Het gebruik van sociale netwerksites op de werkplaats: wat mag en wat mag niet?

Ronny Saelens - VUB
2 april 2015

Inleiding

Vandaag is het voeren van communicatie via de elektronische snelweg een belangrijk aspect van het maatschappelijke leven. Dat is niet anders in de professionele wereld. Voor bedrijven is het zelfs een *must* om hun concurrentiepositie te kunnen handhaven of te versterken. Het gebruik van nieuwe technologieën op het werk is evenwel een mes dat aan twee kanten snijdt. Zeker binnen de arbeidsrelatie. Sociale interactie via het internet kan door de werkgever namelijk ook gebruikt worden als controlemiddel. Daarbij rijst de vraag of en zo ja, in welke mate de werkgever het gebruik van sociale netwerksits (SNS) tijdens en buiten de werkuren kan controleren. Het antwoord op deze vraag wordt beïnvloed door de reikwijdte van zowel de bescherming van de vrijheid van de werknemer en de prerogatieven van de werkgever. Anders gezegd: wat mag en wat mag niet? Waar ligt de grens? De invulling van deze vraag is niet louter afhankelijk van wat door de wet toegelaten of verboden is. Ook afspraken op bedrijfsniveau zijn richtinggevend en onontbeerlijk. Daarom wordt het internetbeleid best in een document, *internet- of ICT policy*, vastgelegd.

Net zoals dat het geval is in privéleven spelen binnen de arbeidsrelatie verschillende belangen. Bij de werknemer gaat het om collectieve en individuele grondrechten: het recht om zich vrijelijk te uiten, de bescherming van de privacy en de communicatie en de bescherming van de persoonsgegevens. Aan de zijde van de werkgever gaat het om de prerogatieven van de werkgever: het gezags- en instructierecht en het controlerecht van de werkgever. Zoals we verder zullen zien, is de afweging van de verschillende belangen een complexe oefening die telkens een case-by-case-benadering vergt.

Dit werk geeft geen uitgebreide analyse van de hiervoor geschetste problematiek. Het geeft veeleer een overzicht van de actuele discussiepunten over de controle van het internetgebruik op het werk en sociale netwerksites in het bijzonder, gebaseerd op de (Europese) rechtspraak en literatuur. Ondanks sociale netwerksites ingeburgerd zijn, heeft dit nieuw communicatiemedium nog geen juridische plaats gekregen. Daarvoor is het nog te vroeg. Rechters leren nog omgaan met dit modern communicatiemiddel.

Deze bijdrage omvat zes paragrafen. Voor een goed begrip van de tekst moeten we eerst invulling geven aan het begrip telecommunicatie. Vervolgens moet deze communicatie een plaats krijgen binnen het kader van de grondrechten. Dat wordt in de tweede paragraaf besproken. Het betreft de uitingsvrijheid, het recht op privacy en het communicatiegeheim en de bescherming van de persoonsgegevens. Deze grondrechten moeten natuurlijk worden afgewogen tegen de prerogatieven

van de werkgever, dat in de derde paragraaf wordt toegelicht. De vierde paragraaf is gewijd aan het juridisch kader van de bescherming van de persoonsgegevens. We gaan zien dat deze rechtsfiguur onlosmakelijk verbonden is met het gebruik van sociale netwerksites. De essentie van wat in de vier paragrafen is uiteengezet, wordt in de vijfde paragraaf besproken. Dit resulteert in het antwoord op de centrale vraag: wat mag en wat mag niet op sociale netwerksites. Deze bijdrage wordt ten slotte afgesloten met een zesde paragraaf waarin wordt samengevat hoe een internet policy er zou kunnen uitzien.

