VADEMECUM
SOCIALE MEDIA & ARBEIDSRELATIES

JURIDISCHE OMKADERING VAN DE CONTROLE OP HET GEBRUIK VAN SOCIALE NETWERKSITES OP HET WERK

AUTEUR: RONNY SAELENS

LSTS
LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES
VRIJE UNIVERSITEIT BRUSSEL
BELGIUM

EMSOC
User Empowerment in a Social Media Culture

DISCLAIMER:

De auteur is niet verantwoordelijk en kan niet aansprakelijk gesteld worden voor schade die rechtstreeks of onrechtstreeks het gevolg is van het volgen van de informatie in deze uitgave. Deze informatie werd gebaseerd wettelijke regeling rond internet- en e-mailgebruik in het algemeen en uit een aantal casussen uit de rechtspraak en kan daarom onderhevig zijn aan veranderingen.

Dit rapport kan teruggevonden en gedownload worden op:

www.ordeexpress.be/artikel/77/845/sociale-media-en-privacy-op-de-werkvloer
&
emsoc.be/5700-sociale-media-op-de-werkvloer

SAMENVATTING

Ontwikkelingen in communicatietechnologieën lijken niet te stoppen. Interacties gebeuren niet langer enkel via traditionele communicatiemiddelen zoals briefwisseling en telefonie. Ondertussen heeft communicatie via de digitale snelweg een belangrijke plaats in het maatschappelijke leven ingenomen. Sociale media vormen daarbij een geliefkoosd instrument. Maar de toename van sociale interacties via digitale applicaties is niet beperkt tot de huiskamer. Ook de ondernemerswereld blijft niet afzijdig. Bedrijven communiceren niet alleen via e-mail, maar zien ook de voordelen van sociale media. De vraag is dan welke invloed het gebruik van sociale media heeft op de arbeidsrelatie. Ondernemingen bepalen de mate van toegang tot sociale media. Als gevolg heerst er op het werk een spanningsveld tussen beroepsactiviteiten enerzijds en privéaangelegenheden anderzijds. Om een goed evenwicht te zoeken tussen het gezag- en controlerecht van de werkgever en de beleving van grondrechten van de werknemer moet toevlucht worden genomen naar bestaande regelgeving en rechtspraak. En dat is geen sinecure. De bestaande toepasselijke regelgeving lijkt niet zonder meer opgewassen tegen het gebruik van nieuwe communicatiekanalen op het werk. Tevens staat de rechtspraak over geschillen inzake het gebruik van sociale media op het werk nog in de kinderschoenen. Het afbakenen van publieke ruimten tegenover private plaatsen, enerzijds, en het onderscheid tussen privécommunicatie en zakelijke communicatie, anderzijds, blijken moeilijke hindernissen. Daarbij wordt doorgaans geen rekening gehouden met de andere deelnemers aan de communicatie. Zij moeten er blijkbaar rekening mee houden dat hun gesprekken kunnen gelezen worden. Of het gebruik van sociale media op het werk afzonderlijk geregeld moet worden, is maar de vraag. De huidige digitale communicatietechnieken zullen in de toekomst wellicht plaats maken voor nieuwe technieken. Misschien zijn goede en duidelijke afspraken op de onderneming waarbij rekening wordt gehouden met ieders belangen een beter middel dan innoverende regelgeving. Op die manier kan men snel inspelen op nieuwe fenomenen. In ieder geval blijft het persoonsgegevensbeschermingsrecht een goede bescherming bieden.

INHOUDSTAFEL

Wat je toont via sociale media zegt wel degelijk iets over je identiteit[1]

INLEIDING

1. Op 19 april 2013 bracht de krant *De Morgen* het schokkende nieuws dat een groot deel van de werkgevers de communicatie van hun medewerkers heimelijk leest.2 Uit een onderzoek van Vacature zou namelijk blijken dat bijna de helft van de werkgevers het mailverkeer van hun medewerkers in real time leest en ook telefoongesprekken afluistert. Een andere elektronische communicatietoepassing die op de werkplaats aanklopt, is het gebruik van sociale media. Sociale media, zoals facebook, You Tube, Twitter, LinkedIn, My Space en Google Plus, zijn een belangrijk aspect van het maatschappelijk leven geworden en hebben ondertussen ook de weg naar de onderneming gevonden.3 Ook daar blijven de bijwerkingen niet uit. Om maar enkele uit de schaarse voorbeelden te noemen. Dertien personen van het boordpersoneel van een Britse luchtvaartmaatschappij werden prompt ontslagen nadat ze zich zeer denigrerend over de passagiers op Facebook hadden uitgelaten. In een andere zaak kreeg een Amerikaanse dienster haar ontslag omdat ze op dezelfde sociale netwerksite had geklaagd over de zeer magere fooi. Een Belgische werknemer werd om dringende reden ontslagen omdat hij op Facebook kritiek uitte op zijn werkgever en tegelijk dreigende taal schreef over de directrice van de onderneming en een aantal collega's. Het zijn voorbeelden die in de rechtsleer en de media worden aangehaald over de gevolgen van het gebruik van sociale media op de werkplaats.4

2.Vandaag is het voeren van communicatie via de elektronische snelweg een belangrijk aspect van het maatschappelijke leven geworden. Dat is niet anders in de professionele wereld. Voor bedrijven is het zelfs een *must* om de concurrentie te kunnen behouden, bij te benen of sneller af te zijn. Producten worden online gepromoot, aangeboden en verkocht. Een bedrijf zonder professionele website is vandaag de dag *simply not done*. De spelregels inzake vraag en aanbod worden immers ook bepaald door de manier waarop de onderneming de voordelen van de elektronische snelweg weet te verzilveren. Daarbij zal de werkgever doorgaans moeten kunnen steunen op zijn medewerkers: aanknopen van eerste contacten, precontractuele onderhandelingen, verkoop en distributie. Daarvoor is de toegang tot het internet onontbeerlijk waarbij aangenomen wordt dat de digitale ruimte prioritair voor professionele doeleinden wordt gebruikt.

3. 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 en sociale media kan door de werkgever namelijk ook gebruikt worden als controlemiddel. Dat brengt ons bij een belangrijk spanningsveld tussen twee belangen en met een het centraal thema in deze bijdrage: de eerbiediging van de grondrechten van de werknemer, in het bijzonder het recht op privacy enerzijds en het controlerecht van de werkgever anderzijds. In dit overzicht stelt zich de vraag of en zo ja, in welke mate de werkgever het gebruik van sociale media tijdens en buiten de werkuren kan beïnvloeden.

4. De rechtspraak op het vlak van de controle over het gebruik van sociale media op de werkplek is schaars. De reden daarvoor is uiteraard het relatief gestaag inburgeringsproces van sociale media in de onderneming. In deze bijdrage belichten we het gebruik van sociale media binnen het huidig wettelijk kader inzake de bescherming van en de controle op het internetgebruik en hoe de rechtspraak daarop reageert.

---

[1] *De Morgen* 1 juni 2013, 'Hoe Facebook een carrière kan maken of kraken', Ben Caudron.

[2] *De Morgen* 19 april 2013, 'Bijna helft werkgevers controleert surfgedrag personeel'.

3 J. LORRE, , 'Facebook en arbeidsrecht: mysterium tremendum et fascinans', RW 2010-11, afl. 36, , 1499; Brussel 3 september 2013, onuitg.

[4] Zie onder meer J. LORRE, *o.c.*, 1499; S. COCKX, 'Sociale media in de arbeidsrelatie: 'vriend' of vijand?', *Or.* 2012, afl. 1, 15.

5. 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.

Deze bijdrage omvat vier delen. In het eerste deel wordt het privacyconcept en het controlerecht van de werkgever besproken, dat wordt voorafgegaan door korte en algemene beschouwing over het fenomeen sociale netwerken. Het tweede deel omvat een opsomming van de internationale normen, gevolgd aansluitend door het derde deel dat handelt over de nationale rechtsinstrumenten die al dan niet rechtstreeks betrekking kunnen hebben op het gebruik van sociale media op de werkplaats. Er zijn daarnaast ook nationale regelingen die van toepassing zijn op de controle van het internet- en e-mailgebruik op de werkplaats. Naast de bescherming van de persoonsgegevens en arbeidsrechtelijke regelingen, nemen ook strafwetten een belangrijke plaats in bij inbreuken op de privacybescherming van de werknemer. In het derde deel worden enkele knelpunten over het verzamelen en gebruik van persoonsgegevens in het licht van de bestaande rechtspraak besproken. In zowel het derde als het vierde deel komt een greep uit de rechtspraak met betrekking tot de traditionele controle op het internet – en e-mailgebruik op het werk aan bod. Uit de analyse zal blijken dat de rechtspraak verdeeld is over de reikwijdte van de communicatiebescherming op het werk. Tot slot wordt deze bijdrage afgerond met een vierde deel met enkele beschouwingen. Daarbij worden de bevindingen in onderhavig werk afgezet tegen het gebruik van sociale netwerken op het werk.

1 DEEL I: COMMUNICATIEVRIJHEID EN CONTROLERECHT

1.1 ALGEMEEN: SOCIALE NETWERKSITES (SNS)

6. De bijdrage richt zich voornamelijk op een bepaalde vorm van sociale media, namelijk Sociale Netwerksites (kortweg SNS). Er bestaat geen wettelijke noch een algemeen aanvaarde definitie van SNS.[5] 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.[6] Het is een virtuele sfeer waar personen niet alleen hun interesses delen, maar ook uiting geven aan gevoelens van liefde en leed die zij die ervaren worden in zowel de private als de professionele sfeer. Naast dergelijke uitingen kunnen ook foto's en ander audiovisueel materiaal aan het virtuele profiel toegevoegd worden,[7] 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 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 de actieve deelname.[8] 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 daarbij een belangrijke factor.[9] 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 werkgevers. Deze verschillende factoren zetten de bescherming van de privacy ongetwijfeld onder druk.

1.2 PRIVACY

7. Het privacybegrip wordt ruim ingevuld en is niet beperkt tot een afweerrecht. De reikwijdte van de privacybescherming is met andere woorden niet beperkt tot *the right to be let alone*, zoals Warren en Brandeis het op het einde van de negentiende eeuw omschreven. Privacy is meer dan het recht om zich af te schermen van anderen. Privacy gaat ook over ongestoord en vrij kunnen participeren in een complexe samenleving, los van elke overheidsbemoeienis. Het privacybegrip omvat tal van deelaspecten die onder de ruime en abstracte formulering van het privacybegrip begrepen worden. Niet alleen de fysieke, psychische en morele integriteit wordt beschermd. Vanwege de ontwikkelingen in de informatie- en communicatietechnologieën (ICT) pleegt men binnen het privacyconcept onderscheid te maken tussen drie soorten privacy: ruimtelijke privacy, rationele privacy en informationele privacy. Ruimtelijke privacy weerspiegelt het recht om afgeschermd van derden een leven te kunnen leiden. Relationele privacy heeft betrekking op het ongestoord relaties met anderen te kunnen aangaan, zoals het vertrouwelijk met anderen te kunnen communiceren. En ten slotte houdt de informationele privacy verband met de bescherming van de persoonsgegevens van de burger. Anderen wensen privacy niet te onderscheiden, maar gaat

[5] M. VERMEULEN & P. DE HERT, 'Toegang tot sociale media en controle door de politie. Een eerste juridische verkenning vanuit mensenrechtelijke perspectief', *Panopticon* 2012, afl. 33 (2), 259.

[6] W. BRUGGEMAN, 'Naar een nieuw concept sociale media voor de Belgische politie', *Panopticon* 2011, afl. 6, 37.

[7] J. LORRE, *l.c.*, 1499.

[8] G. G. FUSTER en S GUTWIRTH, 'Privacy 2.0?', *Privacy en persoonsgegevens*, Politeia 2009, losbl., afl. 27, Titel V, 213-227.

[9] *Ibid*.

het veeleer om aspecten van de privacy te kunnen beschermen tegen evaluaties van derden. Hoe de deelaspecten van de privacy afgebakend moeten worden, hangt af 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.[10] Wat onder de privacy wordt begrepen hangt bijgevolg af van situatie en de maatschappelijke context waarin iemand zich bevindt.[11]

8. Wat de bescherming van de persoonsgegevens betreft, is de Europese rechtspraak (nog) niet eenduidig over de vraag of *alle* persoonsgegevens onder de privacybescherming van artikel 8 (recht op privacy) van het Europees Verdrag voor de Rechten van de Mens (EVRM) vallen. Bij onder meer medische gegevens en informatie over seksuele geaardheid is dat wel het geval.[12] Dat zijn gegevens die tot de kern van de persoonlijke levenssfeer behoren. Toch zien we dat de Europese rechtspraak gaandeweg meer belang hecht aan de bescherming van de persoonsgegevens binnen het privacyconcept. Zo wordt gaandeweg de opslag, bewaring of gebruik van de gegevens onder de bescherming van artikel 8 EVRM begrepen.[13] Dat is vooral zo wanneer de burger niet op de hoogte is van de gegevensverwerking, geen toegang krijgt tot de opgeslagen informatie of niet duidelijk is voor wie de informatie bestemd is. Dat is niet zonder belang voor de problematiek van het gebruik van sociale media en sociale netwerksites in het bijzonder. De informatie dat op sociale netwerksites wordt gedeeld heeft vaak betrekking op individuen, en daarmee op persoonsgegevens. En naargelang het karakter van deze informatie zijn de randvoorwaarden strenger (*infra*).

9. Een moderne visie van het privacybegrip ziet privacy als een (deelaspect van de) individuele vrijheid. In deze visie is privacy het exponent van de individuele vrijheid. Privacy wordt gezien als bescherming tegen interventies van de overheid en particulieren in de autonomie – de zelfbeschikking - van de burger. Privacy is de vrijheid om invulling te geven aan die individuele vrijheid, om de levenswijze naar eigen inzichten te beleven en in te delen naar keuze.[14] Privacy is dan niet het recht om zich te kunnen verbergen, maar wel het recht om zich niet te moeten verbergen.[15] In een vrije samenleving gaat het daarom niet om de vraag of men niets te verbergen heeft. In tegendeel, de vrijheid van de burger betekent dat zijn doen en laten (privacy) niet de klok rond wordt gecontroleerd en geobserveerd.

