98] S. COCKX, "Sociale media in de arbeidsrelatie: 'vriend' of vijand?', *Or.* 2012, afl. 1, (12) 22.
[99] Art. 20, 1° WAO, *supra* noot 79.
[100] Art. 544 Burgerlijk Wetboek 21 maart 1804, *BS* 3 september 1807.
[101] Art. 16 WAO, *supra* noot 79.
[102] S. COCKX, "Sociale media in de arbeidsrelatie: 'vriend' of vijand?', *Or.* 2012, afl. 1, (12) 19.
[103] J. ROUSSEAU en I. PLETS, "Sociale media en arbeidsrecht", *supra* noot 48, (119) 121.
[104] Arbrb. Leuven 17 november 2011 (*Option*).

3.2.4 Vertrouwelijkheid

De werknemer moet zich ervan onthouden geheimen bekend te maken, in het bijzonder deze die de werkgever kunnen schaden. Deze plicht strekt ook tot buiten de werkuren.[105]

3.3 Courante vormen van werkgeverscontrole

De Belgische wetgever en de sociale partners hebben getracht een balans te creëren tussen de belangen van werkgever en werknemer die, zoals uit het voorgaande blijkt, soms lijnrecht tegenover elkaar staan.

De werkgever zal, onder bepaalde voorwaarden, controle kunnen uitvoeren op het gedrag van zijn werknemers. Enkele mogelijkheden zijn toezicht door middel van camera's, uitgangscontroles bij vermoeden van diefstal, medische en psychologische onderzoeken, telefoontap, het opslaan van elektronische gegevens,…

Bepaalde vormen van controle worden door cao's van de Nationale Arbeidsraad (NAR) gereglementeerd. Zo zijn er:

- cao nr. 68 van 16 juni 1998 betreffende camerabewaking;[106]
- cao nr. 81 van 26 april 2002 betreffende controle op elektronische communicatiegegevens;[107]
- cao nr. 89 van 30 januari 2007 betreffende diefstalpreventie en uitgangscontroles, en;[108]
- cao nr. 100 van 1 april 2009 betreffende een preventief alcohol- en drugsbeleid.[109]

Een andere vorm van controle op de werknemer is een gps- en car-tracingsysteem, waarbij de werkgever informatie kan verkrijgen over de locatie van zijn werknemers. Hier bestaat geen collectieve arbeidsovereenkomst over, de WVP is van toepassing.[110]

Hierna zal enkel nog worden ingegaan op de controle van het internetgebruik van de werknemer en hoe de tegengestelde belangen van werkgever en werknemer in deze situatie verzoend worden.

[105] Art. 17, 3° WAO, *supra* noot 79.
[106] Cao nr. 68 van 16 juni 1998 betreffende de bescherming van de persoonlijke levenssfeer van werknemers ten opzichte van de camerabewaking op de arbeidsplaats, *BS* 2 oktober 1998.
[107] Cao nr. 81, *supra* noot 41.
[108] Cao nr. 89 van 30 januari 2007 betreffende de diefstalpreventie en de uitgangscontroles van werknemers bij het verlaten van de onderneming of de werkplaats, *BS* 11 mei 2007.
[109] Cao nr. 100 van 1 april 2009 betreffende een preventief alcohol- en drugsbeleid in de onderneming, *BS* 13 juli 2009.
[110] D. HEYLEN en I. VERREYT, *Arbeidsrecht toegepast*, Antwerpen, Intersentia, 2014, 132.

4 Tussenconclusie

Elektronische communicatie is niet meer weg te denken uit het hedendaagse leven. Informatie kan in een oogwenk uitgewisseld worden via digitale kanalen, wat de huidige maatschappij een razendsnelle mogelijkheid tot dialoog biedt. De snelheid en eenvoud waarmee via de digitale weg gecommuniceerd kan worden, is zowel een grote troef om vlot te communiceren als een gevaar voor het recht op privacy.

Het recht op eerbiediging van het privéleven is een fundamenteel recht dat eigen is aan het mens zijn. Dit recht wordt met name bevestigd door art. 8 EVRM en art. 22 GW. Beheerders en gebruikers van het internet, van e-mail en in het bijzonder van SNS dienen de eisen van de wetgevers te respecteren. Dit zowel wat de supranationale als de nationale normen betreft. De voornaamste rechtsnormen inzake het recht op privacy waarbij hier naar verwezen kan worden zijn richtlijnen 95/46/EG en 2002/58/EG van de Europese Unie, alsook de Belgische Wet Verwerking Persoonsgegevens, art. 124 Wet Elektronische Communicatie en art. 314bis Strafwetboek.

Het recht op privacy is niet absoluut, ook niet binnen de arbeidsrelatie. Het is eigen aan de arbeidsovereenkomst dat de werkgever een gezaghebbende positie heeft ten opzichte van zijn werknemers en dat hij hen verplichtingen en beperkingen kan opleggen. Hoewel de werknemer als natuurlijke persoon dus beschikt over het recht op privacy en vrijheid van meningsuiting, dienen deze fundamentele rechten steeds in afweging te worden gebracht ten opzichte van het gezag, het eigendomsrecht en de loyauteits- en vertrouwelijkheidsverwachting van zijn werkgever. Dit is een moeilijke evenwichtsoefening die veelal geval per geval beoordeeld moet worden.

De Belgische wetgever en de sociale partners hebben regelgeving voorzien voor verscheidene vormen van toezicht door de werkgever op de werknemer, ook wat betreft internetcontrole. Deze regelgeving dient practici te helpen bij het zoeken naar de juiste balans tussen de rechten en belangen van werkgever en werknemer.

Deel 2 Werkgeverscontrole van internetgebruik

1 Inleiding

De aanwezigheid van sociale media binnen de arbeidsverhouding kan druk zetten op de goede verstandhouding tussen werkgever en werknemer. Hoewel het internet vele communicatiemogelijkheden biedt voor werknemers om onder andere een snel contact te hebben met werkrelaties of om bekendheid te geven aan hun bedrijf, wordt de opkomst van het *web 2.0* niet overal toegejuicht. Een van de grootste bedreigingen is het virtueel absenteïsme, waarbij werknemers hun werk laten liggen om op het internet te surfen.[111] Dit zorgt voor frustratie bij de werkgever, die van zijn werknemers toewijding verwacht.[112] Sociale media worden door vele werkgevers aanzien als een kwaal op de werkvloer, in plaats van een mogelijke aanwinst.[113]

Werkgevers zullen dan ook de nood voelen om het online gedrag van hun werknemers onder bepaalde omstandigheden te controleren. Zij het om de vooruitgang van hun dagtaken in het oog te houden, zij het om (het informaticanetwerk van) de onderneming te beschermen tegen de buitenwereld.

Zowel op internationaal als op supranationaal niveau is aandacht besteed aan de spanningsverhouding tussen werkgever en werknemer en de mate van toezicht die de werkgever mag uitoefenen. Toch bevindt het zwaartepunt van relevante wet- en regelgeving zich op nationaal niveau. Ten eerste heeft de omzetting van de relevante richtlijnen van de Europese Unie, richtlijnen 95/46/EG en 2002/58/EG, plaatsgevonden. Daarnaast verdient met name de collectieve arbeidsovereenkomst inzake werkgeverscontrole van internetgebruik op de werkvloer aandacht.[114]

In dit deel volgt een analyse van de relevante wet- en regelgeving ter zake, geplaatst tegenover rechtsleer en rechtspraak. Vervolgens zal onderzocht worden of controle door de werkgever mogelijk is, wat de voorwaarden hiervoor zijn en wat deze regels betekenen in de praktijk. Hierna wordt afgetoetst welke gevolgen de werkgever volgens de wet en de praktijk kan verbinden aan ongeoorloofd internetgebruik en welke bewijslast op hem rust. Ten slotte zullen aanbevelingen worden geformuleerd voor werkgevers en werknemers om op een praktisch haalbare en voor alle partijen bevredigende wijze om te gaan met internetgebruik, voor zover dit juridisch aanvaardbaar is.

---

[111] S. COCKX, "Sociale media in de arbeidsrelatie: 'vriend' of vijand?', *Or.* 2012, afl. 1, (12) 22.
[112] X, *Helft van het werk blijft liggen*, 5 juni 2014, http://www.hrsquare.be/nl/nieuws/6199/helft-van-het-werk-blijft-liggen.
[113] X, *Sociale media nog niet ingeburgerd op de werkvloer*, 6 december 2013, http://www.hrsquare.be/nl/nieuws/5878/sociale-media-nog-niet-ingeburgerd-op-werkvloer.
[114] Cao nr. 81, *supra* noot 41.

2 Werkgeverscontrole op internationaal en supranationaal niveau

Meerdere internationale en supranationale instanties hebben zich uitgesproken over hoe de bescherming van persoonlijke gegevens dient te gebeuren binnen de respectievelijke lidstaten. Weinigen hebben zich echter toegelegd op de bescherming van deze gegevens binnen de arbeidsrelatie, al dan niet omdat dit niet binnen hun bevoegdheidsdomein valt. Dit nichedomein ging, net zoals voor de Belgische wetgever, te ver voor vele internationale en supranationale machtshebbers. Zij spraken zich uit over het recht op privacy in het algemeen, zij het met een eenzame op de arbeidsrechtelijke context toegespitste richtlijnbepaling hier en daar.[115]

Toch was de vrees voor massale gegevensverwerking en -verzameling in de arbeidsrelatie, na de introductie van geïnformatiseerde systemen zoals computers, groot. Hier werd voornamelijk op gereageerd met aanbevelingen, *soft law*, in de hoop dat er zich geen onrechtvaardige situaties zouden voordoen. Deze aanbevelingen dateren voornamelijk van de jaren '90, voor de opkomst van *web 2.0*.[116]

Hiermee kan meteen het geringe belang van de supra- en internationale regelgeving voor de nationale – Belgische – sociale partners gesignaleerd worden. De juridische toepassing van het begrip *privacy* in de arbeidsrechtelijke context is, ondanks recentelijk toegenomen aandacht van internationale instanties, voornamelijk een nationaalrechtelijke aangelegenheid gebleven.[117]

Achtereenvolgend zal een blik worden geworpen op de inspanningen die de Europese Unie en de Raad van Europa tot nog toe hebben geleverd ter bescherming van privacy in het arbeidsrecht. Ter illustratie van de vermelde *soft law* aanbevelingen wordt de gedragscode van de Internationale Arbeidsorganisatie (IAO) aangehaald. De aanbevelingen van de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) inzake gegevensbescherming werden eveneens bestudeerd, maar de gedragscode van de Internationale Arbeidsorganisatie blijkt voldoende om een beeld te geven van de waarde van deze *soft law*.[118]

2.1 Europese Unie

Er bestaat momenteel geen bijzondere regelgeving van de Europese Unie inzake de bescherming van de gegevens van werknemers. Er dient te worden verwezen naar de geldende richtlijnen inzake gegevensbescherming in het algemeen, namelijk richtlijnen 95/46/EG en 2002/58/EG.[119] Deze gelden, bij gebrek aan een *lex specialis*, ook voor gegevensbescherming in de arbeidsrelatie en hun bepalingen zullen naar analogie moeten worden geplaatst in het licht van de spanningsverhouding tussen werkgever en werknemer.

---

[115] Art. 8, eerste en tweede lid, b RL 95/46/EG, *supra* noot 58.
[116] Bijvoorbeeld IAO, *Protection of workers' personal data. An ILO code of practice*, Genève, IAO, 1997; Algemene Vergadering Verenigde Naties, *Guidelines for the Regulation of Computerized Personal Data Files*, New York, Verenigde Naties, 1990 en OESO, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Parijs, 1980.
[117] De Europese Unie lijkt op weg om zich meer expliciet uit te spreken over welke werkgeverscontrole al dan niet aanvaardbaar is op de werkvloer. Zie *infra* inzake de Algemene Verordening Gegevensbescherming, deel 2, 2.1.2.2.
[118] OESO, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Parijs, 1980.
[119] Zie *supra* noot 58 en 60.

De doelstelling van de Europese Unie bij het reguleren van gegevensbescherming is het bewerkstelligen van de interne markt. De grondslag voor de richtlijnen was oud artikel 7 A van het Verdrag tot oprichting van de Europese Gemeenschap, huidig artikel 26 VWEU.[120] Dit artikel bepaalt dat de Unie de maatregelen vaststelt "die ertoe bestemd zijn om de interne markt tot stand te brengen en de werking ervan te verzekeren, overeenkomstig de bepalingen terzake van de Verdragen." Men wil zo goed mogelijk een ruimte bekomen zonder binnengrenzen, waarin goederen, personen, diensten en kapitaal vrij kunnen bewegen.[121]

Ondanks het gebrek aan bijzondere wetgeving heeft de Europese Commissie overleg gehad met de sociale partners en heeft zij aandacht getoond voor de rechten, plichten en belangen die spelen op de werkvloer.[122] In 2012 is zodoende een legislatieve procedure gestart voor een algemene verordening inzake gegevensbescherming, waarin ook aandacht zal zijn voor gegevensbescherming binnen de arbeidsrechtelijke context.[123]

2.1.1 *De lege lata*

Richtlijnen 95/46/EG en 2002/58/EG zijn de twee geldende richtlijnen inzake privacy binnen de Europese Unie. Hoewel deze richtlijnen sinds hun publicatie zijn omgezet in nationale Belgische wetten, loont het toch de moeite om de tekst van deze richtlijnen nader te bestuderen. Deze richtlijnen geven een goed beeld van de *ratio legis* die de Europese Unie hanteerde, en mogelijk nog steeds hoog in het vaandel draagt, inzake het recht op privacy en de verwerking van persoonsgegevens.

2.1.1.1 Richtlijn 95/46/EG

De privacyrichtlijn dateert van 1995, een aantal jaren voor de grote evolutie van *web 1.0* naar *web 2.0* plaatsvond.[124] Het was de bedoeling om de interne markt zoveel mogelijk te vrijwaren en het vrij verkeer van personen en diensten te faciliteren.[125] Gezien een bijzondere wijziging van de richtlijn in het licht van deze ontwikkeling ontbreekt, werd de richtlijn sedertdien geïnterpreteerd om ook van toepassing te zijn in situaties waar ze in aanraking kwam met sociaalnetwerksites, weblogs en andere digitale nieuwigheden.

De richtlijn kwam er door de toename van verwerking van persoonsgegevens en het gemak waarmee dit gebeurde. De Europese Unie – toen nog Europese Gemeenschap – erkende de moderne technologische evoluties en zag dat het vrij verkeer van personen en ondernemingen vele uitdagingen met zich meebracht. Ook overheden zagen er heil in om persoonsgegevens van hun burgers onderling uit te wisselen, denk bijvoorbeeld aan situaties van fiscale belasting of criminele

[120] Verdrag betreffende de Europese Unie, met het Verdrag tot oprichting van de Europese Gemeenschap, *Pb.C.* 31 augustus 1992, afl. 224, 10 en art. 26 Verdrag betreffende de werking van de Europese Unie, *Pb.C.* 26 oktober 2012, afl. 326, 59.
[121] Art. 26 Verdrag betreffende de werking van de Europese Unie, *Pb.C.* 26 oktober 2012, afl. 326, 59.
[122] Europese Commissie, *First stage consultation of social partners on the protection of workers' personal data*, http://ec.europa.eu/social/main.jsp?catId=708 (consultatie 10 november 2014) (hierna verkort Europese Commissie, *First stage consultation*).
[123] Zie *infra* deel 2, 2.1.2, ii.
[124] D. DINUCCI, "Fragmented Future", *Print* 1999, afl. 4, 32 en T. O'REILLY, "What is Web 2.0", *O'Reilly.com*, 30 september 2004, http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html.
[125] Zie *supra* noot 121.

omstandigheden.[126] Een verschil in behandeling van de verwerking van persoonsgegevens per lidstaat zou dan ook een belemmering van de interne markt kunnen vormen.[127]

Een uniform niveau van gegevensbescherming was dus vereist. Het primaire doel van de EU was, naast het beschermen van fundamentele rechten en vrijheden van natuurlijke personen, het bewerkstelligen van haar eigen interne markt binnen de moderniserende samenleving.[128] De richtlijn is van toepassing op alle 28 lidstaten én de overige lidstaten van de Europese Economische Ruimte, zijnde IJsland, Liechtenstein en Noorwegen.[129]

i. Toepassingsgebied

Zoals eerder opgemerkt bij de definities van de WVP, die nagenoeg identiek zijn aan de definities uit de privacyrichtlijn, zijn de bewoordingen in de richtlijn erg ruim.[130] Zo is de richtlijn van toepassing op "de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen."[131] Kortom, elke verwerking van persoonsgegevens met als doel deze gegevens te bewaren.

De belangrijkste uitsluiting van het toepassingsgebied is de verwerking van persoonsgegevens binnen de privésfeer.[132] Zo zullen de regels niet van toepassing zijn wanneer een wantrouwige echtgenoot de private mailbox van zijn partner kraakt en overspelige berichten kopieert. Van zodra er evenwel, om in de geest van het arbeidsrecht te blijven, een arbeidsrelatie aan te pas komt, kan de situatie veranderen. Zo zal de richtlijn wel van toepassing zijn wanneer de echtgenoot bijvoorbeeld de werkgever van zijn partner is en de gegevens zich in de mailbox van het werk bevonden. Hier is immers geen sprake meer van een loutere privésfeer.

Binnen dit toepassingsgebied, dat veel weg heeft van een *catch-all* gebied, krijgen de lidstaten aanzienlijke ruimte om hun eigen beleid uit te stippelen. Zij bepalen immers zelf de voorwaarden opdat een verwerking van persoonsgegevens rechtmatig zal zijn.[133]

De Europese Unie is ook haar mosterd gaan halen bij art. 8 EVRM.[134] In de beginselen betreffende de kwaliteit van de gegevens zijn duidelijk voorwaarden te herkennen die in het EVRM worden gesteld, namelijk het vereiste dat welbepaalde doelen beoogd worden met de gegevensverwerking en dat de verzameling en verwerking proportioneel moet zijn.[135]

[126] Overwegingen 4 en 5 RL 95/46/EG, *supra* noot 58.
[127] Overwegingen 7 en 8 RL 95/46/EG, *supra* noot 58.
[128] Art. 1 RL 95/46/EG, *supra* noot 58.
[129] Art. 34 RL 95/46/EG, *supra* noot 58 en EUROPEES BUREAU VOOR DE GRONDRECHTEN, *Handbook on European data protection law*, Luxemburg, Publicatiebureau EU, 2014, 18.
[130] Zie *supra* noot 63.
[131] Art. 3, eerste lid RL 95/46/EG, *supra* noot 58.
[132] Art. 3, tweede lid RL 95/46/EG, *supra* noot 58.
[133] Art. 5 RL 95/46/EG, *supra* noot 58.
[134] Zie *supra* deel 1, 2.1.1.
[135] Art. 6 RL 95/46/EG, *supra* noot 58.

ii. Arbeidsrechtelijke insteek beperkt

Er is slechts één bepaling in de richtlijn waar de arbeidsrelatie uitdrukkelijk aan bod komt, namelijk deze waarin het verboden wordt gevoelige en mogelijk discriminerende gegevens te verwerken. Dit omvat gegevens waaruit de "raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt, alsook de verwerking van gegevens die de gezondheid of het seksuele leven betreffen."[136] Deze gegevens mogen wel verwerkt worden wanneer dit noodzakelijk is met het oog op de uitvoering van de rechten en plichten van de werkgever. In dergelijk geval is vereist dat de nationale wetgeving dit toestaat en "adequate garanties" biedt.[137] Wat hieronder dient te worden verstaan, wordt niet verduidelijkt.

iii. Ruime beleidsmarges voor lidstaten

De richtlijn voorziet in een hele resem rechten voor de persoon van wie de gegevens verwerkt worden, met name inzake de voorwaarden opdat de verwerking mogelijk is, informatieverstrekking over de verwerking en het recht op toegang tot zijn gegevens. Het staat lidstaten evenwel vrij bij wet hier beperkingen aan te stellen. Onder andere wanneer de openbare veiligheid in het gedrang komt of er een belangrijk economisch en financieel belang van een lidstaat of de EU op het spel staat, maar ook wanneer er rechten en vrijheden van anderen beschermd moeten worden.[138] We denken hierbij aan de positie van de werkgever en zijn controlemogelijkheden.

De opdrachtgever van de verwerking van persoonsgegevens dient aangifte te doen van een (semi-)geautomatiseerde verwerking bij de nationale toezichthoudende autoriteit.[139] Lidstaten kunnen een vrijstelling hiervan verlenen onder bepaalde omstandigheden, wanneer er aangetoond kan worden dat de inbreuk op rechten en vrijheden van de persoon wiens gegevens worden verwerkt "onwaarschijnlijk" is.[140] Het woordgebruik doet hier vermoeden dat deze bepaling nog ruime beleidsmarges geeft voor de lidstaten.

Er kan vastgesteld worden dat, hoewel deze richtlijn een belangrijke stap was in de richting van de harmonisatie van de verwerking van persoonsgegevens in de lidstaten, er voor deze laatste nog steeds een belangrijke mate van eigen beleidsvorming mogelijk is. Het doel van de richtlijn is dan ook het bewerkstelligen van het vrij verkeer en de interne markt, verder wilde men niet gaan. De richtlijn is eveneens relatief formalistisch en gaat vooral in op de manier hoe gegevens verwerkt mogen worden, er wordt weinig bepaald over wat er daarna met deze gegevens gedaan mag worden.

De ruime aard en toepassingsmogelijkheden van de bepalingen beletten meer diepgang. De specificiteit van de arbeidsrechtelijke problemen ter zake toont aan dat er nog vele belemmeringen mogelijk zijn voor het vrij verkeer van werknemers na de eerste fase van gegevensverwerking, zoals voorzien in de richtlijn. Zo stellen zich bijvoorbeeld problemen met de bewijslast van de

[136] Art. 8, eerste lid en tweede lid, b RL 95/46/EG, *supra* noot 58.
[137] Art. 8, eerste lid en tweede lid, b RL 95/46/EG, *supra* noot 58.
[138] Art. 13 RL 95/46/EG, *supra* noot 58.
[139] Art. 18, eerste lid RL 95/46/EG, *supra* noot 58. In België is dit de CBPL.
[140] Art. 18, tweede lid RL 95/46/EG, *supra* noot 58.

legitimiteit van verwerkte persoonsgegevens: de richtlijn stelt niets over aan welke voorwaarden bewijsmateriaal zou moeten voldoen opdat dit rechtmatig tegen de werknemer kan worden gebruikt.

2.1.1.2 Richtlijn 2002/58/EG

Twee jaar na de privacyrichtlijn zag een nieuwe richtlijn het levenslicht, richtlijn nr. 97/66/EG betreffende de verwerking van persoonsgegevens in de sector elektronische communicatie.[141] In 2002 werd deze richtlijn opgevolgd door een nieuw geheel van normen, aangepast aan de moderne digitale ontwikkelingen.[142] De toegang tot digitale mobiele netwerken was voor een groot publiek betaalbaar en toegankelijk geworden, wat nieuwe regelgeving vereiste.[143] Richtlijn 2002/58/EG is een aanvulling op de privacyrichtlijn.[144]

Ook bij richtlijn 2002/58/EG is het doel nog steeds de interne markt te bewerkstelligen. Wel wordt harmonisatie tot een minimum beperkt om ervoor te zorgen dat de ontwikkeling van elektronische-communicatiediensten en –netwerken binnen de EU niet wordt gehinderd.[145]

In het bijzonder werd eveneens beoogd artikelen 7 en 8 van het Handvest van de Grondrechten van de Europese Unie uitwerking te geven. Men wilde het recht op privacy verzekeren en legale, doelmatige en proportionele gegevensverwerking voorzien, waarbij eenieder een recht op inzage en rechtzetting heeft. Ook ziet een onafhankelijke autoriteit toe op de gegevensverwerking. Artikel 8 van het Handvest kan dan ook gezien worden als een samenvatting van richtlijn 95/46/EG en de bevestiging van de beginselen inzake verwerking van persoonsgegevens als een grondrecht binnen de Europese Unie.[146]

i. Toepassingsgebied

Deze richtlijn richt zich op gegevensverwerking in verband met de levering van openbare elektronische communicatiediensten.[147] Aanbieders van dergelijke diensten moeten maatregelen treffen opdat de veiligheid van het netwerk gegarandeerd wordt. Wordt een inbreuk op de bescherming van de persoonsgegevens gesignaleerd, dan moet de nationale toezichthoudende autoriteit meteen worden geïnformeerd. Ook de persoon wiens gegevens worden misbruikt moet geïnformeerd worden wanneer dit waarschijnlijk gevolgen zal hebben op zijn privéleven.[148]

[141] Richtl. Europees Parlement en Raad nr. 97/66/EG, 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, *Pb.L* 30 januari 1998, afl. 24, 1-8.
[142] RL 2002/58/EG *supra* noot 60.
[143] Overweging 5 RL 2002/58/EG, *supra* noot 60.
[144] Overweging 10 RL 2002/58/EG, *supra* noot 60.
[145] Overweging 8 RL 2002/58/EG, *supra* noot 60.
[146] Art. 8 Handvest van de Grondrechten van de Europese Unie, *Pb.C.* 18 december 2000, afl. 364, 10.
[147] Art. 3, eerste lid RL 2002/58/EG, *supra* noot 60, gewijzigd bij art. 2 Richtl. Europees Parlement en Raad nr. 2009/136/EG, 25 november 2009, tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en –diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming, *Pb.L.* 18 december 2009, afl. 337, 29-32 (hierna verkort RL 2009/136).
[148] Art. 4 RL 2002/58/EG, *supra* noot 60, gewijzigd bij art. 2 RL 2009/136, *supra* noot 147.

Verder richt de richtlijn zich op de regulering van ongewenste communicatie, zoals automatische telefoons of e-mails (*spam*), en het gebruik van *cookies*. Dit laatste is het opslaan van internetgegevens van gebruikers om deze later te gebruiken en bijvoorbeeld online advertenties af te stemmen op hetgeen de gebruiker in het verleden heeft opgezocht.[149]

ii. Arbeidsrechtelijke insteek afwezig

Deze richtlijn ontbreekt het eveneens van bepalingen toegespitst op de arbeidsrechtelijke context, er is zelfs geen enkele vermelding van. Het toepassingsgebied van de richtlijn lijkt zich eerder naar concrete situaties te bewegen zoals het online onrechtmatig vergaren van informatie door aanbieders van diensten, hetgeen in principe volledig losstaat van de arbeidsrechtelijke verhouding. Deze richtlijn voegt uiteindelijk dus weinig toe aan de discussie rond werkgeverscontrole.

2.1.2 *De lege ferenda*

De EU is zich bewust van de grondige wijzigingen in het digitale landschap die hebben plaatsgevonden sinds het opstellen van de privacyrichtlijn in 1995. Een bewijs hiervan is de aanvullende richtlijn inzake privacy bij elektronische communicatie.[150]

Rond de eeuwwisseling werd door de Europese Commissie een overleg opgestart met de Europese sociale partners om kennis te krijgen van de noden van de arbeidspartijen.[151] Na een lange stilte werd dan in 2012 een legislatieve procedure opgestart. Het doel van deze procedure is de geldende regelgeving inzake databescherming grondig te herzien, met name door richtlijn 95/46/EG te vervangen door een verordening en richtlijn 2002/58/EG bij te werken.[152] Het zou gaan om een Algemene Verordening Gegevensbescherming, die rechtstreeks bindend is voor de lidstaten.[153]

Vooraleer victorie wordt gekraaid over de herziening van de privacyregels op Europees niveau, moet er op gewezen worden dat deze verordening niet gericht is op de arbeidsrelatie. Wel blijkt dat doorheen de debatten de aandacht hier meer en meer op gevestigd is geworden.

2.1.2.1 Sociaal overleg

Zeggen dat de Europese Unie geen aandacht besteedt aan privacy op de werkvloer zou een brug te ver zijn, maar het is ongetwijfeld nooit een primair doel geweest. Zelfs de bescherming van het recht op privacy *an sich* was slechts een middel om de interne markt te vrijwaren.[154] De rechten van de werknemer op de werkvloer vormen dan ook geen rechtstreekse bedreiging voor de interne markt, gezien dit veelal behoort tot de interne keuken van ondernemingen. Met de toename van internet en sociale media begint dit echter meer en meer een doorslaggevende factor te worden om te spreken van een aangename arbeidscultuur. De nationale regelgeving kan werkgevers vrij

[149] Art. 5, derde lid en 13 RL 2002/58/EG, *supra* noot 60.
[150] Zie *supra* deel 2, 2.1.1.2.
[151] Europese Commissie, *First stage consultation*, *supra* noot 122.
[152] Bijkomend wil men ook een nieuwe richtlijn voorzien inzake de verwerking van gegevens in criminele omstandigheden. Informatie over beide regelgevende documenten is te vinden op de website van het Europees Parlement: http://www.europarl.europa.eu/news/nl/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform (consultatie 4 januari 2015).
[153] J. LORRÉ, *Sociale media en werkgeverscontrole*, Mechelen, Kluwer, 2012, 19.
[154] Zie *supra* deel 2, 2.1.1.1.

laten, waardoor werknemers door de absolute machtspositie van de werkgever mogelijk afgeschrikt worden om in dit land te gaan werken. Zo komt het vrij verkeer mogelijk toch in het gedrang.