1. Telecommunicatie en Sociale netwerksites (SNS)

Als we op SNS interactie voeren dan communiceren we met elkaar. Volgens van Dale is taal een middel van communicatie of een systeem van spraakklanken door middel waarvan mensen met elkaar communiceren en schriftelijke vastleggen. Maar ook andere vunzig of beledigend gebaar van een persoon naar een andere persoon (bijvoorbeeld tong uitsteken, middelvinger opsteken) kan onder de omschrijving vallen, nu er in deze gevallen ook sprake is van non-verbale communicatie. Communiceren in de digitale wereld wordt gevat onder het begrip “telecommunicatie”. Telecommunicatie is niet beperkt tot taal. Het betreft elke overbrenging, uitzending of ontvangst van tekens, seinen, geschriften, beelden, klanken of gegevens van alle aard, per draad, radio-elektriciteit, optische seingeving of een ander elektromagnetisch systeem. Niet alleen (mobiele) telefonie, maar ook telex, telefax, tele-banking, e-mail, surfen op het internet, enz. zijn vormen van telecommunicatie. Beide begrippen, communicatie en telecommunicatie, worden in hun gebruikelijke betekenis gebruikt en hebben dus een ruime draagwijdte. Het gaat samengevat om elke taaluiting, hetzij mondeling of niet mondeling, en gegevens- of informatie-uitwisseling, hetzij rechtstreeks of op afstand, ongeacht het aantal betrokkenen. Ook monologen of het inspreken of laten afdraaien van een dictafoon wordt onder communicatie begrepen.

Een toepassing van telecommunicatie is communiceren op sociale netwerksites, zoals Facebook, Twitter en YouTube. Er bestaat geen wettelijke noch een algemeen aanvaarde definitie van SNS. SNS kunnen worden omschreven als online-plaatsen waar mensen elkaar ontmoeten om sociale netwerken op te zetten, uit te bouwen en te versterken. SNS worden vaak uitingen van de zogeheten *web 2.0* genoemd, en onderscheiden zich van *web 1.0* toepassingen. Waar web 1.0 betrekking heeft op de toegang tot informatie op het internet, staat de interactie tussen mensen op web 2.0 centraal. Uit sociologisch onderzoek blijkt dat SNS succesvol zijn omdat ze rechtstreeks aansluiten bij de menselijke behoeften. Het is een virtuele sfeer waar personen niet alleen hun interesses delen, maar ook uiting geven aan gevoelens van liefde en leed in zowel de private als de professionele sfeer. Naast dergelijke uitingen kan audiovisueel materiaal aan het virtuele profiel toegevoegd worden, zoals foto’s gemaakt op personeelsfeestjes en leuke of minder leuke gebeurtenissen. Dat kan het geval zijn tijdens de werkuren of na de werkuren waar ogenschijnlijk vrijelijk wordt nagepraat over de afgelopen werkdag.

Maar deze groeiende digitalisering van communicatie vormt ook een grote uitdaging voor de bescherming van de persoonlijke levenssfeer en het communicatiegeheim en van de persoonsgegevens. Op SNS worden door de gebruikers veel gegevens verspreid. Op zichzelf is dat niet verwonderlijk. Eén van de principes die aan de basis liggen van ‘web 2.0’ is precies die actieve deelname. Maar vaak worden deze gegevens zonder medeweten van de gebruikers verzameld en voor andere doeleinden gebruikt dan de gebruiker voor ogen had. Naast de ongekende intenties van de medegebruikers, speelt de misleidende en foute informatie over de gebruikersrechten op de SNS een belangrijke factor. Als gevolg wordt de op SNS gedeelde informatie ook gevolgd door derden die in principe geen deelgenoot zijn aan de communicatie. We denken daarbij onder meer aan marketeers, verzekeringsmaatschappijen, politie- en veiligheidsdiensten en, uiteraard, werkgevers. Deze verschillende factoren zetten ongetwijfeld de grondrechten van de gebruiker onder druk.

2. Vrijheid van communiceren: samenspel van grondrechten

2.1 Uitingsvrijheid

In westerse landen zijn grondrechten van fundamenteel belang voor het functioneren van de mens. Communiceren is een wezenlijk kenmerk van het mens-zijn. Daarom heeft iedereen de vrijheid om te communiceren, of dat nu op een publieke plaats of een private plaats gebeurt. De communicatievrijheid is het recht om in alle vrijheid gedachten, ideeën en gevoelens via gelijk welk communicatiekanaal en communicatiemiddel te ventileren. Omgekeerd houdt communicatievrijheid ook de vrijheid in om net niet te communiceren, om niet aan het debat of gesprek deel te nemen.