---

[10] A.H. VEDDER, 'Privacy tussen ethiek en techniek', in S. NOUWT & W. VOERMANS (eds.) *Privacy in het informatietijdperk*, Den Haag: SDU 1996, 22.

[11] M.A.C. DE WIT, 'Privacy van werknemers in het informatietijdperk', *Arbeid*, 2002, afl. 6, 351. Deze auteur opteert in het kader van de bescherming van de privacy op de werkplaats voor de visie van Vedder omdat daar alle (mogelijke) soorten privacyaspecten onder begrepen kunnen worden en de maatschappelijke context waarin de persoon van wie de privacy in he spel is, zich bevindt. Daarmee wordt niet gezegd dat andere visies op het privacybegrip geen of minder privacybescherming op de werkplaats zouden bieden.

[12] Financiële gegevens, bijvoorbeeld, worden 'gevoelige persoonsgegevens' naargelang het gebruik dat ervan wordt gemaakt. Zo oordeelde het Europees Hof van Justitie dat de eenvoudige opslag door de werkgever van nominatieve gegevens betreffende de aan zijn personeel betaalde salarissen als zodanig weliswaar geen inmenging in de persoonlijke levenssfeer vormt, maar dat de mededeling van die gegevens aan een derde, in casu een overheidsorgaan, afbreuk doet aan het recht op eerbiediging van de persoonlijke levenssfeer van de betrokkene, ongeacht het latere gebruik van de aldus meegedeelde gegevens, HvJ 20 mei 2003 *Rechnungshof t./ Österreicherischer Rundfunk e.a. (c-465/00)* en *C. Neukom (c-138/1) en J. Lauremann (c-139/1) t./ Österreichischer Rundfunk*, www.curia.europa.eu/jurisp. Het Europees Hof van Justitie spreekt zich uit over de toepassing van Europese regelgeving, zoals het persoonsgegevensbeschermingsrecht (*infra*).

[13] Voor een diepgaande analyse van de inhaalbeweging van het Straatsburgse Hof, P. DE HERT, S. GUTWIRTH, Data Protection in de Case Law of Straatsbourg and Luxemburg: Constitutionalisation in action, in S. GUTWIRTH, *Reinvening Data Protection?*, Springer Science +Business Media, 2009, 3-44.

[14] Zie uitgebreid hierover S. GUTWIRTH, *Waarheidsaanspraken in recht en wetenschap*, Antwerpen-Apeldoorn, Maklu-VUBPRESS 1993, 614-656;

[15] P. DE HERT, 'Het verzamelen en gebruiken van visuele informatie: foto's, videosurveillance en verkeersradar, *Belgisch Politievakblad*, Politeia 1994, 9 oktober.

1.3 COMMUNICATIEVRIJHEID EN COMMUNICATIEGEHEIM

10. Iedereen beschikt over de vrijheid van 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. Communiceren is bovendien niet beperkt tot woorden en tekst, maar omvat ook (audio)visueel materiaal, zoals foto's en beelden (met gebarentaal).

11. De communicatievrijheid kan vervolgens worden onderscheiden in de vrijheid van openbaarheid en de vrijheid van niet-openbare communicatie. De eerste betreft vrije meningsuiting zoals gewaarborgd door artikel 10 EVRM en 19 van de Grondwet (GW). 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.

12. De tegenhanger van de openbare communicatie is de vrijheid om de communicatie niet kenbaar te maken. De vrijheid om niet openbaar te communiceren wordt doorgaans als een deelaspect van het ruime privacybegrip beschouwd. 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.[16] In dat geval speelt het zogenaamde communicatiegeheim dat op supranationaal niveau beschermd wordt door artikel 8 EVRM (privacy) en nationaal door artikel 22 GW en door enkele strafwetten wordt gewaarborgd (*infra*). Het betreft het zogenaamde communicatiegeheim dat als een deelaspect van de persoonlijke levenssfeer wordt beschouwd.

13. Het besloten karakter van communicatie hoeft evenwel niet meteen een risico te vormen voor de persoonlijke levenssfeer. Slechts wanneer dat wel het geval is, komt de bescherming van de persoonlijke levenssfeer op de voorgrond. In deze opvatting staat het communicatiegeheim bijgevolg niet noodzakelijk in verband met de privacybescherming, maar met de vertrouwelijkheid ervan.[17]

Drie opvolgende voorbeelden kunnen dit illustreren. Het karakter van de communicatie wordt in drie fasen onderscheiden: publiek karakter – besloten karakter zonder impact op de privacy – besloten karakter met impact op de privacy.

Voorbeeld 1

Als ik mij op een publieke plaats bevind en openlijk mijn opinie ventileer over mijn werkgever, dan geef ik uiting aan mijn communicatievrijheid. Mijn uitingen vinden niet alleen plaats op een openbare plaats, het is ook gericht aan een onbepaalde groep personen. Daardoor krijgen mijn uitingen een publiek karakter. Hier speelt de vrije meningsuiting.

[16] Over discussie van de plaats van de grondrechtelijke bescherming van het communicatiegeheim, L. ASSCHER, *Communicatiegrondrechten.*, Otto Cramwinckel Uitgeverij 2002, 13-26; W. STEENBRUGGEN, *Publieke dimensies van privé-communicatie*, Otto Cramwinckel Uitgeverij 2009, 44-60.

[17] Deze redenering bouwt voort op de discussie in de literatuur, L. ASSCHER, *Communicatiegrondrechten.*, Otto Cramwinckel Uitgeverij 2002, 13-26; W. STEENBRUGGEN, *Publieke dimensies van privé-communicatie*, Otto Cramwinckel Uitgeverij 2009, 44-60.

Voorbeeld 2

Wanneer ik mijn opinie op dezelfde plaats kenbaar maak, maar dan expliciet binnen een welbepaalde kring, dan speelt mijn communicatievrijheid opnieuw. Maar nu komt het besloten karakter op de voorgrond: de communicatie is alleen bestemd om door deze personen te worden gehoord. Het gesprek wordt als vertrouwelijk beschouwd; afgeschermd van bemoeienis van derden.

Voorbeeld 3

Wanneer de communicatie (terloops) ook betrekking heeft op mijn persoonlijke of familiale situatie, komen de bescherming van de communicatie- en privacybescherming samen. In dat geval wordt een extra bescherming aan mijn communicatievrijheid toegevoegd, namelijk de bescherming van de persoonlijke levenssfeer. Familiale zaken vallen ontegensprekelijk onder het privacybegrip.[18]

1.4. CONTROLERECHT VAN DE WERKGEVER

14. Op het eerste gezicht lijkt het verbazingwekkend dat SNS door de werkgever als een vorm van toezicht wordt gebruikt. Inderdaad, het controlerecht van de werkgever houdt in dat hij de werknemer kan controleren op de naleving van zijn bevelen, instructies, richtlijnen en de in het bedrijf geldende reglementen. De werknemer is immers verplicht zijn werk zorgvuldig, eerlijk en nauwkeurig uit te voeren.[19] Door het aangaan van een arbeidsrelatie stemt de werknemer immers noodzakelijkerwijs in met een zekere beperking van zijn grondrechten, waaronder het recht op privacy.[20] Maar het controlerecht van de werkgever is niet onbegrensd. De band van ondergeschiktheid van de werknemer, dat inherent is aan de arbeidsrelatie, vertaalt zich niet in een ongelimiteerd recht van toezicht in hoofde van de werkgever. Onder voorbehoud van wat volgt, vormen grondrechten en strafwetten een barrière tegen permanente en disproportionele inmenging in de privacy- en communicatiegrondrechten van de werknemer. Wat betreft de controle op het gebruik van internet en SNS in het bijzonder komen minstens twee grondrechten op de voorgrond: de vrije meningsuiting en het recht op privacy. In de rechtspraak inzake de controle over het gebruik van e-mail en internet op het werk wordt vooral de privacybescherming opgeworpen. Binnen de context van de controle op het gebruik van sociale media zal de uitingsvrijheid ook een belangrijke rol spelen. Bepaalde internetfora zoals Twitter zijn discussieplatforms waarbij de uitingsvrijheid volop speelt. Bij andere sociale netwerksites, zoals Facebook, kan zowel de vrije meningsuiting als de privacybescherming in het geding zijn (*infra*).

15. Tegenover het instructie- en controlerecht van de werkgever staat niet alleen het bezwaar tegen verborgen controles. Het bezwaar tegen de privacy-inmenging op de werkplaats bestaat er ook in dat wat de werknemer (niet) verborgen wil houden, toch geregistreerd en bewaard wordt. Het gaat op de werkplaats met andere woorden niet zozeer om het recht op geheimhouding van het privéleven, dan wel om het recht op de eerbiediging van de

[18] Het vertrouwelijk karakter van informatie kan verschillend worden ingevuld. Vertrouwelijke informatie kan bijvoorbeeld ook slaan op zakelijk geheimen. Zakelijke geheimen *as such* vallen niet onder de privacybescherming. Aan de andere kant kan deze informatie wel door het communicatiegeheim beschermd worden wanneer dat in besloten kring gebeurt. Medische gegevens worden daarentegen als vertrouwelijk beschouwd en behorende tot de kern – innerlijke cirkel – van de persoonlijke levenssfeer. Medische gegevens kunnen bijgevolg worden beschermd door de communicatievrijheid én de privacy. Ook financiële informatie wordt doorgaans als vertrouwelijk bestempeld. Maar uit Europese rechtspraak blijkt dat opslag van financiële informatie, zoals loon, op zich geen risico vormt voor de persoonlijke levenssfeer. Daarentegen wordt het *doorgeven* aan *derden* van deze informatie als een risico voor de privacybescherming aanzien (HvJ 20 mei 2003 *Rechnungshof t./ Österreicherischer Rundfunk e.a. (c-465/00)* en *C. Neukom (c-138/1) en J. Lauremann (c-139/1) t./ Österreichischer Rundfunk*).

[19] Art. 17 wet van 3 juli 1978 betreffende de arbeidsovereenkomsten (WAO).

[20] R. DELARUE, 'Bescherming van de privacy in de onderneming en de begrenzing van de patronale prerogatieven', *SRK* 1992, 135.

fundamentele aspecten van de eigen levenswijze die in het gedrang komt bij een bovenmatige controle van het doen en laten van de werknemer.[21] Daarbij neemt de bescherming van communicatie (besloten karakter) een bijzondere plaats in. Kan de werknemer vrij communiceren tijdens de arbeidsrelatie? Waar ligt de grens? Welke spelregels moet de werkgever naleven om de bescherming van het communicatiegeheim te doorbreken? Wat is de waarde van de "toestemming" van de werknemer en welke gevolgen heeft de toestemming van de werknemer voor de andere deelnemer aan de communicatie? Complexe vragen die niet zonder meer eenduidig kunnen beantwoord worden.

1.5 PRIVACY OP HET WERK: STRAATSBURGSE RECHTSPRAAK

16. Op internationaal niveau wordt het recht op privacy beschermd door artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) en op Europees niveau door artikel 7 van het Handvest van de Grondrechten van de Europese Unie.[22] Op nationaal niveau wordt de privacy beschermd door artikel 22 van de Grondwet (GW). Artikel 8 EVRM beschermt het recht op privéleven, het gezinsleven, de woning en de communicatie. De bescherming van de woning en de briefwisseling is opgenomen in artikel 22 GW. Zij worden afzonderlijk beschermd door respectievelijk de artikelen 15 en 29 GW. Niettegenstaande artikel 8 EVRM ruimer geformuleerd wordt, is artikel 22 GW gewild geschreven naar het model van artikel 8 EVRM.[23]

17. Het recht op privacy is echter niet absoluut. In het tweede lid van artikel 8 EVRM worden de voorwaarden opgesomd waaronder inmenging in het privacygrondrecht toegelaten is. Zo moet de inmenging noodzakelijk zijn en de in het tweede lid limitatief opgesomde legitieme doeleinden nastreven.

Artikel 8 EVRM luidt als volgt:

> "1. Een ieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
>
> 2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid of het economische welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen".

18. Uit de rechtspraak van het Europees Hof voor de Rechten van de Mens volgt dat de privacybescherming niet beperkt is tot de woning en evenmin ophoudt aan de muren van de onderneming. Het privacybegrip is niet afgelijnd of beperkt tot een limitatieve lijst van aspecten die onder het privacybegrip worden begrepen. Integendeel, privacy is dynamisch en context gebonden. 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, respect voor het recht op privacy moet tot op zekere hoogte ook het recht inhouden om relaties met anderen aan te knopen en te ontwikkelen. Daarom is er volgens het Straatsburgse Hof geen reden om professionele activiteiten van de privacybescherming uit te sluiten. Want het is net op het werk dat de (meeste) opportuniteiten

[21] P. DE HERT en S. GUTWIRTH, 'Oude en nieuwe wetgeving op controletechnieken in bedrijven', *SRK* 1995, afl. 3, 108. Zie voor een evolutie in de controle op de werkplaats via moderne technieken, P. DE HERT en S. GUTWIRTH, 'Controletechnieken op de werkplaats' (Deel 1 & 2), *Or.* 1993, 93-109, 125-147.

[22] Het Handvest van 18 december 2000 is sinds 1 december 2009 bindend in de Europese Unie door het Verdrag van Lissabon

[23] *Parl. St.* Kamer 1992-93, nr. 997/5, 12.

liggen om relaties met anderen aan te knopen en uit te bouwen.[24] De privacybescherming geldt bijgevolg ook – tot op zekere hoogte - op de werkplaats.