Evenwel dient in het achterhoofd te worden gehouden dat de EU enkel werk kan maken van harmonisatie in de mate dat lidstaten zelf geen voldoende actie kunnen ondernemen.[155] In dit opzicht consulteerde de Europese Commissie de sociale partners, om hun ervaringen en visies te horen omtrent privacy binnen de arbeidsrelatie.[156]

i. Consultatie van sociale partners

Het bleek dat werkgeversorganisaties begin jaren 2000 geen nood zagen aan richtlijnen betreffende het onderwerp. De bestaande regelgeving was volgens hen afdoende.[157] Zij bepleitten flexibiliteit en nationale diversiteit. Werknemersorganisaties waren dan weer voorstander van een richtlijn over gegevensbescherming op de werkvloer.[158]

De Commissie overwoog of een algemene aanpak nodig was, of dat de bestaande aanpak van *case by case* voldoende was.[159] Wel werd expliciet melding gemaakt van de mening van Groep 29, een werkgroep ingericht door de privacyrichtlijn, dat de toestemming door een werknemer steeds met een korreltje zout moet worden genomen en dat een Europese visie hierover wel wenselijk zou zijn.[160]

De EU constateert dat er wel degelijk nood was aan een gerichte Europese aanpak. Er waren landen met eigen bijzondere wetgeving, maar deze was niet altijd even duidelijk en kon tot verschillende interpretaties en resultaten leiden. De situatie belemmerde op dat moment de rechtszekerheid.[161]

ii. Bevindingen zonder gevolg

De EU beoogde een kader dat voortbouwde op de principes van richtlijn 95/46/EG, maar dan toegepast op de rechten en plichten van de werkgever en werknemer. Het zou handelen over de precieze kwesties die nu nog steeds actueel blijken te zijn in rechtspraak en rechtsleer, zoals het onrechtmatig verkregen bewijs.[162]

Opvallend is de conclusie van de Commissie dat sociale partners evenwel bekwaam genoeg zijn om zelf akkoorden te sluiten over controlemogelijkheden op de werkvloer.[163] De sociale partners op

[155] Art. 5 Verdrag 7 februari 1992 betreffende de Europese Unie, *Pb.C.* 26 oktober 2012, afl. 326, 18.
[156] Europese Commissie, *First stage consultation*, *supra* noot 122, 5.
[157] De werkgeversorganisaties waren BUSINESSEUROPE, UEAPME en BDI. Europese Commissie, *Second stage consultation of social partners on the protection of workers' personal data*, http://ec.europa.eu/social/main.jsp?catId=708, 3 (consultatie 10 november 2014) (hierna verkort Europese Commissie, *Second stage consultation*).
[158] De werknemersorganisaties waren ETUC, CEC en EUROCADRES. Europese Commissie, *Second stage consultation*, *supra* noot 157.
[159] Europese Commissie, *Second stage consultation*, *supra* noot 157, 4.
[160] Art. 29 RL 95/46, *supra* noot 58 en Europese Commissie, *Second stage consultation*, 5, *supra* noot 157.
[161] Europese Commissie, *Second stage consultation*, *supra* noot 157, 7.
[162] Europese Commissie, *Second stage consultation*, *supra* noot 157, 11.
[163] Europese Commissie, *Second stage consultation*, *supra* noot 157, 16.

Europees niveau droegen hetzelfde standpunt: voornamelijk de werknemersorganisaties pleitten voor een limiet op de controlemogelijkheden, maar zowel werkgevers als werknemers zijn voorstander van een regeling via het nationale collectieve arbeidsrecht.[164]

De kernpunten waar de Commissie belang aan zou hechten in een herziening van de regelgeving waren het informeren van werknemersvertegenwoordigers over de controlemechanismen, een controle door de nationale instantie en een beperking op permanente en geheime controle (enkel wanneer er verdenking is van criminele activiteiten of ander ernstig misgedrag).[165] Routineuze controle op individuen zou ook niet mogen.[166]

Na het sociaal overleg bleef het echter gedurende lange tijd stil.

Hendrickx reageerde hierop en achtte een "Europese blauwdruk" inzake controle wenselijk, vooral om de grenzen van het wenselijke en het onwenselijke af te bakenen en grenzen te trekken voor werkgevers en werknemers. Zo bijvoorbeeld zou het nuttig zijn dat de EU stelt waar men het onderscheid tussen private en professionele communicatie kan maken.[167] Dit standpunt dateert uit 2001, maar is gezien de recente technologische ontwikkelingen en de opkomst van *web 2.0*, ongetwijfeld enkel sterker geworden.

2.1.2.2 Algemene Verordening Gegevensbescherming

Op 25 januari 2012 publiceerde de Europese Commissie een voorstel tot een algemene verordening inzake gegevensbescherming. [168] Deze verordening dient de regelgeving inzake gegevensbescherming van de Europese Unie bij te werken en toepasbaar te maken op de vele ontwikkelingen die hebben plaatsgevonden sedert de publicatie van de eerder besproken richtlijnen, zoals de evolutie naar *web 2.0*.

De nieuwe verordening heeft in maart 2014 voor een eerste lezing voorgelegen in het Europees Parlement, waar ze met een grote meerderheid werd goedgekeurd. Ten tijde van het finaliseren van deze scriptie, december 2014, is het document terug gezonden naar de Raad van de Europese Unie. Het meest recente debat vond plaats op 4 december 2014.[169]

In de hypothese dat het voorstel tot verordening aanvaard wordt, zullen de lidstaten 2 jaar de tijd hebben om te voldoen aan de nieuwe eisen.[170] De verordening moet een gewone legislatieve procedure doorlopen en heeft nog een aantal fasen te gaan, maar de eerste aanvaarding van het

[164] Europese Commissie, *Second stage consultation*, *supra* noot 157, 20. Met andere woorden wordt hier gesteld dat de aanpak met cao nr. 81 niet eens zo slecht is, terwijl later in dit deel zal blijken dat bepaalde auteurs beweren dat de sociale partners met het reguleren van dit onderwerp door middel van cao's hun boekje te buiten zijn gegaan en een duidelijke bevoegdheidsoverschrijding hebben begaan, zie *infra* deel 2, 3.1.3.
[165] De nationale instantie in België is de CBPL. Europese Commissie, *Second stage consultation*, *supra* noot 157, 17.
[166] Deze onderwerpen worden in België behandeld door cao nr. 81. Zie *infra* deel 2, 3.2.1.
[167] F. HENDRICKX, *Protection of workers' personal data in the European Union: Two Studies*, website Europese Commissie, 2001, 115.
[168] COM(2012)11def. [Commissiedocument nr. 11 van 2012].
[169] De vooruitgang valt te consulteren op de website van het Europees Parlement: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011(COD)&l=en (consultatie 4 januari 2015).
[170] Art. 91, tweede lid COM(2012)11def. [Commissiedocument nr. 11 van 2012].

Parlement is evenwel een goed teken voor het verdere verloop van de procedure.[171] Echter, het feit dat het om een verordening gaat kan de procedure bemoeilijken. Deze zal immers meteen rechtstreekse gevolgen hebben voor de lidstaten, die meteen gebonden zullen zijn door de bepalingen van de verordening en in grote mate hun beleidsmarge zullen verliezen.[172] Dit in tegenstelling tot de situatie bij een richtlijn, die eerst omgezet moet worden in nationaal recht.[173]

i. Oorspronkelijke inhoud

Oorspronkelijk werd niet bijzonder veel aandacht besteed aan gegevensverwerking in de arbeidsrelatie. Er werd uitdrukkelijk in de overwegingen opgenomen dat de algemene regels ook van toepassing zijn op de arbeidsverhouding en dat de lidstaten een verdere regeling kunnen uitwerken.[174] Ook de reeds bestaande bepaling van art. 8 privacyrichtlijn werd, zij het licht aangepast in bewoordingen, opgenomen in het voorstel.[175]

Toch werd dit keer een apart artikel gewijd aan gegevensverwerking in arbeidsrechtelijke context. Artikel 82 van het voorstel verwijst expliciet naar verwerking van persoonsgegevens in een arbeidscontext, maar geeft de lidstaten nog steeds de ruimte om zelf wetgeving hierover aan te nemen binnen de lijnen van de verordening. Er worden op niet-limitatieve wijze enkele specifieke omstandigheden waarbij gegevensverwerking voorkomt opgesomd waarover de lidstaten zich *kunnen* uitspreken:

- Aanwerving;
- Uitvoering van de arbeidsovereenkomst;
- Beheer;
- Planning en organisatie van het werk;
- Gezondheid en welzijn op het werk;
- Rechten en voordelen verbonden aan de arbeid, en;
- Beëindiging van de arbeidsovereenkomst.

Lidstaten zijn niet verplicht zulke wetgeving te voorzien. De EU eist wel dat dergelijke wetgeving, wanneer deze bestaat, ter kennis wordt gebracht van de Commissie tegen het moment dat de verordening in werking treedt. Elke wijziging na de inwerkingtreding van de verordening moet eveneens ter kennis worden gebracht.[176] De Commissie behoudt zich ook het recht voor om zelf bijkomende regels te voorzien.[177]

[171] P. CRAIG en G. DE BÚRCA, *EU Law: Text, Cases and Materials*, Oxford, Oxford University Press, 2011, 123-125.
[172] Zie *supra* deel 2, 2.1.1.
[173] P. CRAIG en G. DE BÚRCA, *EU Law: Text, Cases and Materials*, Oxford, Oxford University Press, 2011, 105-106.
[174] Overweging 124 COM(2012)11def. [Commissiedocument nr. 11 van 2012].
[175] Art. 9 COM(2012)11def. [Commissiedocument nr. 11 van 2012]. Dit artikel beschrijft welk soort persoonlijke gegevens niet verzameld mag worden, behoudens uitzonderingen. Voor de bepaling van de privacyrichtlijn, zie *supra* noot 136.
[176] Art. 82, tweede lid COM(2012)11def. [Commissiedocument nr. 11 van 2012].
[177] Art. 82, derde lid COM(2012)11def. [Commissiedocument nr. 11 van 2012].

ii. Wijzigingen in het voorstel

Intussen werd dit artikel in het voorstel sterk aangepast, en dit na een tussenkomt van de Commissie Werkgelegenheid en Sociale Zaken tijdens de debatten. In november 2013 deed zij een reeks voorstellen om de belangrijkste beginselen inzake gegevensverwerking op de werkvloer te verankeren in de verordening. Daarbij werd evenwel gepleit voor een aparte regulering, waaraan het nog steeds ontbreekt. Interpretatie van de algemene regels kan immers voor moeilijkheden zorgen, terwijl gegevensverwerking op de werkvloer erg vaak voorkomt. Een geheel aan regels voorzien hiervoor kan echter niet in één artikel, dit artikel dient volgens de Commissie Werkgelegenheid dus voornamelijk als een opstap naar meer.[178]

Uit de tekst die volgde na de eerste stemming in het Parlement blijkt dat een afgeslankte versie van de voorgestelde amendementen van de Commissie Werkgelegenheid is aangenomen. Het artikel is minder gericht op de positie van vertegenwoordigers en het collectief arbeidsrecht dan de Commissie Werkgelegenheid beoogde en meer op de rechten van de individuele werknemers. Zo wilde de Commissie Werkgelegenheid oorspronkelijk een kader voorzien om vertegenwoordigers werknemers te laten vertegenwoordigen in de rechtbank.[179]

Dat men een impuls wil geven voor de lidstaten om zelf actie te ondernemen, blijkt vooreerst uit de wijziging van de titel van het artikel. Deze verandert van "processing in the employment context" naar "minimum standards for processing data in the employment context".[180]

Er wordt in het bijzonder gewezen op het proportionaliteitsbeginsel: dit lijkt het kernwoord te zijn inzake Europese gegevensbescherming op de werkvloer. Het belangrijkste is dat de verwerker van gegevens het redelijke in acht neemt. Er wordt benadrukt dat de opsomming van omstandigheden niet limitatief is en dat er niet per se sprake moet zijn van actie bij wet. Ook collectieve overeenkomsten worden nu uitdrukkelijk vermeld. Er wordt nog veel ruimte gelaten voor nationale gewoontes en beleidsnormen.[181]

Naar aanleiding van de vaststellingen van Groep 29 is ook in het artikel opgenomen dat de instemming door een werknemer geen grond kan zijn voor gegevensverwerking wanneer die instemming niet vrij werd gegeven.[182] Hoewel een nobel streven, stellen wij ons de vraag of de EU hier ook niet beter enkele beoordelingscriteria kan bieden voor de nationale rechters. Dit zou de rechtszekerheid zeker ten goede komen.

---

[178] Advies Commissie Werkgelegenheid en Sociale Zaken, 4 maart 2013, http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A7-2013-0402&language=EN#title3 (consultatie 27 december 2014) (hierna verkort Advies Commissie WSZ).

[179] Amendement 22 Advies Commissie WSZ, *supra* noot 178.

[180] Amendement 192 Wetgevingsresolutie Europees Parlement 12 maart 2014 over het voorstel voor een verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//NL (consultatie 27 december 2014) (hierna verkort Wetgevingsresolutie Europees Parlement 12 maart 2014).

[181] Amendement 192 Wetgevingsresolutie Europees Parlement 12 maart 2014, supra noot 180. Ook dit, net zoals de opinies uit het Europees sociaal overleg, staat haaks op de visie die auteurs als Humblet, Osaer en Nayaert voorhouden, namelijk dat dit buiten het gebied van de cao's gaat.

[182] Amendement 192, art. 82, 1b Wetgevingsresolutie Europees Parlement 12 maart 2014, *supra* noot 180.

Hoe dan ook dienen lidstaten bij hun regulerend optreden de volgende minimumstandaarden te voorzien:[183]

- De werknemer moet op de hoogte zijn van de gegevensverwerking. Een verwerking van gegevens mag enkel zonder diens kennis gebeuren wanneer strikte deadlines worden gesteld voor de verwijdering van de gegevens na verzameling, als er een vermoeden bestaat gebaseerd op feiten omtrent misdrijven of ernstig plichtsverzuim in de arbeidsrelatie, wanneer het vergaren van informatie nodig is om de zaak uit te klaren en als aangetoond wordt dat deze wijze van gegevensverwerking nodig en proportioneel is. Dit moet onderzocht worden door de bevoegde autoriteit.
- Omgevingen die niet publiek toegankelijk zijn, of die privé zijn voor werknemers (zoals toiletten), zullen niet onder toezicht worden geplaatst. Een heimelijk toezicht is verboden.
- Bij verzameling van medische informatie moet ter kennis worden gegeven waarom die informatie wordt verzameld. Men zal deze informatie later ook zelf moeten verkrijgen.
- De grenzen die worden gelegd op privaat gebruik van telefoon, e-mail, internet en andere telecommunicatiemiddelen mogen geregeld worden bij collectieve arbeidsovereenkomst. Is er geen dergelijke overeenkomst, dan zal de werkgever een overeenkomst hierover sluiten met zijn werknemer. Mag men private communicatie voeren op de werkvloer, dan mag deze informatie enkel en alleen verwerkt worden om te verzekeren dat deze data veilig zijn, dat het systeem nog goed kan functioneren en dat tarieven niet de spuigaten uit lopen. In dit laatste geval mag verder worden gegaan onder de voorwaarden van de eerste minimumstandaard.
- Er mogen geen zwarte lijsten van werknemers opgesteld worden op basis van persoonsgegevens. Met zulke zwarte lijsten zouden discriminatoire omstandigheden in de hand gewerkt kunnen worden. Lidstaten zullen hier controle op uitvoeren en sancties voorzien.

Ten slotte zal de Commissie, na het vragen van een advies aan het Europees Comité voor gegevensbescherming, bijkomende regels kunnen aannemen.[184] Dit Comité, een onafhankelijk orgaan dat de consistente toepassing van de verordening moet verzekeren, dient ter vervanging van Groep 29 uit de privacyrichtlijn.[185] Het Comité dient te bestaan uit de voorzitters van de toezichthoudende autoriteiten van de lidstaten en moet zo de samenwerking bevorderen.[186]

iii. Hoopgevende evolutie?

Het voorstel tot verordening van de Europese Commissie lijkt een grote stap te zijn in een eerste concrete regulerende actie van de Europese Unie inzake de spanningsverhouding op de arbeidsvloer. Nochtans leek de Commissie eerder een afwachtende houding te nemen en het vertrouwen te leggen in de handen van de sociale partners. Wel dient opgemerkt te worden dat, ondanks het feit dat het hier om een verordening gaat, artikel 82 van het voorstel de lidstaten

[183] Amendement 192 Art. 82, 1c Wetgevingsresolutie Europees Parlement 12 maart 2014, *supra* noot 180.
[184] Amendement 192 Art. 82, derde lid Wetgevingsresolutie Europees Parlement 12 maart 2014, *supra* noot 180.
[185] Overweging 110 COM(2012)11def. [Commissiedocument nr. 11 van 2012].
[186] Art. 64-72 COM(2012)11def. [Commissiedocument nr. 11 van 2012]. Voor een overzicht van de taken van het Comité, zie art. 66 Wetgevingsresolutie Europees Parlement 12 maart 2014, *supra* noot 180.

toelaat om regulerend te handelen. De verplichting is er niet. Het enige dat verplichtend is, is hetgeen letterlijk in het artikel neergeschreven staat.

De tijd zal uitwijzen of de nieuwe verordening er in de eerste plaats zal komen en, zo ja, in welke mate deze zal ingrijpen op gegevensverwerking in de arbeidsrechtelijke context. Dit artikel biedt wel al meer een rechtsgrond dan er tot nu toe geweest is op specifiek arbeidsrechtelijk niveau. Met een aantal regels inzake minimumbescherming lijkt een goede stap gezet.

2.2 Raad van Europa

De bekendste bron van recht, uitgevaardigd door de Raad van Europa, is uiteraard het EVRM. Art. 8 EVRM is eerder reeds besproken en biedt een primaire rechtsbron voor het recht op privacy. De Raad van Europa en haar organen hebben zich op het domein van privacy verder ook niet onbesproken gelaten.

2.2.1 Documenten inzake gegevensbescherming

De belangrijkste aanleiding voor de regelgeving van de Raad van Europa is het beschermen van de fundamentele vrijheden, zijnde hetgeen vastgelegd in het EVRM.

Verdrag nr. 108 van de Raad van Europa is het eerste en nog steeds enige internationaal bindend instrument dat uitdrukkelijk over gegevensbescherming gaat.[187] Het doel van het verdrag is het waarborgen van de rechten en fundamentele vrijheden van inwoners van elke partij bij het verdrag. Het slaat zowel op gegevensverwerking in de openbare als in de particuliere sector. De verwerking van gevoelige informatie wordt verboden.[188]

Het verdrag werd door België geratificeerd.[189] Het biedt enkel bindende werking ten opzichte van staten en heeft dus geen directe werking. België maakte wel een voorbehoud bij de toepassing van het verdrag in de particuliere sector. In principe is het van toepassing op de verwerking door natuurlijke personen van persoonsgegevens die uit hun aard voor privégebruik bedoeld zijn. In België is dit dus niet het geval.[190]

Ook dit verdrag is niet gericht op conflicten op de werkvloer. Met een aanbeveling wilde het Comité van Ministers in 1989 een toepassing van de regels van het verdrag bieden op deze concrete situatie.[191]

---

[187] EUROPEES BUREAU VOOR DE GRONDRECHTEN, *Handbook on European data protection law*, Luxemburg, Publicatiebureau EU, 2014, 14.
[188] Art. 5 Verdrag nr. 108 van de Raad van Europa 28 januari 1981 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens.
[189] Wet 17 juni 1991 houdende goedkeuring van het Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde werking van persoonsgegevens, opgemaakt te Straatsburg op 28 januari 1981, *BS* 30 december 1993.
[190] P. WATERSCHOOT, "Bespreking van enkele arresten van het Arbeidshof te Gent in verband met het gebruik en misbruik van e-mail en internet op de werkplaats en het controlerecht van de werkgever daarop", *RW* 2009, afl. 18, (730) 732.
[191] Aanbeveling nr. R(89)2 of the Committee of Ministers to Member States on the protection of personal data used for employment purposes, 18 januari 1989.

De aanbeveling richt zich tot (semi-)geautomatiseerde verwerkingen, al kan een lidstaat dit uitbreiden tot manuele handelingen.[192] Werkgevers zouden hun werknemers op voorhand volledig moeten informeren of bevragen over de introductie van een systeem voor gegevensverwerking of toezicht op de werknemers. Toestemming *zou* beoogd *moeten* worden, het blijft immers slechts gaan over een aanbeveling.

Ook hier wordt met dezelfde principes als binnen de EU gewerkt en wordt met name aandacht besteed aan proportionaliteit.[193]

Het verdrag kent evenwel nog niet de uitgediepte criteria zoals deze later zijn uitgewerkt in supranationale regelgeving, zijnde de Europese richtlijnen.[194] Hierdoor en mede door het verouderd karakter van het verdrag en de aanbeveling hebben zij momenteel, althans voor België, veelal een louter historische waarde.

2.2.2 Rechtspraak Europees Hof voor de Rechten van de Mens

Als er één buitenlands rechtscollege is dat een invloed heeft gehad op de Belgische rechtspraak inzake privacy (binnen een arbeidsrechtelijke context), is het het EHRM. Het gaat dan voornamelijk over de vrijwaring van hetgeen bepaald in art. 8 EVRM.

Toch is rechtspraak over schendingen van privacy door de werkgever erg zeldzaam. Er zijn slechts enkele principszaken die hun stempel gedrukt hebben op de interpretatie van art. 8 EVRM, waarvan de meest recente uitspraak dateert van 2007.

Opvallend bij de principsarresten is dat deze zaken nagenoeg uitsluitend gaan over afluisteren van telefoongesprekken, en dus niet om *post factum* controle.[195] Toch kunnen de principes uit deze rechtspraak ook toegepast worden op het onderzoeksgebied van deze scriptie en privacy van de werknemer in het algemeen.

In *Niemietz* (1992) werden de telefoongesprekken van een advocaat afgeluisterd. Hier werd gesteld dat het recht op privéleven ook inhoudt dat een individu het recht heeft om contacten te onderhouden met andere personen. Zelfs wanneer deze telefoontjes gepleegd worden naar privécontacten tijdens de werkuren en zelfs met het toestel van de werkgever. De overheid trachtte aan te halen dat art. 8 EVRM geen communicatie op de werkvloer beschermde omdat dit geen onderdeel van het privéleven zou zijn, maar het Hof oordeelde dat de scheiding tussen privé- en professionele communicatie tijdens de arbeidsuren niet te maken was. De bescherming van art. 8 EVRM geldt dan ook voor beide communicatiesferen.[196]

[192] Art. 1.2 Aanbeveling nr. R(89)2 of the Committee of Ministers to Member States on the protection of personal data used for employment purposes, 18 januari 1989.
[193] Art. 4 Aanbeveling nr. R(89)2 of the Committee of Ministers to Member States on the protection of personal data used for employment purposes, 18 januari 1989.
[194] Zie *supra* deel 2, 2.1.1.
[195] EHRM, *Halford t. Verenigd Koninkrijk*, 25 juni 1997 en EHRM*, Amann t. Zwitserland*, 16 februari 2000.
[196] EHRM *Niemietz t. Duitsland*, 16 december 1992.

Halford (1997) ging over een relatie onder arbeidsovereenkomst. Dit in tegenstelling tot *Niemietz*, dat zich in de vrije beroepensfeer afspeelde. Een politieofficier pleegde tijdens haar diensturen private telefoongesprekken. De tewerkstellende overheid luisterde haar telefoon af en gebruikte het aldus verkregen bewijs. Hier werd eveneens een schending van de privacy vastgesteld.[197]

In *Amann* (2000) werd een telefoongesprek onderschept door een openbare aanklager van Zwitserland, om dit als bewijsmateriaal te gebruiken in een strafzaak. Hier werd het principe gesteld dat wanneer een openbare autoriteit gegevens opslaat inzake een individu zijn privéleven, dit een schending is van art. 8 EVRM.[198]

In *Copland* (2007) ging het ten slotte weer over een arbeidsverhouding, namelijk tussen een lerares en een onderwijsinstelling. Haar telefoon, e-mail- en internetgebruik werden gecontroleerd door de werkgever. De reden die hiervoor werd aangehaald was dat dit diende om aan te tonen dat de werkneemster overmatig gebruik maakte van de apparatuur van de instelling voor persoonlijke doeleinden. Het verzamelen van persoonlijke informatie zonder dat de werkneemster hier kennis van had was een inbreuk op het recht op privéleven.[199] Het Hof verklaarde dit in strijd met het EVRM, omdat er geen nationale wetgeving was. Dergelijke controle zou toelaatbaar zijn indien ze "noodzakelijk" was "in een democratische samenleving", maar dit werd in deze zaak niet als bewezen geacht. [200]

2.3 Verenigde Naties – Internationale Arbeidsorganisatie

De bijdrage van de Verenigde Naties (VN) inzake regelgeving over werkgeverscontrole is beperkt. De VN is evenwel verantwoordelijk voor de Universele Verklaring van de Rechten van de Mens (UVRM). Artikel 12 bepaalt het recht op privéleven en is de grondslag voor de acties die later ondernomen zijn door onder andere de Raad van Europa en de EU, evenals voor het eigen BuPo-verdrag.[201] De belangrijkste bijdrage toegespitst op een arbeidsrechtelijke context is gekomen van één van de agentschappen van de VN.

De Internationale Arbeidsorganisatie (IAO) werd opgericht in 1919, na Wereldoorlog I, om sociale vrede te bewerkstelligen. De IAO kent een tripartiete structuur en biedt een forum voor overheden, werkgevers- en werknemersorganisaties om met elkaar te overleggen. 185 staten, die eveneens lid zijn van de Verenigde Naties, maken deel uit van de IAO. België behoorde anno 1919 reeds tot de oprichtende staten.[202]

---

[197] EHRM, *Halford t. Verenigd Koninkrijk*, 25 juni 1997.
[198] EHRM*, Amann t. Zwitserland*, 16 februari 2000.
[199] EHRM, *Copland t. Verenigd Koninkrijk*, 3 april 2007.
[200] P. WATERSCHOOT, "Bespreking van enkele arresten van het Arbeidshof te Gent in verband met het gebruik en misbruik van e-mail en internet op de werkplaats en het controlerecht van de werkgever daarop", *RW* 2009, afl. 18, (730) 731.
[201] Art. 12 Universele Verklaring van de Rechten van de Mens, 10 december 1948, *BS* 31 maart 1949. Artikel 17 BuPo omschrijft het recht op privéleven, zie *supra* noot 32. Internationaal verdrag 19 december 1966 inzake burgerrechten en politieke rechten, *BS* 6 juli 1983.
[202] http://www.ilo.org/global/about-the-ilo/who-we-are/lang--en/index.htm (consultatie 10 november 2014).

De IAO heeft zich beperkt uitgelaten over het onderwerp van werkgeverscontrole. In 1996 heeft zij een gedragscode uitgevaardigd inzake de bescherming van persoonsgegevens van werknemers.[203] Al snel blijkt dat de inspiratie voor deze *code of conduct* werd gehaald bij de richtlijnen van de Algemene Vergadering van de VN inzake persoonlijke computerbestanden.[204] Hoewel geen enkele bindende kracht hiervan uitgaat, kan dit wel een aanzienlijke aanzet zijn geweest voor een degelijk beleid binnen lidstaten van de Verenigde Naties. De bedoeling was dan ook om wetgevers en sociale partners te inspireren voor een uitgebalanceerde positionering van persoonsgegevens op het werk.[205] Uit de tekst van de code blijkt het belang dat de organisatie hecht aan sociale dialoog.

Ook hier worden de beginselen zoals omschreven in de WVP en de EU-richtlijnen herhaald, zij het niet in dezelfde bewoordingen. Het legaliteits-, finaliteits- en proportionaliteitsbeginsel komen aan bod. Men wil zo duidelijk maken dat enkel controle mag worden uitgevoerd voor duidelijk omschreven doeleinden en dat de vergaarde informatie, die tot het minimum beperkt dient te blijven, niet mag worden misbruikt. Het afstand doen van het recht op privacy wordt uitdrukkelijk verboden.[206]

Eerder in deze scriptie werd gesproken over twee mogelijke zienswijzen: ofwel ziet men de controle van de werkgever als *geknabbel* aan de grondrechten van de werknemer, ofwel ziet men het recht op privacy als een begrenzing van werkgeversgezag.[207] Uit de tekst van de gedragscode blijkt duidelijk dat in 1996 de bescherming van het recht op privacy de voornaamste doelstelling was: de code spreekt bijna uitsluitend over wat de werkgever *niet* mag, amper over waar hij recht op heeft.[208] De belangen van de werkgever wegen, in ieder geval voor de IAO, veel minder door op de schaal dan de rechten van de werknemer.

De bepalingen van deze aanbeveling zijn minder strikt dan andere supranationale normen met wél bindende kracht, zoals de eerder besproken Europese richtlijnen.[209] Voor het Belgisch recht hebben deze bepalingen dus niet meer dan een historische waarde, een gedateerde inspanning ter verzekering van de bescherming van een mensenrecht. Evenwel bracht de Nationale Arbeidsraad in juli van hetzelfde jaar een advies uit, ter voorbereiding op de publicatie van deze gedragscode. Het maakte dus wel degelijk iets wakker op nationaal niveau.[210]

[203] IAO, *Protection of workers' personal data. An ILO code of practice*, Genève, IAO, 1997.
[204] Algemene Vergadering Verenigde Naties, *Guidelines for the Regulation of Computerized Personal Data Files*, New York, 1990.
[205] IAO, *Protection of workers' personal data. An ILO code of practice*, Genève, IAO, 1997, 1.
[206] IAO, *Protection of workers' personal data. An ILO code of practice*, Genève, IAO, 1997, 2.
[207] Zie *supra* deel 1, 3.
[208] IAO, *Protection of workers' personal data. An ILO code of practice*, Genève, IAO, 1997.
[209] Zie *supra* deel 2, 2.1.1.
[210] V. OSAER en S. NAYAERT, "Privacy in de werksfeer", *supra* noot 65, (513) 549.