De communicatievrijheid kan worden onderscheiden in de vrijheid van openbaarheid en de vrijheid van niet-openbare communicatie. De eerste betreft vrije meningsuiting zoals gewaarborgd door artikel 10 Europees Verdrag van de Rechten van de Mens en 19 van de Grondwet. Deze wordt gekenmerkt door het openbaar of niet-besloten karakter van de communicatie; deelname aan het publieke debat. Aldus wordt de communicatie in alle openheid gevoerd en is zij bijgevolg niet beperkt tot een welbepaalde kring van personen.
De tegenhanger van de openbare communicatie is de vrijheid om de communicatie niet openbaar, en dus niet voor iedereen toegankelijk, te voeren. De vrijheid om niet openbaar te communiceren wordt doorgaans als een deelaspect van het ruime privacybegrip beschouwd, dat hierna wordt toegelicht. Kenmerkend is het besloten karakter van de communicatie. Er wordt gecommuniceerd in beperkte of afgebakende kring zodat in principe geen toegang door derden wordt geduld. We spreken dan van “privécommunicatie”, communicatie dat niet bestemd is om door anderen te worden gehoord of te worden ontvangen. Of en in welke mate het gesprek ook buiten de kring van deelnemers openbaar kan gemaakt worden, is afhankelijk van de intentie van de deelnemers aan het gesprek en de context waarin het gesprek wordt gevoerd. In dat geval speelt het zogenaamde communicatiegeheim.

2.2 Privacy en persoonsgegevens

Het recht op privacy is ondertussen goed ingeburgerd. Omwille van zijn ruime formulering wordt dit grondrecht als een algemeen recht op privacy omschreven. Het recht op privacy omvat vier deelrechten: het recht op privéleven, gezin- en familie, woning en communicatie.
Maar wat houdt dit recht precies in? Het begrip “privacy” wordt ruim ingevuld en is niet beperkt tot een afweerrecht. Privacy is meer dan het recht om zich af te schermen van anderen. Behalve bescherming van de fysieke, psychische en morele integriteit, afstamming, identiteit, gezondheid, seksuele leven en de bescherming van uw persoonsgegevens, gaat privacy over ongestoord en vrij kunnen participeren in een complexe samenleving, los van elke overheidsbemoeienis of derden. Onder deze laatste vallen particulieren en andere private entiteiten, zoals SNS. Aldus is privacy niet beperkt tot een bepaalde kern waarbinnen het individu zijn levenswijze ongestoord kan invullen en zich tegelijkertijd afsluit van de buitenwereld. Nee, het omvat ook relaties met anderen aanknopen en ontwikkelen.

Uit de rechtspraak volgt dat de privacybescherming niet beperkt is tot de woning en evenmin ophoudt aan de muren van de onderneming of overheidsadministratie. Dit wordt logischerwijs afgeleid uit het gegeven dat werken als een belangrijk aspect voor het participeren in de maatschappij wordt beschouwd en een groot deel van het dagelijks leven inneemt. Er is dus geen reden om professionele activiteiten van de privacybescherming uit te sluiten. Want het is net op het werk dat de (meeste) opportuniteiten liggen om relaties met anderen aan te knopen en uit te bouwen. De privacybescherming geldt bijgevolg ook op de werkplaats, zij het, zoals verder zal blijken, tot op zekere hoogte.

Nauw verbonden met de privacy, is de bescherming van de persoonsgegevens. Hoewel de bescherming van de persoonsgegevens ondertussen een zelfstandige grondrechtelijke status heeft gekregen, wordt de bescherming van de persoonsgegevens vaak als een aspect van het ruime privacybegrip beschouwd. Een reden is dat persoonsgegevens iets zeggen over wie we zijn en wat we doen. Persoonsgegevens is alle informatie aan de hand waarvan iemand kan geïdentificeerd worden. Met “alle” informatie wordt gedoeld op gelijk welke objectieve informatie die herleidbaar is tot een bepaald persoon. Bij het communiceren op SNS moet bijgevolg rekening worden gehouden met dit juridisch kader (*infra*).

Uit bovenstaande volgt dat het invullen van privacy afhankelijk is van verschillende factoren. Conventies, tradities, ontwikkelingen in de technologie, organisatiestructuren van instellingen, de economie en de samenleving in zijn geheel spelen een rol. Daarbij moet rekening worden gehouden met het welzijn van de burger, de persoonlijke autonomie en de menselijke waardigheid. Wat onder de privacy wordt begrepen hangt bijgevolg af van de situatie en de maatschappelijke context waarin iemand zich bevindt.