19. Daarmee is nog niet gezegd welke aspecten onder de bescherming van het recht op privacy begrepen worden. Naast privéleven beschermt artikel 8 EVRM ook het recht op bescherming van de communicatie. Geldt de bescherming van de communicatie ook op de werkplaats? Uitgaande van het dynamisch karakter vaan het privacyconcept, heeft het Mensenrechtenhof de reikwijdte van de bescherming van het privéleven en de correspondentie gaandeweg verruimd tot nieuwe technologieën. Nadat het Hof in 1978[25] de bescherming van het privéleven en correspondentie in artikel 8 lid 1 EVRM had verruimd tot telefoongesprekken, kon de bescherming van het communicatiegeheim in de arbeidsrechtelijke sfeer niet uitblijven. Voortbouwend op haar eerdere rechtspraak, dat onder meer betrekking had op telefoongesprekken op de werkplek, benadrukt het Hof dat het begrip correspondentie ruimer is dan privécommunicatie en bijgevolg ook betrekking heeft op professionele communicatie.[26]

20. Het was voorspelbaar dat nieuwe elektronische communicatiemiddelen binnen de professionele sfeer niet aan de privacytoets van het Straatsburgse Hof zouden kunnen ontsnappen. Hoewel het Hof zich nog niet heeft moeten uitspreken over de controle op het gebruik van SNS in de arbeidsrelatie, lijkt met het *Copland*-arrest alle twijfel weggenomen. In deze zaak oordeelde het Hof niet alleen dat ook het e-mailverkeer binnen de professionele relatie onder de privacybescherming van artikel 8 EVRM valt. Met een ogenschijnlijke vooruitblik zegt het Hof in één adem dat niet valt in te zien waarom informatie verkregen door controle over het gebruik van het internet niet onder het privacyconcept zou vallen.[27] Het lijkt daarom verdedigbaar dat ook het gebruik van sociale media onder de reikwijdte van de begrippen “privéleven” en “correspondentie” kan gerekend worden.

21. Zoals gezegd is het recht op privacy is niet absoluut. Het tweede lid van artikel 8 voorziet dat onder voorwaarden de privacy van de burger kan beperkt worden. Een analyse van de beperking op de privacybeleving (op het werk) is slechts toegestaan wanneer de inmenging:

1) Bij wet voorzien is (legaliteitsbeginsel), waarbij het begrip “wet” een materiele invulling heeft, zodat ook rechtspraak en zelf ongeschreven recht onder “wet” kan begrepen worden. Voorwaarde is dat de regel voldoende toegankelijk is en de burger zijn gedrag kan afstemmen.
2) Voor wettige doeleinden (legitimiteitsbeginsel – finaliteitsbeginsel)
3) En bovendien nodig is in een democratische samenleving (noodzakelijkheids- en proportionaliteitsbeginsel)

De wettige doeleinden zijn:

De nationale veiligheid of het economische welzijn van het land;

Het voorkomen van wanordelijkheden en strafbare feiten;

De bescherming van de gezondheid of de goede zeden;

[24] EHRM 16 december 1992, *Niemietz v. Duitsland*.

[25] EHRM 6 september 1978, *Klass v Duitsland*.

[26] EHRM 2 augustus 1984, *Malone v. Verenigd Koninkrijk*; EHRM16 december 1992, *Niemietz v. Duitsland*; EHRM 25 juni 1997, *Halford v. Verenigd Koninkrijk*. Deze visie is natuurlijk ook voor een stuk gebaseerd op de wetenschap dat de we een groot deel van leven op het werk doorbrengen.

[27] EHRM 3 april 2007, *Copland v. Verenigd Koninkrijk*, § 41.

Of voor de bescherming van de rechten en vrijheden van anderen.[28]

22. Omwille van de specifieke aard van de arbeidsrelatie kan de werknemer echter niet dezelfde "privacyverwachting" doen gelden op de werkplaats als in pakweg de privéwoning. Aangenomen wordt dat ondergeschiktheid, dat inherent is aan de arbeidsrelatie, de privacyverwachting van de werknemer beperkt. 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).

23. Binnen 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. Het resultaat 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 extra privacybescherming wanneer hij buiten de grenzen van de afgesproken privacyverwachting treedt.

Voorbeeld:

Het bedrijf beschikt over een intranet en internettoegang. Het gebruik van internet is alleen toegelaten voor werknemers met een duidelijk omschreven functie. De andere werknemers kunnen gebruik maken van het intranet. Een werknemer die niet de juiste functie heeft, en toch gebruik maakt van internet tijdens de werkuren, verschaft zich op ongeoorloofde wijze toegang tot het internet. Wanneer het bedrijf beschikt over een wettig ingevoerd controlesysteem om ongeoorloofd internetgebruik te onderzoeken, moet de werknemer deze controlemaatregel van de werkgever dulden. Op zichzelf is deze controlemaatregel geen schending van het recht op privacy van deze werknemer.

---

24. De werkgever moet de controle van het internet- en e-mailgebruik op de werkvloer kenbaar maken. Het moet voor de werknemer namelijk duidelijk zijn wanneer en waarom controle kan uitgevoerd worden. Bijgevolg is heimelijke controle van het internet- en e-mailgebruik op het werk in principe ongeoorloofd. Maar deze (onbewuste) "vergetelheid" wordt niet zelden ondergeschikt gemaakt aan de waarheidsvinding. Niet zelden wordt door de rechter het beoogde en verworven resultaat afgewogen tegen de vastgestelde onregelmatigheid. Daarbij

[28] Hoewel de legitieme doeleinden limitatief zijn opgesomd, blijkt duidelijk dat de beperkingsgronden toch ruim kunnen omschreven worden. Zo kan de controle op het internetgebruik (inclusief sociale media) quasi onder alle doeleinden geschaard worden. Het is dan ook niet verwonderlijk dat het Straatsburgse Hof aan de legitimiteitstoest niet zoveel belang hecht.

zal het inroepen van de privacybescherming vaak aanzien worden als een manier om de bestraffing van het wangedrag te ontlopen waardoor de rechter meer gewicht zal toekennen aan de waarheidsvinding.[29]

Voorbeeld: camerabewaking

Een werkgever installeert een verborgen camera teneinde het vermoeden van het plegen van diefstal door de kassierster vast te stellen. De mogelijkheid tot controle is niet voorafgaand bekendgemaakt. Ondanks de onwettigheid van de controlemaatregel oordeelt de rechter dat de camerabeelden toch als bewijs worden aanvaard. Het ophelderen van de diefstal weegt zwaarder dan de schending van het privacygrondrecht.

Voorbeeld: internetgebruik

Op een bedrijf zijn de werknemers op de hoogte van het ICT-policy. In strijd met het ICT-beleid maakt de werknemer op buitensporige wijze gebruik van het internet via een bedrijfscomputer. Zonder de werknemer de waarschuwen wordt op de computer een *protocol analyser* geïnstalleerd waardoor een analyse van het individueel gebruik van het internet door de werknemer mogelijk wordt gemaakt. Ondanks deze onregelmatigheid wordt het gebruik van het onwettig bewijs om het ongeoorloofde internetgedrag van de werknemer aan te tonen toch toegelaten.[30]

1.6 KARAKTER VAN DE COMMUNICATIE

25. Een ander heikel punt blijft de discussie over het onderscheid tussen professionele en privécommunicatie. De razendsnelle ontwikkelingen in de technologie en flexibiliteit dat van zowel de werkgever als de werknemer wordt gevraagd, maakt dat dit onderscheid vaak moeilijk, zo niet quasi onmogelijk kan gemaakt worden. Dat blijkt niet alleen uit de hiervoor besproken Europese rechtspraak, maar ook uit de mobiliteit van de arbeidsrelatie waarbij de notie "tijdens de werkuren" vervaagt of eveneens moeilijk te definiëren is. Denken we bijvoorbeeld aan handelsreizigers, vertegenwoordigers en het fenomeen van het afwisselend of gedeeltelijk thuiswerken.[30] Niet zelden worden beroepshandelingen doorheen privéaangelegenheden gesteld waardoor het karakter van de communicatie alle vormen kan aannemen en op voorhand niet kan ingeschat worden. Verder gaan we zien dat bepaalde Belgische rechtspraak toch alles in het werk stelt om het onderscheid tussen zakelijke communicatie en

[29] R. DE CORTE, 'De achterkant van de privacy: kan het beroep op privacy leiden tot straffeloosheid?' noot onder Gent 22 maart 2002, *NJW* 2003, 798-810; Zie hierover ook P. VAN EECKE en B. OOMS, 'De controle van het e-mail- en internetgebruik door de werkgever in België: ambiguïteit in de rechtspraak', noot onder Arbrb. 17 oktober 2005, Brussel 13 september 2005 en Gent 9 mei 2005, *Compterr.* 2006, afl. 44, 107-120. Dit heeft vooral te maken met een gewijzigde visie over het lot van het onrechtmatig verkregen bewijs. Traditioneel werd het bewijs dat op onwettige manier wet verkregen uit de debatten geweerd. Als gevolg mocht de rechter het geweerde bewijs niet aan aanmerking nemen bij het vormen van zijn oordeel. Door het zogenaamde Antigoon-arrest van 14 oktober 2003 kwam daar verandering in. Sindsdien is bewijsuitsluiting aan strenge regels onderworpen. Onrechtmatig verkregen bewijs kan nog slechts worden uitgesloten wanneer de norm op straffe van nietigheid is voorgeschreven, de betrouwbaarheid van het bewijs is aangetast of door het gebruik van het bewijs het recht op een eerlijk proces is geschonden (B. DE SMET, 'Criteria voor de beoordeling van onrechtmatig verkregen bewijs', noot onder Cass. 4 november 2007, *RW* 2008-09, 111-113) Hoewel het Hof van Cassatie in een arrest van 10 maart 2008 oordeelt dat de Antigoontoets ook in een sociaalrechtelijke zaken moet toegepast worden, blijft de discussie levendig over de vraag of deze nieuwe bewijsuitsluitingsleer rechtspraak zonder meer in de civiele rechtspraak kan gelezen worden, (F. KEFER, 'Antigone et Manon s'invitent en droit social. Qeulqeus propos sur la légalité de la preuve, *RCJB* 2009, 325-352; F. KEFER, La légalité de la preuve confrontée au droit à la vie privée', in G. DE LEVAL (ed.), *La preuve et la difficile quête de la vérité judiciare*, Luik, Anthémis 2011, 1758; K. KILDONCK, 'Privacy werknemers. Onrechtmatig verkregen bewijs op het werk', *NJW* 2010, 181-183. Zo weigerde het hof van beroep te Brussel in een arrest van 7 februari 2013 het hof van beroep te Brussel in een arbeidszaak de Antigoontoets toe te passen. Zie hierover Y.S. VAN DER SYPE, '(Anti)Antigoon in het arbeidsrecht', *P&I* 2013, afl. 4, 198-199. Ondertussen ligt een wetsvoorstel om de drie opgesomde voorwaarden voor bewijsuitsluiting in een wet te gieten (Wetsvoorstel tot wijziging van het Wetboek van Strafvordering wat betreft de nietigheden, *Parl. St*. Kamer 2010, nr. 53 0041/1 en nr. 53 001/3.

[30] Een voor beeld is het zogenaamde telewerk. Het telewerk wordt geregeld door de collectieve arbeidsovereenkomst nr. 85 van 9 november 2005. Net zoals de verder in deze bijdrage te bespreken CAO inzake de controle van de online-communicatiegegevens, is de CAO nr. 85 alleen van toepassing in de private sector, en dus niet op de overheidssector.

privécommunicatie bloot te leggen om op die manier de controle van de communicatie van de werknemer te rechtvaardigen. Doorgaans wordt daarbij overigens geen aandacht besteed aan de deelnemer aan de communicatie, waardoor zijn communicatiebescherming zeer problematisch wordt.

Voorbeeld:

Een vertegenwoordiger neemt tijdens een vrij weekend de tijd om via de computer op het bedrijf enige contacten te leggen met klanten. Tevens onderhoudt hij via een sociale netwerksite contacten met “vrienden”. Uit de gegeven feitelijke omstandigheden is niet ontegensprekelijk vast te stellen of er sprake is van professionele dan wel privécommunicatie. Daarnaast stelt zich de vraag of van de deelnemers aan de communicatie (klanten en “vrienden”) kan verwacht worden dat zij er rekening moeten mee houden dat hun gesprekken aan een controle van de werkgever van de vertegenwoordiger onderworpen worden.

---

26. Uit het bovenstaande blijkt dat het privacyconcept een complexe aangelegenheid is waarbij de plaats van het communicatiegeheim binnen de privacy niet ontegensprekelijk vast staat. Tegelijk speelt het spanningsveld tussen de bescherming van de privacy (en communicatiegeheim) en de patronale prerogatieven ten aanzien van het instructie en controlerecht van de werkgever. In dat verband beschikken zowel de werkgever als de werknemer over wettelijke instrumenten om hun respectievelijke belangen te waarborgen. Hierna volgt een overzicht van de bestaande internationale en nationale juridische instrumenten

2 DEEL II: JURIDISCH KADER

27. In deze paragraaf worden de juridische instrumenten belicht die van toepassing zijn op de controle op het gebruik van internet op de werkplaats. Zowel op supranationaal als op nationaal niveau ontbreekt een wettelijke regeling over het gebruik van sociale media in de onderneming. Dat neemt niet weg dat enkele fundamentele beginselen uit het gemeen recht en enkele specifieke wettelijke regelingen van toepassing (kunnen) zijn op de controle van het gebruik van SNS.

2.1 SUPRANATIONAAL

28. Het is ook de Raad van Europa niet ontgaan dat door een gebrek aan een afgelijnd wettelijk kader in verband met ongeoorloofd gebruik van het internet door de werknemer enerzijds en de ongebreidelde cybersurveillance door de werkgever anderzijds de bescherming van de grondrechten in het gedrang komen. Dat heeft geleid tot een omvangrijke catalogus van wettelijke regelingen en aanbevelingen die op supranationaal niveau bewerkstelligd werden. Niet alle hierna te bespreken regelingen zijn specifiek voor de arbeidsrechtelijke sfeer opgemaakt. Wat alle rechtsinstrumenten wel gemeen hebben, is dat de verwerking van informatie over de werknemer (persoonsgegevens) op een eerlijke en rechtmatige manier moet gebeuren. Daarbij geldt dat controletechnieken slechts bij uitzondering kunnen aangewend worden en geheime observatie slechts mogelijk is in de gevallen door de wetgever bepaald. Een voorafgaande algemene toestemming van de werknemer op de beperking van het recht op privacy wordt niet aanvaard.