3 Werkgeverscontrole in België

Zoals eerder gesteld is het regelgevend kader op Europees en internationaal niveau momenteel erg beperkt in omvang. Er zijn geen regels inzake internetcontrole in het arbeidsrecht voorhanden, enkel algemene bepalingen inzake de bescherming van privacy. Op nationaal niveau kan min of meer hetzelfde gesteld worden: de voornaamste rechtsbronnen, door de wetgever voorzien, zijn de Wet Verwerking Persoonsgegevens en de Wet Elektronische Communicatie. [211]

Dit heeft de sociale partners ertoe aangezet zelf actie te ondernemen. In hetgeen volgt zullen het belang, de inhoud en de gevolgen van de collectieve arbeidsovereenkomst ter zake uiteengezet worden, alsook de interpretatie en toepassing ervan. Hiermee wordt in het bijzonder gedoeld op de aanpak van de sociale partners, de CBPL en de rechter.

3.1 Controle door de werkgever: cao nr. 81

Art. 17 WAO bepaalt dat de werknemer ondergeschikt is aan de beslissingen van zijn werkgever. Bij gebrek aan bijzondere regelgeving geldt dit ook wat betreft internetcontrole. Toch dient dit, rekening houdend met de praktijk, genuanceerd te worden. De nood aan meer doorzichtige rechtsnormen, verder gaand dan het louter naar analogie toepassen van de WVP, werd opgevangen door een collectieve arbeidsovereenkomst.

In 2002 kwam het resultaat van besprekingen tussen de sociale partners ten tonele in de vorm van cao nr. 81 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische onlinecommunicatiegegevens.[212]

3.1.1 Totstandkoming

Een cao is "een akkoord gesloten tussen een of meer werknemersorganisaties enerzijds en een of meer werkgevers of een of meer werkgeversorganisaties anderzijds, waarbij de individuele en collectieve betrekkingen tussen werkgevers en werknemers in de ondernemingen of in een bedrijfstak worden vastgesteld en de rechten en verplichtingen van de contracterende partijen worden geregeld".[213]

Deze cao, nr. 81, werd bij koninklijk besluit van 12 juni 2002 algemeen verbindend verklaard voor de hele private sector. De oefening in het afwegen van de tegengestelde rechten en belangen van werkgever en werknemer leidde tot een overeenkomst waarbij met name zowel de privacy van de werknemer als het gezag van de werkgever in acht worden genomen. De cao kwam er na advies 10/2000 van de CBPL.[214]

---

[211] Zie *supra* deel 1, 2.2.2. V. BUELENS en P. STROOBANTS, *Is 'facebooken' een werkwoord?*, Mechelen, Kluwer, 2012, 10-11.
[212] Cao nr. 81, *supra* noot 41.
[213] E. DIRIX, B. TILLEMAN en P. VAN ORSHOVEN (eds.), *De Valks Juridisch Woordenboek*, Antwerpen, Intersentia, 2010, 29.
[214] COMMISSIE TER BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, advies nr. 10/2000 betreffende het toezicht door de werkgever op het gebruik van het informaticasysteem op de werkplaats, 3 april 2000, 8 p. (hierna verkort CBPL, advies nr. 10/2000).

De sociale partners vonden het opportuun om een concretisering van de bestaande rechtsnormen, met name de WVP, te creëren en deze af te stemmen op de arbeidsrechtelijke situatie. De Nationale Arbeidsraad heeft eerst de reeds bestaande rechtsnormen, zowel internationaal, Europees als nationaal, bestudeerd en wilde hierop een verduidelijking bieden.

Het "enige doel" van de cao is ervoor te zorgen dat de persoonlijke levenssfeer van de werknemer wordt geëerbiedigd bij het verzamelen van elektronische onlinecommunicatiegegevens om ze te controleren en te verwerken zodat ze aan een werknemer kunnen worden toegeschreven.[215] Een aandachtspunt hierbij was het voorzien van de nodige soepelheid om zo goed mogelijk in te spelen op de feitelijke situatie van de werkgevers, de werknemers en hun vertegenwoordigers.[216]

Ook voor de cao geldt dus het uitgangspunt dat de arbeidsrelatie bedreigingen inhoudt voor de grondrechten van de werknemer.[217] Dit lijkt meteen veel te verraden over het uitgangspunt van de NAR. Het grondrecht op privacy moet beschermd worden, "rekening houdend met de behoeften voor een goede werking van de onderneming."[218]

Andere wetgeving blijft onverkort gelden en vult de cao aan in zoverre de algemene wetgeving strenger is of een toepassingsgebied dekt dat door de cao niet wordt behandeld. [219] De cao dient als bijzondere rechtsnorm enkel om de bestaande rechtsnormen te preciseren en toch de nodige soepelheid te bieden voor de partijen.[220] Het staat vrij aan paritaire comités en ondernemingen om gunstigere bepalingen te voorzien.[221]

3.1.2 Bepalingen

De cao is gebaseerd op twee beginselen. Ten eerste erkennen werknemers dat de werkgever het *recht* heeft controle uit te oefenen op hun werkinstrument en hoe zij hiervan gebruik maken. Ten tweede eerbiedigen werkgevers het recht op bescherming van de persoonlijke levenssfeer van hun werknemers binnen de dienstbetrekking.[222] In ruil voor verloning doen werknemers dus bewust ten dele afstand van hun rechten.[223]

3.1.2.1 Toepassingsgebied

Werkgevers kunnen controle uitoefenen op "elektronische onlinecommunicatiegegevens", dit zijn "elektronische onlinecommunicatiegegevens sensu lato ongeacht de drager via welke een en ander door een werknemer wordt overgebracht of ontvangen in het kader van de dienstbetrekking."[224] Afgezien van het pleonasme in deze definitie, namelijk dat het te definiëren woord in de definitie

[215] Cao nr. 81, *supra* noot 41, 4.
[216] Cao nr. 81, *supra* noot 41, 3.
[217] Cao nr. 81, *supra* noot 41, 4.
[218] Art. 1, §1 cao nr. 81, *supra* noot 41.
[219] Cao nr. 81, *supra* noot 41, 3.
[220] W. VAN EECKHOUTTE, *Sociaal compendium Arbeidsrecht '14-'15 met fiscale notities*, Mechelen, Kluwer, 2014, 807.
[221] Art. 1, §, eerste lid cao nr. 81, *supra* noot 41.
[222] Art. 3 cao nr. 81, *supra* noot 41.
[223] Zie *supra* deel 1, 2.1.2.
[224] Art. 2 cao nr. 81, *supra* noot 41.

zelf voorkomt, valt te constateren dat deze uitlegging zo breed is gehouden dat ze bijna zichzelf uitholt. Het toepassingsgebied is ontzettend ruim.[225]

Een ruime definitie, gezien de snelle evoluties van het elektronische landschap, is echter geen overbodige luxe. Terwijl er over sociale media in 2002 ongetwijfeld niet sterk gedebatteerd werd, vallen deze communicatieplatformen nu eveneens onder het toepassingsgebied van de cao.[226] Ook wordt "dienstbetrekking" niet gedefinieerd, waardoor eender welke handeling tussen werkgever en werknemer als "in het kader van de dienstbetrekking" kan worden beschouwd, ook wanneer deze buiten de werkuren plaatsvindt.[227]

Dit alles zou evenwel niet slaan op de controle van telefoongebruik, noch op de inhoud van e-mails.[228] Dit zou vreemd zijn, aangezien de opkomst van elektronische communicatiemiddelen, inclusief e-mail, expliciet door de NAR wordt aangehaald als aanleiding voor het opstellen van de cao.[229] De Hert klaagt de onduidelijkheid hieromtrent aan: het verbod op het kennisnemen van de inhoud van e-mails zou om "opportuniteitsredenen" niet in de cao opgenomen zijn. Toch leest men soms tussen de regels van de cao een impliciet verbod op inzage van e-mails.[230] Het arbeidshof te Brussel oordeelde dat opgeslagen e-mailberichten ook onder de noemen "elektronische onlinecommunicatiegegevens" vallen.[231]

De cao voorziet geen enkel beletsel in controle wanneer men zeker is dat het om professionele communicatie gaat, de werkgever is dan vrij om de communicatie door te lichten. Dit is gebaseerd op de idee dat de goede werking van de onderneming gewaarborgd moet blijven.[232] De bepalingen van de WVP moeten evenwel steeds gerespecteerd worden.[233]

Een belangrijke beperking van het materieel toepassingsgebied van de cao is dat deze enkel van toepassing is op de oppervlakkige *controle van het gebruik* van elektronische communicatie. Regels met betrekking tot toegang en/of gebruik van elektronische onlinecommunicatiemiddelen zijn het prerogatief van de werkgever.[234] Deze kan dus vrij beslissen, weliswaar rekening houdend met andere relevante regelgeving, welke praktijken al dan niet toegelaten zijn binnen de onderneming.

---

[225] Art. 2 en commentaar bij art. 2 cao nr. 81, *supra* noot 41.
[226] Art. 2 cao nr. 81, *supra* noot 41.
[227] Commentaar bij art. 2 cao nr. 81, *supra* noot 41. De werknemer kan dus ook verplicht worden tot loyaal gebruik van internet in zijn privétijd, voornamelijk wanneer hij zich op dat moment identificeert als personeelslid van zijn werkgever. S. COCKX, "Sociale media in de arbeidsrelatie: 'vriend' of vijand?', *Or.* 2012, afl. 1, (12) 19-20.
[228] P. DE HERT, "C.A.O. nr. 81 en advies nr. 10/2000 over controle van internet en e-mail", *RW* 2003, afl. 33, (1281) 1281.
[229] Cao nr. 81, *supra* noot 41, 1.
[230] P. DE HERT, "C.A.O. nr. 81 en advies nr. 10/2000 over controle van internet en e-mail", *RW* 2003, afl. 33, (1281) 1285-1286.
[231] Arbh. Brussel 13 september 2005, *Computerr.* 2006, afl. 2, 100.
[232] Cao nr. 81, *supra* noot 41, 6.
[233] P. WATERSCHOOT, "Bespreking van enkele arresten van het Arbeidshof te Gent in verband met het gebruik en misbruik van e-mail en internet op de werkplaats en het controlerecht van de werkgever daarop", *RW* 2009, afl. 18, 737.
[234] Art. 1 §1 cao nr. 81, *supra* noot 41.

Van zodra toegang en/of gebruik van elektronische onlinecommunicatiemiddelen is toegestaan, moet de werkgever er wel voor zorgen dat dit ongestoord kan gebeuren, dit wil zeggen zonder dat anderen er kennis van kunnen nemen.[235]

De cao handelt enkel over de verhouding tussen werkgever en werknemer, er wordt niets gezegd over bescherming naar derden toe. Daarvoor is de WVP van toepassing.[236]

3.1.2.2 Beginselen

De cao geeft de werkgever een controlerecht, dit wordt als een vaststaand gegeven beschouwd.[237] Om echter op rechtmatige wijze controle uit te oefenen op de elektronische onlinecommunicatiegegevens van zijn werknemers, dient de werkgever aan drie beginselen te voldoen. Dit zijn het finaliteitsbeginsel, het proportionaliteitsbeginsel en het transparantiebeginsel.

i. Finaliteitsbeginsel

De werkgever mag eerst en vooral enkel omwille van bepaalde redenen een controle uitvoeren, namelijk:[238]

- het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of de waardigheid van een andere persoon kunnen schaden;
- de bescherming van de economische, handels- en financiële belangen van de onderneming die vertrouwelijk zijn alsook het tegengaan van ermee in strijd zijnde praktijken;
- de veiligheid en/of de goede technische werking van de IT-netwerksystemen van de onderneming, met inbegrip van de controle op de kosten die ermee gepaard gaan alsook de fysieke bescherming van de installaties van de onderneming, en/of;
- het te goeder trouw naleven van de in de onderneming geldende beginselen en regels voor het gebruik van onlinetechnologieën.

Dit noemt men het finaliteitsbeginsel.[239] Dit omvat dat werkgevers op voorhand doelstellingen van hun handelen moeten vooropstellen en zich hiertoe beperken bij het daadwerkelijk handelen.[240]

Wat betreft het eerste doeleinde worden bedoeld: het kraken van computers, het raadplegen van pornografische of pedofiele sites,…[241] Bij de bescherming van economische, handels- en financiële belangen denkt men aan een toezichtsfunctie op afbrekende berichten over de onderneming en de verspreiding van zakengeheimen.[242] Het derde doeleinde kan inhouden dat de werkgever wil voorkomen dat virussen het netwerk van de onderneming kunnen doordringen. Ten slotte kan de werkgever ook zelf gedragsregels opleggen voor zijn werknemers, bijvoorbeeld dat zij zich moeten

[235] A. PEIFFER, "Controle van e-mail en internetgebruik" in K. STAPPERS (ed.), *Privacy in de arbeidsrelatie: gids voor het voeren van een privacybeleid*, Gent, Story Publishers, 2008, (49) 50.
[236] Zie *supra* noot 63.
[237] Art. 4 cao nr. 81*, supra* noot 41.
[238] Art. 5 cao nr. 81, *supra* noot 41.
[239] Art. 5 cao nr. 81, *supra* noot 41.
[240] P. DE HERT, "C.A.O. nr. 81 en advies nr. 10/2000 over controle van internet en e-mail", *RW* 2003, afl. 33, (1281) 1289.
[241] Commentaar bij art. 5 cao nr. 81, *supra* noot 41.
[242] Commentaar bij art. 5 cao nr. 81, *supra* noot 41.

houden aan een maximum van aantal te downloaden bestanden per maand. Merkt de werkgever dat er over dit maximum wordt gegaan, dan kan hij een controle uitvoeren.

ii. Proportionaliteitsbeginsel

Is inmenging in het privéleven noodzakelijk, dan dient deze inmenging "tot een minimum beperkt" te blijven. Dit is het proportionaliteitsbeginsel.[243] In beginsel dient de werkgever zich echter nog steeds te onthouden van inmenging in het privéleven van zijn werknemers.

Hiermee wordt ook geïmpliceerd dat de verworven gegevens zo beperkt mogelijk dienen te zijn, voor zover ze nodig zijn om het nagestreefde doeleinde te bereiken.

iii. Transparantiebeginsel

De cao vereist ten slotte de bekendmaking van de doelstellingen van de werkgever, dit is het transparantiebeginsel.[244] Er rust een informatieverplichting op de werkgever om zijn werknemers in te lichten over de controlesystemen waarvan hij gebruikmaakt en alle andere aspecten die daarbij komen kijken.[245] Dit kan via het arbeidsreglement.[246] Hij dient evenwel ook de ondernemingsraad in te lichten over alle aspecten van de controle.[247]

Artikel 9 van de cao bepaalt welke informatie meegedeeld moet worden, zijnde welke doelstellingen nagestreefd worden met de controle en voor welke duur de controle wordt gepland. Ook moet de werkgever zijn controlebeleid en prerogatieven signaleren en aangeven of de verzamelde gegevens al dan niet worden bewaard. Ten slotte dient de werkgever aan de werknemers te laten weten hoe zij de ter hun beschikking gestelde instrumenten mogen gebruiken, wat hun rechten en plichten zijn inzake elektronische onlinecommunicatiemiddelen van de onderneming en welke gevolgen aan onrechtmatig gebruik kunnen worden verbonden ten gevolge van het arbeidsreglement.[248]

Naast deze informatieverplichting zijn de controlesystemen van de werkgever ook onderworpen aan een regelmatige evaluatie van de ondernemingsraad, het comité voor preventie en bescherming op het werk of de vakbondsafvaardiging.[249]

---

[243] Art. 6 cao nr. 81, *supra* noot 41.
[244] Art. 7 e.v. cao nr. 81, *supra* noot 41.
[245] Art. 8 cao nr. 81, *supra* noot 41 en S. FEYEN en J. MARTENS, "Sociale media en de (kandidaat-)werknemer" in P. VALCKE, P.J. VALGAEREN en E. LIEVENS, (eds.), *Sociale media: actuele juridische aspecten*, Antwerpen, Intersentia, 2013, (157) 171.
[246] Commentaar bij art. 8 cao nr. 81, *supra* noot 41.
[247] Art. 7 §2 cao nr. 81, *supra* noot 41. Indien er geen ondernemingsraad aanwezig is, voorziet deze bepaling in een cascadesysteem waarbij het comité voor preventie en bescherming op het werk, de vakbondsafvaardiging of de werknemers geïnformeerd dienen te worden.
[248] Art. 9 cao nr. 81, *supra* noot 41.
[249] Art. 10 cao nr. 81, *supra* noot 41. In tegenstelling tot bij art. 7, §2 cao nr. 81 stopt deze cascade bij de vakbondsafvaardiging en wordt (althans niet expliciet) de kans gegeven voor werknemers zelf om de controlesystemen te evalueren, zie *supra* noot 247.

iv. Individualisering van verzamelde gegevens

Is de werkgever niet zeker of de verzamelde gegevens beroepsmatig zijn, dan dient hij de regels voor individualisering van elektronische onlinecommunicatiegegevens in acht te nemen.[250] Individualiseren houdt in dat de werkgever de verzamelde gegevens verwerkt om ze aan een bepaalde persoon toe te schrijven.[251] Bij individualiseren dient, net zoals bij het instellen van een controle, de werkgever de beginselen van finaliteit, proportionaliteit en transparantie te respecteren.[252]

Er zijn twee procedures die gevolgd kunnen worden. Deze zijn afhankelijk van de doeleinden die beoogd worden met de controle.

a) Directe individualisering

Wanneer de controle plaatsvindt om ongeoorloofde feiten te voorkomen, de economische belangen te beschermen of de goede werking van het netwerksysteem te verzekeren, dan mag er een directe individualisering plaatsvinden.[253] Dit moet de werkgever toelaten om snel te kunnen handelen wanneer hij opmerkt dat er gevaren bestaan voor de bescherming van deze doeleinden.

b) Indirecte individualisering

In het geval men de naleving van de in de onderneming geldende beginselen en regels voor het gebruik van onlinetechnologieën wil controleren, dient men een indirecte individualiserings-procedure te doorlopen.[254] Deze procedure start met een alarmbelfase, waarbij werknemers "op een duidelijke en begrijpelijke wijze" ingelicht worden over het bestaan van een gedetecteerde onregelmatigheid en dat gegevens geïndividualiseerd zullen worden wanneer opnieuw een onregelmatigheid wordt vastgesteld.[255]

Vindt er hierna toch een individualisering plaats en wordt een werknemer ervan beticht een onrechtmatigheid te hebben begaan, dan dient er een gesprek te komen met de werkgever vooraleer deze individuele sancties kan nemen.[256] De werknemer krijgt de kans zijn bezwaren uiteen te zetten tegen de beslissing die mogelijk genomen wordt, alsook om het veroordeelde gebruik te rechtvaardigen. Dit gesprek komt er niet wanneer er een schorsing van uitvoering van de arbeidsovereenkomst is.[257]

Deze procedure geeft meer ruimte voor een bemiddelend traject dan de directe individualisatieprocedure, de partijen wordt verplicht in dialoog te gaan. De eerste drie doelstellingen van het finaliteitsbeginsel worden hoger ingeschat dan het naleven van de in de onderneming geldende beginselen, hetgeen slechts regels zijn die de werkgever zelf heeft bepaald.

[250] Art. 11 e.v. cao nr. 81, *supra* noot 41.
[251] Art. 12 cao nr. 81, *supra* noot 41.
[252] Art. 13-17 cao nr. 81, *supra* noot 41.
[253] Dit zijn de eerste drie doelstellingen zoals omschreven onder het finaliteitsbeginsel, zie *supra* noot 238. Art. 15 cao nr. 81, *supra* noot 41.
[254] Dit is de vierde doelstelling die omschreven wordt onder het finaliteitsbeginsel, zie *supra* noot 238. Art. 16 §1 cao nr. 81, *supra* noot 41.
[255] Art. 16 §2 cao nr. 81, *supra* noot 41.
[256] Art. 17 §1 cao nr. 81, *supra* noot 41.
[257] Art. 17 §2 cao nr. 81, *supra* noot 41.

3.1.3 Kritiek

Er zijn vele kritische stemmen gerezen in verband met de inhoud van de cao: niet zozeer over de motieven waaronder werkgeverscontrole getolereerd wordt, wel over de manier waarop deze mag plaatsvinden en de voorwaarden die eraan verbonden zijn. Ook is er kritiek gekomen op de rol van de NAR en de sociale partners in het opstellen van een gezaghebbend document.

Cao nr. 81 is bekritiseerd, maar heeft wel als verdienste een toegankelijke richtlijn te zijn voor private – en, *de facto* publieke – werkgevers. Hierdoor heeft de cao een preventieve werking, ten opzichte van de curatieve werking die een wet in de strikte zin heeft.[258]

In hetgeen volgt wordt getracht een overzicht te geven van de in de rechtsleer meest gepubliceerde kritiek over cao nr. 81 inzake de totstandkoming ervan, het toepassingsgebied, de geponeerde beginselen en de praktische problemen die rijzen.

3.1.3.1 Totstandkoming

Inzake de totstandkoming van de cao bestaat aanzienlijke discussie. Zo rijst de vraag of een cao een wet is in de zin van art. 8 EVRM. Deze bepaling stelt immers een legaliteitsvereiste opdat een uitzondering op het recht op privéleven kan worden bepaald.

Eerder in deze scriptie werd reeds gesteld dat het EVRM geen wet in de formele zin vereist. Elke duidelijk geformuleerde norm van intern recht, geschreven of ongeschreven, volstaat, zolang de betrokken personen er maar kennis van kunnen krijgen.[259]

In principe is een cao een louter verbintenisrechtelijke overeenkomst, evenwel met reglementaire kenmerken.[260] Gezien het feit dat werknemers collectief sterker staan dan individueel, lijkt het ons dat een gedogen van de cao, in het licht van voormelde uitlegging van "wet", aangewezen is.

Een bepaalde strekking gaat hier echter niet mee akkoord. Volgens Humblet kan een cao zoals nr. 81 niet omdat werknemers zodoende afstand doen van hun recht op privacy zonder de vakbonden hiervoor gemandateerd hebben.[261] Eerder werd gezien dat het in principe onmogelijk is om afstand te doen van het recht op privacy.[262] Ook zou een cao in het verlengde moeten liggen van sociaalrechtelijke wetgeving, maar zoals eerder reeds gesteld is er geen op zichzelf staande arbeidsregeling omtrent controle van internetgebruik.

Een cao kan volgens Blanpain daarnaast geen effect hebben op privégebruik van communicatiemiddelen door de werknemer, aangezien het enkel de arbeidsverhouding kan regelen

[258] Introductietekst 'Dossier cybersurveillance' CBPL, 4, http://www.privacycommission.be/sites/privacycommission/files/documents/2011-07-03-introductietekst-cybersurveillance.pdf (consultatie 2 januari 2015) (hierna verkort Introductietekst CBPL).
[259] Zie *supra* deel 1, 2.1.1.1.
[260] F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, 65-66.
[261] Antwerpen 12 februari 2004, *RW* 2005, afl. 30, (1186) 1188, noot P. HUMBLET.
[262] Zie *supra* deel 1, 2.1.2.

en niets daarbuiten.[263] Hij vindt de cao overbodig en noemt werkgeverscontrole vanzelfsprekend, zolang voldaan wordt aan de voorwaarden van finaliteit, proportionaliteit en transparantie.[264]

3.1.3.2 Toepassingsgebied

De Hert noemt de cao een onevenwichtig document, waarbij de relevante grondrechtaspecten en strafbepalingen onvoldoende of eenvoudigweg niet worden erkend, terwijl door de hedendaagse nadruk op grondrechten er toch een evolutie plaatsvindt van *citoyen-salarié* naar *salarié-citoyen*: het *mens zijn* krijgt voorrang op het *werknemer zijn*.[265] Deze onvrede uitte De Hert eerder al bij de onduidelijkheid rond het feit of e-mailcontrole al dan niet gereguleerd wordt door de cao.[266]

Eveneens wordt het door Buelens en Stroobants opgeworpen dat het zeer moeilijk is controle te richten op louter privécommunicatie. De grenzen tussen privé en professioneel zullen vaak erg vaag zijn. Het toepassingsgebied van de cao zou dan ook erg moeilijk vast te stellen zijn.[267]

De cao spreekt zelf van het verduidelijken van de reeds geldende rechtsnormen als doelstelling, net zoals het voorzien van een zekere soepelheid om in te spelen op de situatie van werkgevers, werknemers en/of hun vertegenwoordigers.[268] Volgens Van Eekchoutte heeft de cao evenwel niet tot verduidelijking, maar net tot verwarring geleid. Zo schrijft de cao niets over het vereiste van voorafgaande toestemming van werknemers voor controle, hetgeen in de WEC en het Strafwetboek net erg belangrijk is.[269]

Ook over deze vereiste van voorafgaande toestemming, die voortkomt uit de WVP, bestaat discussie. Volgens het dossier *Cybersurveillance* van de CBPL is deze commissie van oordeel dat werknemers onder geen enkele omstandigheid toestemming kunnen gegeven aan hun werkgever om hun gegevens te controleren. Dit vanwege hun ondergeschikte positie: het gezag van de werkgever zou voorkomen dat een werknemer in eender welke omstandigheid vrij een keuze zou kunnen maken. Cockx betwist dit en haalt alsook aan dat er mogelijkheden zijn om als werkgever toch met toestemming kennis te nemen van gegevens van werknemers. In de rechtspraak zou immers wel rekening worden gehouden met toestemming door de werknemer. [270]

3.1.3.3 Beginselen

De cao hanteert erg ruime begrippen: niet enkel wat de definitie van "elektronische onlinecommunicatiegegevens", maar ook wanneer het gaat over de invulling van het

[263] R. BLANPAIN en M. VAN GESTEL, *Gebruik en controle van e-mail, intranet en internet in de onderneming*, Brugge, Die Keure, 2003, 216.
[264] R. BLANPAIN en M. VAN GESTEL, *Gebruik en controle van e-mail, intranet en internet in de onderneming*, Brugge, Die Keure, 2003, 217.
[265] P. DE HERT, "C.A.O. nr. 81 en advies nr. 10/2000 over controle van internet en e-mail", *RW* 2003, afl. 33, (1281) 1281-1283.
[266] Zie *supra* noot 230.
[267] V. BUELENS en P. STROOBANTS, *Is 'facebooken' een werkwoord?*, Mechelen, Kluwer, 2012, 35.
[268] Zie *supra* noot 216.
[269] Art. 124 WEC, *supra* noot 61, art. 314bis Strafwetboek 8 juni 1867, *BS* 9 juni 1867 en W. VAN EECKHOUTTE, *Sociaal compendium Arbeidsrecht '14-'15 met fiscale notities*, Mechelen, Kluwer, 2014, 807.
[270] Verantwoordingstekst 'Dossier cybersurveillance' CBPL, 2-3, http://www.privacycommission.be/sites/privacycommission/files/documents/2011-07-11-verantwoordingstekst-cybersurveillance.pdf (consultatie 2 januari 2015) (hierna verkort Verantwoordingstekst CBPL) en S. COCKX, "Sociale media in de arbeidsrelatie: 'vriend' of vijand?', *Or.* 2012, afl. 1, (12) 13.

finaliteitsvereiste. Volgens sommige auteurs leidt dit ertoe dat werkgevers in erg veel gevallen controle kunnen uitvoeren. Volgens Dekeyser gaat de cao hier uit de bocht en dienen werkgevers zich er toch van te verzekeren dat zij een gegronde reden tot controle hebben, een beoordeling die niet enkel zou moeten gebeuren met hetgeen voorzien wordt door de cao.[271]

Een meerderheidsstrekking oordeelt daarentegen dat de cao heeft geleid tot een veel te verregaande bescherming voor de werknemer. De balans is volgens deze auteurs zoek, waardoor er in de praktijk op kunstmatige wijze een tempering van de bepalingen van de cao wordt gehanteerd.[272] Het kernwoord hierbij is proportionaliteit: volgens Waterschoot zal dit *het* criterium worden om te beoordelen of werkgeverscontrole geoorloofd is, niet de drieledigheid van beginselen uit de cao.[273]

De indirecte individualiseringsperiode is volgens De Hert omslachtig en misleidend: in de meerderheid van de gevallen is een mogelijkheid tot directe individualisering voorzien, wat vlottere toegang geeft dan voorzien door advies 10/2000 van de CBPL.[274]

3.1.3.4 Praktische problemen

Gilson en Westrade zijn kritisch ten opzichte van het huidige systeem én de arbitraire aanpak in de rechtspraak. Mede door een gebrekkige kennis van practici worden de regels nogal los toegepast in de rechtszaal, maar ook omdat deze té stringent zijn ten opzichte van de werkgever. Het wordt volgens deze auteurs praktisch onmogelijk om op een legale manier bewijsmateriaal te verzamelen wanneer men moet voldoen aan de regels van de privacywet, de WEC en de cao. Terwijl de bedoeling van de cao was om meer duidelijkheid te scheppen en eenvoudigere situaties te creëren, wordt het nog moeilijker om een controle uit te voeren op het internetgebruik van de werknemer.[275]

Volgens Waterschoot is de cao veel te rigide en moeilijk bruikbaar voor werkgevers.[276] In de praktijk wordt dit in evenwicht gebracht door de werkgever minder snel af te straffen wanneer deze de formalistische bepalingen van de privacywetgeving en de cao miskent.[277] Het EHRM keurt deze manier van werken niet af.[278]

[271] H. DEKEYSER, "Internet op het werk en privacy", *Bibliotheek- & archiefgids* 2003, afl. 6, (3) 5.
[272] Onrechtmatig verkregen bewijs wordt onder bepaalde omstandigheden toch toegelaten in de rechtszaal. Zie *infra* deel 2, 3.2.
[273] P. WATERSCHOOT, "De C.A.O. nr. 81 en de privacybescherming van de werknemer, een afdwingbare norm of een papieren tijger?", *RW* 2014, afl. 40, (1563) 1574.
[274] P. DE HERT, "C.A.O. nr. 81 en advies nr. 10/2000 over controle van internet en e-mail", *RW* 2003, afl. 33, 1291. Inzake de CBPL, zie *infra* deel 2, 3.1.4.
[275] M. WESTRADE en S. GILSON (eds.), *Discipline et surveillance dans la relation de travail*, Limal, Anthemis, 2013, 384-388.
[276] P. WATERSCHOOT, "De C.A.O. nr. 81 en de privacybescherming van de werknemer, een afdwingbare norm of een papieren tijger?", *RW* 2014, afl. 40, (1563) 1565.
[277] Zie *infra* deel 2, 3.2. P. WATERSCHOOT, "De C.A.O. nr. 81 en de privacybescherming van de werknemer, een afdwingbare norm of een papieren tijger?", *RW* 2014, afl. 40, 1565.
[278] C. PREUMONT, "Les médias sociaux à l'épreuve du droit du travail", JTT 2011, afl. 22, (353) 356 en P. WATERSCHOOT, "De C.A.O. nr. 81 en de privacybescherming van de werknemer, een afdwingbare norm of een papieren tijger?", *RW* 2014, afl. 40, (1563) 1566. EHRM, *Lee Davies t. België*, 28 juli 2009.