Uitgaande van het dynamisch karakter van het privacyconcept, heeft de rechtspraak de reikwijdte van de bescherming van het privéleven en de correspondentie gaandeweg uitgebreid tot nieuwe communicatietechnologieën, zoals het internetgebruik en e-mailberichten. Ook binnen de arbeidsrelatie geldt deze bescherming.
De razendsnelle ontwikkelingen in de technologie en flexibiliteit dat van zowel de werkgever als de werknemer wordt gevraagd, maakt een onderscheid tussen professionele en privécommunicatie bovendien moeilijk, zo niet onmogelijk. Zo heeft de toenemende flexibiliteit van de arbeidsprestatie tot gevolg dat de notie “tijdens de werkuren” vervaagt of nog moeilijk te definiëren valt. Denken we bijvoorbeeld aan handelsreizigers, vertegenwoordigers en het fenomeen van het afwisselend of gedeeltelijk thuiswerken. Daarnaast worden beroepshandelingen niet zelden doorheen privéaangelegenheden gesteld waardoor het karakter van de communicatie alle vormen kan aannemen en op voorhand niet kan ingeschat of gestuurd worden. We gaan verder zien dat deze maatschappelijke tendens ook gevolgen heeft voor het controlerecht van de werkgever op het gebruik van het internet en SNS in het bijzonder.

3. Controlerecht van de werkgever

Zoals in de inleiding reeds aangegeven, zijn grondrechten niet absoluut. Naargelang de specifieke context kunnen de belangen van anderen uw en mijn aanspraken beperken. Voor onderhavige bijdrage gaat het om de zogenaamde prerogatieven van de werkgever: het gezags- en instructierecht van de werkgever. En deze prerogatieven brengen een controlerecht voor de werkgever met zich mee. Inderdaad, het controlerecht van de werkgever houdt in dat hij de werknemer kan controleren op de naleving van zijn bevelen, instructies, wetgeving en de in het bedrijf geldende reglementen. De werknemer is namelijk verplicht zijn werk zorgvuldig, eerlijk en nauwkeurig uit te voeren. Door het aangaan van een arbeidsrelatie stemt de werknemer noodzakelijkerwijs in met een zekere beperking van zijn grondrechten, waaronder de uitingsvrijheid en het algemeen recht op privacy. Maar het controlerecht van de werkgever is niet onbegrensd. De band van ondergeschiktheid van de werknemer, die inherent is aan de arbeidsrelatie, vertaalt zich niet in een ongelimiteerd controlerecht van de werkgever. Grondrechten en strafwetten werpen een barrière op tegen een permanente en disproportionele inmenging in de privacy- en communicatiegrondrechten van de werknemer.

Redelijk privacyverwachting

Precies omwille van de specifieke aard van de arbeidsrelatie kan de werknemer niet dezelfde privacy-aanspraken doen gelden op de werkplaats als in pakweg de privéwoning. Aangenomen wordt dat ondergeschiktheid, die inherent is aan de arbeidsrelatie, de privacyverwachting van de werknemer beïnvloedt. Het controle- en instructierecht van de werkgever veronderstelt namelijk een zekere mate van inmenging in privacybescherming op de werkplaats. Denken we bijvoorbeeld aan de toegangscontrole tot het bedrijf (via individuele badge), de aanwezigheidscontrole en het inloggen en invoeren van de geleverde dag-prestaties (controle op de arbeid). Welnu, dit controlerecht strekt zich ook uit over de toegang tot de digitale wereld.

Binnen de arbeidsrelatie worden de privacyverwachtingen overigens doorgaans onderhandeld en vastgelegd in een door de sociale partners afgesloten collectieve arbeidsovereenkomst. Het is immers een taak van de werkgevers- en werknemersvertegenwoordiging om sociale akkoorden af te sluiten waarbij gezocht wordt naar een evenwicht tussen de belangen van de werkgever en de belangen van de werknemer. De uitkomst van deze evenwichtsoefening resulteert in een pragmatisch afbakening van de privacybescherming. Wie buiten deze grenzen treedt, pleegt een ongeoorloofde inbreuk op de privacyverwachting en schendt daardoor het privacygrondrecht. Omgekeerd kan de werknemer geen rechtmatig beroep doen op - de verhoopte - privacybescherming wanneer hij buiten de grenzen van de afgesproken privacyverwachting treedt.