2.1.1 Algemene rechtsinstrumenten

29. Wanneer sprake is van het verzamelen, opslaan en gebruiken van informatie over het gedrag van de werknemer komt de werkgever op het terrein van het persoonsgegevensbeschermingsrecht. Van zodra informatie wordt verwerkt aan de hand waarvan een persoon kan geïdentificeerd worden, speelt de regelgeving inzake het persoonsgegevensbeschermingsrecht of *data protection*.

30. Traditioneel is de wettelijke omkadering van de bescherming van de persoonsgegevens gebaseerd op artikel 8 EVRM. Aldus wordt de bescherming van de persoonsgegevens als een deelaspect van het ruimere privacybegrip van artikel 8 EVRM beschouwd. Daarbij denken we in de eerste plaats aan het Verdrag nr. 108 van 18 september 1980 van de Raad van Europa dat de personen met betrekking tot geautomatiseerde verwerking van persoonsgegevens beschermt. Dit verdrag schept een internationaal wettelijk kader voor de verdragstaten (dat ruimer is dan de Europese Unie) ten aanzien van de geautomatiseerde verwerking van persoonsgegevens en werd door België pas in 1993 door de wet van 8 december 1992 betreffende de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens geconcretiseerd (*infra*).[31]

31. Omwille van de verschillen binnen de lidstaten van de Europese Unie inzake het persoonsgegevensbeschermingsrecht en de belemmering voor de interne markt, kwam ten behoeve van de harmonisatie op Europees niveau de Richtlijn 95/46/EC van 25 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens tot stand.[32] In de Richtlijn werden de basisprincipes van het Verdrag nr. 108 overgenomen en verder uitgewerkt. Hoewel deze richtlijn drie jaar na deze datum in de nationale rechtsordes van de lidstaten moest

[31] *BS* 18 maart 1993

[32] Deze Richtlijn wordt momenteel herzien. Zie hierover P. DE HERT en V. PAPAKONSTANTINOU, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', *Computer law & Security Review* 2012, 130-142.

geïmplementeerd zijn, werd de richtlijn in België pas in 1998 omgezet door de wet van 11 december 1998 tot omzetting van de Richtlijn 95/46/EG van 25 oktober 1995.[33] Door deze wet werd de oorspronkelijke wet op de verwerking van persoonsgegevens van 8 december 1992 aangepast.[34] Binnen het bestek van deze bijdrage volstaat het te vermelden dat de bescherming van persoonsgegevens van Richtlijn 95/46/EG van 1995 niet beperkt is tot geautomatiseerde verwerking van persoonsgegevens. Ook manuele bestanden met persoonsgegevens worden beschermd. Daarnaast ligt sinds de Richtlijn de nadruk op de verwerking van persoonsgegevens terwijl het Verdrag nr. 108 zich (eerder) focust op de houder van het bestand. Gaandeweg rees het besef dat het risico voor de privacybescherming van de persoonsgegevens in de aard van de verwerking ligt. Denk bijvoorbeeld aan het aanleggen van profielen met persoonsgegevens voor marketingdoeleinden. Het samen en in verband brengen van persoonsgegevens via informaticatoepassingen (algoritmes) kan een gepersonaliseerd beeld van iemand genereren die voorheen voor niemand kenbaar was, ook niet voor de betrokkene. Zo krijgt de betrokkene een bepaalde sociale identiteit aangemeten, zonder daar vat op te hebben, met allerlei verwachtingen en anticipaties tot gevolg, die dan weer een bedreiging zijn voor zijn autonomie.[35] Momenteel ligt een wijzigingsvoorstel op tafel die de bescherming van persoonsgegevens op bepaalde punten wil versterken, zoals ten aanzien van het aanleggen van profielen, gebruik van persoonsgegevens binnen en door sociale medianetwerken en het invoeren van een recht op vergetelheid.[36]

32. Ondertussen heeft de bescherming van de persoonsgegevens sinds 1 december 2009 zelfstandig plaats gekregen in het Handvest van de grondrechten van de Europese Unie. In het Handvest worden het recht op bescherming van de privacy (art. 7) en de bescherming van persoonsgegevens (art. 8) netjes onder elkaar maar afzonderlijk vermeld. Op die manier wordt duidelijk dat ook persoonsgegevens die niet onder de ruime privacybescherming vallen ook een grondrechtelijke waarborg genieten.

33. De besproken Richtlijn maakt het mogelijk dat het wettelijke kader wordt aangevuld met sectorale wetgeving. In het telecommunicatielandschap is de Richtlijn 2002/58/EG van 12 juli 2002 als een *lex specialis* ten opzichte van de Richtlijn 95/46/EG opgevat. De Richtlijn 2002/58/EG regelt namelijk onder meer de bescherming van de privacy in de telecomsector, met name in het bijzonder de bescherming van het telecommunicatiegeheim.[37] Ook deze Richtlijn is van toepassing in de arbeidsrechtelijke sfeer wat betreft de controle van het internetgebruik in het algemeen en de controle van de telecommunicatie in het bijzonder. De Richtlijn stipuleert uitdrukkelijk dat de nodige maatregelen worden getroffen om de vertrouwelijkheid van de communicatie via openbare communicatienetwerken en openbare elektronische communicatiediensten te beschermen (art. 5 lid 1). Deze bescherming geldt zowel voor de inhoud van privécommunicatie en zakelijke communicatie als voor de gegevens over die communicatie. Wat betreft de zakelijk communicatie laat de Richtlijn wel een uitzondering toe met betrekking tot de *registratie* van zakelijke communicatie met het oog op de bewijslevering van de zakelijke transacties en communicatie (art. 5 lid 2). In tegenstelling van wat deze uitzondering doet vermoeden, kan deze uitzondering ons inziens geen vrijgeleide zijn als om de telecommunicatie op de werkvloer te controleren.

---

[33] Wet van 11 december 1998 tot omzetting van de Richtlijn 95/46/EG van 25 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en het vrije verkeer van die gegevens, *BS* 3 februari 1999.

[34] Uitgebreid hierover D. DE BOT, *Verwerking van persoonsgegevens*, Kluwer 2001, 403 p.

[35] R. SAELENS, P. DE HERT, S. GUTWIRTH, Openbaarheid van rechtspraak en het verwerken van persoonsgegevens: categorisch denken vermijden', *AM* 2012, afl. 6, 520-523. Vgl. M. HILDEBRANDT, 'Profiling and the Identitty of the European citizen', in M. HILDEBRANDT en S. GUTWIRTH (eds.) *Profiling the European citizen – Cross-disciplinary perspectives*, Dordrecht, Springer Science 2008

[36] Voorstel voor een verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), COM(2012)11 final

[37] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector van de elektronische telecommunicatie (richtlijn betreffende privacy en elektronische communicatie).

2.1.2 Werkplaats

34. Binnen de arbeidssfeer hebben nog andere internationale organisaties stappen ondernomen in het kader van de bescherming van de zowel de belangen van de werkgever als deze van de werknemer. We vermelden in de eerste plaats de Aanbeveling nr. R(89) inzake de bescherming van persoonsgegevens bij de arbeid.[38] In de tweede plaats denken we aan de Gedragscode van 1996 van de Internationale Arbeidsorganisatie met betrekking tot de bescherming van persoonsgegevens in het kader van de arbeidsrelatie.[39] Deze gedragscode is van toepassing op de publieke en private sector en maakt geen onderscheid naargelang de persoonsgegevens al dan niet via een automatisch procedé worden verwerkt. Ook hier wordt opnieuw duidelijk gesteld dat de werknemer niet *a priori* bij wijze van algemene toestemming afstand kan doen van zijn privacybescherming (art. 5.13). Hoewel de Gedragscode niet juridisch bindend is, heeft zij een hoge morele waarde binnen het internationale en nationale arbeidsrecht.[40]

35. Een ander Europees regelgevend initiatief is het voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens van werknemers en de bescherming van de persoonlijke levenssfeer in de arbeidsrechtelijke sfeer van 2004. Hoewel dit voorstel tot op vandaag echter nog niet aan de Europese Commissie werd voorgelegd, is het toch interessant bij de uitgangspunten kort te bespreken. Het voorstel van richtlijn concretiseert de besproken richtlijnen 95/46/EG en 2002/58/EG en regelt de verwerking van uiteenlopende categorieën van privacygevoelige persoonsgegevens, waaronder de controle op het internet en e-mailgebruik van de werknemer. Het uitgangspunt is dat de controle van het internet- en e-mailgebruik principieel verboden is, met als uitzondering wanneer ernstige aanwijzingen voorhanden zijn dat de werknemer de communicatiemiddelen van de werkgever misbruikt. Daarbij moet de werkgever eerst onderzoeken of er geen andere minder privacykrenkende maatregelen kunnen genomen worden (subsidiariteitsbeginsel) en zo dat niet het geval is, moet de verwerking van persoonsgegevens tot het minimum herleid worden (*data minimisation principle*). Deze voorwaarden geven uiting aan het principiële verbod van inmenging in de privacybescherming van artikel 8 EVRM en in daarin vervatte beginsel van proportionaliteit en subsidiariteitsbeginsel. Tegelijk wordt uiting gegeven aan het uitgangspunt van het persoonsgegevensbeschermingsrecht dat alleen persoonsgegevens worden verwerkt als dat echt nodig is. Wat betreft de toestemming van de werknemer wordt gezegd dat de privécommunicatie van de werknemer dezelfde bescherming moet krijgen als de private correspondentie buiten de arbeidsrechtelijke sfeer. Van belang daarbij is dat de werknemer het privékarakter van de communicatie expliciet moet vermelden. Hierbij moet ook gedacht worden aan de bescherming van de communicatie van de ontvanger. Interessant is dat de werknemer geen afstand van het privékarakter van de communicatie op de werkplaats kan doen bij wijze van algemene toestemming. Verder in deze bijdrage komen we op de problematiek van de toestemming nog terug.

36. Aansluitend op het bovenstaande kan ten slotte nog verwezen worden naar de het advies (en dus niet juridisch binnend) van de Groep Gegevensbescherming artikel 29. In dit advies wordt gepleit voor een gescheiden gebruik van e-mailaccounts op de werkplek: een e-mailaccount voor privédoeleinden en een e-mailaccount voor uitsluitend professionele doeleinden. Het is een praktische oplossing die de werkgever er moet van weerhouden om in de

[38] Aanbeveling nr. R (89)2 van 18 januari 1989 van de Raad van Europa betreffende de bescherming van persoonsgegevens bij de arbeid.

[39] Code of practice on the protection of workers' personal data, Geneva, International Labour Organisation (ILO) 1997.

[40] Op een schriftelijke vraag aan de Europese Commissie inzake camerabewaking van werknemers antwoordde de Commissie met verwijzing naar de Gedragscode. Behalve dat rekening moet worden gehouden met de Richtlijn 95/46/EG van 25 oktober 1995 inzake de verwerking van persoonsgegevens moet de werkgever volgens de Commissie ook rekening houden met de Gedragscode van de ILO van 1997. Zo moeten de werknemers op de hoogte zijn van de mogelijke controle, moet het risico voor de privacy vooraf ingeschat worden en zijn geheime controles uitgesloten, tenzij de wetgeving van de lidstaten in deze mogelijkheid voorzien, Schriftelijke vraag E-1388/99, 1 september 1999, *PIEG* C 27/E40 van 29 januari 2000.

persoonlijke levenssfeer van de werknemers binnen te dringen.[41] Ook de Belgische Commissie voor de bescherming van de persoonlijke levenssfeer zal in een advies van 2012 deze praktische oplossing aanbevelen (*infra*).

Voorbeeld:

Werknemer A verstuurt een e-mailbericht naar persoon B. Het e-mailbericht wordt vergezeld met een automatische waarschuwing dat de inhoud een privékarakter heeft. Wanneer de ontvanger een bericht naar A terugstuurt mag hij verwachten dat de communicatie privé is en niet door derden gecontroleerd wordt.

Voorbeeld:

Werknemer A verstuurt een e-mailbericht naar persoon B. Het e-mailbericht wordt vergezeld met een automatische waarschuwing dat de inhoud een professioneel karakter heeft. Wanneer de ontvanger een bericht naar A terugstuurt kan hij verwachten dat de communicatie beroepsmatig is en door de werkgever of andere medewerkers kan gelezen worden.

2.1.3 Sociale netwerksites (SNS) algemeen

37. Juridische (bindende) instrumenten ten aanzien van het gebruik en de controle van sociale mediasites binnen de arbeidsrelatie zijn er niet. Wel heeft de Raad van Europa verschillende aanbevelingen inzake de bescherming van mensenrechten met betrekking tot sociale media uitgebracht. Hoewel de arbeidsrelatie zich toch afspeelt binnen een enigszins specifieke context is de vermelding van deze rechtsinstrumenten niet zonder belang. Denken we bijvoorbeeld aan de aanbeveling van 1999 inzake de bescherming van de privacy op het internet.[42] In deze aanbeveling wordt het anoniem, minstens onder pseudoniem, gebruik van internet geadviseerd. Het gebruik van de werkelijke identiteit is wel mogelijk (verplicht) om aan de wettelijke (contractuele) verplichtingen te voldoen ten opzichte van de internet service provider (ISP). Anoniem gebruik of gebruik van een pseudoniem lijkt niet onverkort mogelijk binnen de arbeidsrelatie wanneer de werkgever de communicatiemiddelen aan de werknemer verschaft. Bij een (beperkt) toegestaan privégebruik van de door de werkgever ter beschikking gestelde communicatiemiddelen lijkt het gebruik van bijvoorbeeld pseudoniemen op SNS tijdens de werkuren echter niet meteen op gespannen voet te staan met de arbeidsrechtelijke context.[43]

38. Wat betreft sociale media is de aanbeveling van 4 april 2012 meer concreet. Het betreft de aanbeveling inzake de bescherming van mensenrechten bij het gebruik van SNS.[44] Opnieuw duikt de mogelijkheid tot het gebruik van pseudoniemen en controle over de eigen informatie op. Zo zou er moeten voorzien worden in privacyvriendelijke instellingen en tools zodat de gebruiker zijn privacy naar eigen inzichten moet kunnen afschermen zonder dat zijn vrije deelname aan het openbaar of gesloten debat eenzijdig wordt beperkt. Daarbij zou de gebruiker moeten

---

[41] Groep artikel 29, Werkdocument over de controle op de elektronische communicatie op het werk, goegekeurd op 29 mei 2002, www.europa.eu.int/comm/privacy.