Dekeyser benadrukt ten slotte de praktische moeilijkheden bij beschuldigingen door de werkgever: wie is verantwoordelijk voor het binnenhalen van internetvirussen of het uitsturen en ontvangen van illegale bestanden? In vele gevallen zal dit niet zo duidelijk zijn. Preventieve actie, bijvoorbeeld door middel van filtersoftware waarmee werknemers bepaalde websites niet *kunnen* oproepen, wordt aangeraden.[279]

3.1.4 Visie Commissie ter bescherming van de persoonlijke levenssfeer

3.1.4.1 Voor 2012: werkgeverscontrole bij uitzondering

De Commissie ter bescherming van de persoonlijke levenssfeer (CBPL), zoals opgericht bij de WVP, heeft twee adviserende documenten inzake controle door de werkgever van internetgebruik door de werknemer uitgevaardigd.[280] Deze adviezen zijn niet bindend, ook niet voor de werkgever, maar kunnen wel richting geven aan het normerend kader.[281]

In haar eerste advies uit 2000, vooraleer er sprake was van cao nr. 81, luidde de mening als volgt: de werkgever mag zijn informatica-infrastructuur niet op buitensporige wijze gebruiken als elektronisch controlemiddel op zijn werknemers.[282] De visie van de CBPL liet vroeger de privacy van de werknemer nagenoeg steeds voorgaan op controle door de werkgever. Slechts het proportionaliteitscriterium moest nu en dan voor evenwicht zorgen en de werkgever voldoende mogelijkheden voor controle geven om zijn belangen tot uiting te laten komen.[283]

3.1.4.2 Aanbeveling nr. 08/2012: genuanceerde visie

Het mag duidelijk zijn dat de mening van de CBPL uit 2000 veel kanttekeningen en nuances teweegbrengt, en dat op elke situatie een uitzondering mogelijk is. Op 2 mei 2012 publiceerde de CBPL een aanbeveling uit eigen beweging inzake de controle door de werkgever op het gebruik van elektronische communicatie-instrumenten op de werkvloer. Dit naar aanleiding van de vele vragen die de CPBL kreeg inzake de toepassing van de bestaande regels, alsook de evolutie naar een wijdverspreid gebruik van internet, ook tijdens de diensturen. De in de rechtsleer sterk bekritiseerde visie uit nr. 10/2000 werd hiermee herzien.[284]

De CBPL slaat *mea culpa* in haar tekst: het advies in 2000 voorzag geen enkele wettelijke controlemogelijkheid met betrekking tot het bestaan en de inhoud van zowel private als professionele communicatie, tenzij alle betrokkenen ermee instemden.[285] Sedertdien is cao nr. 81 gekomen, net zoals de WEC, wat nieuwe perspectieven met zich meebrengt. De CBPL is tevreden

---

[279] H. DEKEYSER, "Internet op het werk en privacy", *Bibliotheek- & archiefgids* 2003, afl. 6, (3) 7-8.
[280] Art. 23 e.v. WVP, *supra* noot 63.
[281] W. VAN EECKHOUTTE, *Sociaal compendium Arbeidsrecht '14-'15 met fiscale notities*, Mechelen, Kluwer, 2014, 802.
[282] Voorwoord 'Dossier cybersurveillance' CBPL, 1, http://www.privacycommission.be/sites/privacycommission/files/documents/2011-07-11-verantwoordingstekst-cybersurveillance.pdf (consultatie 2 januari 2015).
[283] D. CUYPERS en P. FOUBERT, *Schets van het Belgische arbeidsrecht*, Antwerpen, Intersentia, 2011, 94.
[284] COMMISSIE TER BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, aanbeveling nr. 08/2012 betreffende de controle door de werkgever op het gebruik van elektronische communicatie-instrumenten op de werkvloer, 2 mei 2012, 2.
[285] Verantwoordingstekst CBPL, *supra* noot 270, 2.

met de inhoud van cao nr. 81 en omschrijft het als een document met een juist evenwicht tussen de conflicterende belangen.[286]

De visie van de CBPL is sinds 2000 dus gewijzigd, op zijn minst genuanceerd. De Commissie schetst dit, in haar verantwoordingstekst van het online te raadplegen dossier *Cybersurveillance*, als een evolutie doorheen de jaren, met de standpunten geponeerd in de verschillende adviezen omtrent het onderwerp. Met name merkt de Commissie een lacune op in het advies van 2000: er is geen regeling voorzien voor toegang tot professionele informatie, het gaat enkel over privé-informatie. Nochtans is het beoogde doel van de werkgever bij kennisname van informatie cruciaal om te bepalen of zijn daden voldoen aan de reeds eerder geponeerde beginselen van legaliteit, transpariteit en proportionaliteit. Ook was de Commissie anno 2000 sterk gekant tegen patronale controle, dit zou slechts onder uitzonderlijke omstandigheden moeten kunnen.[287]

Op de laatste pagina van haar verantwoordingstekst omschrijft de Commissie haar uiteindelijke mening: heeft de werkgever bepaald dat via het professionele e-mailadres enkel professionele communicatie mag verlopen, dan kan hij relatief vrij controle hierop uitoefenen. Dit is anders wanneer ook privécommunicatie wordt toegestaan, dan moeten de regels van cao nr. 81 strikt nageleefd worden. [288]

De CBPL wil de hiaten in haar vorige aanbeveling en cao nr. 81 opvullen met een interpretatie van de WVP, voornamelijk wat professionele communicatie betreft. Blijft er evenwel sprake van een gemengde inbox van e-mails, dan moeten er best afspraken worden gemaakt tussen de contractspartijen en dient de procedure van cao nr. 81 gevolgd te worden.

De Commissie acht de bestaande wetgeving evenwel voldoende om te bepalen in welke mate de werkgever over een controlerecht beschikt.[289] De CBPL is, in tegenstelling tot de rechtsleer, opvallend mild voor de bestaande regelgeving. Zoals later zal blijken formuleert zij een reeks aanbevelingen voor toepassing van de regels in de praktijk, maar een echt kritische noot over de bepalingen van de cao is er niet.[290] Dit zou verklaard kunnen worden door het feit dat de geldende normen in het voordeel van de werknemer zijn, de partij die de CBPL reeds in 2000 toch de meeste bescherming wilde bieden. De CBPL bleek anno 2012 vooral kritisch ten opzichte van zichzelf en haar eigen visie.

[286] Verantwoordingstekst CBPL, *supra* noot 270, 4.
[287] Zo zou de werkgever steeds de instemming van alle betrokkenen moeten bekomen, vooraleer over te gaan tot controle. Verantwoordingstekst CBPL, *supra* noot 270, 2.
[288] Verantwoordingstekst CBPL, *supra* noot 270, 4.
[289] COMMISSIE TER BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, aanbeveling nr. 08/2012 betreffende de controle door de werkgever op het gebruik van elektronische communicatie-instrumenten op de werkvloer, 2 mei 2012, 36.
[290] Zie *infra* deel 2, 4.2.

3.2 Gevolgen van ongeoorloofd internetgebruik

Nadat de werkgever ongeoorloofd gedrag heeft opgemerkt en dit gedrag heeft kunnen individualiseren tot een bepaalde werknemer, kan hij het noodzakelijk achten om tot actie over te gaan.[291] Het spreekt voor zich dat de werkgever gevolgen kan verbinden aan onaanvaardbaar gedrag van zijn werknemer, anders heeft controle weinig zin.

Wil de werkgever ten gevolge van de ontdekking een wijziging maken in zijn beleid inzake internetgebruik, dan kan verwezen worden naar de bespreking van cao nr. 81. Althans wat het invoeren van modaliteiten op gebruik betreft: het is immers het prerogatief van de werkgever om al dan niet toe te laten dat werknemers gebruik mogen maken van het internet.

De werkgever kan ook verdergaande maatregelen nemen, zoals het beëindigen van de arbeidsovereenkomst. In hetgeen volgt zullen, door middel van een bloemlezing uit de rechtspraak ter zake, drie mogelijke bronnen van conflict bij ontslag besproken worden. Er kan discussie ontstaan omtrent de redelijke privacyverwachtingen, er kan gebruik worden gemaakt van onrechtmatig verkregen bewijs en er kan een gebrek zijn aan een zwaarwichtige reden bij het ontslag.

3.2.1 Belang van redelijke privacyverwachtingen

Een werkneemster ging in hoger beroep tegen de beslissing van de arbeidsrechtbank te Gent, waarbij haar ontslag werd goedgekeurd.[292] Zij werd ontslagen nadat haar werkgever vaststelde dat zij systematisch via mobiele telefoon, door de werkgever ter beschikking gesteld, belde naar astrolijnen. Dit zijn betalende telefoonlijnen waarop "kenners" advies geven, gebaseerd op horoscopen. Volgens de werkneemster zou de werkgever een inbreuk hebben gepleegd op haar recht op privacy bij het vergaren van bewijs van haar tekortkoming. Het hof besteedde aandacht aan de redelijke privacyverwachting wanneer men art. 8 EVRM toepast.

- Bewijs van tekortkoming

De werkneemster maakte gebruik van een gsm die de werknemer haar ter beschikking had gesteld. Gezien deze impliciet behoorde tot het arbeidsgereedschap, moest de gsm gebruikt worden op een wijze die in overeenstemming is met de goede trouw. De werkgever mocht dus beslissen waarvoor de gsm gebruikt mocht worden. De werkgever had eveneens het recht het gsm-gebruik te controleren; bij de periodieke afrekening zat telkens een overzicht van de opgeroepen nummers en de duur van de gesprekken. De werkneemster kon aldus verwachten dat dit zou gebeuren en kon zich niet beroepen op een redelijke privacyverwachting. Hiermee was de kous af, althans voor het hof, en oordeelde het dat het niet nodig was verder te bekijken of het recht op privacy geschonden was.

Deze uitspraak lijkt ons correct, maar kort door de bocht. Een privacyschending kan immers zo vreselijk zijn dat zelfs redelijke privacyverwachtingen daar geen rechtvaardiging voor kunnen

[291] Art. 17 §1, tweede lid cao nr. 81, *supra* noot 41. Dit artikel stelt dat de werkgever beslissingen kan nemen of evaluaties kan organiseren, gericht op een bepaalde werknemer.
[292] Arbh. Gent 12 mei 2014, *JTT* 20 oktober 2014, 320-321 afl. 1194.

uitmaken. Een werknemer zit immers in een ondergeschikte positie, waarin zijn of haar toestemming van nagenoeg gener waarde is.

- Fout van werkneemster

Wat de fout van de werkneemster betreft waren er geen concrete afspraken met de werkgever over het gsm-gebruik, doch moest zij nog steeds te goeder trouw te werk gaan. Op de loonfiches werd het voordeel van de gsm ingebracht ter waarde van 5 euro, wat meteen impliceerde dat het te behalen voordeel gering zou moeten zijn. Deze telefoontjes leidden tot een factuur van 90 euro. Het hof stelde zelfs dat – zij het met misschien wat te veel vertrouwen in de mensheid – de werkneemster niet kon geloven in de goedheid van zij die achter de astrolijnen schuil gingen. Op een maand tijd waren slechts 30 belminuten van de 2.285 gewijd aan andere lijnen dan astrolijnen. Na waarschuwingen ging de werkneemster zelfs nog meer bellen, hetgeen van kwade trouw zou getuigen.

Het hof sprak van loondiefstal. Het feit dat de werkgever traag en weinig daadkrachtig had opgetreden, vormde voor het hof geen bezwaar om het handelen van de werkgever toch goed te keuren.

3.2.2 Onrechtmatig verkregen bewijs: Antigoon-doctrine

Ongeoorloofd internetgebruik kan leiden tot ontslag om dringende reden. Of er al dan niet wordt overgegaan tot ontslag zal natuurlijk steeds afhangen van de concrete elementen in de zaak.

Art. 35 WAO stelt dat wanneer een partij een dringende reden inroept, deze tijdig het bewijs hiervan dient te leveren. De werkgever moet zwart op wit kunnen aantonen welk gedrag zijn werknemer heeft gesteld en dat dit uit den boze is.

In principe dient dit bewijs, overeenkomstig de bepalingen van de privacywet en cao nr. 81, rechtmatig verkregen te zijn. De leer van de redelijke privacyverwachtingen wordt hier vaak bij betrokken. Zo was er een zaak voor het arbeidshof te Antwerpen waarbij de werkgever alle regels had gevolgd, behalve de voorafgaande kennisgeving aan de werknemer. Het hof oordeelde dat de werknemer toch redelijkerwijze had kunnen verwachten dat de werkgever zou overgaan tot het toetsen van de opvolging van zijn IT-policy.[293]

Het principe van rechtmatigheid van bewijs is dus niet absoluut. Dit is te danken aan de Antigoon-doctrine, een leer die stamt uit het strafrecht.[294]

3.2.2.1 Principes uit het strafrechtelijk contentieux

Bij toepassing van de Antigoon-doctrine kan onrechtmatig verkregen bewijs in de rechtbank enkel nog geweerd worden uit de debatten wanneer:

[293] S. COCKX, "Sociale media in de arbeidsrelatie: 'vriend' of vijand?', *Or.* 2012, afl. 1, (12) 18.
[294] Cass. 14 oktober 2003, nr. P.03.0762.N en J. LORRÉ, *Sociale media en werkgeverscontrole*, Mechelen, Kluwer, 2012, 148-160.

- de naleving van bepaalde vormvoorwaarden voorgeschreven wordt op straffe van nietigheid;
- de begane onrechtmatigheid de betrouwbaarheid van het bewijs heeft aangetast;
- het gebruik van het bewijs in strijd is met het recht op een eerlijk proces.[295]

3.2.2.2 Antigoon in het arbeidsrecht

In het Chocolatier Manonarrest, een strafrechtelijke zaak in een arbeidsrechtelijke context, besliste het Hof van Cassatie dat de feitenrechter rekening mocht houden met videobeelden die in strijd met cao nr. 68 waren verkregen.[296] Hiermee werd geheim cameratoezicht aanvaard.

Op 10 maart 2008 aanvaardde het Hof van Cassatie dat de Antigoon-doctrine ook van toepassing is in een arbeidsrechtelijke, burgerlijke zaak.[297] De rechter kan bij zijn belangenafweging rekening houden met:

- het zuiver formeel karakter van de onregelmatigheid;
- de weerslag op het recht of de vrijheid die door de overschreden norm zijn beschermd;
- het feit dat de ernst van de inbreuk de begane onrechtmatigheid overstijgt;
- het feit dat de onregelmatigheid volstrekt onevenredig is met de ernst van de inbreuk;
- de omstandigheid dat de overheid die met de opsporing, onderzoek en vervolging van misdrijven is belast, al dan niet de onrechtmatigheid opzettelijk heeft begaan;
- het feit dat het onrechtmatig verkregen bewijs enkel een materiaal element van het bestaan van de inbreuk betreft. [298]

Belangrijk criterium is of de ernst van de inbreuk van de werknemer de onregelmatigheid van de werkgever al dan niet overstijgt. Dit doet geen afbreuk aan de geldende bepalingen, het toont enkel des te meer aan dat de rechter een zeer grote appreciatiemarge heeft in zaken omtrent internetcontrole door de werkgever. Er wordt gekeken naar de concrete omstandigheden en de ernst van de tekortkoming van de werknemer. De CBPL spreekt zich hier zelfs positief over uit.[299]

De leer van redelijke privacyverwachtingen wordt eveneens betrokken bij het beoordelen van bewijs, zij het in het voordeel van de werkgever. De werknemer kan wel verwachten dat de werknemer soms controle uitvoert, zelfs al werd deze niet expliciet ter kennis gebracht.[300]

Dit alles heeft ertoe geleid dat ook in het arbeidsrecht men minder snel onrechtmatig verkregen bewijsmateriaal zal weren. In het verleden werd dit bewijs immers automatisch buiten de beoordeling van de rechter gelaten.[301]

---

[295] Cass. 14 oktober 2003, nr. P.03.0762.N en V. BUELENS en P. STROOBANTS, *Is 'facebooken' een werkwoord?*, Mechelen, Kluwer, 2012, 65-67.
[296] Cass. 2 maart 2005, nr. P.04.1644.F/1.
[297] Cass. 10 maart 2008, nr. S.07.0073.N/1 en K. VAN KILDONCK, "Privacy werknemers: onrechtmatig verkregen bewijs op het werk", *NJW* 2010, afl. 218, (180) 181.
[298] Cass. 10 maart 2008, nr. S.07.0073.N/1 en K. VAN KILDONCK, "Privacy werknemers: onrechtmatig verkregen bewijs op het werk", *NJW* 2010, afl. 218, (180) 181.
[299] S. COCKX, "Sociale media in de arbeidsrelatie: 'vriend' of vijand?', *Or.* 2012, afl. 1, (12) 18 en Juridisch rapport 'Dossier cybersurveillance', 25, http://www.privacycommission.be/sites/privacycommission/files/documents/2011-07-05-juridisch-rapport-cybersurveillance.pdf (consultatie 2 januari 2015).
[300] S. COCKX, "Sociale media in de arbeidsrelatie: 'vriend' of vijand?', *Or.* 2012, afl. 1, (12) 17.

3.2.2.3 Gemengde reacties

Voor het eerst werden de Antigoon-principes in burgerlijke zaken toegepast. Dit betekende een enorme ommezwaai in de rechtspraak, aangezien de mogelijke gronden tot aanvaarding van onrechtmatig verkregen bewijs zo ruim zijn.[302] Er is evenwel tegenstrijdige rechtspraak, zo oordeelde de Franstalige kamer van Cassatie in november 2008 dat automatische wering van onrechtmatig verkregen bewijs toch de regel is.[303] Voor het strafrecht is de doctrine ingebed in art. 32 Voorlopige Titel Wetboek van Strafvordering, voor het arbeidsrecht blijft er verdeeldheid.[304]

Er is een strekking in de rechtsleer die de implementatie van de Antigoon-doctrine in een sociale context toejuicht, in het bijzonder wat betreft werkgeverscontrole van internetgebruik. Dit zou het evenwicht tussen het recht op privacy en het controlerecht van de werkgever herstellen en tegemoetkomen aan het rechtvaardigheidsgevoel van de werkgever.[305]

Dit lijkt een goed standpunt, zij het onder voorbehoud. Gelet op het feit dat er nog strafsancties en burgerlijke schadevergoedingen bestaan op de schending van het recht op privacy, is deze bittere pil (namelijk het gebruik van onrechtmatig verkregen bewijs) makkelijker te aanvaarden en zal de werknemer veelal niet ten onrechte aan het kortste eind trekken.[306]

Een andere strekking vreest echter voor een correcte uitvoering van de privacywetgeving. Waarom zou een werkgever zich immers nog aan de regels gesteld in de wet en de cao houden wanneer zijn bewijsmateriaal toch niet uit de debatten zal worden geweerd, zelfs al was de manier van bekomen onrechtmatig? Nadeel is dat de Antigoon-doctrine misbruikt kan worden, ze is erg vaag en een *passe-partout*. Volgens Waterschoot kan de cao formeel beter vereenvoudigd worden en de Antigoon-doctrine terug gelimiteerd worden tot een strafrechtelijke aangelegenheid.[307]

Hier speelt de belangenafweging van de rechter ons inziens een belangrijke rol: deze kan een recidiverende werkgever immers afstraffen. Feit blijft echter dat ook in dit geval de rechter in zekere mate de wet stelt. De vraag dringt zich in welke mate een rechter recht spreekt: past hij de wet toe, of vormt hij ze zelf?

De meeste rechtspraak blijkt evenwel te getuigen van een zekere redelijkheid, zodat de Antigoon-doctrine geen grote bedreiging vormt voor de rechten van de werknemer. De werkgever mag niet

[301] W. VAN EECKHOUTTE, *Sociaal compendium Arbeidsrecht '14-'15 met fiscale notities*, Mechelen, Kluwer, 2014, 816.
[302] K. VAN KILDONCK, "Privacy werknemers: onrechtmatig verkregen bewijs op het werk", *NJW* 2010, afl. 218, (180) 182.
[303] K. VAN KILDONCK, "Privacy werknemers: onrechtmatig verkregen bewijs op het werk", *NJW* 2010, afl. 218, (180) 182.
[304] Wet 24 oktober 2013 tot wijziging van de voorafgaande titel van het Wetboek van strafvordering wat betreft de nietigheden, *BS* 12 november 2013 (Wet-Landuyt). P. WATERSCHOOT, "De C.A.O. nr. 81 en de privacybescherming van de werknemer, een afdwingbare norm of een papieren tijger?", *RW* 2014, afl. 40, 1573 en W. VAN EECKHOUTTE, *Sociaal compendium Arbeidsrecht '14-'15 met fiscale notities*, Mechelen, Kluwer, 2014, 816.
[305] K. VAN KILDONCK, "Privacy werknemers: onrechtmatig verkregen bewijs op het werk", *NJW* 2010, afl. 218, (180) 183.
[306] K. VAN KILDONCK, "Privacy werknemers: onrechtmatig verkregen bewijs op het werk", *NJW* 2010, afl. 218, (180) 183.
[307] P. WATERSCHOOT, "De C.A.O. nr. 81 en de privacybescherming van de werknemer, een afdwingbare norm of een papieren tijger?", *RW* 2014, afl. 40, (1563) 1574-1575.

te ver gaan, flagrant onrechtvaardig gedrag wordt niet getolereerd. Zo werd het openbreken van een locker van de werknemer gekwalificeerd als een schending van de redelijke privacyverwachtingen en werd het onrechtmatig verkregen bewijs geweerd.[308]

3.2.3 Gebrek aan zwaarwichtige reden

Er kan op worden gewezen dat, wanneer de werknemer wil overgaan tot ontslag omwille van dringende reden, erop gelet moet worden dat er ook een dringende reden aanwezig is.

Belangrijk bij ontslag is of verdere samenwerking door de feiten onmogelijk is geworden of niet, alsook of dit een weerslag kan hebben op de toekomstige werkprestaties van de werknemer en het imago van de werkgever. Zo werd een werkneemster van een warenhuisketen ontslagen omdat zij in haar vrije tijd van weinig fatsoen getuigende webcamshows verzorgde. De rechter verklaarde het ontslag om dringende reden ongerechtvaardigd. Er was volgens deze geen blijk van negatieve weerslag op de goede werking van de onderneming en de professionele samenwerking met de werkneemster.[309]

3.2.3.1 Arbeidsrechtbank Brussel, 2 mei 2000

In een zaak voor de arbeidsrechtbank te Brussel in 2000 liet een werknemer van een kantoor voor gerechtsdeurwaarders na zijn werk als informaticaverantwoordelijke op bevredigende wijze uit te voeren. Hierdoor werd zijn online tijdverdrijf door de werkgever gecontroleerd. Uit zijn e-mails bleek dat hij doorheen de dag via het intranet privéberichten verzond naar een collega van het kantoor. [310]

De rechtbank vond het niet nodig dat de precieze inhoud werd gecontroleerd en dat er aan de hand van de informatie over hoeveel berichten er werden verstuurd voldoende afgeleid kon worden. Het proportionaliteitsbeginsel moest in acht genomen worden.[311]

Er zou geen voldoende zwaarwichtige reden zijn om tot ontslag om dringende reden over te gaan. De rechtbank oordeelde dat het overmatig gebruik van e-mail voor private doeleinden minstens een lichte fout was, maar doordat de werkgever eerder had kunnen en moeten ingrijpen werd de zwaarwichtigheid van deze fout verminderd.[312] De handelingen van de werkgever vormen dus een belangrijk criterium in de beoordeling van de dringende reden. Soms zal de rechter evenwel milder zijn omdat degene wie iets verweten wordt, zich effectief naar de beschuldigingen heeft gedragen.[313]

Bijzonder aan de uitspraak van de Brusselse rechtbank is dat men amper reageert op het feit dat de werkgever privéconversaties controleert, de wet treedt hier in principe immers sterk tegen op.

---

[308] S. COCKX, "Sociale media in de arbeidsrelatie: 'vriend' of vijand?', *Or.* 2012, afl. 1, (12) 18 en Arbrb. Brussel 2 mei 2011, A.R. 09/7124.A, onuitg.
[309] Arbrb. Kortrijk 8 oktober 2008, onuitg. en T. STRUBBE, "Is er plaats voor sociale media op de werkvloer?", *supra* noot 8, (45) 59-64.
[310] Arbrb. Brussel 2 mei 2000, *Computerr.* 2001, afl. 1, 26, noot D. CASAER.
[311] Arbrb. Brussel 2 mei 2000, *Computerr.* 2001, afl. 1, 27, noot D. CASAER.
[312] Arbrb. Brussel 2 mei 2000, *Computerr.* 2001, afl. 1, 27-28, noot D. CASAER.
[313] Arbrb. Namen 10 januari 2011, *JTT* 2011, afl. 28, 462-463.

De rechtbank hecht duidelijk meer belang aan het eigendoms- en controlerecht van de werkgever dan gebruikelijk is bij de afweging tegenover het recht op privacy van de werknemer.[314]

3.2.3.2 Arbeidsrechtbank Leuven, 17 november 2011

In *Option*, een zaak van de arbeidsrechtbank te Leuven, ging het over negatieve berichtgeving over halfjaarlijkse resultaten van een bedrijf op Facebook geplaatst door een kaderlid van dit bedrijf. [315] De werknemer had stelselmatig de gang van zaken smalend beschreven. Hij overschatte zijn positie binnen het bedrijf. De werkgever ontsloeg hem dan ook om dringende reden.[316]

Aangezien de werknemer zijn profiel openbaar ingesteld stond, vond de rechter dat hier geen sprake was van enige schending van privacy. Veel belang werd gehecht aan de context van een beursgenoteerd bedrijf dat onderhevig is aan geruchten of commentaren, de functie als manager en het cruciale moment van de uitlatingen, op een moment waarop de algemene directeur met man en macht probeerde de financiële markten gerust te stellen.[317]

3.2.3.3 Arbeidshof Brussel, 3 september 2013

Het Brusselse arbeidshof ging minder snel dan de Leuvense rechtbank over tot het aanvaarden van een dringende reden bij een zaak over een lid van het CPBW, het Comité voor Preventie en Bescherming op het Werk. Een openbare Facebook-groep werd niet bestempeld als volledig toegankelijk, er moest al bewust naar gezocht worden om kennis te krijgen van de berichten die erop geplaatst werden. De reputatieschade en het aangevoerde ernstig nadeel werd niet bewezen. Er was geen sprake van een ernstige tekortkoming die de samenwerking onmiddellijk en definitief onmogelijk maakte.[318]

Het arbeidshof oordeelde wel dat een werknemer moet begrijpen dat zijn Facebookpagina vrij toegankelijk is en dat er dan geen schending zal zijn van zijn redelijke privacyverwachtingen. De werkgever is doelbewust op zoek gegaan naar informatie die niet voor hem bestemd was, hetgeen een schending vormde van de WEC. Het bewijs kan echter wel gebruikt worden als er geen op straffe van nietigheid voorgeschreven vorm werd miskend en er geen gebrek in de betrouwbaarheid van het bewijs bewezen kan worden of dat het eerlijk proces in gedrang komt. Met andere woorden werd de Antigoon-doctrine toegepast. Het ontslag bleek gerechtvaardigd, verdere samenwerking omwille van openbare negatieve uitlatingen was onmogelijk.[319]

Deze zaak, waarin de discussies over redelijke privacyverwachtingen, onrechtmatig verkregen bewijs en de aanwezigheid van zwaarwichtige reden samenkomen, toont aan dat de rechter in zijn beoordeling de zaken vaak zal beoordelen op de aanwezigheid van gezond verstand. De beoordeling of er al dan niet een recht op privacy aanwezig is krijgt zo een bijzondere invulling.