4 Algemeen juridisch kader

Naast de privacy en de communicatievrijheid is de wet van 8 december 1992 betreffende de verwerking van persoonsgegevens (WVP) een zeer belangrijk rechtsinstrument bij het uitwisselen van informatie op SNS. Deze wet waarborgt sinds 1992 de bescherming van het individu wanneer zijn of haar persoonsgegevens worden verwerkt of gebruikt. Onder persoonsgegevens wordt alle informatie verstaan aan de hand waarvan iemand kan geïdentificeerd worden. Voor triviale gegevens, zoals naam en adres, is de toestemming, een wettelijke regel of een zwaarwegend belang van de verantwoordelijke voor de verwerking voldoende om uw persoonsgegevens te verwerken Voor zogenaamde gevoelige persoonsgegevens gelden die strengere eisen omdat de verwerking van deze gegevens de kern van de privacybescherming kunnen raken. Het betreft gezondheidsgegevens, afstamming, etnische afkomst, ideologische of religieuze informatie en gerechtelijke gegevens. Voor deze laatste kan zelfs de toestemming van de betrokkene de verwerking van diens gegevens niet rechtvaardigen. Wat betreft de gerechtelijke gegevens, kan alleen een wet in de verwerking ervan voorzien.

De ontwikkelingen in de informatie- en communicatietechnologie maken het aanleggen van bestanden en het uitwisselen van persoonsgegevens makkelijker. Daarbij is het koppelen van persoonsgegevens een efficiënt hulpmiddel om, bijvoorbeeld gepersonaliseerde reclameboodschappen uit te sturen. Gebruikers van SNS zijn hierbij een makkelijk doelwit. Het samenbrengen van gegevens en het in verband brengen van gegevens genereert ongeziene mogelijkheden tot het aanleggen van profielen van personen. Meer en meer wordt de burger aan de hand van deze profielen beoordeeld. Het leidt geen twijfel dat op profielen gebaseerde beslissingen een gevoelige impact kunnen hebben op het maatschappelijke leven en de rechten en vrijheden van de burger. Hierdoor komt een zeer belangrijk beginsel van het gegevensbeschermingsrecht onder druk te staan, namelijk het beginsel van transparantie. Personen van wie de persoonsgegevens worden verwerkt moeten daarvan op de hoogte worden gebracht. Degene die persoonsgegevens verwerkt moet zich kenbaar maken en duidelijk aangeven waarom en waarvoor hij die persoonsgegevens wil gebruiken. In de praktijk is het echter vaak moeilijk, of zelfs onmogelijk, om na te gaan wie onze persoonsgegevens verwerkt.

De WVP biedt een algemeen wettelijk kader bij het verwerken van persoonsgegevens. Daardoor moeten de randvoorwaarden van deze wet in iedere regeling of overeenkomst die voorziet in de verwerking van persoonsgegevens opgenomen zijn. Als gevolg moet het verwerken van persoonsgegevens op SNS in overeenstemming zijn met deze randvoorwaarden. En dat is niet anders in de arbeidsrelatie. Vandaar dat ook arbeidsrechtelijke regelingen in het kader van de controle op het gebruik van e-mail en internet op het bedrijf in overeenstemming moeten zijn met de WVP. Controle van het e-mail- en internetgebruik veronderstelt immers de identificatie van de gebruiker en daarom de verwerking van zijn persoonsgegevens. Wanneer op de gegeven situatie geen arbeidsrechtelijke regeling van toepassing is, zal de WVP als vangnet dienen voor de rechtmatigheid van controle. Vandaar dat de spelregels over het gebruik van het internet en SNS tijdens de werkuren idealiter in een bedrijfsreglement worden vastgelegd.

5. Wat mag en wat mag niet?

Hiervoor werd een globale schets gemaakt van de belangen van de werknemer en de werkgever. In deze paragraaf wordt kort besproken hoe bovenstaande uiteenzetting antwoord kan geven op de vraag wat nu precies wel en niet mag, zowel voor de werkgever als de werknemer. Daarnaast rijst ook de vraag naar de bescherming van andere deelnemers aan de communicatie voor zover zij niet onder het gezag van dezelfde werkgever vallen.