[42] Recommendation nr. R(99) van 23 februay of the Committee of Ministers to member States for the protection of privacy on the internet.

[43] Vaak is de registratie van de werkelijke identiteit op een SNS verplicht (inzake toegangsbevoegdheid bijvoorbeeld). Dat belet niet dat het gebruik van een pseudoniem mogelijk moet kunnen zijn, waarbij de link tussen het pseudoniem en de werkelijke identiteit vertrouwelijk door de SNS wordt opgeslagen. De werkelijk identiteit is op die manier afgeschermd van derden of onbevoegden. Slechts op uitdrukkelijke toestemming van de betrokkene is het gebruik van de werkelijke identiteit toegestaan. Op die manier wordt de privacybescherming van de gebruiker verhoogd. Alleen wanneer de gebruiker het pseudoniem aanwendt om zijn werkelijke identiteit te verhullen met het oog op het gebruik van ongeoorloofde uitingen, kan de privacybescherming, mits wettelijke waarborgen, doorbroken worden.

[44] Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social media services.

kunnen weten wanneer de gedeelde informatie een publiekelijk of privékarakter heeft. Het onderscheid tussen het publieke en private karakter van de communicatie (informatie) zou aan de gebruiker op een begrijpelijke manier moeten uitgelegd worden. De moeilijke scheidingslijn tussen het publieke en privékarakter van communicatie op het internet en sociale media in het bijzonder zorgt voor discussie en controverse. Heeft de communicatie die enkel toegankelijk is voor 'vrienden' een privékarakter? Is de kring van beslotenheid doorbroken wanneer de communicatie gedeeld wordt met 'vrienden' van 'vrienden'. Ervan uitgaande dat er sprake is van privécommunicatie wanneer de communicatie niet bestemd is om door anderen te worden gehoord of 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 van het gesprek.[45] Wat is de reikwijdte van de notie "privécommunicatie" op sociale netwerksites?(*infra*).

39. Ten slotte is nog de resolutie van het Parlementaire Assemblee van 2011 met betrekking tot de bescherming van de privacy en persoonsgegevens op het internet en online media vermeldenswaard.[46] Ook in dit supranationaal document staat de controle door de gebruiker over het gebruik van zijn informatie en de vertrouwelijkheid van de informatie centraal. Verder gebruik van de informatie zonder de toestemming van de gebruiker is principieel uit den boze. Ook in deze resolutie is geen rekening gehouden met de specifieke problemen van het gebruik van sociale media binnen de context van de arbeidsrelatie.

40. Algemeen beschouwd kunnen we concluderen dat er op supra nationaal niveau veel aandacht wordt besteed aan de privacybescherming en de bescherming van de persoonsgegevens van de gebruiker. De besproken rechtsinstrumenten geven evenwel geen voldoende houvast voor de noden en verzuchtingen waarmee zowel de werkgever als de werknemer op en naast de werkplaats worden geconfronteerd. Bij het opstellen van deze documenten moet uiteraard rekening worden gehouden met de culturele verschillen die tussen de verschillende lidstaten speelt. Vanuit deze vaststelling biedt de nationale wetgever meer perspectieven. Daarbij zal echter ook blijken dat deze instrumenten niet kritiekloos op de problematiek van het gebruik van sociale media op de werkplaats kunnen toegepast worden.

2.2 NATIONAAL

2.2.1 De bescherming van persoonsgegevens

41. Doorgaans weten gebruikers van SNS het niet, maar een zeer belangrijk rechtsinstrument bij het uitwisselen van informatie op SNS is de wet van 8 december 1992 betreffende de verwerking van persoonsgegevens (WVP).[47] Deze wet waarborgt sinds 1992 de bescherming van het individu wanneer zijn of haar persoonsgegevens op geautomatiseerde wijze of in een manueel dossier worden verwerkt. Dat geldt voor iedereen die

[45] *Parl.St.* Senaat 1992-1993, nr. 843/1, 6-7; *Parl. St.* Senaat, 1992-1993, nr. 843/2,10. Zie ook de Groep gegevensbescherming artikel 29, 'Werkdocument over de controle op elektronische communicatie op het werk' van 29 mei 2002. De Art. 29 Groep ontleent haat naam aan het gelijkaardig artikel 29 van de Richtlijn 95/46/EG. De Groep is een adviesorgaan dat is samengesteld uit vertegenwoordigers van de nationale gegevensbeschermingsautoriteiten en die vraagstukken beantwoordt met betrekking tot een eenvormige toepassing van de bepalingen van Richtlijn in de lidstaten.

[46] Resolution 1843 (2011) of the Parliamentary Assemblée on the protection of privacy and personal data on the Internet and online media.

[47] De wet van 8 december 1992 betreffende de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (*B.S.* 18 maart 1993) en het KB van 3 februari 2001 ter uitvoering van de wet van 8 december 1992 betreffende de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking persoonsgegevens (*BS* 13 maart 2001). Aan de basis van de oorspronkelijke WVP lag het Verdrag nr. 108 van 28 januari 1981 tot bescherming van personen bij de geautomatiseerde verwerking van persoonsgegevens. De oorspronkelijk WVP van 1992 werd grondig gewijzigd door de wet van 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.

persoonsgegevens van iemand anders verwerkt. Zowel in de publieke als de private sector. Voor een wettige verwerking van persoonsgegevens moeten enkele basisvoorwaarden nageleefd worden Deze basisvoorwaarden vallen uiteen in transparantie (openbaarheid), legitiem doeleinde, noodzakelijkheid en proportionaliteit, veiligheid van de verwerkingen, en tenslotte het controlerecht op verwerkingen en het recht van verzet. Bij SNS staat daarbij de toestemming van de gebruiker centraal.

42. Maar deze basisvoorwaarden staat dagelijks onder zware druk. Door de ontwikkelingen in de informatie- en communicatietechnologieën is het aanleggen van bestanden en het uitwisselen van persoonsgegevens gemakkelijk geworden. Het koppelen van bestanden met persoonsgegevens is een efficiënt hulpmiddel om bijvoorbeeld gepersonaliseerde reclameboodschappen uit te sturen. Gebruikers van SNS zijn hierbij een makkelijk doelwit. Het samenbrengen van en 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 dergelijke 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. Vandaag is het vaak niet meer mogelijk om te kunnen weten wie welke gegevens (op het internet) heeft verwerkt, laat staan waarvoor ze gebruikt worden.

43. Tot voor kort was de bescherming van de persoonsgegevens niet als een zelfstandig grondrecht vastgelegd. Dit werd in ons land doorgaans geconstrueerd en geconcipieerd als deelaspect op het grondrecht op bescherming van de persoonlijke levenssfeer. In België is dit deelaspect als een algemene wet geregeld in de Wet van 8 december 1992 betreffende de verwerking van persoonsgegevens. Recent werd op Europees niveau beslist om aan de bescherming van persoonsgegevens een grondwettelijk karakter te geven. Dit gebeurde in het Europees Handvest van 2000,[48] die sinds de inwerkingtreding van het Verdrag van Lissabon rechtskracht heeft gekregen.[49] In dit Handvest is de bescherming van de privacy en de bescherming van persoonsgegevens in twee afzonderlijke bepalingen opgenomen. Voortaan is de bescherming van persoonsgegevens als een zelfstandig grondrecht in de catalogus van de fundamentele rechten en vrijheden verankerd.[50]

[48] Handvest van de Grondrechten van de Europese Unie, *PbEG* 18 december 2000, 364. Zie hierover P. DE HERT, *Privacy en Persoonsgegevens,* Politeia, 2004, afl. 12, 29-32, 171-172; *NJCM-Bull.* 2000, 924- 967; *Maastricht Journal* 2001, 1-114; M.K. BULTERMAN en R.A. LAWSON, 'Het EU-grondrechtenhandvest: méér dan een festijn voor juristen', *Int. Spectator* 2000, 423-429; LENAERTS, K. en DE SMIJTER, E., 'Een "Bill of Rights" voor de Europese Unie', in *Bijdragen aan een Europese Grondwet* (Staatsrechtconferentie 2000), 107-138; HIRSCH BALLIN, E., 'Het Handvest van de Grondrechten van de Europese Unie: het eerste hoofdstuk van een Europese Constitutie?', *Ars Aequi* 2001, 50, 2, 88- 93.

[49] Art. 6 Verdrag Europese Unie

[50] Art. 7: "Eenieder heeft recht op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie".
Art. 8: "1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.
2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op **basis** van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.
3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels".

44. De WVP wordt als een algemene wet beschouwd.[51] Daardoor moeten de randvoorwaarden van deze wet gerespecteerd worden in iedere regeling of overeenkomst die voorzien in de verwerking van persoonsgegevens. Als gevolg moeten de afspraken tussen de gebruikers en SNS in overeenstemming zijn met deze randvoorwaarden. 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 beoogd immers de identificatie van de vermeende malafide gebruiker en daarom de verwerking van zijn persoonsgegevens. Wanneer in dat verband geen arbeidsrechtelijke regeling van toepassing is op de gegeven situatie in het bedrijf, zal de WVP als vangnet dienen voor de rechtmatigheid van controle (*infra*).

Toepassingsgebied van de WVP

46. De WVP is van toepassing zodra persoonsgegevens via een geheel of gedeeltelijk geautomatiseerd procedé worden verwerkt of in een manueel bestand worden opgenomen die zodanig wordt opgezet dat het bestand systematisch kan geraadpleegd worden (art. 3 WVP). Behalve wanneer sprake is van huishoudelijk gebruik van persoonsgegevens, is dat het geval bij het gebruik van persoonsgegevens door de overheden, openbare instellingen en organisaties, bedrijven enz.

Wat zijn persoonsgegevens? Persoonsgegevens omvat iedere informatie aan de hand waarvan een individu identificeerbaar is. Het gaat niet alleen om de naam en adres van een persoon, maar bijvoorbeeld ook om het notitienummer op een proces-verbaal en een dossiernummer die via een repertorium verwijst naar de betrokkene.[52] Onder verwerking wordt iedere bewerking of geheel van bewerkingen met persoonsgegevens verstaan.[53] De door de WVP omschreven definities van de begrippen 'persoonsgegevens', 'verwerking' en 'bestand' zijn zodanig ruim dat het moeilijk kan ontkend worden dat persoonsgegevens op het internet en SNS onder toepassing van de WVP vallen.[54]

Voorbeeld:

Werknemer A voert tijdens de werkuren met klant X een gesprek op Facebook. De WVP is van toepassing wanneer de klant identificeerbaar is.

[51] Recent heeft het Grondwettelijk Hof in een arrest van 14 februari 2008 benadrukt dat bij elke maatregel waarbij persoonsgegevens worden verwerkt, rekening moet worden gehouden met deze minimumvoorwaarden van de WVP (GwH 14 februari 2008, nr. 15/2008). In hetzelfde jaar beslist het Mensenrechtenhof dat op de overheid de positieve plicht rust om de veiligheid bij de verwerking van persoonsgegevens te garanderen (EHRM 17 juli 2008, nr. 20511/03, I. t. Finland, EHRC 2008/9, 1136). Ondertussen is de Europese richtlijn van 24 oktober 1995 aan herziening toe en vervangen worden door een Europese verordening. Een belangrijk nieuwe gegeven is de aandacht voor het verwerken van persoonsgegevens op het internet. Voor aanleggen van profielen van gebruikers zou de expliciete toestemming vereist zijn. Een nieuwkomer is het 'recht op vergetelheid'. Hierdoor zouden de persoonsgegevens na verloop van tijd uit het bestand van de verwerker of op het internet op moeten geschrapt worden, wanneer geen een wettige verwerkingsgrond meer voorhanden is. Zie over het voorstel van nieuwe Europese verordening inzake de verwerking van persoonsgegevens, P. DE HERT en V. PAPAKONSTANTINOU, 'The proposed data protection Regulation Directive 95/46/EC: A sound systeem for the protection of individuelas', Computer law & Security Review, 2012, afl. 28, 130-142.

[52] Het gaat om informatie aan de hand waarvan de persoon direct of indirect kan geïdentificeerd worden, zoals een identificatienummer of één of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit (art. 1, § 1 WVP).

[53] De wet somt een niet-limitatieve lijst met bewerkingen op, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzingen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere welke wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsook het afschermen, uitwissen en vernietigen van persoonsgegevens (art. 1, § 2 WVP). Zie uitgebreid D. DE BOT, *Verwerken van persoonsgegevens*, Kluwer 2001, 403 p; P. DE HERT en D. PISSOORT 'De wet verwerking van 8 december 1992 met betrekking tot de verwerking van persoonsgegevens', in P. DE HERT (ed.) *Privacy en persoonsgegevens*, Politeia 2005, losbladig, afl. 16, 1-179.

[54] Zie ook H. GRAUX, 'Privacybescherming op de sociale netwerken: heeft u nog een privéleven?', in P. VALCKE, P.J. VALGAEREN en E. LIEVENS (eds) *Sociale media. Actuele juridische aspecten*, Intersentia 2013, 1-28.

Voorbeeld:

Wanneer de werkgever de communicatie tussen A en X, over de schouders van A, kan volgen, zonder enige handeling (muisklik) op de computer uit te voeren, is de WVP werkgever niet van toepassing.

Basisvoorwaarden van de WVP

47. Zoals hiervoor gezegd gelden bij de verwerking van persoonsgegevens een aantal grondbeginselen. Het eerste beginsel zegt dat iedere burger bij de verwerking van zijn persoonsgegevens recht heeft op bescherming van zijn fundamentele rechten en vrijheden, inzonderheid op de bescherming van zijn persoonlijke levenssfeer. Hieruit volgt dat niet elke gebruik van persoonsgegevens een risico vormt voor de privacy van de burger. Ook andere belangen spelen mee, zoals de vrije meningsuiting, het verbod van discriminatie en niet louter beoordeeld worden aan de hand van geautomatiseerde beslissingen.[55]

De sleutelbegrippen bij het verwerken van persoonsgegevens zijn het finaliteitsprincipe, of doelbindingsbeginsel, het proportionaliteitsbeginsel en het transparantiebeginsel. Deze basisbeginselen lopen als een rode draad doorheen het gegevensbeschermingsrecht, waarbij de noodzakelijkheid van de verwerking een essentiële voorwaarde is. Deze basisvereisten worden hierna uitvoerig besproken.