[314] Arbrb. Brussel 2 mei 2000, *Computerr.* 2001, afl. 1, 28, noot D. CASAER.
[315] Arbrb. Leuven 17 november 2011 (*Option*).
[316] Arbrb. Leuven 17 november 2011 (*Option*).
[317] J. LORRÉ, *Sociale media en werkgeverscontrole*, Mechelen, Kluwer, 2012, 76-77.
[318] J. LORRÉ, *Sociale media en werkgeverscontrole*, Mechelen, Kluwer, 2012, 78-79.
[319] Arbh. Brussel 3 september 2013, *RW* 2014, afl. 40, 1586-1590, noot.

4 Aanbevelingen

4.1 Rechtsleer

De rechtsleer, alsook de praktijk, klaagt een gebrek aan aangepaste wetgeving aan. In afwachting hiervan gaan sommige bedrijven zelfregulerend te werk en stippelt men een eigen beleid of *policy* uit, op maat van individuele ondernemingen.[320]

Een compleet verbod op internet op de werkvloer is niet de oplossing, dit heeft allesbehalve positieve gevolgen voor de productiviteit van werknemers.[321] De betrekking wordt voor de werknemer immers niet aantrekkelijk als er aanzienlijke belemmeringen worden gelegd op zijn communicatiemogelijkheden, alsook beknopt dit de mogelijkheden voor profilering van de onderneming naar buiten toe.[322] Werknemers kunnen ingezet worden als ambassadeurs van de onderneming, hun communicatie kan dan ook aangemoedigd worden. Zij het met, zo valt aan te raden, zekere regulering.[323]

Doet de werkgever niets, dan kan dit geïnterpreteerd worden als het *de facto* gedogen van een zekere mate van internetgebruik op de werkvloer. In conflictsituaties zal dit de zaak voor de werkgever enkel maar bemoeilijken.[324]

4.1.1 Voorzien van beleid

Een zeker gedoogbeleid moet kunnen, een beleid is evenwel noodzakelijk. De ene onderneming kiest voor afdwingbare regels via het arbeidsreglement, de andere opteert voor een minder dwingende gedragscode die de werknemers vooral dient te sensibiliseren.[325] Een neergeschreven beleid is onmisbaar voor een werkgever: zowel om zelf de rechten van zijn werknemers te respecteren, alsook om sancties en een aanpassing in gedrag te kunnen afdwingen. En, al dan niet in meest ondergeschikte orde, om de rechter gunstig te stemmen.[326]

Peiffer stelt een bepaald stappenplan voor, dat de werkgever kan hanteren bij het implementeren van een *social media* policy. Dit plan zou ervoor moeten zorgen dat werkgevers bij hun handelen de geldende rechtsnormen respecteren.[327]

---

[320] J. ROUSSEAU en I. PLETS, "Sociale media en arbeidsrecht", *supra* noot 48, (119) 119.
[321] In 2012 werd 4 op de 10 werknemers de toegang tot sociale media ontzegd. X, "Vier op de tien werkgevers blokkeren toegang tot sociale media", Algemeen persbericht Het Nieuwsblad, 28 februari 2012, http://www.standaard.be/cnt/dmf20120228_235.
[322] V. BUELENS en P. STROOBANTS, *Is 'facebooken' een werkwoord?*, Mechelen, Kluwer, 2012, 34.
[323] V. BUELENS en P. STROOBANTS, *Is 'facebooken' een werkwoord?*, Mechelen, Kluwer, 2012, 40.
[324] J. LORRÉ, "Facebook en arbeidsrecht: *mysterium tremendum et fascinans*", *RW* 2011, afl. 36, (1498) 1503 en Arbh. Antwerpen 1 oktober 2003, *JTT* 2004, afl. 902, 510-512.
[325] J. ROUSSEAU en I. PLETS, "Sociale media en arbeidsrecht", *supra* noot 48, (119) 119.
[326] J. ROUSSEAU en I. PLETS, "Sociale media en arbeidsrecht", *supra* noot 48, (119) 121.
[327] Dit tiendelig plan ziet uit als volgt:
1. De werkgever kiest welke communicatiemiddelen hij ter beschikking stelt van het personeel;
2. De werkgever informeert de ondernemingsraad over de invoering van e-mail en/of internet;
3. De werkgever bezorgt relevante informatie aan de ondernemingsraad;
4. De werkgever organiseert een overleg binnen de ondernemingsraad;
5. De werkgever stelt een internetreglement op;
6. De werkgever laat het reglement voor kennisname en akkoord ondertekenen door de werknemer;
7. Het arbeidsreglement wordt bijgewerkt met inachtneming van het nieuwe reglement;
8. De werkgever doet aangifte bij de CBPL;
9. De werkgever voert de nodige technische aanpassingen door om het voorziene internetgebruik te faciliteren, en;

4.1.2 Vorm en afdwingbaarheid van beleid

Een beleidslijn kan in verschillende vormen neergeschreven worden: dit kan variëren van een bijlage bij de arbeidsovereenkomst, tot een paragraaf in het arbeidsreglement, een interne nota,… De belangrijkste onderscheidende factor hierbij zal de afdwingbaarheid zijn.[328] Hierbij is het van belang vooreerst te bepalen in welke mate men een zeker gedrag wil aanmoedigen, dan wel wil afdwingen.[329]

In het algemeen kunnen, op basis van afdwingbaarheid, drie vormen van een internetbeleid onderscheiden worden:

- opname in de arbeidsovereenkomst, als integraal deel hiervan;
- opname in het arbeidsreglement;
- eenzijdig opstellen van richtlijnen, door middel van een policy, gedragscode, protocol,…

De bron bepaalt de waarde en binding die de regels hebben. Dit is volgens bepaalde auteurs evenwel niet van belang. Volgens deze strekking gaat het om instructies van de werkgever, die hoe dan ook dienen te worden opgevolgd overeenkomstig de wet arbeidsovereenkomsten.[330]

Het sociale draagvlak zal evenwel grondig verschillen, aangezien bij een opname in de arbeidsovereenkomst of het arbeidsreglement instemming van de werknemer of werknemersorganisatie nodig is. Bij een ander document is dit niet vereist. Bij een policy is er dus geen werknemersinspraak.[331] Voor een optimale dekking is de opname van regels in de arbeidsovereenkomst dan ook aangewezen.[332]

Via de arbeidsovereenkomst kan eenzijdig worden gewerkt, zonder inspraak van de werknemers over sanctioneringsmogelijkheden. Dit is voor de werkgever eenvoudiger en de werknemer is meteen op de hoogte van zijn rechten en plichten.[333]

Het arbeidsreglement is een erg rigide document, de aanpassingsprocedure is erg omslachtig.[334] Het paritair comité of de sociale inspectie kunnen tussenkomen, alsook de ondernemingsraad. Evenwel, wanneer een werkgever sancties wil opleggen op zijn werknemers dienen deze in het arbeidsreglement te zijn opgenomen.[335] Bij invoering in het arbeidsreglement moet de sociale inspectie geïnformeerd worden.[336]

---

10. De werkgever organiseert periodieke evaluatie van het controlesysteem in de ondernemingsraad.
A. PEIFFER, "Controle van e-mail en internetgebruik" in K. STAPPERS (ed.), *Privacy in de arbeidsrelatie: gids voor het voeren van een privacybeleid*, Gent, Story Publishers, 2008, (49) 62-64.

[328] V. BUELENS en P. STROOBANTS, *Is 'facebooken' een werkwoord?*, Mechelen, Kluwer, 2012, 34.
[329] J. ROUSSEAU en I. PLETS, "Sociale media en arbeidsrecht", *supra* noot 48, (119) 126.
[330] V. BUELENS en P. STROOBANTS, *Is 'facebooken' een werkwoord?*, Mechelen, Kluwer, 2012, 37-39 en J. ROUSSEAU en I. PLETS, "Sociale media en arbeidsrecht", *supra* noot 48, (119) 129.
[331] J. ROUSSEAU en I. PLETS, "Sociale media en arbeidsrecht", *supra* noot 48, (119) 129.
[332] J. ROUSSEAU en I. PLETS, "Sociale media en arbeidsrecht", *supra* noot 48, (119) 130.
[333] J. ROUSSEAU en I. PLETS, "Sociale media en arbeidsrecht", *supra* noot 48, (119) 131.
[334] Art. 11 en 12 wet 8 april 1965 tot instelling van de arbeidsreglementen, *BS* 5 mei 1965.
[335] V. BUELENS en P. STROOBANTS, *Is 'facebooken' een werkwoord?*, Mechelen, Kluwer, 2012, 41.
[336] Art. 15, laatste lid wet 8 april 1965 tot instelling van de arbeidsreglementen, *BS* 5 mei 1965.

Door middel van een policy kan de werkgever tonen dat hij niet akkoord gaat met bepaalde handelingen van zijn werknemers. Staat dit neergeschreven, dan zal de werkgever een betere verdediging hebben wanneer hij later een werknemer wil sanctioneren omwille van zulk ongewenst gedrag.[337]

De aanwezigheid van duidelijke richtlijnen vergroot de kans dat de rechter het gedrag van de werknemer als dringende reden voor ontslag aanvaardt. De afwezigheid kan een reden zijn om de dringende reden te verwerpen.[338]

4.1.3 Inhoud van beleid

Wat de inhoud van een internetbeleid betreft, kan worden aangeraden om op alle aspecten van internetgebruik te focussen. De meeste bestaande richtlijnen gaan over privégebruik, maar ook het gebruik in het kader van het werk dient gereguleerd te worden.[339]

Wordt er een social media policy opgesteld, dan dient best de nadruk te worden gelegd op de vertegenwoordigingsfunctie van een werknemer, om eveneens online goed gedrag aan te moedigen. Dit zonder nadruk te leggen op alle handelingen die niet mogen.[340]

Osaer en Nayaert pleiten voor een wet die bepaalt welke controlemiddelen mogen worden aangewend. Zij menen immers dat de sociale partners hun boekje te buiten zijn gegaan met cao nr. 81 en dat de daaropvolgende rechtspraak zo verdeeld is dat het rechtsonzekerheid teweeg brengt.[341] Een wet met een allesomvattende regeling kan alles oplossen, maar dit lijkt bijzonder positief ingesteld. Een allesomvattende wet zit er immers niet aan te komen.

Een goed opgestelde policy is onontbeerlijk, op grond hiervan zal immers al dan niet tot sanctionering kunnen worden overgegaan.[342] Het werkgeversgezag is sneller afdwingbaar, het legaliteitsbeginsel wordt benaderd, de werknemer wordt gecontroleerd na een voorafgaande informatie(plicht) en het is redelijkerwijs te verwachten dat er controle komt. Mochten alle ondernemingen op even correcte wijze dergelijk beleid uitstippelen, dan zouden vele problemen uit de praktijk meteen opgelost zijn.

4.2 Commissie ter bescherming van de persoonlijke levenssfeer

De CBPL raadt werknemers af het e-mailsysteem op het werk ook voor privézaken te gebruiken. Splits je duidelijk je soorten communicatie, dan is het veel gemakkelijker om een controle uit te voeren zonder – al dan niet onwetend – het recht op privacy te schenden.[343]

De CBPL voorziet enkele juridische gedragsregels, louter aanbevelingen. De Commissie raadt preventieve handelingen aan die maximaal uitgewerkt worden, om de nood aan controle tot het

[337] J. ROUSSEAU en I. PLETS, "Sociale media en arbeidsrecht", *supra* noot 48, (119) 128.
[338] J. ROUSSEAU en I. PLETS, "Sociale media en arbeidsrecht", *supra* noot 48, (119) 155.
[339] J. ROUSSEAU en I. PLETS, "Sociale media en arbeidsrecht", *supra* noot 48, (119) 124.
[340] V. BUELENS en P. STROOBANTS, *Is 'facebooken' een werkwoord?*, Mechelen, Kluwer, 2012, 40.
[341] V. OSAER en S. NAYAERT, "Privacy in de werksfeer", *supra* noot 65, (513) 558.
[342] S. COCKX, "Sociale media in de arbeidsrelatie: 'vriend' of vijand?', *Or.* 2012, afl. 1, (12) 23.
[343] Introductietekst CBPL, *supra* noot 258, 6.

minimum te beperken. Dit vraagt niet enkel een preventieve gedachtegang van de werkgever, maar ook een verantwoordelijkheid van de werknemers.[344]

De CBPL stelt 7 verschillende acties voor:

- Het wordt aangeraden professionele en privé-informatie zoveel mogelijk gescheiden te houden, bijvoorbeeld door private informatie af te schermen in een map met een naam waaruit duidelijk blijkt dat het gaat over private informatie. Het gebruik van verschillende e-mailaccounts wordt ook aangeraden;
- Risicovolle handelingen zouden uitgesloten moeten worden. Zo kan de werkgever bepaalde websites waarvan geweten is dat zij niet-geschikte inhoud bevatten, geblokkeerd worden op de werkvloer;
- Een specifieke omkadering kan voorzien worden voor de toegang tot persoonlijke communicaties, zo kan men bijvoorbeeld uitdrukkelijk het woord *vertrouwelijk* in de titel van een e-mail plaatsen;
- Het toezicht dient beperkt te worden tot de noodzakelijke gegevens, bijvoorbeeld het bekijken van logbestanden waarmee te zien is welke websites men bezoekt en niet wat hierop staat. Ook mogen ingezamelde gegevens niet hergebruikt worden;
- Voer onverenigbaarheden in voor de toegangsrechten voor eenzelfde persoon, zodat iemand bijvoorbeeld sporen van zijn eigen fraude niet kan uitwissen;
- Beheer de sporen, en;
- Bepaal de functioneringsregels in uitzonderlijke gevallen, bijvoorbeeld het verplicht maken voor werknemers om een out-of-office in te stellen, of criteria te bepalen voor de vertrouwenspersoon die wordt aangesteld.[345]

De CBPL is van oordeel dat, als deze vuistregels in acht worden genomen, er geen herziening van de wet nodig is. Het huidig wettelijk arsenaal voorziet volgens haar genoeg actiemogelijkheden voor alle partijen en laat eveneens genoeg ruimte voor specifieke regels bij elke organisatie.[346]

[344] COMMISSIE TER BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, aanbeveling nr. 08/2012 betreffende de controle door de werkgever op het gebruik van elektronische communicatie-instrumenten op de werkvloer, 2 mei 2012, 40.
[345] COMMISSIE TER BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, aanbeveling nr. 08/2012 betreffende de controle door de werkgever op het gebruik van elektronische communicatie-instrumenten op de werkvloer, 2 mei 2012, 47-53.
[346] COMMISSIE TER BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, Infobrochure "Cybersurveillance", http://www.privacycommission.be/sites/privacycommission/files/documents/Cybersurveillance_NL.pdf (consultatie 2 januari 2015).

5 Tussenconclusie

De internationale en supranationale rechtsbronnen hebben een geringe rechtstreekse impact op het Belgisch recht. Zij zijn echter wel belangrijk geweest als impuls voor de nationale instanties om een beleid ter zake uit te stippelen.

Hoewel er momenteel een herziening in de stijgers staat van de Europese richtlijnen rond privacy, stelt zich de vraag in welke mate deze zal ingrijpen op het arbeidsrecht. De Europese Commissie lijkt veel vertrouwen te willen leggen in de handen van de sociale partners. Als voor de Algemene Verordening Gegevensbescherming de debatten dezelfde koers blijven varen, zal er voor het eerst een rechtstreeks bindende regel inzake privacy op de werkvloer vanuit de EU uitgevaardigd worden. Hoewel deze waarschijnlijk niet meer dan enkele, in het Belgisch stelsel reeds voor zichzelf sprekende, beginselen zal verankeren, is dit toch een belangrijke stap in de gewaarwording van het belang van regelgeving omtrent het onderwerp.

Wat de Belgische situatie betreft, dient er vooral te worden gekeken naar de bepalingen van cao nr. 81. Hoewel deze cao erg kritisch werd onthaald en velen van mening zijn dat de cao de situatie enkel maar bemoeilijkt, trekken practici hun plan met hetgeen hen gegeven is. Gevolg hiervan is evenwel dat er vele verschillende strekkingen bestaan binnen rechtsleer en rechtspraak. Ook door middel van de Antigoon-doctrine wordt er toch een manier gevonden om af te wijken van de, veelal als de streng beoordeelde, criteria voor werkgeverscontrole van cao nr. 81.

Toch moet de situatie niet overdreven worden. Er is sprake van een zekere rechtsbedeling, ook nu er nieuwe vormen van elektronische communicatie hun intrede hebben gedaan. Sociaalnetwerksites zijn immers geen determinerende factor voor een nieuw soort rechtspraak, zij vormen slechts een nieuw kanaal. [347]

Het voornaamste probleem van de gedifferentieerde aanpak is de rechtsonzekerheid die dit tot gevolg heeft. De nood aan initiatief op internationaal en supranationaal niveau is echter niet zo groot dat de bescherming van een mensenrecht in het gedrang komt.

Practici hebben al vele aanbevelingen gedaan om de situatie te verbeteren en te zorgen voor een coherente visie. De beste wijze om de problematiek als werkgever te benaderen zou zijn om duidelijke afspraken te maken door middel van een *social media* policy, maar dit lost het probleem natuurlijk nog steeds niet op. Pas als er op internationaal, supranationaal of nationaal niveau initiatieven worden ondernomen, kan er rechtszekerheid bekomen worden.

[347] J. LORRÉ, "Facebook en arbeidsrecht: *mysterium tremendum et fascinans*", *RW* 2011, afl. 36, (1498) 1506.

Deel 3 Werkgeverscontrole van internetgebruik in de Verenigde Staten van Amerika

1 Inleiding

De hoeveelheid aangepaste wet- en regelgeving inzake werkgeverscontrole op de werkvloer in Europa en België is miniem. Dit brengt uitdagingen met zich mee voor de partijen die in de praktijk in aanraking komen met deze controlemogelijkheden. Werkgevers zijn voor een groot deel op zichzelf aangewezen om te bepalen wat zij toelaten op de werkvloer en hoe zij eventuele surveillance aanpakken.

De regels inzake gegevensbescherming op het Europese continent zijn afgestemd op de leefwereld van de Europeanen. Buiten Europa, bijvoorbeeld in de Verenigde Staten van Amerika (VS), zullen andere regels en gewoonten aangetroffen worden. Er is sprake van een gediversifieerd beleid over de hele wereld.[348]

Net zoals in Europa valt op te merken dat de evolutie van *web 1.0* naar *web 2.0* een belangrijke impuls is geweest voor een nieuwe wending in de aanpak van gegevensbescherming. Terwijl rechtsleer en rechtspraak daterend van de vorige eeuw een relatief simplistische visie erop na houden, wordt de discussie vanaf de opkomst van sociale media veel ingewikkelder. Oudere regels dienen met de actualiteit indachtig geïnterpreteerd te worden. Werkgevers hebben er steeds meer belang bij dat ze het gedrag van hun werknemers controleren.[349]

Dit deel dient een rechtsvergelijkende analyse te bieden van het rechtsstelsel van de Verenigde Staten van Amerika met de regels zoals geldend binnen België en de Europese Unie. De vraag stelt zich of de regelgeving inzake werkgeverscontrole op internetgebruik, thans een wijdverspreid fenomeen, in het *social media*tijdperk, waarvan zeker ook sprake is in de VS, anders is geëvolueerd dan op het Europese continent. Ook wordt onderzocht of de aanpak in de VS een oplossing kan bieden voor de problemen die zich stellen in België en de Europese Unie en of er bepaalde ideeën zijn die een meerwaarde kunnen bieden in de Europese discussie.

Eerst wordt een situering geboden van de Amerikaanse arbeidsrelatie en haar voornaamste kenmerken. Hierna volgt een overzicht van de voornaamste wet- en regelgeving inzake werkgeverscontrole in de VS. Ten slotte wordt een blik geworpen op enkele relevante en opvallende uitspraken van de rechterlijke macht en hoe in de praktijk wordt omgegaan met de geldende bepalingen.

[348] P.M. SCHWARTZ en J.R. REIDENBERG, *Data Privacy Law*, Charlottesville, Michie, 1996, 1-2.
[349] C.J. MUHL, "Workplace e-mail and Internet use: employees and employers beware", *Monthly Labor Review* 2003, afl. 2, (36) 40-43.

2 De arbeidsverhouding

Net zoals Europeanen werken Amerikanen. Zij gaan arbeidsrelaties aan met een andere persoon, zij het als werkgever, dan wel als werknemer. Naast hetgeen zij onderling overeenkomen, zijn zij voor het aangaan, het uitvoeren en het beëindigen van deze arbeidsrelatie onderworpen aan vier rechtsbronnen: het grondwettelijk recht, de *statutes* of wetten en de administratieve bepalingen, van de Verenigde Staten alsook de staten zelf, en *common law*. Wetgeving van de Verenigde Staten is federaal en bindend voor alle 50 deelstaten. De wetgeving die de deelstaten zelf uitvaardigen, is enkel geldig op het grondgebied van de betreffende staat.[350]

Common law is het geheel van rechterlijke uitspraken die als belangrijkste rechtsbron een bindende kracht hebben binnen het rechtsgebied waarin de uitspraak kadert.[351] Hiermee onderscheiden rechtsstelsels zoals het Amerikaanse en het Britse zich van *civil law*-systemen, zoals België en nagenoeg het hele Europese continent. *Civil law* steunt in de eerste plaats op codificatie van het recht in tegenstelling tot vertrouwen op gewoonterecht.[352] Dit heeft tot gevolg dat rechtspraak in de Verenigde Staten zeer belangrijk is en dat de rechterlijke macht, in nog grotere mate dan in België, recht *spreekt*.

2.1 *Employment-at-will*

In principe omvat de arbeidsovereenkomst de kern van de arbeidsrelatie. Toch ligt de situatie in de Verenigde Staten fundamenteel anders dan in de Europese Unie. De meerderheid van de Amerikaanse arbeidsrelaties is gestoeld op de *employment-at-will* doctrine.[353]

Employment-at-will is een product van het begin van de 20ste eeuw, toen het arbeidsrecht nog volledig afhankelijk was van hetgeen in *common law* bepaald werd.[354] In grote fabrieken waren gedurende een beperkte periode veel werknemers nodig om productie bij te houden. Werkgevers wilden echter niet opgezadeld raken met contracten van lange duur of peperdure ontslagvergoedingen, waarop de *employment-at-will* doctrine het levenslicht zag.[355] Hierdoor waren werkgevers, maar ook werknemers, vrij om op elk moment de arbeidsrelatie stop te zetten.

Deze doctrine houdt in dat een arbeidsovereenkomst gebaseerd is op de loutere wil van de partijen om samen te werken.[356] Wanneer die wil verdwijnt, kan hetzelfde gebeuren met de arbeidsrelatie:

---

[350] J.D. BIBLE en D.A. MCWHIRTER, *Privacy in the workplace: A guide for human resource managers*, New York, Quorum Books, 1990, 3.
[351] E. DIRIX, B. TILLEMAN en P. VAN ORSHOVEN (eds.), *De Valks Juridisch Woordenboek*, Antwerpen, Intersentia, 2010, 85.
[352] M.L. MURILLO, "The evolution of codification in the civil law legal systems: towards decodification and recodification", *Journal of Transnational Law & Policy* 2001, afl. 1 (1) 3.
[353] Werknemers aangesloten bij een vakbond vormen de grootste groep van werknemers die niet behoren tot de *at-will*-groep. Anno 2010 wees onderzoek uit dat slechts 11,9% van werknemers bij een vakbond was aangesloten. R. SPRAGUE, "Invasion of the social networks: blurring the line between personal life and the employment relationship", *University of Louisville Law Review* 2014, afl. 1, (1) 19.
[354] J.D. BIBLE en D.A. MCWHIRTER, *Privacy in the workplace: A guide for human resource managers*, New York, Quorum Books, 1990, 17.
[355] J.D. BIBLE en D.A. MCWHIRTER, *Privacy in the workplace: A guide for human resource managers*, New York, Quorum Books, 1990, 18.
[356] C. CRANE, "Social networking v. the employment-at-will doctrine: a potential defense for employees fired for Facebooking, terminated for Twittering, booted for blogging, and sacked for social networking", *Washington University Law Review* 2012, afl. 3, (639) 640-641 (hierna verkort C. CRANE, "Social networking v. the employment-at-will doctrine").

zonder enige formaliteit kan het samenwerkingsverband meteen beëindigd worden.[357] Zo kunnen werknemers zonder motivering ontslagen worden en kan de werknemer zelf beslissen niet meer te gaan werken wanneer het aan engagement ontbreekt.

Het spreekt voor zich dat een dergelijke situatie, hoe vrij en gelijk voor de partijen deze ook lijkt, voor onevenwichtige gevolgen zorgt ten nadele van de werknemer.[358] Deze is in de overgrote meerderheid van de gevallen immers de persoon die het meeste belang heeft bij het behoud van de arbeidsrelatie. De werkgever houdt in deze doctrine *de facto* de absolute macht.[359]

2.2 Recht op privacy

2.2.1 Grondrecht…

De Amerikaanse Grondwet is, wanneer vergeleken met de 198 artikelen van de Belgische Grondwet, uiterst summier.[360] Bij de inwerkingtreding in 1789 bestond de moeder der Amerikaanse wetten slechts uit zeven artikelen. Doorheen de jaren werd het document aangepast en vandaag staat de teller op zevenentwintig wijzigingen of *amendments*.[361]

Door middel van het vierde amendement is er een zeker recht op privacy ingevoerd, waarvan de tekst luidt als volgt:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[362]

Om te beoordelen of er een inbreuk is op het vierde amendement, wordt overwogen of er sprake was van een *reasonable expectation of privacy*, een redelijke privacyverwachting.[363] Cruciaal beoordelingscriterium hierbij is, net zoals in België, de openbaarheid en locatie van hetgeen ter discussie staat.[364] Communiceert men bewust in het openbaar, op een vrije toegankelijke plaats, dan geldt als vuistregel dat er geen sprake kan zijn van redelijke privacyverwachtingen.[365]

Amendement 4 van de Amerikaanse Grondwet beschermt enkel tegen *state action*, overheidsoptreden.[366] Enkel werknemers van overheidsondernemingen kunnen hier dus een beroep op doen, werknemers van private ondernemingen niet.[367]

---

[357] C. CRANE, "Social networking v. the employment-at-will doctrine", *supra* noot 356, (639) 640-641.
[358] J.D. BIBLE en D.A. MCWHIRTER, *Privacy in the workplace: A guide for human resource managers*, New York, Quorum Books, 1990, 18-19 en R. SPRAGUE, "Invasion of the social networks: blurring the line between personal life and the employment relationship", *University of Louisville Law Review* 2014, afl. 1, (1) 19-20.
[359] C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 290-291.
[360] Belgische Grondwet 17 februari 1994, *BS* 17 februari 1994.
[361] U.S. Const.
[362] U.S. Const. amend. IV. Dit amendement houdt geen letterlijk recht op privacy in, dit werd door de Supreme Court als zodanig geïnterpreteerd in *Katz v. United States*, 389 US 347, 351 (1967).
[363] B. DE WINTER, *Privacy in het internettijdperk*, Den Haag, Sdu uitgevers, 2011, 27.
[364] Zie *supra* deel 1, 2.2.3.
[365] B. DE WINTER, *Privacy in het internettijdperk*, Den Haag, Sdu uitgevers, 2011, 28.
[366] L. DETERMANN en R. SPRAGUE, "Intrusive monitoring", *supra* noot 378, 986-987. Dit in tegenstelling tot de Grondwet van California, die uitdrukkelijk het recht op privacy toekent aan alle personen. Cal. Const. art. I, §1.

2.2.2 … in evolutie

In de jaren '80 van de 20ste eeuw kwamen de eerste conflicten omtrent privacy echt op de voorgrond. Zo werden sollicitanten onderworpen aan polygraaftesten, urinecontroles en psychiatrische evaluaties. Dit alles in de naam van veiligheid, hetgeen door de Supreme Court, het hoogste federale rechtscollege van de Verenigde Staten, goedgekeurd werd.[368] Dit, gecombineerd met de *employment-at-will* doctrine, leidde ertoe dat werknemers geen enkel verweer hadden tegen de beslissingen van hun werkgever. Sindsdien is de aandacht voor een degelijke behandeling van werknemers en aandacht voor hun privacy over het algemeen toegenomen. De theorie van *wrongful discharge* of onrechtmatig ontslag kreeg een bredere omvang, waarmee rechters tegemoet kwamen aan de benadeelde werknemers.[369]

Een andere opmerkelijke evolutie is dat er een kentering is op te merken in de opinie rond redelijke privacyverwachtingen. Lange tijd heeft men volgehouden dat openbare communicatie geen redelijke privacyverwachtingen met zich kan dragen. De laatste jaren zijn er steeds meer stemmen gekomen die oordelen dat een dergelijke strikte visie niet meer houdbaar is. Ook vanuit de Supreme Court.[370] Sociale media en digitale communicatie zijn zo ingebed in het hedendaagse leven, er zou enigszins ruimte moet zijn voor het koesteren van redelijke privacyverwachtingen.