5.1 Kan de werkgever meekijken?

Zoals uit bovenstaande volgt, kan de werkgever niet verbieden dat zijn werknemers tijdens de werkuren tot op zekere hoogte met privézaken bezig zijn. Rijst de vraag wanneer de werkgever zich wel met de communicatie van de werknemer kan bemoeien. Het is van belang te onderstrepen dat de werkgever de communicatie die via persoonlijke middelen van de werknemer verloopt niet kan controleren. De controle van de persoonlijke smartphone of computer van de werknemer is dus uit den boze. Indien de werknemer gebruik maakt van de internetverbinding van het bedrijf, dan kan de werkgever alleen de toegang tot en het gebruik van dit netwerk controleren. Wat betreft de door de werkgever ter beschikking gestelde communicatiemiddelen ligt dat anders. Daarbij wordt doorgaans onderscheid gemaakt tussen privé- en professionele communicatie. Maar zoals hiervoor reeds gezegd, kan de vraag worden gesteld of dat wel realistisch is? Met de convergentie van het communicatieveld en de mobiliteit van de arbeidssfeer is het onderscheid tussen privé- en professionele communicatie moeilijk aan te houden. Om dat onderscheid toch te kunnen behouden wordt door de Privacycommissie aanbevolen om bij de communicatie in dienstverband onderscheid te maken tussen privécommunicatie en professionele communicatie. Dat kan bijvoorbeeld door twee verschillende accounts in te voeren: een account voor privédoeleinden en een account waarmee louter werk gerelateerd is. De inhoud van de e-mailberichten met een beroepsmatig karakter zouden dan het voorwerp kunnen uitmaken van een inhoudelijke controle. Telkens wanneer de andere deelnemer een bericht ontvangt wordt hij van de mogelijkheid van controle gewaarschuwd. Wanneer de ontvanger de interactie vervolgens voortzet, wordt zijn impliciete toestemming verondersteld.

Het is maar de vraag of dit onderscheid onverkort op SNS kan toegepast worden. De communicatie op facebook verloopt niet via (gescheiden) e-mailaccounts. Aangenomen wordt dat SNS kunnen ondergebracht worden in openbare en niet openbare communicatiefora. Wanneer SNS voorzien in instellingen, privé-setting, die dat onderscheid mogelijk maken, althans op die manier voorhouden, dan gelden de hiervoor besproken richtlijnen. Communicatie die enkel voorbehouden is voor “vrienden” kan als besloten of niet voor iedereen toegankelijk worden beschouwd. Wie zonder de toestemming van alle deelnemers aan de communicatie toch op slinkse wijze kennis neemt van de communicatie van anderen kan strafrechtelijke vervolgd worden. Geldt dat ook voor de werkgever? Verdedigd kan worden dat deze vraag positief moet beantwoord worden, omdat de bescherming van het communicatiegeheim ook van toepassing is op de werkplaats. Dat is anders wanneer de communicatie op een voor iedereen toegankelijk forum wordt geplaatst. In dat geval is de toegang vrij en onbeperkt zodat de werkgever in principe kan meekijken. Een voorbeeld is Twitter en YouTube. Deze SNS is per definitie voor iedereen toegankelijk; als het ware een publieke plaats waar met een onbepaalde groep wordt gecommuniceerd.

Degene die communicatie post kiest vrij voor wie de communicatie toegankelijk is: Wall, via chat, “vrienden” of “vrienden van vrienden”. Men kan aannemen dat alleen de Wall als een publiek toegankelijke plaats wordt aanzien. De overige combinaties zijn vergelijkbaar met een besloten kring waarbij de communicatie alleen voor de gekozen categorie toegankelijk is. In zoverre de werkgever niet tot één van deze categorieën behoort, mag hij geen kennis nemen van de communicatie. Maar

duidelijkheid hierover is er (nog) niet. Zo is juridische kwaificatie van de setting “vrienden van vrienden” onzeker. Participanten kunnen overigens wel een afzonderlijk professioneel profiel aanmaken waardoor de communicatie voor de werkgever toegankelijk is. Door het profiel duidelijk een beroepsmatig karakter te geven, zou de werkgever controle op de communicatie kunnen uitoefenen.