48. Grosso modo kunnen we zeggen dat het gegevensbeschermingsrecht uitgaat van de premisse dat de verwerking van persoonsgegevens toegelaten is, mits degene die persoonsgegevens verwerkt enkele basisregels naleeft. Het gaat dan om persoonsgegevens die men dagelijks gebruikt om op een normale wijze aan het maatschappelijke leven te kunnen deelnemen, zoals naam en adres. Voor een bijzondere categorie persoonsgegevens ligt dat anders. Het gaat om gegevens waarvan het gebruik een groter risico inhoudt voor de bescherming van de persoonlijke levenssfeer. Vaak worden deze persoonsgegevens als 'gevoelige gegevens' omschreven. Naast gerechtelijke gegevens en gezondheidsgegevens, worden onder meer ook bepaalde gegevens die kenmerkend zijn voor de afkomst van de persoon of zijn politieke overtuiging als gevoelige gegevens beschouwd. Voor deze categorie van bijzondere persoonsgegevens geldt een verwerkingsverbod, tenzij de verwerking gesteund is op een of meer van de limitatief opgesomde bijzondere voorwaarden in de WVP. Niet zelden wordt ook gevoelige informatie op SNS gedeeld met andere gebruikers. De vraag in welke mate de verwerking van deze persoonsgegevens toegestaan is, hangt af van de vraag of de betrokkene daarvoor zijn of haar uitdrukkelijke toestemming heeft gegeven (*infra*). Daarnaast kan ook een wettelijke regeling in de verwerking van persoonsgegevens voorzien, zoals binnen de arbeidsrelatie (art. 5-8 WVP).

Het finaliteits- en proportionaliteitsbeginsel

49. Persoonsgegevens kunnen slechts rechtmatig worden verwerkt indien rekening wordt gehouden met de grondbeginselen van de WVP. De beginselen van finaliteit of doelbinding en proportionaliteit zijn belangrijke toetsstenen. Dit houdt in dat persoonsgegevens voor een welbepaalde, uitdrukkelijk omschreven en gerechtvaardigd doeleinden moeten verkregen worden en niet verder worden verwerkt op een wijze die onverenigbaar is met het oorspronkelijke doeleinde van de verwerking. Daarbij moet rekening worden gehouden

[55] Art. 12*bis* WVP.

met de alle relevante factoren, met name met de redelijke verwachtingen van de betrokkene en met de toepasselijke wettelijke en reglementaire bepalingen (art. 4, § 1, 2° WVP). Bovendien moet de verwerking eerlijk gebeuren. Dat wil zeggen dat de verwerking in principe niet gebeurt zonder medeweten van de betrokkene, tenzij uitzonderlijke omstandigheden dit rechtvaardigen. De burger moet dus vooraf kunnen inschatten welke gegevens van hem worden verkregen en waarom dat het geval is. Deze verplichting geldt trouwens niet alleen ten opzichte van de burger, maar tevens tegenover de CBPL. Ook de CBPL moet zo nauwkeurig mogelijk weten wat er met persoonsgegevens gebeurt of zal gebeuren.[56] Dat is één van de voorwaarden voor een rechtmatige verwerking.

50. Vervolgens dienen de persoonsgegevens tevens toereikend, ter zake dienend en niet overmatig te zijn uitgaande van de doeleinde van de verwerking of waarvoor ze verder zullen gebruikt worden (art. 4, § 1, 3° WVP). Hierin zit het criterium van noodzakelijkheid en proportionaliteit vervat. Hoewel beide criteria onontbeerlijk zijn voor een rechtmatige verwerking, blijken zij in de praktijk vaak moeilijk ingevuld te worden. Het is niet omdat een bepaling de verwerking van persoonsgegevens toelaat dat de effectieve verwerking van persoonsgegevens automatisch gerechtvaardigd is. Er geldt een bijkomende voorwaarde: de verwerking van de persoonsgegevens moet tevens noodzakelijk zijn. Deze vereiste vloeit eigenlijk voort uit de onderliggende gedachte van het gegevensbeschermingsrecht, namelijk het minimalisatieprincipe: ook al is de verwerking toegestaan, dan nog alleen indien dat noodzakelijk is met liefst zo weinig mogelijk persoonsgegevens. Of anders gezegd: geen persoonsgegevens verwerken als het niet echt nodig is.[57] Is de verwerking wel nodig, dan nog mogen slechts die gegevens verwerkt worden die relevant zijn om het doel te bereiken. In een maatschappij waarin de informatiebehoefte (blijkbaar) zeer groot is, komt deze oefening nog meer op de voorgrond. En dat is een oefening die de verantwoordelijke voor de verwerking zelf moet maken. De WVP biedt met andere woorden geen pasklare antwoorden. Op degene die de persoonsgegevens verwerkt rust de plicht om na te gaan of de verwerking noodzakelijk is (ook laat de wet de verwerking toe of is de toestemming van de betrokkene verkregen) en de gevraagde of verkregen gegevens van belang zijn om het gewenste resultaat (doeleinde) te bekomen. Persoonsgegevens (*ad hoc*) verwerken voor het geval ze wel eens in de toekomst nuttig kunnen zijn, is een idee die niet voldoet aan de principes van noodzakelijkheid en proportionaliteit.

Voorbeeld:

SNS sporen hun gebruikers aan om zoveel mogelijk (intieme) informatie te delen. Er kan van u niet vereist worden dat u meer informatie uitwisselt dan nodig om te participeren op het SNS. Zo is informatie over u seksuele geaardheid niet van belang bij een discussie over nieuw automodel, of het aanhoudende slechte weer. Maar wellicht wel nuttig voor de marketeers die persoonsgegevens opkopen van SNS om hun producten ongevraagd aan de gepaste categorie van persoon aan te bieden. De SNS mag deze informatie alleen met uw toestemming verwerken én voor zover u ook akkoord gaat met het doel van de verwerking (specifieke reclame, nieuwsbrieven over dat onderwerp, …).

[56] P. DE HERT en D. PISSOORT, *o.c.*, 88.

[57] In dat verband werd door de Nederlandse Hoge Raad op 9 september 2011 een interessante uitspraak gedaan. De zaak gaat over de gevolgen van wanbetaling bij een kredietovereenkomst. Wanneer de kredietnemer geen gehoor geeft aan de aanmaning om het openstaande bedrag te betalen, moet de kredietverlener de wanbetaler registreren bij het Bureau Kredietregistratie (BKR). In deze zaak oordeelde de Hoge Raad dat de verantwoordelijke voor de verwerking (*in casu* de kredietverlener) bij iedere gegevensverwerking steeds een belangenafweging moet maken tussen zijn eigen belang en het belang van de betrokkene (*in casu* de kredietnemer), ondanks de wettelijke verplichting tot verwerking (*in casu* de registratie bij het BKR). Dus, een wettelijke verplichting om persoonsgegevens te verwerken rechtvaardigt volgens de Hoge Raad op zichzelf niet de verwerking van persoonsgegevens, HR 9 september 2011, LNJ: BQ8097, 10/03988.

Nauwkeurigheid en bewaartermijn

51. Daarnaast moeten de gegevens nauwkeurig zijn. Persoonsgegevens waarvan men twijfelt of zij wel correct zijn mogen niet verwerkt worden. Wanneer blijkt dat de oorspronkelijk verwerkte persoonsgegevens niet meer correct zijn, moeten de gegevens bijgewerkt worden (art. 4, § 1, 4° WVP). Deze voorwaarde lijkt voor zichzelf te spreken. Persoonsgegevens die foutief worden verwerkt kunnen desastreuze gevolgen hebben voor de burger wanneer op basis van foutieve persoonsgegevens over hem een beslissing wordt genomen. Bovendien blijkt vaak de oorsprong van de foutieve verwerking moeilijk te achterhalen. Illustratief is de ophefmakende zaak van de Nederlandse zakenman die jaren onterecht in de politiedatabanken opgetekend stond als gevaarlijke crimineel, terwijl hij het slachtoffer was van identiteitsdiefstal. Daardoor liep zowel zijn sociaal als professioneel leven op de klippen, met alle gevolgen vandoen.

52. Vervolgens legt de WVP de plicht op aan de verantwoordelijke voor de verwerking om de persoonsgegevens te bewaren op een manier dat de betrokkene kan geïdentificeerd worden (art. 4, § 1, 5° WVP). Daarbij geldt overigens de voorwaarde dat de persoonsgegevens niet langer mogen bewaard worden dan nodig is om de doeleinden te verwezenlijken. Indien de wetgever de termijnen niet wettelijk heeft vastgelegd, is ook dit een oefening die de verantwoordelijke voor de verwerking zelf moet maken. Heeft hij de persoonsgegevens niet meer nodig of zijn deze niet meer relevant voor het doeleinde, dan moeten ze vernietigd worden. Ook op dat vlak speelt het vereiste van transparantie. De burger moet weten hoelang zijn gegevens worden bewaard. Anders kan hij onmogelijk nagaan hoe lang hij zijn controlerecht kan uitoefenen.

Voorbeeld:

Een SNS mag uw persoonsgegevens slechts bewaren voor de duur dat u participeert op de SNS. Hetzelfde geldt voor de gebruikers met wie u informatie deelt.

Wanneer iemand op de SNS vertelt dat u gisteren bent overleden, maar deze informatie onwaar is, moet deze foute informatie geschrapt en rechtgezet worden. Wanneer iemand daarentegen een opinie over u heeft gevormd, en u bent het niet eens met deze opinie, is er geen sprake van incorrecte informatie in de zin van de WVP. Het moet dus gaan om objectiveerbare informatie, zoals het overlijden van iemand, zijn gezondheidstoestand, enz. Een opinie is een subjectieve uiting over iets of iemand.

De verantwoordelijke voor de verwerking

53. Hiervoor is reeds de term 'verantwoordelijke voor de verwerking' gevallen.[58] Naast de betrokkene speelt deze persoon, organisatie, bedrijf of overheid, een belangrijke rol in het gegevensbeschermingsrecht. Op hem of haar rust namelijk de plicht om de bepalingen van de WVP na te leven (art. 4, § 2 WVP). Hij kan niet alleen

[58] Onder de verantwoordelijke voor de verwerking wordt onder meer verstaan de (rechts)persoon of het openbaar bestuur die alleen of samen met anderen het doel en de middelen voor de verwerking van persoonsgegevens bepaalt. Wordt het doel en de middelen door of krachtens een wet, een decreet of een ordonnantie bepaald, dan is de verantwoordelijke *in casu* het openbaar bestuur die door deze wettelijke regeling wordt aangewezen (art. 1, § 4 WVP). Voluit luidt deze bepaling als volgt: "*Onder verantwoordelijke voor de verwerking wordt de natuurlijke persoon of rechtspersoon, de feitelijke vereniging of het openbaar bestuur verstaan die alleen of samen met anderen het doel en de middelen voor de verwerking van persoonsgegevens bepaalt.*
Indien het doel en de middelen voor de verwerking door of krachtens de wet, een decreet of een ordonnantie zijn bepaald, is de verantwoordelijke voor de verwerking de natuurlijke persoon, de rechtspersoon, de feitelijke vereniging of het openbaar bestuur die door of krachtens de wet, het decreet of de ordonnantie als de voor de verwerking verantwoordelijke wordt aangewezen".

aansprakelijk gesteld worden wanneer de verwerking van persoonsgegevens niet volgens deze spelregels verloopt (art. 15*bis* WVP). Hij kan bovendien strafrechtelijk gesanctioneerd worden (art. 39 WVP).[59]

54. Het is lang niet altijd makkelijk om vast te stellen wie de verantwoordelijke voor de verwerking is. Er moet gekeken naar de feitelijke situatie. Wie beslist over de wijze waarop de persoonsgegevens worden verwerkt? Bij de informatieverwerking op SNS kan de verantwoordelijkheid in het algemeen aan drie spelers worden toegeschreven: de SNS, de ontvanger van informatie door de SNS en de gebruiker. De SNS verwerken persoonsgegevens van de gebruikers, zoals de registratiegegevens en andere informatie die met het SNS wordt gedeeld. SNS overleven grotendeels door de participatie van marketeers. Zij kopen informatie die op SNS wordt gedeeld. In dat geval zijn de respectievelijke bedrijven die deze informatie van SNS ontvangen ook als verantwoordelijke voor de verwerking aan te merken

Rechtvaardigingsgronden voor de verwerking van persoonsgegevens

55. Algemeen gesteld is de verwerking van persoonsgegevens toegelaten mits toestemming van de betrokkene, wanneer een wettelijke regeling de verwerking oplegt of mogelijk maakt en wanneer het belang van de verantwoordelijke voor de verwerking zwaarder weegt dan het belang van de betrokkene. Wie wil deelnemen aan de communicatie op SNS, zal zich doorgaans moeten registreren en akkoord verklaren met de 'Privacy policy'. Maar doorgaans zijn dergelijke reglementen niet transparant en moeilijk of niet te begrijpen voor de gebruiker, strijdig met het Europees persoonsgegevensbeschermingsrecht en vormen zij een ontoelaatbare beperking van de keuzevrijheid van de gebruiker. Er kan in dit geval slechts bezwaarlijk sprake zijn van een vrije toestemming.[60]

Gevoelige gegevens

56. De term 'gevoelige gegevens' wordt als zodanig niet in de WVP omschreven. Het is een ingeburgerde term binnen het kader van de toepassing van het gegevensbeschermingsrecht en omvat gegevens die door hun aard een (groter) risico vormen voor de bescherming van de persoonlijke levenssfeer van het individu.

57. Artikel 6 WVP omschrijft de persoonsgegevens die kenmerken of eigenschappen dragen die eigen zijn aan het individu. Het gaat om gegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakbond kan worden afgeleid. Volgens de memorie van toelichting bij de WVP moet dit op redelijke wijze uitgelegd worden, in die zin dat de gevoelige informatie met aan zekerheid grenzende waarschijnlijkheid uit de gegevens kan afgeleid worden.[61] Ook gezondheidsgegevens worden in het gegevensbeschermingsrecht als een bijzondere categorie persoonsgegevens beschouwd (art. 7 WVP).