Ondanks deze evolutie is er een duidelijk mentaliteitsverschil op te merken tussen Europa en de Verenigde Staten wat het recht op privacy betreft. Terwijl de Europese gedachtegang het recht op privacy als een primair belang aanschouwt en ethische overwegingen in acht neemt, wordt in de VS veel meer aandacht besteed aan productiviteit op de werkvloer en de belangen van de werkgever.[371] De rechten van de werknemer worden dus niet automatisch aanzien als belangrijker dan de belangen van de werkgever, het feit dat de werknemer zich vrijwillig heeft onderworpen aan het gezag van de werkgever weegt in de Verenigde Staten veel sterker door.

Hoewel het recht op privacy in de Verenigde Staten dus een fragiel recht is dat veel minder kracht inhoudt dan zijn Europese tegenhanger, is er toch een evolutie naar een toegenomen bescherming voor de werknemer.

---

[367] In het verleden bleek een louter verband met de overheid soms reeds voldoende om een private onderneming toch te onderwerpen aan de regels gesteld door het vierde amendement, bijvoorbeeld wanneer een private werkgever taken uitvoerde die in principe voor de overheid waren voorbehouden. Toch kan over het algemeen gesteld worden dat private werkgevers zelden onderworpen zullen worden aan de privacyregeling zoals geponeerd in de Grondwet van de Verenigde Staten. J.D. BIBLE en D.A. MCWHIRTER, *Privacy in the workplace: A guide for human resource managers*, New York, Quorum Books, 1990, 12-13.

[368] J.D. BIBLE en D.A. MCWHIRTER, *Privacy in the workplace: A guide for human resource managers*, New York, Quorum Books, 1990, 11 en 24-25.

[369] J.D. BIBLE en D.A. MCWHIRTER, *Privacy in the workplace: A guide for human resource managers*, New York, Quorum Books, 1990, 28.

[370] D. MILLER, "Legislating our reasonable expectations: making the case for a statutory framework to protect workplace privacy in the age of social media", *University of Miami Business Law Review* 2013, afl. 1, (49) 75-76 en *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). Dit in tegenstelling tot hetgeen prof. em. Blanpain stelt, namelijk dat wat men op het internet zet, als publiek moet worden beschouwd. Zie *supra* inleiding.

[371] M.W. ALLEN, S.J. COOPMAN, J.L. HART en K.L. WALKER, "Workplace surveillance and managing privacy boundaries", *Management Communication Quarterly* 2007, afl. 21, (172) 175 (hierna verkort M.W. ALLEN, S.J. COOPMAN, J.L. HART en K.L. WALKER, "Worplace surveillance").

3 Regulering van werkgeverscontrole

3.1 Situering

Surveillance op private en professionele communicatie is geen vreemd gegeven in de VS. Met name sinds de aanslagen op het World Trade Center en het Pentagon op 11 september 2001 is er een toegenomen waakzaamheid te bespeuren bij de Amerikanen.[372] Niet alleen een verhoogde toegangscontrole op vliegvelden valt op, ook wanneer het gaat over online toezicht als weerwerk tegen diefstal en sabotage binnen een onderneming is het Amerikaans beleid niet onbesproken.[373]

Het algemene uitgangspunt in de Verenigde Staten is dat het slechts normaal is dat de werkgever controle uitoefent op hetgeen zijn werknemers doen tijdens de werkuren.[374] Gevolg hiervan is dat er een gebrek is aan relevante afdwingbare regels inzake werkgeverscontrole en bescherming voor de rechten van werknemers, zowel op het federaal niveau als op dat van de staten.[375]

3.1.1 Motieven van de werkgever

Een breed scala aan redenen ligt aan de basis van de wil van de werkgever om controle uit te oefenen op het internetgebruik van zijn werknemer. Sewell en Barker onderscheiden *coercive control* en *caring*, oftewel dwingende controle dan wel controle uit zorgzaamheid.[376] In het eerste geval surveilleert men uit voorzorg, om te voorkomen dat er sabotage of fraude plaatsvindt. In de tweede situatie gebeurt de controle om er zorg voor te dragen dat werknemers niet overbelast worden, of om slechte individuen te lokaliseren ten voordele van de hele groep.[377] Dit is evenwel een kunstmatig onderscheid en vele vormen van controle zullen tussen beide uitersten vallen.

Andere auteurs ontwarren dan weer drie mogelijke redenen. Werkgevers zullen controleren ter bescherming van informatie en intellectuele eigendom of ter verhoging van de productiviteit. Ook kan men aansprakelijkheid willen voorkomen voor illegale en strafbare activiteiten op het netwerk, zoals bijvoorbeeld pedofilie.[378]

Eerder werd *virtueel absenteïsme* als een gevaar voor productiviteit aangemerkt.[379] Determann en Sprague spreken dan weer van *junk computing* of *cyberloafing*.[380]

---

[372] M.W. ALLEN, S.J. COOPMAN, J.L. HART en K.L. WALKER, "Worplace surveillance", *supra* noot 371, (172) 173.
[373] X, "Airport Security", Flightglobal, http://www.flightglobal.com/features/9-11/airport-security/ en M.W. ALLEN, S.J. COOPMAN, J.L. HART en K.L. WALKER, "Worplace surveillance", *supra* noot 371, (172) 173.
[374] J.D. BIBLE en D.A. MCWHIRTER, *Privacy in the workplace: A guide for human resource managers*, New York, Quorum Books, 1990, 173.
[375] M.W. ALLEN, S.J. COOPMAN, J.L. HART en K.L. WALKER, "Worplace surveillance", *supra* noot 371, (172) 192.
[376] M.W. ALLEN, S.J. COOPMAN, J.L. HART en K.L. WALKER, "Worplace surveillance", *supra* noot 371, (172) 188.
[377] G. SEWELL en J.R. BARKER, "Coercion versus care: using irony to make sense of organizational surveillance", *Academy of Management Review* 2006, afl. 4, 1-24.
[378] L. DETERMANN en R. SPRAGUE, "Intrusive monitoring: employee privacy expectations are reasonable in Europe, destroyed in the United States", *Berkeley Technology Law Journal* 2014, afl. 2, (979) 982 (hierna verkort L. DETERMANN en R. SPRAGUE, "Intrusive monitoring").
[379] Zie *supra* noot 98.
[380] *Junk computing* is het gebruiken van een informaticasysteem voor doeleinden die niet rechtstreeks de doelen van de organisatie behartigen. Hieronder vallen ook andere bedreigingen voor de productiviteit zoals het langdurig en contraproductief perfectioneren van een document of het overdreven gebruik van massamail binnen een onderneming, terwijl slechts enkele personen belang hebben bij de mail. L. DETERMANN en R. SPRAGUE, "Intrusive monitoring", *supra* noot 378, (979) 983 en R. GUTHRIE en P. GRAY, "Junk Computing: Is it Bad for an Organization?", *Information Systems Management* 1996, afl. 1, (23) 23.
Cyberloafing wordt omschreven als elke vrijwillig gestelde handeling van werknemers om tijdens de werkuren het netwerk van de werkgever te gebruiken om naar websites te surfen, die niet relevant zijn voor het werk, of

De reden dat er een verlies aan efficiëntie zou zijn in het werk van de werknemer wordt veel minder aangehaald in Amerikaanse rechtsleer dan in Europese. De motivatie van werkgevers om controle uit te oefenen lijkt veeleer te draaien rond een principiepszaak, waarbij gevolg geven aan werkgeversgezag het belangrijkste is. Dit alles sluit aan bij de focus die in de Verenigde Staten wordt gelegd op de bescherming van de werkgever.[381]

Er zijn nog vele andere redenen denkbaar, waarvan nog enkele zullen blijken uit de volgende analyse van Amerikaanse wetgeving. Een voornaam gevolg, afhankelijk van de soort beweegredenen die de werkgever tot controle aanzet, is de perceptie en de verdraagzaamheid van werknemers. Hun reactie bepaalt veel over de opportuniteit en rechtvaardigheid van controle.[382]

3.1.2 Positie van de werknemer

Technologie dringt meer en meer door in het dagdagelijkse leven, ook op de werkvloer, en werknemers spenderen steeds meer tijd op hun werkplaats. Ongeremde controle zou een enorme impact hebben op de moraal van werknemers.[383]

Toch bieden werknemers over het algemeen weinig weerwerk tegen de praktijken waaraan de werkgever hen onderwerpt, ook wat betreft elektronisch toezicht. De werkgever bevindt zich ten slotte in een bovengeschikte positie: protesteren werknemers, dan riskeren zij hun job te verliezen.[384]

Eerder in deze scriptie werden de relevante rechten en belangen van werkgevers en werknemers opgesomd.[385] Hieruit bleek een spanningsveld, waarvoor een goed beleid rond internetcontrole is aangewezen. Een eerste stap hierin kan in aangepaste wetgeving te vinden zijn.

3.2 Federaal recht

3.2.1 *De lege lata*

Het federaal wetgevingsarsenaal in de Verenigde Staten van Amerika inzake werkgeverscontrole op internetgebruik is nagenoeg onbestaande. Zo is het eerder besproken *fourth amendment* van de Amerikaanse Grondwet enkel van toepassing op publieke ondernemingen, waarbij sprake is van bescherming tegen overheidsoptreden. De Grondwet biedt geen recht op privacy voor werknemers

om persoonlijke e-mails te bekijken. Deze term is dan weer specifieker dan *virtueel absenteïsme*. Terwijl deze laatste term duidt op het aanwezig zijn van werknemers maar een gebrek aan professionele inzet, duidt *cyberloafing* rechtstreeks op het misbruiken van het netwerk van de werkgever voor privaat internetgebruik. L. DETERMANN en R. SPRAGUE, "Intrusive monitoring", *supra* noot 378, (979) 983 en V.K.G. LIM en T.S.H. TEO, "Cyberloafing and Organizational Justice: The Moderating Role of Neutralization Technique" in M. ANANDARAJAN, T.S.H. TEO en C.A. SIMMERS (eds.), *The Internet and Workplace Transformation*, New York, M.E. Sharpe, 2006, (241) 243.

[381] C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 287-288.

[382] M.W. ALLEN, S.J. COOPMAN, J.L. HART en K.L. WALKER, "Worplace surveillance", *supra* noot 371, (172) 189.

[383] C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 291.

[384] De *employment-at-will* doctrine leidt ertoe dat er niet eens veel hoeft te gebeuren opdat een werkgever zijn werknemer kan ontslaan. Zie *supra* deel 3, 2.1.

[385] Zie *supra* deel 1, 3.

in een private onderneming.[386] Hetzelfde kan gezegd worden voor de bepalingen van de Privacy Act van 1974.[387]

Een andere, in de rechtsleer vaak als relevant aangehaalde, rechtsnorm is de Computer Fraud and Abuse Act van 2006. Deze wet verbiedt het bewust toegang nemen tot een computer zonder toestemming, of door buiten de perken te treden van hetgeen waarvoor toestemming is gegeven.[388] Meteen is duidelijk dat deze bepalingen enkel van toepassing kunnen zijn wanneer een werknemer op onrechtmatige wijze toegang verkrijgt tot het netwerk van de werkgever en fraude pleegt of misbruik maakt van het systeem.[389] Dit heeft weinig te maken met controle van de werkgever op het gedrag van de werknemer.

Er kunnen evenwel twee *acts* onderscheiden worden waarop in de praktijk het meest beroep wordt gedaan in een discussie rond toezicht op internetgebruik door de werkgever. Meer bepaald de Electronic Communications Privacy Act en de National Labor Relations Act verdienen meer aandacht.

3.2.1.1 Electronic Communications Privacy Act

De Electronic Communications Privacy Act (ECPA) zag het levenslicht in 1986 ter amendering van de Omnibus Crime Control and Safe Streets Act van 1968, waarin enkel bescherming bestond voor privacy tijdens telefoongesprekken.[390] Titel III van deze Omnibus Act wilde praktijken inzake telefoontap bestraffen nadat het Congres opmerkte dat dergelijke handelingen onbestraft bleven. Hiervoor wilde men een uniforme basis creëren voor de beoordeling van omstandigheden en voorwaarden waaronder een tap al dan niet toegelaten kon worden.[391]

Men kwam anno 1986 reeds tot de vaststelling dat de technologische ontwikkelingen de Omnibus Act voorbijgestreefd waren. Zo werd *wire communication* gedefinieerd als "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications."[392]

De bedoeling van de ECPA diende om het toepassingsgebied van de Omnibus Act te verbreden tot elektronische communicatie, wat indertijd zoveel wilde zeggen als e-mail.[393] Elektronische communicatie wordt door de ECPA gedefinieerd als:

---

[386] Zie *supra* deel 3, 2.2.1.
[387] C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 290.
[388] B.N. WHITFIELD, "Social media @ work: #policyneeded", *Arkansas Law Review* 2013, afl. 3, (843) 860.
[389] C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 294.
[390] D.N. ANDRISANI, "Employer-employee rights on the internet: is there an effective balance?", *Journal of Internet Law* 2000, 3, (24) 24.
[391] Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C §2510-2520.
[392] Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C § 2510(1).
[393] D.N. ANDRISANI, "Employer-employee rights on the internet: is there an effective balance?", *Journal of Internet Law* 2000, 3, (24) 24.

> "Any transfer of signs, signals, writing, images, sound, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce." [394]

Titel I van de ECPA, ook wel de Wiretap Act genoemd, is van toepassing op het onderscheppen van schriftelijke, mondelinge en elektronische communicatie *in overdracht*. Deze *in transfer*-voorwaarde is overgenomen van de Omnibus Act, die als doel had hen te bestraffen die telefoongesprekken afluisterden. [395] Om van toepassing te zijn zou de werkgever dus kennis moeten krijgen van de informatie op hetzelfde moment als de verzending ervan. [396] Dit is vergelijkbaar met de vereisten van art. 314bis Sw. en zal eveneens weinig toepassing vinden bij werkgeverscontrole van internetgebruik, aangezien controle in de praktijk nagenoeg enkel toegepast wordt op opgeslagen informatie.

Titel II van de ECPA, de Stored Communications Act (SCA), gaat over de toegang tot deze *opgeslagen* elektronische communicatie.[397]

De ECPA is vandaag de dag moeilijk toe te passen. Er bestaat aanzienlijke discussie over het toepassingsgebied van de wet, die intussen bijna 30 jaar oud is en dus niet meer is aangepast aan de moderne technologische ontwikkelingen.[398]

Ten slotte zijn er nog drie uitzonderingen die controle toelaten en het dus nog moeilijker maken om de ECPA toe te passen. Vooreerst is er de *consent exception*, waarbij controle is toegelaten wanneer slechts één van de communicerende partijen haar toestemming hiertoe heeft gegeven.[399] De *course of business exception* laat controle toe wanneer deze betrekking heeft op normale, dagdagelijkse activiteiten.[400] Ten slotte kan door de *provider exception* degene die het systeem voorziet waarmee gecommuniceerd wordt, steeds de berichten daarop raken.[401] Een werkgever zal bijvoorbeeld steeds toegang kunnen verkrijgen tot gegevens die zich bevinden op een elektronische communicatiedienst zoals een e-mailbox die hij voor zijn werknemers voorziet.

De ouderdom van de wet en de klassieke voorkeursbehandeling voor de werkgever maken het moeilijk om de ECPA vandaag de dag toe te passen op conflicten tussen werkgever en werknemer. Later zal blijken dat in de rechtspraak wel een inspanning wordt geleverd om deze bepalingen een

---

[394] De ECPA sluit echter enkele communicatievormen expliciet uit van haar toepassingsgebied. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510(12).
[395] C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 293.
[396] C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 292. Deze nauwe interpretatie leidt ertoe dat de bepaling maar enkele seconden van toepassing kan zijn op elektronische communicatie. Werkgevers zullen zichzelf sneller toegang verlenen tot opgeslagen communicatie, in plaats van communicatie in transmissie.
[397] L. DETERMANN en R. SPRAGUE, "Intrusive monitoring", *supra* noot 378, (979) 996-997.
[398] L. DETERMANN en R. SPRAGUE, "Intrusive monitoring", *supra* noot 378, (979) 998-999.
[399] Electronic Communications Privacy Act of 1986, 18 U.S.C. 2511(2)(d). In de Belgische rechtsleer wordt net sterk bepleit dat een werknemer zijn toestemming niet kan geven aan een werkgever, vanwege de bovengeschikte positie van die laatste.
[400] Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511(1)(a)(i).
[401] Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701(c)(1).

interpretatie te geven met een eerlijke behandeling voor beide partijen, de ene keer al met meer succes dan de andere.[402]

3.2.1.2 National Labor Relations Act

De *National Labor Relations Act* (NLRA) is een document dat het recht voor werknemers voorziet om gecoördineerde activiteiten aan te gaan met als doel het collectief onderhandelen of andere gemeenschappelijke hulp of bescherming.[403] Hieronder worden onder andere het vormen van een vakbond of het organiseren van stakingen verstaan.[404]

De bescherming uit dit artikel kan echter ook een impact hebben op de aanwezigheid van sociale media op de werkvloer, bijvoorbeeld wanneer vakbondslieden via een Facebookgroep contact met elkaar houden en over het werk discussiëren.[405] De werkgever kan de werknemer niet *a priori* de mond snoeren via een policy. [406]

In de zaak *Sears Holding* wilde een vakbondsorganisatie via sociale media, waaronder sociaalnetwerksite Facebook, communiceren. Sears, een grootwarenhuis, stelde in juni 2009 een beleid vast waarin het werd verboden om via sociale media minachtend te communiceren over de werkgever.[407] De adviserende afdeling van de National Labor Relations Board bepaalde dat er geen schending was van sectie 157 NLRA, omdat er geen bewijs werd geleverd dat de voormelde vakbondsactie op Facebook geviseerd werd door de policy en dat de rechten van de werknemers, zoals bepaald in de NLRA, door deze policy niet beknopt werden. Er volgden immers geen sancties voor de vakbondslieden, het enige doel van de policy was om het bedrijf beter te beschermen.[408]

Desalniettemin moet de werkgever voorzichtig handelen met de NLRA in gedachten: sectie 158 bepaalt immers dat ondernomen beleidsacties voldoende precies moeten zijn. Indien het toepassingsgebied aangemerkt wordt als "te breed", dan wordt dit veel sneller beoordeeld als zijnde een inbreuk op sectie 157. [409] Dit bleek in de zaak *Karl Knauz Motors*, waarbij werknemers van een garage verplicht werden "beleefd en vriendelijk" te zijn tegen klanten en collega's en het imago van de garage niet mochten schenden. Dit zou de werknemers zo doen vrezen voor wat zij wel of niet mochten, waardoor hun rechten onder de NLRA werden gekrenkt.[410]

---

[402] Zie *infra* deel 3, 4.
[403] B.N. WHITFIELD, "Social media @ work: #policyneeded", *Arkansas Law Review* 2013, afl. 3, (843) 848. In het Engels luidt de definitie van *concerted activity* als volgt: "when two or more employees take action for their mutual aid or protection regarding terms and conditions of employment for 'mutual benefit' in the labor relations context". National Labor Relations Act of 1935, 29 U.S.C. § 151-169.
[404] R. SPRAGUE, "Invasion of the social networks: blurring the line between personal life and the employment relationship", *University of Louisville Law Review* 2014, afl. 1, (1) 20-22.
[405] M.B. MILLER, "Avatars and social media: employment law risks and challenges in the virtual world", *FDCC Quarterly* 2013, afl. 4, (279) 289. De acties van werknemers die beschermd worden onder de NLRA worden steeds ruimer geïnterpreteerd. B.N. WHITFIELD, "Social media @ work: #policyneeded", *Arkansas Law Review* 2013, afl. 3, (843) 851.
[406] J. LORRÉ, *Sociale media en werkgeverscontrole*, Mechelen, Kluwer, 2012, 79-82.
[407] *Sears Holdings (Roebucks),* 18-CA-19081 (December 4, 2009), WL 5593880.
[408] *Sears Holdings (Roebucks),* 18-CA-19081 (December 4, 2009), WL 5593880.
[409] B.N. WHITFIELD, "Social media @ work: #policyneeded", *Arkansas Law Review* 2013, afl. 3, (843) 852.
[410] *Karl Knauz Motors, Inc.*, 13-CA-046452 (September 28, 2012), WL 4482841.

Hieruit volgt, samen met de uitspraak in de zaak *Costco Wholesale Corp.*, dat de National Labor Relations Board met name de context en het toepassingsgebied van een policy allesbepalend acht voor de geoorloofdheid van een werkgeversbeleid. [411]

3.2.2 *De lege ferenda*

Anno 2012 werd een voorstel naar het federale Congres gestuurd voor een Social Networking Online Protection Act, oftewel SNOPA.[412] Het voorstel werd, nadat geen akkoord kon worden bereikt, terug ingeleid voor het 113de Congres in 2013. Sinds april 2013 is er echter niets meer gebeurd met dit voorstel.[413]

De bedoeling van het document zou zijn om werkgevers te verbieden gegevens van werknemers te eisen waardoor zij een persoonlijk account van deze werknemers op een sociaalnetwerksite zouden kunnen openen. Ook zou het de werkgever worden verboden om sancties op te leggen aan de werknemer die zou weigeren deze gegevens vrij te geven.[414]

3.3 *Common law*

Terwijl in België en de Europese Unie het arbeids- en contractenrecht de voornaamste bron is voor werknemers om rechten uit te putten, dient in de Verenigde Staten ook rekening te worden gehouden met vorderingen uit onrechtmatige daad, oftewel *tort*. In de praktijk wordt aanvaard dat er sprake kan zijn van een onrechtmatige daad bij, bijvoorbeeld, een onrechtmatig ontslag.[415]

Er bestaan vier soorten van *tort* die van belang kunnen zijn inzake privacy:

- *Intrusion upon seclusion;*
- *Public disclosure of embarrassing private facts;*
- *Publicity which places a person in a false light in the public eye,* of*;*
- *Commercial appropriation of a person's name or likeness.*[416]

De eerste vorm, *intrusion upon seclusion*, vormt de voornaamste bron van eventuele vordering voor iemand wiens recht op privacy op de werkvloer is geschonden. Dit wordt gedefinieerd als volgt:

---

[411] B.N. WHITFIELD, "Social media @ work: #policyneeded", *Arkansas Law Review* 2013, afl. 3, (843) 853. In *Costco* hanteerde de werkgever eveneens erg ruime verbodsbepalingen ter vrijwaring van enige schade aan het imago van het bedrijf of een individu aangaande uitspraken van werknemers over hoe zij behandeld werden. *Costco Wholesale Corp.,* 34-CA-012421 (September 7, 2012) WL 3903806 en *Karl Knauz Motors, Inc.*, 13-CA-046452 (September 28, 2012), WL 4482841.

[412] D. MILLER, "Legislating our reasonable expectations: making the case for a statutory framework to protect workplace privacy in the age of social media", *University of Miami Business Law Review* 2013, afl. 1, (49) 52.

[413] https://www.congress.gov/bill/113th-congress/house-bill/537/all-actions (consultatie 4 januari 2015). SNOPA zou de regels inhouden zoals deze in IEPA werden vastgelegd voor de staat Utah in 2013, zie *infra* noot 432. Verder is de tekst van SNOPA erg summier en wordt er bijvoorbeeld geen rekening gehouden met toestellen van de werknemers zelf. Ook hier wordt geen sluitend systeem voorzien, wat eveneens tot kritiek leidde. Ook wordt *persoonlijk* niet gedefinieerd in SNOPA, waardoor het toepassingsgebied niet helder is. D. MILLER, "Legislating our reasonable expectations: making the case for a statutory framework to protect workplace privacy in the age of social media", *University of Miami Business Law Review* 2013, afl. 1, (49) 80.

[414] https://www.congress.gov/bill/113th-congress/house-bill/537/text (consultatie 4 januari 2015).

[415] J.D. BIBLE en D.A. MCWHIRTER, *Privacy in the workplace: A guide for human resource managers*, New York, Quorum Books, 1990, 9-10.

[416] L. DETERMANN en R. SPRAGUE, "Intrusive monitoring", *supra* noot 378, (979) 990-991.

> "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[417]

Hieruit kunnen twee voorwaarden ontleend worden. Ten eerste dient men over privacy te beschikken. Met andere woorden zal de werknemer in een positie moeten verkeren waarin hij redelijke privacyverwachtingen mag koesteren om op deze *tort* beroep te doen.[418] De voorwaarde van het vierde amendement van de Amerikaanse Grondwet wordt hier dus hernomen, zij het nu ook voor private ondernemingen.[419]

Inzake zijn verwachtingen is de werknemer dus grotendeels afhankelijk van de werkgever, deze bepaalt immers via een policy zelf wat de te verwachten graad van privacy is. [420] Daarnaast speelt ook de mate waarin de werknemer zelf inspanningen levert om zijn communicatie te beschermen: als hij zijn mailbox met een wachtwoord kan beveiligen, zou hij dat ook moeten doen.[421] Toch zijn de redelijke privacyverwachtingen beperkt tot de verwachtingen "die de maatschappij bereid is te aanvaarden als redelijk."[422]

De tweede voorwaarde is dat de inbreuk "highly offensive to a reasonable person" moet zijn. Deze voorwaarde is sterk verbonden aan de eerste en zal, nog meer dan de redelijke privacyverwachtingen, geval per geval beoordeeld moeten worden. Hierdoor wordt men dus onderworpen aan de beoordeling van de rechter, of hetgeen bepaald wordt in eventuele federale of statelijke *statutes*.[423]

3.4 Wetgeving van de deelstaten

3.4.1 Statenautonomie

Naast de Amerikaanse Grondwet, de federale wetten, de *common law* en hetgeen bepaald wordt tussen partijen onderling, rest er nog de wetgeving die deelstaten afzonderlijk invoeren. Ook in het gebied van privacy in de arbeidsrelatie hebben de staten zich niet onbetuigd gelaten, zij het met zeer uiteenlopende regels met een erg beperkt toepassingsgebied.[424]

Connecticut en Delaware hebben elk een regeling rond kennisgeving aan werknemers van controle door de werknemer.[425] Anno 2011 was zulke voorafgaande kennisgeving slechts in drie staten verplicht.[426]

---

[417] Restatement (second) of torts §625B (1997).
[418] B.N. WHITFIELD, "Social media @ work: #policyneeded", *Arkansas Law Review* 2013, afl. 3, (843) 862.
[419] Zie *supra* deel 3, 2.2.1.
[420] D. MILLER, "Legislating our reasonable expectations: making the case for a statutory framework to protect workplace privacy in the age of social media", *University of Miami Business Law Review* 2013, afl. 1, (49) 54.
[421] *Fischer v Mt. Olive Lutheran Church, Inc.*, 207 F. Supp. 2d 914, 928 (W.D. Wis. 2002) en C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 358.
[422] *Katz t. Verenigde Staten*, 389 US 347, 361 (1967) (Harlan, J., concurring).
[423] L. DETERMANN en R. SPRAGUE, "Intrusive monitoring", *supra* noot 378, (979) 992-993.
[424] B.N. WHITFIELD, "Social media @ work: #policyneeded", *Arkansas Law Review* 2013, afl. 3, (843) 863-866.
[425] L. DETERMANN en R. SPRAGUE, "Intrusive monitoring", *supra* noot 378, (979) 994.
[426] De derde staat, naast Connecticut en Delaware, is Colorado. C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 361.

In Connecticut is voorafgaande kennisgeving van controle verplicht, tenzij de werkgever redelijke verdenkingen heeft dat er gedrag wordt gepleegd dat de wet of de rechten van andere werknemers schendt, oftewel dat er een onaangename werkomgeving wordt gecreëerd. Wordt deze wet niet gerespecteerd, dan is er een boete van 500 dollar voorzien, die in stijgende lijn gaat voor recidivisten.[427]

In Delaware mag men geen controle uitoefenen op internet- en e-mailgebruik, tenzij zulk toezicht ten minste eenmaal per dag dat de werknemer zijn professionele mailbox of het internet betreedt ter kennis wordt gegeven. Deze mailbox of het internet dient tevens voorzien te zijn door de werkgever. Deze kennisgeving kan vervangen worden door een eenmalige schriftelijke kennisgeving van de controle die door de werknemer wordt gelezen en goedgekeurd. Gebeurt dit niet, dan is er een boete van 100 dollar per inbreuk voorzien.[428]

Het valt buiten het bestek van deze scriptie om dieper in te gaan op de wetgeving van de Amerikaanse deelstaten, maar met dit voorbeeld kan aangetoond worden dat het voor zowel werkgevers als werknemers moeilijk wordt als elke staat eigen regels vaststelt. Voor de werkgever omdat hij zo geen coherent, eenvormig beleid kan hanteren over staatsgrenzen heen.[429] Voor de werknemer omdat zijn vrij verkeer tussen staten belemmerd wordt, gelijkaardig aan de situatie die men in de Europese Unie heeft willen remediëren.[430] Indien de werkgever vrij spel heeft inzake controle, zal het werken in een staat zonder goede regelgeving minder aantrekkelijk zijn dan het werken in een staat waar de positie van de werknemer wel goed wordt geregeld, in evenwicht met de belangen van de werkgever.[431]

Ter illustratie van de positionering van de privacy van werknemers in de deelstaten volgt ter afsluiting een korte blik op de wetgeving van Utah. Meer bepaald deze inzake het controlerecht van de werkgever op logingegevens van persoonlijke internetpagina's van werknemers.