5.2 Thuiswerk

Hiervoor hebben we opgemerkt dat de toenemende flexibiliteit van de arbeidsrelatie er toe leidt dat vaker thuis wordt gewerkt. Daardoor vervaagt de traditionele aanwijzing van de “werkplaats”. Kan de werkgever in dat geval uw internetgebruik controleren? Deze vraag moet genuanceerd en omzichtig beantwoord worden. Wanneer de werknemer vanuit zijn private plaats inlogt op de server van het bedrijf en op deze manier verbinding maakt met het internet lijkt controle van de werkgever aannemelijk. Dat is anders wanneer de werknemer (met de pc van het bedrijf) vanuit zijn woning buiten de professionele sfeer e-mailberichten verstuurd. Wanneer de werknemer zijn werktijd daarentegen grotendeels spendeert op SNS, dan moeten we onderscheid maken tussen publiek toegankelijke communicatie en besloten communicatie. Op publiek toegankelijke internetfora kan iedereen meekijken omdat de communicatie voor een onbepaald aantal personen toegankelijk is. In een besloten context is dat precies andersom. In welke mate is Facebook en Twitter een publiek toegankelijke dan wel besloten communicatieforum? Niet zelden heeft de werknemer (on)bewust zijn privacy-instellingen zo ingesteld dat iedereen de gesprekken kan volgen. Wanneer de communicatie beperkt is tussen ‘vrienden” zou de kennisname van de gesprekken onrechtmatig zijn. Het is echter de vraag of daarmee de werknemer de dans ontspringt. Steeds vaker wordt na een afweging van belangen het onrechtmatig verkregen bewijs toch aanvaard. Op die manier wordt de werknemer toch op straat gezet.

5.3 SNS buiten de werkuren

Het controlerecht van de werkgever is begrensd tot het einde van de werkdag. Het beslissingsrecht van de werkgever inzake de toegang tot het internet en participeren op SNS geldt dus alleen op de werkplaats. De werkgever kan het gebruik van sociale netwerken buiten de werkuren niet verbieden. Zijn gezag reikt niet zo ver dat hij zich met het doen en laten van zijn medewerkers buiten de kantooruren mag bemoeien of hun communicatie controleren. Daarnaast moet rekening worden gehouden met de privacy-aanspraken van de deelnemers aan de communicatie. Zonder de toestemming van alle deelnemers is de tussenkomst van de werkgever onwettig en zelfs strafbaar.
Niettemin kan de werkgever ook buiten de werkuren het gebruik van SNS beïnvloeden. Beiden moeten zowel tijdens de arbeidsrelaties als daarbuiten respectvol met elkaar omgaan. Zoals hierna zal blijken, zijn ongeoorloofde uitingen uit den boze. En dat geldt natuurlijk ook voor de deelnemers aan de communicatie. Alle deelnemers aan de communicatie moeten zich ervan bewust zijn dat ongepaste communicatie negatieve gevolgen kan hebben tijdens en buiten de arbeidsrelatie.

5.4 Ongeoorloofde en ondoordachte uitingen

Aldus reikt de uitingsvrijheid van de werknemer niet zo ver dat hij onfatsoenlijke zaken ten opzichte van de werkgever kan ventileren. Net zoals bij het gebruik van e-mailberichten, kunnen de gesprekken op sociale netwerksites ook ongeoorloofd zijn. Uit de schaarse rechtspraak die over het gebruik van SNS op de werkplaats voorhanden is, lijkt het uiten van ongeoorloofde of lasterlijke beweringen ten opzichte van de werkgever de kroon te spannen. Echter het uiting geven aan bepaalde gevoelens en opinies over de werkgever worden beschermd door het grondrechtelijk beschermde vrijheid van

meningsuiting. Een voorbeeld. Een werknemer laat zich op een SNS uit over de werkomstandigheden op de werkplaats. Uitingen zoals “dit is de meest saaie baan ooit” kunnen beschouwd worden als toelaatbare uitingen. Daarentegen kunnen uitingen zoals “het bedrijf sjoemelt met de bedrijfsresultaten” als laster en eerroof worden beschouwd.
Doorgaans gaat het om situaties waarbij werknemers op onbezonnen wijze informatie op sociale netwerken delen waarbij zelden worden gedacht aan de gevolgen van hun handelingen. Ook de werkgever kijkt en luister soms mee. Een werknemer die zich onterecht ziek meldt op het werk, begaat een inbreuk op de arbeidsovereenkomstenwet. Daarnaast mag een werknemer zonder de toestemming van de werkgever geen belangrijke of gevoelige bedrijfsinformatie wereldkundig maken.