---

[59] Het niet naleven van de bepalingen van de WVP wordt gestraft met een geldboete van 100 tot 100.000 euro. Daarnaast kan de rechtbank bevelen dat het vonnis in zijn geheel of bij uittreksel wordt opgenomen in één of meer dagbladen op de wijze die zij bepaalt en op kosten van de veroordeelde (art. 40 WVP) en de verbeurdverklaring uitspreken van manuele bestanden, magneetschrijven of magneetbanden of de uitwissing gelasten. De rechter kan ook een beroepsverbod tot twee jaar opleggen om het beheer te hebben van enige verwerking van persoonsgegevens en zelfs bij herhaling een gevangenis van drie maanden tot twee jaar met een geldboete van 100 tot 100.000 euro of één van deze die straffen afzonderlijk opleggen (art. 41 WVP).

[60] Zie G. G. FUSTER en S GUTWIRTH, *l.c.*, 213-227.

[61] Memorie van toelichting bij het wetsontwerp 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, *Parl. St.*, Kamer 1997-1998, nr. 1566/1, 33.

58. Het Europees Hof voor de Rechten van de Mens heeft geoordeeld dat de bescherming van gezondheidsgegevens voor het individu van fundamenteel belang is om het recht van personen op respect voor hun privéleven en gezin- en familieleven, zoals gewaarborgd in artikel 8 EVRM, te verzekeren.[62] Ten tweede worden mensen op basis van hun gezondheidstoestand in het maatschappelijke leven anders beoordeeld. Vandaar dat gezondheidsgegevens, anders dan gewone persoonsgegevens zoals naam en adres, door hun aard een groter risico voor de bescherming van de persoonlijke levenssfeer vormen. De verwerking van deze gegevens wordt dan ook aan strengere voorwaarden onderworpen dan zogenaamde gewone gegevens.[63] Sinds de uitspraak van het Europees Hof van Justitie van 6 november 2003 is het duidelijk dat de term 'gezondheidsgegevens' niet beperkt is tot louter medische gegevens, zoals een diagnose van de dokter.[64] Het Hof zegt dat aan de uitdrukking "gegevens die de gezondheid betreffen" een ruime uitleg moet gegeven worden. Het betreft informatie over alle – zowel fysieke als psychische – aspecten van iemands gezondheid. De vermelding van het feit dat iemand zijn voet heeft bezeerd en met (gedeeltelijk) ziekteverlof is, is dan ook een persoonsgegeven betreffende gezondheid in de zin van de WVP.[65]

Voorbeeld:

De werknemer meldt zich ziek op het werk. Het doktersbriefje, waarop staat vermeldt dat de werknemer 'arbeidsongeschikt' is, is een 'gezondheidsgegeven in de zin van de WVP.

Voorbeeld:

Een werkgever/werknemer kondigt op Facebook met veel blijdschap aan dat zijn werknemer/werkgever terug op het bedrijf is na een chemokuur ter bestrijding van zijn longkanker De werkgever/werknemer mag dergelijke informatie niet verspreiden zonder de uitdrukkelijke toestemming van de werknemer/werkgever. Dat is strafbaar (art. 39 WVP). Als de patiënt deze informatie zelf op de SNS verspreidt, mag de werkgever/werknemer daarop inspelen en reageren. De werkgever/werknemer mag die informatie echter niet ergens een bestand opslaan omdat u oordeelt dat het weleens later eens van pas zou kunnen komen.

---

[62] EHRM 29 april 2002, *Pretty t/Verenigd Koninkrijk*; EHRM 17 februari 2005, *K.A. en D.A. t/België*, , EHRM 17 juli 2008 *I. t/. Finland*, nr. 20511/3 § 38.

[63] Zie hierover R. SAELENS en P. DE HERT, *De wet patiëntenrechten en de verwerking van gezondheidsgegevens*, Politeia 2010, 122. In de praktijk worden evenwel in grote mate gezondheidsgegevens verwerkt. Het principiële verbod van verwerking van gezondheidsgegevens moet dan ook gezien worden in het licht van het risico voor de persoonlijke levenssfeer dat met de verwerking ervan gepaard gaat. Vandaar een verwerkingsverbod, tenzij een bijzondere rechtvaardigingsgrond kan ingeroepen worden.

[64] Het Europees Hof van Justitie oordeelt over de toepassing en van Europese regelgeving, zoals de Europese Richtlijn 95/46/EG van 24 oktober 1995 betreffende de verwerking van persoonsgegevens.

[65] Europees Hof van Justitie 6 november 2003, nr. C-101/01, www.curia.eu.int; zie ook G-J. ZWENNE, noot bij Europees Hof van Justitie 6 november 2003 (zaak C101/01), *JAVI* 2004/2. Ook in Nederland wordt een ruime interpretatie van gezondheidsgegevens aangenomen. Uit de memorie van toelichting bij de Nederlandse Wet Bescherming Persoonsgegevens (WBP) blijkt dat het niet louter gaat om gegevens in het kader van een medisch onderzoek of een medische behandeling door een arts worden verwerkt. Ook wanneer een chef van een werknemer vaststelt dat de werknemer lichamelijk gehandicapt is, is er sprake van een gezondheidsgegevens in de zin van de WBP. In de lijn met het besproken Lindqvist-arrest is ook het enkele gegeven dat iemand ziek is een gegeven omtrent de gezondheid, hoewel dat gegeven op zichzelf nog niets zegt over de aard van de aandoening, *Kamerstukken II*, 1997-1998, 25 892, nr. 3, 109.

Gerechtelijke gegevens

59. Een volgende categorie van gegevens die door hun aard een risico dragen voor de bescherming van de persoonlijke levenssfeer zij gerechtelijke persoonsgegevens.[66] Ook voor deze categorie van gevoelige gegevens geldt een principieel verwerkingsverbod. De verwerking is slechts toegestaan in de limitatief opgesomde voorwaarden. Naast politie en gerechtelijke overheden, kunnen ook particulieren deze gegevens verwerken wanneer de wet daarin voorziet, of in geval van geschil. We denken daarbij aan advocaten en vakbonden die uw zaak behartigen. Het is van belang om te onderstrepen dat de toestemming van de betrokkene het verwerkingsverbod van gerechtelijke persoonsgegevens niet kan opheffen. Aldus kan de toestemming van de gebruiker van een SNS de onwettigheid van de verwerking van diens gerechtelijke persoonsgegevens niet ongedaan maken. Zodoende stelt de SNS of andere gebruiker zich bloot aan strafrechtelijke vervolging.

Uit de parlementaire voorbereidingen blijkt dat het begrip 'verdachte' niet moet begrepen worden in de zin van het Wetboek van Strafvordering. Het begrip 'verdachte' moet ruim geïnterpreteerd worden en dus niet in de strikt juridische betekenis van het woord. Wanneer men vermoedt dat iemand een misdrijf gepleegd heeft, ook al is er geen sprake van een formele handeling tot inbeschuldigingstelling, is er sprake van gerechtelijke persoonsgegevens.[67] Indien bijvoorbeeld een winkelier een bestand aanlegt van personen die hij betrapt heeft op winkeldiefstal, dan verwerkt de winkelier gerechtelijke persoonsgegevens. De winkelier zal voor deze verwerking bijgevolg een bijzondere toelaatbaarheid voorwaarde moeten kunnen aantonen en bovendien duidelijk kunnen aangeven waarvoor hij die gegevens wil gebruiken.

Voorbeeld:

U vertelt aan uw "vrienden" op Facebook dat uw schoonbroer vandaag de gevangenis heeft mogen verlaten nadat hij voor een diefstal enkele maanden heeft vastgezeten. U mag deze informatie niet verwerken (verspreiden). U stelt zich daarmee bloot aan strafrechtelijke vervolging (art. 39 WVP).

Recht van inzage en verbetering

60. Tegenover de mogelijkheid om van de burger (zonder toestemming) zijn persoonsgegevens te verwerken, staat het recht van de betrokkene om inzage te krijgen in zijn gegevens (art. 10 WVP). Deze bevoegdheid moet gezien worden als een uiting van het beginsel van transparantie die het tegengewicht vormt voor de bevoegdheid om van iemand zijn persoonsgegevens te verwerken. De burger van wie persoonsgegevens worden verwerkt, moet persoonlijk kunnen controleren waarvoor zijn persoonsgegevens worden verwerkt en of dat op een correcte manier gebeurt. Dat wil zeggen dat de betrokkene moet kunnen nagaan of zijn persoonsgegevens wettig worden verwerkt en nauwkeurig zijn. Indien de gegevens niet nauwkeurig zijn, moeten deze worden bijgewerkt, verbeterd en desnoods verwijderd (art. 12 WVP). In de praktijk kunnen beide vormen van controlerecht samenvallen, maar dat is niet noodzakelijk. Een eenvoudig en vaak voorkomend voorbeeld is een verkeerde opgave van adres

[66] Artikel 8 WVP herhaalt het principieel verbod van deze categorie van gevoelige gegevens. De verwerking van persoonsgegevens inzake geschillen voorgelegd aan hoven en rechtbanken alsook aan administratieve gerechten, inzake verdenkingen, vervolgingen of veroordelingen met betrekking tot misdrijven, of inzake administratieve sancties of veiligheidsmaatregelen, is verboden. In de memorie van toelichting wordt verduidelijkt dat het begrip "verdenkingen, vervolgingen of veroordelingen met betrekkingen tot misdrijven" aantoont dat het niet enkel strafrechtelijke veroordelingen onder de toepassing van artikel 8 vallen, maar dat het artikel ook betrekking heeft op gegevens waaruit blijkt dat iemand verdacht wordt van of vervolgd wordt van misdrijven. Memorie van toelichting, *Parl. St.* Kamer 1997-1998, nr. 1566/1, 42.

[67] Verslag namens de Commissie voor de Justitie, *Parl. St*. Kamer 1997-1998, nr. 1566/10, 83.

(huisnummer) of naamspelling. Hierbij is het doorgaans voldoende dat aan de instelling of organisatie wordt gezegd dat de gegevens moeten aangepast worden. Daarvoor is in beginsel een effectieve inzage in de gegevens niet nodig, hoewel het inzagerecht kan uitgeoefend worden.[68]

Veiligheid van de verwerkingen

61. De SNS of de werkgever moeten ook toezien op de veiligheid van de verwerkingen. Zij moeten daartoe niet alleen de gepaste technische en organisatorische maatregelen nemen die nodig zijn voor de bescherming van de persoonsgegevens tegen onbevoegde toegang tot de gegevens, maar ook tegen toevallig verlies of ongeoorloofde vernietiging en iedere andere niet toegelaten verwerking van persoonsgegevens (art. 16 WVP). Niet alleen moeten de persoonsgegevens beschermd worden tegen ongeoorloofde toegang. Er moet ook een historiek van de verwerking bijhouden worden. Deze beveiligingsmaatregel moet gezien worden als vorm van controlerecht en bewijsfunctie voor de persoon van wie de persoonsgegevens worden verwerkt. Dat betekent dat de historiek van de verwerkingen in het informatiesysteem gedurende een voldoende termijn moet bewaard worden zodat de betrokkene de toelaatbaarheid van de verwerkingen (raadpleging) kan controleren. Anderszins wordt hij met een onredelijke bewijslast opgezadeld, wat als een schending van de beschermingsplicht van de persoonsgegevens in hoofde van de verwerker kan beschouwd worden.

Voorbeeld:

Facebook moet er zorg voor dragen dat de informatie op een veilige manier worden verwerkt. Zo moet de SNS zorgen dat de gebruiker zijn persoonlijke gegevens van andere kan afschermen in geval deze niet publiek toegankelijk zijn. Zo niet kan de SNS strafrechtelijk aansprakelijk worden gesteld voor inbreuken op deze veiligheidsvereiste (art. 38 WVP).

Aangifte bij de CBPL

62. Een ander aspect van het transparantiebeginsel (openbaarheid) is dat van het voornemen om persoonsgegevens te verwerken aangifte wordt gedaan bij de CBPL. En die aangifte moet gebeuren voordat wordt overgegaan tot één of meer volledig geautomatiseerde verwerkingen die betrekking hebben op de vooropgestelde doeleinden (art. 17, § 1 WVP). Dit register wordt bij de CBPL bijgehouden en is door iedereen raadpleegbaar (art. 18 WVP).

Lang niet alle verwerkingen moeten aan de CBPL aangegeven worden. Naast de uitzonderingen die in de WVP zelf worden opgesomd, zoals openbare registers en manuele bestanden, zijn er nog talrijke vrijstellingen van aangifte vastgelegd in het uitvoeringsbesluit bij de WVP (art. 51 *et seq* uitvoeringsbesluit WVP). Voorbeelden zijn personeel- en loonadministratie, klantenbeheer, ledenadministratie en boekhouding.

[68] Hier is een kanttekening op zijn plaats. Dat de gegevens correct moeten zijn, houdt niet in dat er sprake is van foutieve verwerking van persoonsgegevens wanneer de informatie resulteert in een welbepaalde beoordeling waarmee de betrokkene het niet eens is. Dat is een subjectieve kwestie. De vraag of de gegevens accuraat zijn slaat op de objectieve gegevens. U kunt het bijvoorbeeld niet eens zijn met uw veroordeling, maar dat maakt deze informatie nog niet incorrect in de zin de artikel 12 WVP. Zie een uitgebreide analyse van het begrip 'persoonsgegevens', Groep Gegevensbescherming Artikel 29, Advies 4/2007 over het begrip "persoonsgegevens", goedgekeurd op 20 juni 2007 (WP 136), http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.

Voorbeeld:

Een werkgever moet geen aangifte doen van de personeelsadministratie. Wanneer er daarnaast ook een personeelsdossier wordt aangelegd waarin tuchtmaatregelen en gerechtelijke informatie wordt verwerkt, is aangifte daarvan verplicht.

Voorbeeld:

Facebook moet geen aangifte doen van hun gebruikers (klantenbeheer). Dat is anders wanneer Facebook ook gevoelige gegevens verwerkt, zoals gezondheidsgegevens, gerechtelijke gegevens en andere gevoelige informatie zoals seksuele geaardheid van de gebruikers.