3.4.2 Uitgelicht: bescherming van private accounts in Utah

Sinds 2013 geldt in Utah de Internet Employment Privacy Act (IEPA).[432] Met deze wet wordt de situatie gereguleerd waarin werkgevers de logingegevens van werknemers vragen om toegang te verkrijgen tot hun persoonlijke internetaccounts. Deze wet is geldig voor alle private en publieke werkgevers op het grondgebied van Utah en de verhouding met hun werknemers, onder welke vorm van contract dan ook aangenomen.[433]

---

[427] C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 295 en Conn. Gen. Stat. § 31-48d(b)(1).
[428] Del. Code Ann. Tit. 19, §705.
[429] D.N. ANDRISANI, "Employer-employee rights on the internet: is there an effective balance?", *Journal of Internet Law* 2000, 3, (24) 29, C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 358 en L. DETERMANN en R. SPRAGUE, "Intrusive monitoring", *supra* noot 378, (979) 993.
[430] Zie *supra* noot 128 en 145.
[431] Zie ook *supra* deel 1, 3.
[432] Utah Code Ann. §34-48-101-301.
[433] Utah Code Ann. §34-48-102(2).

Werkgevers mogen werknemers niet vragen hun gebruikersnaam en wachtwoord te geven, of het wachtwoord dat toegang geeft tot een persoonlijk account. Werkgevers mogen geen sancties opleggen wanneer dit geweigerd wordt.[434] Een persoonlijk internetaccount wordt gedefinieerd als "an online account that is used by an employee or applicant *exclusively* for personal communications unrelated to any business purpose of the employer."

Het is werkgevers wel toegelaten werknemers te disciplineren indien zij weigeren de logingegevens te overhandigen wanneer dit gevraagd wordt, op voorwaarde dat de werkgever gedeeltelijk of geheel betaald heeft om het account voor de werknemer voor professionele doeleinden ter beschikking te stellen. Dit geldt ook wanneer het zou gaan over vertrouwelijke informatie van de werkgever die naar het account werd overgedragen zonder toestemming. Daarnaast kan van de werknemer gevraagd worden dat hij meewerkt aan een onderzoek over activiteit op het account inzake wangedrag op de werkplaats. Hetgeen openbaar wordt gepubliceerd kan ook vrijuit gecontroleerd worden door de werkgever. Is het zichtbaar op Facebook en zijn de privacy-instellingen niet aangepast, dan is er dus geen verweer op grond van redelijke privacyverwachtingen, ondanks de eerder positieve stemmen die opgingen in de Supreme Court.[435]

Bij schending van rechten van werknemers onder deze wet is een boete van 500 dollar voorzien.[436]

Uit het voorgaande blijkt dat, ondanks de goede bedoelingen en ongetwijfeld geïnspireerd door de bepalingen van SNOPA, de werknemer hiermee niet veel geholpen is.[437] Het toepassingsgebied is ten eerste enorm beperkt: het dient te gaan over accounts die *exclusief* voor persoonlijke doeleinden worden gebruikt. Dit is moeilijk te beoordelen voor werknemers, die vaak communicatiewegen zullen hebben die een mix zijn van privé en professioneel, zoals LinkedIn.[438] Werkgevers kunnen dan nog steeds hun werknemers onder druk zetten om hun logingegevens vrij te geven voor eender welk ander account. Daarnaast zijn er nog een aantal uitzonderingen op het verbod voor de werkgever. De bescherming van de werknemer is hier dus allesbehalve sluitend.

3.5 Evaluatie van het wet- en regelgevend kader

Rechtsgeleerden roepen om een eenduidig beleid inzake werkgeverscontrole op het niveau van de federale staat.[439] Net zoals in de EU zou het dan de bedoeling zijn om te zorgen voor rechtszekerheid voor werknemers en werkgevers. Daarnaast wil men de werkgever de mogelijkheid geven één nationaal beleid te hanteren, in plaats van per staat te moeten onderzoeken wat wel of niet mag.

---

[434] C.B. SNOW, "To snoop or not to snoop? Legal considerations under Utah's Internet Employment Privacy Act", *Utab Bar Journal* 2014, afl. 3, (20) 21.
[435] C.B. SNOW, "To snoop or not to snoop? Legal considerations under Utah's Internet Employment Privacy Act", *Utab Bar Journal* 2014, afl. 3, (20) 22. Zie *supra* noot 370.
[436] Utah Code Ann. § 34-48-301.
[437] Zie *supra* deel 3, 3.2.2.
[438] C.B. SNOW, "To snoop or not to snoop? Legal considerations under Utah's Internet Employment Privacy Act", *Utab Bar Journal* 2014, afl. 3, (20) 21-22.
[439] C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 324-325.

Ciocchetti stelt, in het bijzonder wat internetcontrole betreft, een beperking voor van de mogelijkheden waarover de werkgever beschikt om controle uit te oefenen. Hij suggereert een *Privacy Judgment Rule*, die zou inhouden dat:

- werkgevers enkel mogen handelen wanneer zij redelijkerwijze menen dat actie nodig is voor een belang van de onderneming;
- dat de controle op de minst schofferende manier moet gebeuren om snel en accuraat informatie te verzamelen;
- dat enkel gecontroleerd mag worden bij de werknemers waar het nodig bij is. Ciocchetti verduidelijkt dit criterium niet, maar lijkt te impliceren dat rekening kan worden gehouden met het verleden van werknemers of bepaalde vermoedens. Controle dient ook beperkt te blijven tot wanneer de werkgever zijn aansprakelijkheid wil beperken ten gevolge van acties van werknemers, of wanneer er voor een ander feit onderzoek vereist is.[440]

Dit voorstel lijkt erg veel weg te hebben van hetgeen wordt gesteld in de privacyrichtlijn, zo komt het laatste voorstel van Ciocchetti neer op het respecteren van het proportionaliteitsbeginsel.[441]

Opvallend is dat er geen uitgesproken regel is over controle op private communicatie. Voorafgaande kennisgeving van controle is niet verplicht.[442] Zo is het in België verboden om de persoonlijke mailbox van werknemers te controleren, terwijl in de Amerikaanse rechtsleer wordt *gesuggereerd* om controle hiervan te beperken tot de mate van gebruik en niet te kijken naar de inhoud. Dat dit slechts een suggestie is en geen vaste regel zegt veel over de manier waarop men in de VS omgaat met werkgeverscontrole.[443]

Crane lijkt een oplossing te zien in de bepalingen van de SCA, die door bepaalde rechtspraak worden toegepast op moderne technologieën.[444] Hoewel dit inderdaad een zekere oplossing lijkt te bieden en evolueert naar de visie zoals deze in de EU geldt, stelt zich maar de vraag of rechtspraak de problemen alleen zal kunnen ondervangen.

Het gaat hier om losse ideeën van bepaalde rechtsgeleerden. De Amerikanen gaan veelal zelfregulerend te werk. Regels en wetten dienen slechts ter ondersteuning van de praktijk. Net zoals in de EU wordt werkgevers vanuit de rechtsleer aangeraden een geschreven beleid op te zetten.[445] Er is dan ook een gebrek aan een coherent geheel van rechtsregels rond het onderwerp.[446] Er wordt veel vertrouwen gelegd in de handen van de rechterlijke macht, die curatief dient op te treden.[447] Mogelijk loont het om ter afsluiting een blik te werpen op enkele arresten.

---

[440] C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 333.
[441] Zie *supra* deel 2, 2.1.1.1.
[442] C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 325.
[443] D.N. ANDRISANI, "Employer-employee rights on the internet: is there an effective balance?", *Journal of Internet Law* 2000, 3, (24) 29.
[444] C. CRANE, "Social networking v. the employment-at-will doctrine", *supra* noot 356, (640) 672.
[445] R. RAYSMAN, "A practical look at social media policies", *Computer & Internet Lawyer* 2012, afl. 3, (10) 10-13.
[446] C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 290.
[447] B. DE WINTER, *Privacy in het internettijdperk*, Den Haag, Sdu uitgevers, 2011, 28.

4 Rechtspraak

Traditioneel wordt aangenomen dat werknemers niet te veel privacy moeten verwachten, ook niet voor de rechter. In rechtspraak trekt de werkgever overwegend vaker aan het langste zeel.[448] De rechtspraak hecht immers nog steeds veel aandacht aan de belangen van de werkgever en dat hij, om zichzelf te beschermen, de communicatie van zijn werknemers moet kunnen controleren. Dit moet zeker kunnen wanneer hij het netwerk ter beschikking heeft gesteld via welk de werknemer communiceert.[449]

Het gerecht gaat ervan uit dat de werkplaats bestaat voor werkdoeleinden, dat werknemers loon en toegang tot bepaalde technologie krijgen in ruil voor arbeid en dat aansprakelijkheidsproblemen meer doorwegen dan de privacy van werknemers.[450]

Vooraleer over te gaan tot een conclusie, wordt nog een blik geworpen op enkele oudere en recentere arresten die hun stempel hebben gedrukt op enkele knelpunten inzake privacy van werknemers in de Verenigde Staten van Amerika.

4.1 Geen redelijke privacyverwachtingen: *Smyth*

In *Smyth* waren de feiten als volgt: een werkgever voorzag een e-mailsysteem om de interne communicatie tussen zijn werknemers te verbeteren. De werkgever had herhaaldelijk aan de werknemers verzekerd dat hetgeen gecommuniceerd werd via dit systeem vertrouwelijk zou blijven, dat er geen controle zou worden uitgevoerd en dat het niet gebruikt zou worden in hun nadeel.[451]

Desondanks kreeg een *at-will* werknemer in januari 1995 bericht dat hij ontslagen werd omwille van het versturen van "inappropriate and unprofessional comments" naar een overste via voormeld e-mailsysteem.

De werknemer stapte naar de rechter in Pennsylvania om een onrechtmatig ontslag aan te kaarten. Hoewel de rechter aanhaalde dat een *at-will* werknemer in principe zonder meer ontslagen kan worden, werden toch enkele uitzonderingen erkend wanneer er een schending zou zijn van een publiek beleid. Het zou dan moeten gaan over de schending van een regel die aan de basis ligt van een burger zijn sociale rechten, plichten en verantwoordelijkheden.[452]

---

[448] D.N. ANDRISANI, "Employer-employee rights on the internet: is there an effective balance?", *Journal of Internet Law* 2000, 3, (24) 29, R. SPRAGUE, "Invasion of the social networks: blurring the line between personal life and the employment relationship", *University of Louisville Law Review* 2014, afl. 1, (1) 33 en D. MILLER, "Legislating our reasonable expectations: making the case for a statutory framework to protect workplace privacy in the age of social media", *University of Miami Business Law Review* 2013, afl. 1, (49) 50.
[449] D.N. ANDRISANI, "Employer-employee rights on the internet: is there an effective balance?", *Journal of Internet Law* 2000, 3, (24) 25. Zie ook *Smyth v. The Pillsbury Co.*, 914 F. Supp. 97 (E.D.Pa. 1996).
[450] C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 290.
[451] *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D.Pa. 1996).
[452] *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D.Pa. 1996).

De werknemer steunde zijn vordering op *common law*, meer bepaald *intrusion upon seclusion*. Om te beoordelen of er sprake was van een "substantial and highly offensive invasion" van privacy maakte de rechter een afweging tussen de belangen van beide partijen.

De rechtbank oordeelde vooreerst dat de werknemer geen redelijke privacyverwachtingen kon koesteren, aangezien het e-mailsysteem door de werkgever zelf werd voorzien. Dit ondanks hetgeen de werkgever beloofd had, dat er geen controle zou plaatsvinden. Ook werd opgemerkt dat er geen private informatie werd ontdekt, de reden van ontslag waren gewelddadige berichten die de werknemer naar zijn overste had gestuurd. Zo had hij gedreigd enkele werknemers te vermoorden.[453]

Zelfs al zouden er redelijke privacyverwachtingen hebben kunnen zijn, dan nog zou de rechtbank het geen substantiële en aanstootgevende inbreuk van privacy hebben gevonden, aangezien er in feite geen private informatie op het spel stond.[454] De belangen van de onderneming wogen uiteindelijk meer door dan die van de werknemer.[455]

Recente rechtsleer raadt werkgevers aan om voorzichtig te zijn met controle van e-mails, meer dan bij algemeen internet- en sociale mediagebruik. Werknemers ervaren dit als een grotere inbreuk van hun privacy.[456] E-mails worden over het algemeen immers meer als persoonlijk ervaren: terwijl gebruikers van openbare websites of SNS er bewust voor kiezen om informatie openbaar te stellen voor een ruimer publiek, zijn e-mails in principe gericht naar een select publiek. De privacyverwachtingen zijn hier van nature groter.

Uit dit principearrest, dat vandaag nog steeds stand houdt, kan echter worden afgeleid dat de werknemer inderdaad aan het kortste eind trekt wanneer het over redelijke privacyverwachtingen gaat.

4.2 Rondneuzende werkgevers

4.2.1 *Konop*

Ondanks de bewering dat de werknemer vaak de minder bevoordeelde partij is voor de rechter, is het niet steeds kommer en kwel. Robert C. Konop, een piloot voor Hawaiian Airlines, beheerde een website waarop hij kritische berichten plaatste over onder andere zijn werkgever. Konop bepaalde zelf wie wel of niet toegang kreeg tot deze website door bezoekers een account te laten creëren dat door hem aanvaard moest worden. Ook had hij in de algemene voorwaarden, die men moest erkennen vooraleer men toegang kreeg tot de website, opgenomen dat het voor het management van Hawaiian Airlines verboden was om de website te betreden.[457]

[453] *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D.Pa. 1996).
[454] *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D.Pa. 1996).
[455] C.J. MUHL, "Workplace e-mail and Internet use: employees and employers beware", *Monthly Labor Review* 2003, afl. 2, (36) 37-38.
[456] C.A. CIOCCHETTI, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, (285) 343.
[457] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002).

In december 1995 slaagde een kaderlid van Hawaiian Airlines er evenwel in de berichten te lezen. Hij had toestemming verkregen van een werknemer om diens naam te gebruiken voor een account en zo Konop zijn controle te omzeilen. Het kaderlid bleef de website herhaaldelijk bezoeken.

Toen Konop hier lucht van kreeg, stelde hij een vordering in bij het district court op grond van de bepalingen van onder andere de ECPA en *tort law*.[458] Deze rechtbank oordeelde dat er geen schending was van de wet wanneer een niet-toegelaten gebruiker toegang verkrijgt dankzij een toegelaten gebruiker.

Konop ging in beroep, waarbij de beroepsrechter een andere mening was toegedaan. Vooreerst merkte deze op dat de bepalingen van de ECPA dateren van voor de opkomst van het internet. Het federale Congres werd hierbij veroordeeld voor gebrekkige wetgeving.[459]

Toch moest de rechtbank de bepalingen zo goed mogelijk trachten toe te passen, waarbij het tot de conclusie kwam dat er ten eerste geen schending was van de Wiretap Act. De rechtbank respecteerde de strikte definitie die reeds was gegeven aan "interception" van communicatie.[460] Hiermee sloot de rechter zich aan bij de uitspraak van het district court.

Dat de SCA niet geschonden werd, daar werd dan weer niet in gevolgd. Men oordeelde dat er geen sprake was van een gebruiker, in de zin van de SCA, die het kaderlid toegang had gegeven. Dit omdat de werknemer, die zijn naam als het ware in bruikleen had gegeven, de website van Konop nooit eerder had bezocht. Hij kon dus niet in aanmerking worden genomen als een gebruiker. De uitzondering van de SCA, §2701(c)(2) was niet van toepassing.[461]

4.2.2 *Pietrylo*

Uit de uitspraak van *Konop* kan worden afgeleid dat een werkgever geen inbreuk pleegt op de ECPA wanneer hij via een werknemer toegang verkrijgt tot een afgeschermde website, wanneer die werknemer voorheen reeds toegang had bekomen en de website ook effectief bezocht.

De district court van New Yersey stelde hier echter ook perk en paal. In *Pietrylo t. Hillstone Restaurant Group* hadden werkgevers een werkneemster onder druk gezet om haar inloggegevens voor MySpace, een SNS, te overhandigen. Zo konden zij inloggen op een afgeschermde gespreksgroep voor werknemers.[462]

De werkgever stelde dat hij gebruik konden maken van een uitzondering van de SCA doordat hij toegang had verkregen via een gebruiker van de gespreksgroep.[463]

---

[458] Een district court is vergelijkbaar met een rechtbank van eerste aanleg in België.
[459] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002), para. 16.
[460] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002), para. 29-31.
[461] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002), para. 37.
[462] *Pietrylo v. Hillstone Restaurant Group*, 06-5754 (FSH) 2009 WL 3128420 en C. CRANE, "Social networking v. the employment-at-will doctrine", *supra* noot 356, (640) 666.
[463] Electronic Communications Privacy Act of 1986, 18 U.S.C. §2701(c)(2).

De rechtbank oordeelde echter dat de werkneemster inderdaad geen toestemming had kunnen gegeven om toegang te krijgen tot de groep. In het geval een werkgever een werknemer onder druk zet of hoe dan ook ongeoorloofd toegang verkrijgt tot een beschermde webpagina, dan is er "most likely" of waarschijnlijk sprake van een schending van de SCA.[464]

4.2.3 *Crispin*

In *Crispin* wilde een modehuis informatie verkrijgen vanop de Facebook- en MySpace-pagina's, inclusief privéberichten, van een kunstenaar, Crispin.[465] Het wilde daarmee bewijs aanleveren omtrent afspraken over intellectuele rechten. Crispin beschuldigde het bedrijf er immers van dat het had nagelaten mondelinge afspraken na te komen, namelijk dat zijn naam en logo vermeld zouden worden bij zijn ontwerpen.[466]

De rechter oordeelde dat het doel van de SCA eruit bestaat om niet alleen private Facebook- en MySpace-berichten te beschermen, maar ook openbare berichten op Facebook en MySpace als de privacy-instellingen zo waren ingesteld dat het grote publiek deze niet kon zien.[467] De rechter vergeleek de berichten die via Facebook en MySpace verstuurd werden met "e-mailachtige functies".[468]

Voor de openbare berichten werd niet expliciet gesteld dat de SCA van toepassing is, maar oordeelde de rechtbank wel dat de privacy-instellingen en de bedoelingen van de persoon die berichten plaatst van groot belang zijn.[469]

Deze zaak is een belangrijke stap richting de bescherming van gegevens die werknemers privé willen houden en desondanks toch verkregen worden door hun werkgever.

4.3 Evaluatie

In principe zijn er geen redelijke privacyverwachtingen wanneer een werknemer surft op het netwerk van de werkgever, dit blijkt uit *Smyth*. Wel mag de werknemer er van uitgaan dat er toch enige privacy is wanneer hij een private mailbox opent op dat netwerk.[470]

Privacyverwachtingen zijn de basis van het recht op privacy, maar door werkgevers de kans te geven dit uit te hollen vooraleer een arbeidsovereenkomst wordt aangegaan, is de bescherming in de VS miniem.[471] Er is geen preventieve, enkel een *post factum* bescherming mogelijk voor de werknemer door naar de rechter te stappen en proberen aan te kaarten dat zijn redelijke privacyverwachtingen geschonden zijn. De Amerikaanse rechters zijn schijnbaar tevreden met deze *case-by-case* aanpak.[472]

---

[464] C. CRANE, "Social networking v. the employment-at-will doctrine", *supra* noot 356, (640) 667.
[465] *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010).
[466] *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010).
[467] C. CRANE, "Social networking v. the employment-at-will doctrine", *supra* noot 356, (640) 669.
[468] *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010).
[469] C. CRANE, "Social networking v. the employment-at-will doctrine", *supra* noot 356, (640) 670-671.
[470] L. DETERMANN en R. SPRAGUE, "Intrusive monitoring", *supra* noot 378, (979) 1008 en *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, S.D.N.Y. 2008, 587 F. Supp. 2d 548.
[471] L. DETERMANN en R. SPRAGUE, "Intrusive monitoring", *supra* noot 378, (979) 1018.
[472] L. DETERMANN en R. SPRAGUE, "Intrusive monitoring", *supra* noot 378, (979) 1018.

Met de zaken *Konop, Pietrylo* en *Crispin* kan goed worden aangetoond dat rechtspraak in staat is om evoluties teweeg te brengen bij de interpretatie van wetten. In dit geval werd aan de bepalingen van de SCA steeds een nieuwe interpretatie gegeven, waarmee tegemoet werd gekomen aan de nieuwe technologische ontwikkelingen. Het gebeurt wel degelijk dat de werknemer het pleidooi van zijn werkgever overwint.

5 Tussenconclusie

Als men zoekt naar een coherent geheel van wet- en regelgeving inzake de gegevensbescherming bij internetgebruik van werknemers op de werkvloer, zijn de Verenigde Staten van Amerika en de Europese Unie in hetzelfde bedje ziek. Het probleem is in de VS zelfs nog acuter, aangezien er amper bepalingen bestaan die werknemers van private ondernemingen een recht op privacy toemeten. In Utah bestond er tot voor kort bijvoorbeeld nog geen bijzondere wetgeving die het aan werkgevers verbood om werknemers onder druk te zetten om inloggegevens te verkrijgen. Mogelijk werden dergelijke situaties in de praktijk bestraft door meer algemene wetgeving, bijvoorbeeld via het strafrechtelijk contentieux. Het feit dat er toch de nood bestond deze regels te codificeren spreekt echter boekdelen.

Dit gebrek aan bijzondere wetgeving heeft in belangrijke mate te maken met het rechtssysteem van de Amerikanen, waar het gerecht overduidelijk de plak zwaait. Hiernaast speelt de historiek van de Verenigde Staten: van de nood aan een *employment-at-will* doctrine aan het begin van de 20ste eeuw, een vrije arbeidsverhouding die nog steeds veel toegepast wordt, tot toegenomen *big brother*-praktijken na de aanslagen op 9/11.

Deze evolutie zorgt voor een continue rechtsontwikkeling die nog steeds aan de gang is en langzaamaan toch bepaalde Europese gedachten over privacy lijkt over te nemen. Zo blijkt uit rechtspraak dat de werknemer met de tijd meer weerwerk is kunnen gaan bieden tegen de absoluut dominante rechtspositie van de werkgever. Dergelijke uitdieping van het onderwerp kan echter ook voordelen bieden voor de werkgever. Wanneer het aan omvattende wetgeving ontbreekt, kan rechtspraak een manier vinden om tegemoet te komen aan de onzekerheid over welke controle nu wel en niet mag. De werkgever zal verplicht worden omzichtiger om te gaan met de privacy van zijn werknemers, zij het dat de rechtspraak het probleem aanpakt op een minder allesomvattende manier dan nieuwe wetgeving zou kunnen bewerkstelligen.

Ondanks dat er een andere weg is afgelegd, is de voorlopige eindbestemming van de regulering van werkgeverscontrole op beide continenten dezelfde. Overkoepelende instanties, de Europese Unie en de Verenigde Staten, voorzien een beperkt ruim kader dat naar goeddunken wordt ingevuld door de lid- en deelstaten. Het is aan de rechters en de sociale partners om dit beperkte regelarsenaal zo goed mogelijk te interpreteren en tot uitvoering te brengen. Momenteel is het Europees stelsel wel opvallend werknemer-vriendelijker. Misschien is een lichte verschuiving van de balans tussen werkgever en werknemer in de Europese Unie en België geen slecht idee. Het mag de werkgever niet onmogelijk worden gemaakt controle uit te oefenen door een ondoorzichtig geheel van regels, een verwijt dat over cao nr. 81 al vaak heeft weerklonken. De Verenigde Staten kunnen dan weer wat leren van de Europese bescherming van werknemersrechten.

Determann en Sprague vatten het samen in een slagzin die relatief kort door de bocht is, maar toch een kern van waarheid herbergt: "employee privacy expectations are reasonable in Europe, destroyed in the United States".[473]

[473] L. DETERMANN en R. SPRAGUE, "Intrusive monitoring", *supra* noot 378, (979) 979.

Deel 4 Conclusie

Deze masterscriptie ging van start met de volgende onderzoeksvraag: voldoet de momenteel geldende wet- en regelgeving betreffende werkgeverscontrole op internetgebruik van een werknemer aan de noden van een arbeidsrelatie in de hedendaagse technologische samenleving? Via een reeks subvragen, ondergebracht in drie kerndelen, werd getracht een antwoord te zoeken op deze centrale onderzoeksvraag.

Ten eerste kwamen we tot de conclusie dat het internet, en met name de sociale media, voor een revolutie heeft gezorgd in het dagdagelijkse leven van elk individu in – althans de westerse – wereld. Personen kunnen op elk moment van de dag met elkaar verbonden zijn en voortdurend communiceren: zij het via hun laptop, dan wel via tablet of smartphone, middelen die ze steeds bij zich hebben. Men kan informatie delen met andere gebruikers, tot over de kleinste details van hun leven, en dat op elk moment van de dag. Daarnaast is surfen op het internet door de evolutie van *web 1.0* naar *web 2.0* en de toegenomen interactiviteit tussen beheerder en gebruiker, alsook tussen gebruikers onderling, een tijdrovende bezigheid geworden. Een bezigheid die zich manifesteert binnen de arbeidsverhouding en een impact daarop heeft, zowel tijdens als na de werkuren.

Een belangrijk gegeven voor elk individu is zijn recht op eerbiediging van zijn privéleven. Dit recht wordt gewaarborgd door art. 8 van het Europees Verdrag voor de Rechten van de Mens en art. 22 van de Belgische Grondwet. Dit recht, ook wel het recht op privacy genoemd, komt door voormelde revolutie onder druk te staan. Vele persoonlijke gegevens worden al dan niet bewust achtergelaten op het internet en kunnen door andere partijen gebruik en misbruikt worden. In principe mag geen afbreuk worden gedaan aan het recht op privacy, dat een persoonlijkheidsrecht is, inherent aan het leven. Toch kan men onder bepaalde voorwaarden zich mengen in iemands privéleven: men dient te voldoen aan het legaliteits-, finaliteits- en proportionaliteitsbeginsel. De inmenging dient bij wet voorzien te zijn, het mag enkel omwille van welbepaalde doeleinden gebeuren en hoort enkel te gebeuren in de mate dat het nodig is om dit streefdoel te bereiken.

De primaire rechtsbronnen omtrent het recht op privacy dateren van vooraleer er sprake was van moderne elektronische communicatiemiddelen, waardoor aangepaste normering niet kon uitblijven. Toch is het regelgevend arsenaal ter zake beperkt: De bescherming van persoonlijke gegevens wordt binnen de Europese Unie gereguleerd door richtlijnen 95/46/EG en 2002/58/EG en in België door de Wet Verwerking Persoonsgegevens uit 1992, de Wet Elektronische Communicatie uit 2005 en art. 314bis Strafwetboek.

Een arbeidsovereenkomst kan grenzen stellen aan het recht op privacy. Dit blijkt nodig te zijn om de rechten en belangen ter zake proberen te verzoenen. Aan de kant van de werknemer kan zijn fundamenteel recht op privacy onderscheiden worden, alsook zijn recht op vrijheid van meningsuiting. De werkgever kan zich in bepaalde omstandigheden beroepen op zijn eigendomsrecht, namelijk wanneer een werknemer op ongeoorloofde wijze gebruik maakt van apparatuur door de werkgever voorzien. Verder dient de werkgever te steunen op een reeks

belangen, feiten die voortvloeien uit de verantwoordelijkheid die hij draagt als "patron" van zijn werknemers. Het belangrijkste element dat hier speelt is zijn gezaghebbende verhouding met zijn werknemers. Ondergeschikten worden geacht prestaties te leveren zoals in hun arbeidsovereenkomst is overeengekomen. Dit werk kan in gedrang komen wanneer de werknemer te veel tijd spendeert op het internet. Ten slotte verwacht de werkgever een zekere loyauteits- en vertrouwelijkheidszin van zijn werknemers: zij zullen noch onbehoorlijk kwaad spreken over hun werkgever, noch diens geheimen onthullen. Deze verwachtingen laten zich ook gelden na de werkuren.

Het overheersend recht op privacy van een individu dient dus getemperd te worden om het voor zijn werkgever mogelijk te maken zijn recht en belangen te doen gelden. Wat controle op elektronische communicatiegegevens in België betreft, werd door de sociale partners cao nr. 81 in het leven geroepen.

Een uitgebreide blik op de internationale, Europese en nationale aanpak van het spanningsveld tussen de rechten en belangen van werkgevers en werknemers leverde een aantal bevindingen op. Wat de Europese Unie betreft, kan geconcludeerd worden dat de momenteel geldende richtlijnen slechts miniem aandacht hebben voor gegevensbescherming binnen een arbeidsrechtelijke context. De Europese Unie heeft enkel gehandeld in de mate het nodig was om de Europese interne markt en het vrij verkeer te bewerkstelligen. De algemene richtlijnen dienen naar analogie te worden toegepast, waardoor het zwaartepunt van wet- en regelgeving onvermijdelijk op de schouders van de lidstaten valt.

De toekomst lijkt beterschap te bieden: na een dialoog tussen de Europese Commissie en de Europese sociale partners en de evolutie naar *web 2.0* zag de Europese Unie de nood voor een gemoderniseerd coherent geheel aan regels inzake gegevensbescherming. De Algemene Verordening Gegevensbescherming, die momenteel de gewone legislatieve procedure doorloopt, wijdt één – zij het zeer uitgebreid – artikel aan minimumstandaarden voor het verwerken van gegevens binnen een arbeidsrechtelijke context. Dit zou de eerste rechtstreeks bindende bepaling zijn die uitgevaardigd is door de Europese Unie inzake privacy op de werkvloer. Deze bepaling, die reeds enkele wijzigingen doorheen de debatten heeft ondergaan, lijkt ons op het eerste zicht weinig nieuws te introduceren voor het Belgisch rechtsstelsel. Toch is reeds in het verleden gebleken dat dergelijke initiatieven een sterke impuls kunnen zijn om lidstaten te doen nadenken over hun beleid en zo het heft in eigen handen te doen nemen.