5.6 Andere deelnemers aan de communicatie

De controle van SNS door de werkgever heeft nog een andere negatief gevolg. Hiermee komt namelijk de precaire positie van de andere deelnemers aan de communicatie op de voorgrond. Zij worden immers onrechtstreeks aan een controle van hun communicatie onderworpen.
De bescherming van het communicatiegeheim strekt zich uit tot alle deelnemers aan de communicatie. De bescherming geldt zowel voor de verzender als de ontvanger. Maar in de praktijk zal de ontvanger er zich lang niet altijd van bewust zijn dat zijn communicatie wordt gecontroleerd. Hoe wordt dat doorgaans opgevat? In de besproken CAO nr. 81 wordt geen aandacht besteed aan de communicatie bescherming van de andere deelnemer. Ook in het recente advies van de Privacycommissie inzake de cybercontrole op de werkplaats, wordt de problematiek van de andere deelnemers aan de communicatie niet of onvoldoende belicht. Opnieuw moet het aanhouden van onderscheiden e-mailaccounts soelaas brengen. Door te reageren of op eigen initiatief berichten te sturen, wordt zijn toestemming voor een mogelijke controle van de communicatie impliciet gegeven. Deze impliciete toestemming wordt doorgaans soms ook aangenomen wanneer de communicatie niet wordt aangemerkt als privéberichten. En, zoals gezegd, moeten ook zij die niet aan de werkgever van de ander gebonden zijn zich onthouden van lasterlijke, ongeoorloofde en schadelijke uitingen.

6 Internet policy: wat moet daar in staan?

Uit bovenstaande volgt dat het opmaken van een *social media policy* een must is. Daarin moet de werkgever duidelijk de doelstellingen van het reglement uiteenzetten. Tevens moet de procedure volgens welke de controle wordt uitgevoerd duidelijk omschreven worden en aan de werknemer kenbaar gemaakt worden.

Of en onder welke voorwaarden de werknemer toegang heeft tot het internet - en SNS in het bijzonder - is afhankelijk van de bereidwilligheid van de werkgever. De werkgever beslist namelijk zelf voor welke doeleinden de aan de werknemer ter beschikking gestelde instrumenten en communicatiekanalen kunnen gebruikt worden. Maar om een breder sociaal draagvlak te creëren, is het beter de werknemers(vertegenwoordigers) bij het opmaken van het reglement te betrekken. Een nuchtere kijk op de realiteit van vandaag leert ons echter dat het internetgebruik op de werkvloer moeilijk, zo niet onmogelijk, kan uitgesloten worden. Daarbij wordt aangenomen dat de digitale ruimte prioritair voor professionele doeleinden wordt gebruikt. Hoe de werkgever de toegang tot het internet organiseert, is door hem te bepalen, en, zoals gezegd liefst met inspraak van de werknemers.

Daarbij heeft de werkgever verschillende opties. Zo kan het internetgebruik toegezegd worden in functie van de specifieke taak van de werknemer, beperkt worden in tijd en ruimte en kan de toegang tot bepaalde websites worden afgeschermd. Er moet duidelijkheid worden verschaft omtrent de toegang tot het internet en de toegang tot SNS. Zo kan afgesproken worden dat het internet tijdens de werkuren toegankelijk. Naar gelang het model kan geopteerd worden voor een ongelimiteerd internetgebruik of gefaseerd gebruik naargelang de functie of de aanwezigheid op het bedrijf. Er kan bijvoorbeeld afgesproken worden dat slechts in de (middag)pauze toegang tot het internet mogelijk is. Via registratie van de login en individueel paswoord (of badge) kan de naleving ervan gecontroleerd worden. Bovendien kan de werkgever welbepaalde computers aanwijzen waarmee de werknemer op het internet kan surfen en communiceren.

In de tweede plaats wordt aanbevolen om in de policy op te nemen wat wel en niet kan gezegd worden op SNS, zowel tijdens of na de werkuren. Een en ander is niet zonder belang voor functies doe toegang hebben tot bedrijfsgeheimen, financiële informatie of andere gevoelige informatie die onder het beroepsgeheim of discretieplicht valt. Bovendien is het aanbevolen om ook aandacht te besteden aan de privacy-aanspraken van de deelnemers aan de communicatie. Worden zij verwittigd dat hun communicatie indirect kan gecontroleerd worden en op welke manier wordt dat kenbaar gemaakt?
Tot slot moet duidelijk worden gemaakt in welke gevallen en op welke manier tot controle van het internetgebruik kan worden overgegaan. Vanuit een breder perspectief is het aangewezen om ook het fenomeen van het cyberpesten een plaats te geven. Op die manier kan het reglement een algemene standpunt innemen ten aanzien van grensoverschrijdend gedrag.