De Raad van Europa krijgt vandaag voornamelijk nog een plaats in de discussie door de rechtspraak van het Europees Hof voor de Rechten van de Mens. Dit Hof heeft enkele arresten voortgebracht die zelfs de lagere nationale rechtspraak helpen met het interpreteren van de relevante bepalingen en met name art. 8 EVRM. Andere organisaties, zoals de Organisatie voor Economische Samenwerking en Ontwikkeling en de Internationale Arbeidsorganisatie, hebben zich beperkt tot het uitvaardigen van *soft law*, niet-afdwingbare gedragscodes.

Het enige bijzondere geheel van regels omtrent de bescherming van elektronische persoonlijke gegevens van werknemers in België is een collectieve arbeidsovereenkomst, cao nr. 81. Wat betreft de discussie of de sociale partners al dan niet bevoegd waren om zulke regels te stellen, hebben wij het standpunt ingenomen dat dergelijke regelgeving moet kunnen worden aanvaard gezien de ruime interpretatie van het legaliteitsbeginsel van art. 8 EVRM.

De cao heeft veel kritiek moeten doorstaan door zowel rechtsleer als practici. De voornaamste klachten omvatten dat het toepassingsgebied onduidelijk is, dat sommige discussiepunten zijn vergeten te worden beslecht en dat de balans tussen rechten en belangen van werkgevers en werknemers doorslaat in het voordeel van de werknemer. Zij het zo dat in elk van deze klachten een grond van waarheid zit, de situatie mag niet overdreven worden. Net zoals met zovele rechtsnormen worden ook deze bepalingen geïnterpreteerd door de rechterlijke macht en wordt er waar nodig een uitleg gegeven aan de letter van de wet. Bij deze beoordeling wordt zoveel mogelijk rekening gehouden met de redelijkheid en proportionaliteit. Hieruit vloeit de toepassing van de Antigoon-doctrine in het arbeidsrechtelijk contentieux voort. De geciteerde rechtspraak ter zake toont eveneens aan dat deze, op het eerste zicht voor de werkgever erg voordelige doctrine, geenszins betekent dat het recht op privacy van de werknemer in het gedrang komt.

De voornaamste aanbeveling die voor werkgevers wordt aangebracht is om een geschreven beleid uit te werken inzake internetgebruik van werknemers. Op deze manier kan preventief gewerkt worden en kan controle zelfs overbodig worden. Mocht er toch nog ongeoorloofd internetgebruik ontdekt worden, dan kan het geschreven beleid zowel voor de contractuele partijen als voor de rechter meteen duidelijkheid verschaffen over eventuele twistpunten.

Het hanteren van een beleid, zij het in een arbeidsovereenkomst, arbeidsreglement of *policy*, blijft evenwel een lapmiddel voor het eigenlijke probleem, namelijk het gebrek aan rechtszekerheid voor de contractspartijen. Deze kwestie zal enkel opgelost kunnen worden door middel van nieuw wetgevend optreden. Dit gebeurt bij voorkeur op Europees niveau om de interne markt een nieuwe dimensie te geven op het vlak van gegevensbescherming. Het handelen van de nationale wetgever lijkt desalniettemin een minimumvereiste, hoe positief partijen zoals de Commissie ter bescherming van de persoonlijke levenssfeer ook staan ten opzichte van cao nr. 81.

Uit een rechtsvergelijking met de Verenigde Staten van Amerika bleek dat men aan de andere kant van de Atlantische Oceaan in de eerste plaats een zeer ander rechtsstelsel kent. Niet alleen is er het verschil tussen de *common law*- en *civil law*-systemen, ook de *employment-at-will* doctrine zorgt voor een compleet verschillende benadering van de arbeidsverhouding. Hierdoor komt de principiële voorrang van het recht op privacy op het werkgeversgezag, zoals wij het in België kennen, op losse schroeven te staan. Nog niet zo lang geleden zou het zelfs niet verkeerd zijn geweest om te stellen dat de belangen van de werkgever in de Verenigde Staten absoluut primeerden op de rechten van de werknemer. Recentelijk lijkt de verhouding zich meer in balans te trekken, hetgeen opvallend blijkt uit de evolutie in de arresten *Konop, Pietrylo* en *Crispin*.

Toch kennen de Verenigde Staten ondanks vele historische verschillen hetzelfde probleem als de Europese Unie en België, zijnde een gebrek aan duidelijke bijzondere wetgeving. Ook hier bestaat er rechtsonzekerheid door een amalgaam van verouderde rechtsnormen met een beperkt toepassingsgebied, een allegaartje dat afhankelijk is van de interpretatie door de rechterlijke macht. Het is slechts door deze laatste partij dat wetgeving zoals de Stored Communications Act bijna 30 jaar na publicatie nog toegepast kan worden.

Afsluitend kan worden gesteld dat de momenteel geldende wet- en regelgeving betreffende werkgeverscontrole op internetgebruik van een werknemer niet voldoet aan de noden van een arbeidsrelatie in de hedendaagse technologische samenleving. Zowel de Europese Unie als de Verenigde Staten van Amerika zouden baat hebben bij een ruim omvattend, duidelijk wetgevend kader dat zorgt voor eenheid binnen hun respectievelijke lid- en deelstaten. De werkgevers en werknemers op beide continenten zouden een veel grotere rechtszekerheid bekomen.

Ondanks het gemeenschappelijk probleem en de verschillende historische achtergronden kunnen Amerikanen en Europeanen toch wat van elkaar leren. De Europese en Belgische wetgever kunnen de Amerikaanse voorkeur voor werkgeversbelangen bestuderen en de Amerikaanse wetgever kan inspiratie halen uit het befaamde Europees recht op privacy. Indien dit gebeurt, kan inzake internetcontrole binnenkort misschien op beide werelddelen gesproken worden van een effectief evenwicht tussen de belangen van werkgevers en werknemers.

Bibliografie

1 Wetgeving (in de meest brede zin)

1.1 Internationaal en supranationaal

Verdrag betreffende de Europese Unie, *Pb.C.* 26 oktober 2012, afl. 326, 13-46.

Verdrag betreffende de werking van de Europese Unie, *Pb.C.* 26 oktober 2012, afl. 236, 47-200.

Verdrag betreffende de Europese Unie, met het Verdrag tot oprichting van de Europese Gemeenschap, *Pb.C.* 31 augustus 1992, afl. 224, 1-130.

Handvest van de Grondrechten van de Europese Unie, *Pb.C.* 18 december 2000, afl. 364, 1-22.

Internationaal verdrag 19 december 1966 inzake burgerrechten en politieke rechten, *BS* 6 juli 1983.

Verdrag nr. 108 van de Raad van Europa 28 januari 1981 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens.

Verdrag 4 november 1950 tot bescherming van de rechten van de mens en de fundamentele vrijheden, *BS* 19 augustus 1955, *erratum BS* 29 juni 1961.

Richtl. Europees Parlement en Raad nr. 2014/104/EU, 26 november 2014 betreffende bepaalde regels voor schadevorderingen volgens nationaal recht wegens inbreuken op de bepalingen van het mededingingsrecht van de lidstaten en van de Europese Unie, *Pb.L.* 5 december 2014, afl. 349, 1-19.

Richtl. Europees Parlement en Raad nr. 2009/136/EG, 25 november 2009, tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming, *Pb.L.* 18 december 2009, afl. 337, 29-32.

Richtl. Europees Parlement en Raad nr. 2002/58/EG, 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, *Pb.L.* 31 juli 2002, afl. 201, 37-47.

Richtl. Europees Parlement en Raad nr. 97/66/EG, 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, *Pb.L* 30 januari 1998, 1-8.

Richtl. Europees Parlement en Raad nr. 95/46/EG, 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb.L.* 23 november 1995, afl. 281, 31-50.

Wetgevingsresolutie Europees Parlement 12 maart 2014 over het voorstel voor een verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//NL (consultatie 27 december 2014).

Aanbeveling 2013/396/EU van de Europese Commissie, 11 juni 2013 over gemeenschappelijke beginselen voor mechanismen voor collectieve vorderingen tot staking en tot schadevergoeding in de lidstaten betreffende schendingen van aan het EU-recht ontleende rechten, *Pb.L.* 26 juni 2013, afl. 201, 60-65.

COM(2012)11def. [Commissiedocument nr. 11 van 2012].

1.2 België

Gecoördineerde Grondwet 17 februari 1994, *BS* 17 februari 1994.

Wet 24 oktober 2013 tot wijziging van de voorafgaande titel van het Wetboek van strafvordering wat betreft de nietigheden, *BS* 12 november 2013 (Wet-Landuyt).

Wetboek van economisch recht 28 februari 2013, *BS* 29 maart 2013.

Wet 13 juni 2005 betreffende de elektronische communicatie, *BS* 20 juni 2005.

Wet 11 december 1998 tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *BS* 3 februari 1999.

Wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS* 18 maart 1993.

Wet 17 juni 1991 houdende goedkeuring van het Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde werking van persoonsgegevens, opgemaakt te Straatsburg op 28 januari 1981, *BS* 30 december 1993.

Wet 3 juli 1978 betreffende de arbeidsovereenkomsten, *BS* 22 augustus 1978, *erratum BS* 30 augustus 1978.

Wet 8 april 1965 tot instelling van de arbeidsreglementen, *BS* 5 mei 1965.

Wet 10 maart 1900 op de arbeidsovereenkomst, *BS* 14 maart 1900.

Strafwetboek 8 juni 1867, *BS* 9 juni 1867.

Burgerlijk Wetboek 21 maart 1804, *BS* 3 september 1807.

Cao nr. 100 van 1 april 2009 betreffende een preventief alcohol- en drugsbeleid in de onderneming, *BS* 13 juli 2009.

Cao nr. 89 van 30 januari 2007 betreffende de diefstalpreventie en de uitgangscontroles van werknemers bij het verlaten van de onderneming of de werkplaats, *BS* 11 mei 2007.

Cao nr. 81 van 26 april 2002 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische onlinecommunicatiegegevens, *BS* 29 juni 2002.

Cao nr. 68 van 16 juni 1998 betreffende de bescherming van de persoonlijke levenssfeer van werknemers ten opzichte van de camerabewaking op de arbeidsplaats, *BS* 2 oktober 1998.

Vr. en Antw. Kamer 1999-00, 28 april 2000, 3816 (Vr. Nr. 93 Bourgeois).

1.3 Verenigde Staten van Amerika

U.S. Const.

Cal. Const.

Restatement (second) of torts.

National Labor Relations Act of 1935, 29 U.S.C. §151-169.

Electronic Communications Privacy Act of 1986, 18 U.S.C. §2510-2522; §2701-2712.

Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §2510-2520.

Conn. Gen. Stat.

Del. Code Ann.

Utah Code Ann.

Congres, *Social Networking Online Protection Act*, https://www.congress.gov/bill/113th-congress/house-bill/537/all-actions (consultatie 4 januari 2015).

2 Overige publicaties wetgevende instanties

2.1 Europese Unie

Advies Commissie Werkgelegenheid en Sociale Zaken, 4 maart 2013, http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A7-2013-0402&language=EN#title3 (consultatie 27 december 2014).

Europese Commissie, *Second stage consultation of social partners on the protection of workers' personal data*, http://ec.europa.eu/social/main.jsp?catId=708 (consultatie 10 november 2014).

Europese Commissie, *First stage consultation of social partners on the protection of workers' personal data*, http://ec.europa.eu/social/main.jsp?catId=708 (consultatie 10 november 2014).

2.2 Andere

IAO, *Protection of workers' personal data. An ILO code of practice*, Genève, IAO, 1997.

Algemene Vergadering Verenigde Naties, *Guidelines for the Regulation of Computerized Personal Data Files*, New York, Verenigde Naties, 1990.

Aanbeveling nr. R(89)2 of the Committee of Ministers to Member States on the protection of personal data used for employment purposes, 18 januari 1989.

OESO, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Parijs, 1980.

3 Rechtspraak

3.1 Internationaal en supranationaal

EHRM, *Lee Davies t. België,* 28 juli 2009.

EHRM, *Copland t. Verenigd Koninkrijk*, 3 april 2007.

EHRM, *Amann t. Zwitserland*, 16 februari 2000.

EHRM, *Halford t. Verenigd Koninkrijk*, 25 juni 1997.

EHRM, *Niemietz t. Duitsland*, 16 december 1992.

HvJ C-13/94, *P v S en Cornwall County Council*, 30 april 1996.

3.2 België

Cass. 10 maart 2008, nr. S.07.0073.N/1.

Cass. 2 maart 2005, nr. P.04.1644.F/1.

Cass. 14 oktober 2003, nr. P.03.0762.N.

Arbh. Gent 12 mei 2014, *JTT* 2014, afl. 20, 320-312.

Arbh. Brussel 3 september 2013, *RW* 2014, afl. 40, 1586-1590, noot.

Arbh. Brussel 2 mei 2011, A.R. 09/7124.A, onuitg.

Arbh. Brussel 4 maart 2010, A.R. 2010/AG/0014, onuitg.

Arbh. Brussel 13 september 2005, *Computerr.* 2006, afl. 2, 100.

Antwerpen 12 februari 2004, *RW* 2005, afl. 30, 1186-1189, noot P. HUMBLET.

Arbh. Antwerpen 1 oktober 2003, *JTT* 2004, afl. 28, 510-512.

Arbrb. Leuven 17 november 2011 (*Option*).

Arbrb. Namen 10 januari 2011, *JTT* 2011, afl. 28, 462-463.

Arbrb. Kortrijk 8 oktober 2008, onuitg.

Arbrb. Brussel 2 mei 2000, *Computerr.* 2001, afl. 1, 26-29, noot D. CASAER.

3.3 Verenigde Staten van Amerika

United States v. Jones, 132 S. Ct. 945 (2012) (Sotomayor, J., concurring).

Katz v. United States, 389 US 347 (1967).

Konop v. Hawaiian Airlines, Inc., 9th circuit, 2002, 302 F.3d 868, 874.

Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914, 928 (W.D. Wis. 2002).

Pietrylo v. Hillstone Restaurant Group, 06-5754 (FSH) 2009 WL 3128420.

Crispin t. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010).

Pure Power Boot Camp, Inc. t. Warrior Fitness Boot Camp, LLC, S.D.N.Y. 2008, 587 F. Supp. 2d 548.

Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996).

Karl Knauz Motors, Inc., 13-CA-046452 (September 28, 2012), WL 4482841.

Costco Wholesale Corp., 34-CA-012421 (September 7, 2012) WL 3903806.

Sears Holdings (Roebucks), 18-CA-19081 (December 4, 2009), WL 5593880.

4 Rechtsleer

4.1 Europese Unie en België

4.1.1 Boeken

BLANPAIN, R. en VAN GESTEL, M., *Gebruik en controle van e-mail, intranet en internet in de onderneming*, Brugge, Die Keure, 2003, 264 p.

BUELENS, V. en STROOBANTS, P., *Is 'facebooken' een werkwoord?*, Mechelen, Kluwer, 2012, 69 p.

CAERS, R., *Human Resource Management in essentie*, Antwerpen, Intersentia, 2013, xiii+219 p.

CUYPERS, D. en FOUBERT, P., *Schets van het Belgische arbeidsrecht*, Antwerpen, Intersentia, 2011, xxi+209 p.

CRAIG, P. en DE BÚRCA, G., *EU Law: Text, Cases and Materials*, Oxford, Oxford University Press, 2011, clvii+1155 p.

DE WINTER, B., *Privacy in het internettijdperk*, Den Haag, Sdu uitgevers, 2011, 158 p.

DIRIX, E., TILLEMAN, B. en VAN ORSHOVEN, P. (eds.), *De Valks Juridisch Woordenboek*, Antwerpen, Intersentia, 2010, 621 p.

EUROPEES BUREAU VOOR DE GRONDRECHTEN, *Handbook on European data protection law*, Luxemburg, Publicatiebureau EU, 2014, 202 p.

HENDRICKX, F., *Elektronisch toezicht op het werk*, Mechelen, Kluwer, 2005, x+197 p.

HENDRICKX, F., *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, xxi+358 p.

HENDRICKX, F., *Protection of workers' personal data in the European Union: Two Studies*, website Europese Commissie, 2001, 121 p.

HEYLEN, D. en VERREYT, I., *Arbeidsrecht toegepast*, Antwerpen, Intersentia, 2014, xxiv+434 p.

LORRÉ, J., *Sociale media en werkgeverscontrole*, Mechelen, Kluwer, 2012, 163 p.

S. SMIS, C. JANSSENS, S. MIRGAUX en K. VAN LAETHEM, *Handboek Mensenrechten*, Antwerpen, Intersentia, 2011, xxiv+660 p.

VAN EECKHOUTTE, W., *Sociaal compendium Arbeidsrecht '14-'15 met fiscale notities*, Mechelen, Kluwer, 2014, xxxix+3011 p.

WESTRADE, M. en GILSON, S. (eds.), *Discipline et surveillance dans la relation de travail*, Limal, Anthemis, 2013, 602 p.

4.1.2 Bijdragen in verzamelwerken

FEYEN, S. en MARTENS, J., "Sociale media en de (kandidaat-)werknemer" in VALCKE, P., VALGAEREN, P.J. en LIEVENS, E. (eds.), *Sociale media: actuele juridische aspecten*, Antwerpen, Intersentia, 2013, 157-198.

OSAER, V. en NAYAERT, S., "Privacy in de werksfeer" in VERMEULEN, G. (ed.), *Privacy en strafrecht: nieuwe en grensoverschrijdende verkenningen*, Antwerpen, Maklu, 2007, 513-564.

PEIFFER, A., "Controle van e-mail en internetgebruik" in STAPPERS, K. (ed.), *Privacy in de arbeidsrelatie: gids voor het voeren van een privacybeleid*, Gent, Story Publishers, 2008, 49-64.

ROUSSEAU, J. en PLETS, I., "Sociale media en arbeidsrecht. Een praktische leidraad voor sociale-mediarichtlijnen" in VALCKE, P., VALGAEREN, P.J. en LIEVENS, E. (eds.), *Sociale media: actuele juridische aspecten*, Antwerpen, Intersentia, 2013, 119-156.

STRUBBE, T., "Is er plaats voor sociale media op de werkvloer?" in DE MEULENAERE, B. (ed.), *Internet &/@ Recht*, Gent, Larcier, 2013, 45-64.

4.1.3 Artikels

CLAEYS, T. en DEJONGHE, D., "Gebruik van e-mail en internet op de werkplaats en controle door de werkgever", *JTT* 2001, afl. 792, 121-134.

COCKX, S., "Sociale media in de arbeidsrelatie: 'vriend' of vijand?", *Or.* 2012, afl. 1, 12-27.

DEKEYSER, H., "Internet op het werk en privacy", *Bibliotheek- & archiefgids* 2003, afl. 6, 3-8.

DE HERT, P., "C.A.O. nr. 81 en advies nr. 10/2000 over controle van internet en e-mail", *RW* 2003, afl. 33, 1281-1294.

DE PAUW, E., "Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?", *Orde van de dag* 2010, afl. 49, (5) 7.

LORRÉ, J., "Facebook en arbeidsrecht: *mysterium tremendum et fascinans*", *RW* 2011, afl. 36, 1498-1510.

PORTUGAELS, N., SAMYN, I., VANDENBUSSCHE, W. en VAN DER SYPE, Y.S., "Sociale netwerksites en class actions", *Juristenkrant*, afl. 295, 8 oktober 2014, 16.

PREUMONT, C., "Les médias sociaux à l'épreuve du droit du travail", *JTT* 2011, afl. 22, 353-360.

VANTHOURNOUT, J., "Privacy, informatica en arbeidsverhouding: de catenaccio voorbij?", *TSR* 2002, afl. 4, 479-528.

VAN KILDONCK, K., "Privacy werknemers: onrechtmatig verkregen bewijs op het werk", *NJW* 2010, afl. 218, 180-183.

WAUTERS, E., LIEVENS, E. en VALCKE, P., "Bescherming van gebruikers van sociale media. Juridisch perspectief op algemene voorwaarden van socialenetwerksites", *NJW*, afl. 312, 10 december 2014, 866-880.

WATERSCHOOT, P., "Bespreking van enkele arresten van het Arbeidshof te Gent in verband met het gebruik en misbruik van e-mail en internet op de werkplaats en het controlerecht van de werkgever daarop", *RW* 2009, afl. 18, 730-744.

WATERSCHOOT, P., "De C.A.O. nr. 81 en de privacybescherming van de werknemer, een afdwingbare norm of een papieren tijger?", *RW* 2014, afl. 40, 1563-1575.

4.2 Verenigde Staten van Amerika

4.2.1 Boeken

BIBLE, J.D. en MCWHIRTER, D.A., *Privacy in the workplace: A guide for human resource managers*, New York, Quorum Books, 1990, 306 p.

ROTHSTEIN, M.A., CRAVER, C.B., SCHROEDER, E.P. en SHOBEN, E.W., *Employment law*, Eagan, West, 2010, 1093 p.

SCHWARTZ, P.M. en REIDENBERG, J.R., *Data Privacy Law*, Charlottesville, Michie, 1996, xxiv+486 p.

4.2.2 Bijdragen in verzamelwerken

LIM, V.K.G. en TEO, T.S.H., "Cyberloafing and Organizational Justice: The Moderating Role of Neutralization Technique" in ANANDARAJAN, M., TEO, T.S.H. en SIMMERS, C.A. (eds.), *The Internet and Worplace Transformation*, New York, M.E. Sharpe, 2006, 241-258.

4.2.3 Artikels

ALLEN, M.W., COOPMAN, S.J., HART, J.L. en WALKER, K.L., "Workplace surveillance and managing privacy boundaries", *Management Communication Quarterly* 2007, afl. 21, 172-200.

ANDRISANI, D.N., "Employer-employee rights on the Internet: is there an effective balance?", *Journal of Internet Law* 2000, 3, 24-31.

CIOCCHETTI, C.A., "The eavesdropping employer: a twenty-first century framework for employee monitoring", *American Business Law Journal* 2011, afl. 2, 285-369.

CRANE, C., "Social networking v. the employment-at-will doctrine: a potential defense for employees fired for Facebooking, terminated for Twittering, booted for blogging, and sacked for social networking", *Washington University Law Review* 2012, afl. 3, 639-672.

DETERMANN, L. en SPRAGUE, R., "Intrusive monitoring: employee privacy expectations are reasonable in Europe, destroyed in the United States", *Berkeley Technology Law Journal* 2014, afl. 2, 979-1036.

GUTHRIE, R. en GRAY, P., "Junk Computing: Is it Bad for an Organization?", *Information Systems Management* 1996, afl. 1, 23-28.

MILLER, D., "Legislating our reasonable expectations: making the case for a statutory framework to protect workplace privacy in the age of social media", *University of Miami Business Law Review* 2013, afl. 1, 49-81.

MILLER, M.B., "Avatars and social media: employment law risks and challenges in the virtual world", *FDCC Quarterly* 2013, afl. 4, 279-294.

MUHL, C.J., "Workplace e-mail and Internet use: employees and employers beware", *Monthly Labor Review* 2003, afl. 2, 36-45.

MURILLO, M.L., "The evolution of codification in the civil law legal systems: towards decodification and recodification", *Journal of Transnational Law & Policy* 2001, afl. 1, 1-20.

RAYSMAN, R., "A practical look at social media policies", *Computer & Internet Lawyer* 2012, afl. 3, 10-14.

SEWELL, G. en BARKER, J.R., "Coercion versus care: using irony to make sense of organizational surveillance", *Academy of Management Review* 2006, afl. 4, 1-24.

SNOW, C.B., "To snoop or not to snoop? Legal considerations under Utah's Internet Employment Privacy Act", *Utab Bar Journal* 2014, afl. 3, 20-24.

SPRAGUE, R., "Invasion of the social networks: blurring the line between personal life and the employment relationship", *University of Louisville Law Review* 2014, afl. 1, 1-34.

WHITFIELD, B.N., "Social media @ work: #policyneeded", *Arkansas Law Review* 2013, afl. 3, 843-878.

5 Andere publicaties

COMMISSIE TER BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, aanbeveling nr. 08/2012 betreffende de controle door de werkgever op het gebruik van elektronische communicatie-instrumenten op de werkvloer, 2 mei 2012, 53 p.

COMMISSIE TER BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, advies nr. 10/2000 betreffende het toezicht door de werkgever op het gebruik van het informaticasysteem op de werkplaats, 3 april 2000, 8 p.

COMMISSIE TER BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, dossier Cybersurveillance, http://www.privacycommission.be/nl/cybersurveillance (consultatie 2 januari 2015).

DINUCCI, D., "Fragmented Future", *Print* 1999, afl. 4, 32.

O'REILLY, T., 'What is Web 2.0", *O'Reilly.com*, 30 september 2004, http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html.

X, "Airport Security", Flightglobal, http://www.flightglobal.com/features/9-11/airport-security/.

X, "Aldi Genk controleert alle handtassen ondanks gewijzigd beleid directie", *Het Belang van Limburg*, 12 augustus 2014, http://www.hbvl.be/cnt/dmf20140811_01213853/aldi-genk-controleert-alle-handtassen-ondanks-gewijzigd-beleid-directie.

X, "Belg wil minder tijd spenderen aan sociale media", *De Standaard*, 1 januari 2015, http://www.standaard.be/cnt/dmf20150101_01453912.

X, "Facebook zet dino in om privacy te controleren", *De Standaard*, 23 mei 2014, http://www.standaard.be/cnt/dmf20140522_01115386.

X, "Helft van het werk blijft liggen", *hrsquare.be*, 5 juni 2014, http://www.hrsquare.be/nl/nieuws/6199/helft-van-het-werk-blijft-liggen.

X, "Oostenrijkse advocaat wil Europeanen mobiliseren tegen Facebook", *De Standaard*, 1 augustus 2014, http://www.standaard.be/cnt/dmf20140801_01200554.

X, "Personeel van Ikea lacht met 'domme klanten'. Meubelketen werkt aan richtlijnen voor gedrag op Facebook", *De Standaard*, 16 februari 2012, http://www.standaard.be/cnt/gvb3m9age.

X, "Professor Blanpain: 'Flauwe kul dat Facebookpagina privé is'", *De Standaard*, 17 november 2011, http://www.standaard.be/cnt/dmf20111117_145.

X, "Ruim 20.000 deelnemers voor rechtszaak tegen Facebook", *De Standaard*, 6 augustus 2014, http://www.standaard.be/cnt/dmf20140806_01206581.

X, "Sociale media nog niet ingeburgerd op de werkvloer", *hrsquare.be*, 6 december 2013, http://www.hrsquare.be/nl/nieuws/5878/sociale-media-nog-niet-ingeburgerd-op-werkvloer.

X, "Vier op de tien werkgevers blokkeren toegang tot sociale media", Algemeen persbericht Het Nieuwsblad, 28 februari 2012, http://www.standaard.be/cnt/dmf20120228_235.

X, "Zeven op tien Belgen actief op sociale netwerken", algemeen persbericht IAB Belgium, 23 januari 2013, http://www.iab-belgium.be/wp-content/uploads/2013/01/Persbericht-IAB-Zeven-op-tien-Belgen-actief-op-sociale-netwerken.pdf.

6 Websites

Europees Parlement: http://www.europarl.europa.eu (consultatie 4 januari 2015).

Facebook: http://www.facebook.com (consultatie 24 december 2014).

Internationale Arbeidsorganisatie: http://www.ilo.org/global/lang--en/index.htm (consultatie 10 november 2014).

LinkedIn: http://www.linkedin.com (consultatie 24 december 2014).

Twitter: http://www.twitter.com (consultatie 24 december 2014).

Auteursrechtelijke overeenkomst

Ik/wij verlenen het wereldwijde auteursrecht voor de ingediende eindverhandeling:
Werkgeverscontrole op het internetgebruik van de werknemer in het social media tijdperk: een (Europese) update vereist?

Richting: **master in de rechten-rechtsbedeling**
Jaar: **2015**

in alle mogelijke mediaformaten, - bestaande en in de toekomst te ontwikkelen - , aan de Universiteit Hasselt.

Niet tegenstaand deze toekenning van het auteursrecht aan de Universiteit Hasselt behoud ik als auteur het recht om de eindverhandeling, - in zijn geheel of gedeeltelijk -, vrij te reproduceren, (her)publiceren of distribueren zonder de toelating te moeten verkrijgen van de Universiteit Hasselt.

Ik bevestig dat de eindverhandeling mijn origineel werk is, en dat ik het recht heb om de rechten te verlenen die in deze overeenkomst worden beschreven. Ik verklaar tevens dat de eindverhandeling, naar mijn weten, het auteursrecht van anderen niet overtreedt.

Ik verklaar tevens dat ik voor het materiaal in de eindverhandeling dat beschermd wordt door het auteursrecht, de nodige toelatingen heb verkregen zodat ik deze ook aan de Universiteit Hasselt kan overdragen en dat dit duidelijk in de tekst en inhoud van de eindverhandeling werd genotificeerd.

Universiteit Hasselt zal mij als auteur(s) van de eindverhandeling identificeren en zal geen wijzigingen aanbrengen aan de eindverhandeling, uitgezonderd deze toegelaten door deze overeenkomst.

Voor akkoord,

Janssen, Joren

Datum: **4/01/2015**