2.2.2 Arbeidsrechtelijk

63. Controlemiddelen op de werkplaats moeten niet alleen voldoen aan de vereisten van artikel 8 EVRM maar moeten ook aan de nationale arbeidsrechtelijke voorschriften getoetst worden.[69] In de arbeidswetgeving zijn geen specifieke bepalingen met betrekking tot de beperking van de privacy opgenomen. Een evenwicht tussen de bescherming van de grondrechten in de onderneming en het controlerecht van de werkgever wordt vaak afgeleid uit open normen uit het privaatrecht en het arbeidsrecht. Doorgaans worden twee bepalingen uit de wet van 3 juli 1978 betreffende de arbeidsovereenkomsten (WAO) in stelling gebracht, namelijk de artikelen 16 en 17 WAO. Artikel 16 WAO bepaalt namelijk dat de werkgever en werknemer elkaar eerbied verschuldigd zijn.[70] Tegelijk bepaalt artikel 17 WAO dat de werknemer verplicht is de bevelen en de instructies van de werkgever uit te voeren. Uit beide algemeen geformuleerde bepalingen wordt zowel het respect voor de effectieve beleving van de privacy enerzijds en de beperking op het privacygrondrecht omwille van het controlerecht van de werkgever anderzijds gelezen. Het is opvallend dat de wetgever de verantwoordelijkheid voor de wettelijke omkadering ten aanzien van de beperking van de grondrechten binnen de arbeidsrelatie naar de sociale partner (werkgevers- en werknemersvertegenwoordigers doorschuift. Wellicht omdat de wetgever van mening is dat de sociale partners op dat vlak beter geplaatst zijn. Zij kennen de specifieke context en hebben meer voeling met de specifieke problematiek die voorligt.

64. Naast deze algemene of open normen speelt ook de wet van 8 april 1965 tot instelling van de arbeidsreglementen een belangrijke rol. Wat betreft de aspecten die verplicht in het arbeidsreglement moeten opgenomen worden, bepaalt artikel 6, 2° dat de wijzen van meting van en controle op de arbeid met het oog op het bepalen van het loon expliciet in het arbeidsreglement moet opgenomen worden. Er wordt doorgaans aangenomen dat deze bepaling vereist dat wanneer de controle op de arbeid van de werknemer via spionagetechnieken, zoals camera's en controle van het internetgebruik, in het arbeidsreglement van de onderneming moeten opgenomen worden. Aldus is de werkgever verplicht op de controlemiddelen die hij in het bedrijf wenst te installeren kenbaar te maken. Op die manier lijken heimelijke controles onmogelijk. Maar op dat punt is de rechtspraak niet eenduidig. Lang niet in alle gevallen wordt stiekeme controle van het internetgebruik (e-mail) afgestraft. Het is ook lang niet duidelijk of alleen de mogelijkheid van de controle of tevens de modaliteiten

[69] R. DELARUE, *L.c.*, 133; P. DE HERT, 'Oude en nieuwe wetgeving op controletechnieken in bedrijven', *SRK* 1995, 108.

[70] In een arrest van 26 maart 1990 oordeelde het Hof van Cassatie dat een controle op de werknemers met een videocamera en het afluisteren van gesprekken een inbreuk maakt op de privacy van de werknemers en artikel 16 WAO schendt, Cass. 26 maart 1990, *SRK* 1992, 154.

van de controle in het arbeidsreglement moeten omschreven worden, dan wel een privacy-policy op zichzelf reeds voldoende is.[71]

C.A.O. nr. 81

65. Aangezien de besproken WVP geen pasklare antwoorden biedt voor specifieke situaties, hebben de sociale partners dat willen oplossen via de collectieve arbeidsovereenkomst nr. 81 van 26 april 2002 (CAO nr. 81).[72] Het enige specifiek arbeidsrechtelijk instrument dat voor controle van het internetgebruik vandaag in stelling kan worden gebracht Onder de volgende voorwaarden is controle van het internet- en e-mailgebruik door de werkgever toegestaan. Het betreft de beginselen van finaliteit, noodzakelijkheid, proportionaliteit en ten slotte transparantie. Wat betreft de finaliteit gaat het om vier vastgelegde ruime doelstellingen, die de werkgever evenwel voorafgaand aan de controle nader moet concretiseren en communiceren op de werkvloer (art. 5 §1 en 2 cao nr. 81).

Toepassingsbied CAO nr. 81

66.Het is van belang om op te merken dat deze CAO alleen de controle op elektronische on-linecommunicatiegegevens van de werknemers regelt, en niet de toegang het internet op de onderneming. De werkgever is in principe niet verplicht om de werknemers toegang tot het internet te verlenen. Het staat de werkgever vrij de toegang en tot het internet en de modaliteiten zelf te bepalen, al gebeurt dat beter in overleg met de werknemers(vertegenwoordiging).

67. In de eerste plaats is de CAO nr. 81 van toepassing op alle elektronische “on-linecommunicatiegegevens”, ongeacht de drager via dewelke een en ander door een werknemer wordt overgebracht of ontvangen in het kader van zijn dienstbetrekking. In de tweede plaats moet de elektronische communicatie gebeuren via het netwerk van de onderneming.[73] Aldus valt zowel het intranet op het bedrijf en het gebruik van internet op het bedrijf onder het toepassingsgebied.[74] Daarnaast zijn de waarborgen van de CAO nr. 81 niet van toepassing op telecommunicatie waarvan het beroepsmatig karakter van de communicatie niet betwist wordt. De reden is dat de goede werking van de onderneming moet gewaarborgd blijven. In dat geval zou de werkgever de inhoud van deze communicatie mogen controleren.[75] Uiteraard kan ook in dat geval de controle niet heimelijk worden uitgevoerd en moeten de hierna opgesomde algemene beginselen worden nageleefd.

---

[71] Zie voor een goed overzicht 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* 2009-09, afl. 18, 730-744.

[72] Collectieve arbeidsovereenkomst nr. 81 van 26 april 2002 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische on-linecommincatiegegevens.

[73] Art. 2 CAO nr. 81.

[74] In de rechtsleer is men het oneens over de vraag of een door de werkgever aangeboden GSM die niet via het netwerk van de onderneming verloopt ook onder het toepassingsgebied van de CAO nr. 81 valt. *Pro*: D. DEJONGHE, ‘Werkgeverscontrole op e-mail- en internetgebruik: C.A.O. nr. 81 schetst de krijtlijnen’, *Or* 2002, 225; *Contra*: L. CORNIL, ‘Werkgeverscontrole op e-mail en internetgebruik van zijn werknemers: een verdere stand van zaken’, *Overlegorganen – Actuele voorinformatie*, nr. 297.1, 5, aangehaald door D. DEJONGHE, *l.c.*, 225. Zo oordeelde de rechtbank van arbeidsrechtbank van Hasselt op 29 augustus 2007 dat de CAO nr. 81 niet van toepassing is op niet door de werkgever geïnstalleerde firewall en de daartoe gebruikte software. Nog volgens het arbeidshof te Brussel zou de collectieve arbeidsovereenkomst ook niet van toepassing zijn op de controle van informatie die op de harde schrijf van de door de werkgever terbeschikkingestelde computer staat, Brussel 14 oktober 2011. Dat zou anders zijn wanneer het gaat om opgeslagen e-mailberichten, Brussel 13 september 2005. We kunnen de discussie ondertussen opentrekking naar de problematiek van het gebruik van het WiFi-netwerk. Is de CAO nr. 81 van toepassing wanneer de communicatie op een door de werkgever aangeboden laptop via WiFi-netwerk van een derde verloopt?

[75] Uit het verslag bij de CAO nr. 81.

Voorbeeld:

De ICT-policy van de onderneming bepaalt privégebruik van de e-mailaccount van de onderneming niet toegestaan is waardoor alle e-mailberichten als beroepsmatig worden aangemerkt. Werknemer A verstuurt een e-mailbericht naar persoon B. Het e-mailbericht wordt vergezeld met een automatische waarschuwing dat de inhoud een professioneel karakter heeft. In dat geval zou kunnen geargumenteerd worden dat de cao nr. 81 niet van toepassing is.

68. Het valt echter te betwijfelen of deze uitzondering werkbaar is, laat staan juridisch verdedigbaar is. Uit Europese rechtspraak volgt dat de controle van de inhoud van e-mailverkeer op de werkplaats mogelijk is, zij het onder strenge voorwaarden en wanneer dat strikt noodzakelijk is.[76] Van belang is dat de controle noodzakelijk en proportioneel is en dat geen ander minder privacykrenkende maatregel tot hetzelfde resultaat kan leiden Op algemene wijze het e-mailverkeer binnen de onderneming als beroepsmatig bestempelen, lijkt onvoldoende om de bescherming van de communicatie van alle deelnemers te doorbreken. Al is het voor de werknemer duidelijk dat het e-mailgebruik enkel toegestaan is voor professionele doeleinden, dan zal dat niet meteen het geval zijn voor anderen die geen werknemer zijn van die onderneming. Doorgaans hebben zij *a priori* geen weet van het louter beroepsmatig karakter van de communicatie waardoor de bescherming van hun communicatiegrondrecht ernstig in het gedrang komt.

Voorbeeld:

Ontvanger B stuurt een bericht over zijn precaire persoonlijke situatie naar werknemer A. B weet niet dat alle e-mailverkeer op de onderneming, waar A werkt, als beroepsmatig wordt beschouwd. Kan B verwachten dat het geheim karakter van de inhoud van de communicatie gewaarborgd is? Kan de werkgever tot controle van het e-mailverkeer van A en B overgaan, zonder de spelregels van de CAO nr. 81 na te leven?

Algemene beginselen CAO nr. 81

69. De controle van de elektronische communicatie is aan enkele basisvoorwaarden onderworpen. Deze basisvoorwaarden zijn gebaseerd op de wet verwerking persoonsgegevens die van toepassing is zodra persoonsgegevens worden verwerkt. Aangezien de WVP een algemeen wettelijk kader schept voor een rechtmatige verwerking van persoonsgegevens, zijn deze voorwaarden nader geconcretiseerd in de CAO nr. 81. Het betreft de beginselen van finaliteit (doelomschrijving), transparantie (kenbaarheid van de controle) en proportionaliteit (alleen noodzakelijke en relevante informatie kan verwerkt worden).

Finaliteit: doelstellingen

1) Het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of de waardigheid van een ander persoon kunnen schaden;

[76] Vgl EHRM 3 april 2007, Copland v. Verenigd Koninkrijk, met noot P. DE HERT en A. HOEFMANS, 'Het arrest *Copland* in het kader van de verdieping van de Europese rechtspraak op het gebied van privacybescherming', *EHRC* 2007, afl. 6, 665-674.

2) De bescherming van de economische, handels- en financiële belangen van de onderneming die vertrouwelijk zijn alsook het tegengaan van ermee in strijd zijnde praktijken;

3) De veiligheid en/of de goede technische werking van de IT-netwerksystemen van de onderneming, met inbegrip van de controle op de kosten van die ermee gepaard gaan alsook de fysieke bescherming van de installaties van de onderneming;

4) Het te goede trouw naleven van de in de onderneming geldende beginselen en regels voor het gebruik van on-linetechnologieën.

70. Net zoals bij gebruik van e-mailberichten kunnen de gesprekken op sociale netwerksites ook in strijd zijn met de hierboven opgesomde doelstellingen. 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. In dat opzicht kan de CAO nr. 81 in stelling worden gebracht wanneer deze uitingsvrijheid buiten de toelaatbare grenzen treedt, door bijvoorbeeld de eer en goede naam van de werkgever of het bedrijf aan te tasten of racistische opmerkingen over de collega's of werkgever te maken.

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. In dat laatste geval is ontslag om dringende reden niet uitgesloten.

Transparantie

71. Geheime controles zijn verboden. Indien de werkgever controle van het internetgebruik wil installeren moet hij de werknemers (binnen de overlegorganen in de onderneming) informeren. Dat kan op verschillende manieren gebeuren: via individuele circulaires, het arbeidsreglement, de arbeidsovereenkomst of via een waarschuwing op de computer. Daarbij moet de werkgever duidelijk de invoering van de controle uiteenzetten (artt.7 - 9 cao nr. 81). Ook moet de procedure volgens welke de controle wordt uitgevoerd duidelijk omschreven worden en kenbaar zijn voor de werknemers. Pas dan is de werknemer voldoende geïnformeerd over de mogelijkheid tot controle van het e-mail- en internetgebruik.

Noodzakelijkheid en proportionaliteit

72. Het uitgangspunt is dat de controle op communicatiegegevens van de werknemer geen inmenging op de bescherming van de persoonlijke levenssfeer van de werknemer tot gevolg mag hebben (art. 6). Is dat niet mogelijk dan moet de intrusie van de privacy tot een minimum herleid worden. Deze voorwaarde geeft uiting aan het beginsel van proportionaliteit, dat inhoudt dat alleen de nodige en relevante gegevens mogen verwerkt worden. Het is niet alleen een belangrijk beginsel in zowel de beperkingsleer van de grondrechten als in het kader van de

bescherming van persoonsgegevens (respectievelijk art. 8 tweede lid EVRM en art. 4, 3° WVP). De toepassing van de proportionaliteit vraagt telkens een case-by-case benadering.

73. Een permanente controle op het internetgebruik- e-mailgebruik is moeilijk te rijmen met het noodzakelijkheids- en proportionaliteitsbeginsel. Wat wil dat nu zeggen? Dat telkens een afzonderlijke toets van de casus vereist is:

(1) is de controle noodzakelijk (is geen andere maatregel voorhanden die tot hetzelfde resultaat kan leiden)?; en

(2) welke informatie is relevant om het bewijs te leveren?

Telkens opnieuw moet onderzocht worden welke informatie noodzakelijk en relevant is om het beoogde resultaat te bereiken. Er moeten ernstige aanwijzingen zijn die doen vermoeden dat misbruik wordt gemaakt van de communicatiemiddelen.[77] Daarom is een algemene controle *a priori* op alle telecommunicatiegegevens, alsook de systematische registratie van alle gegevens disproportioneel.

Permanente controle van het internetgebruik is evenwel niet uitgesloten.[78] Wanneer ernstige aanwijzingen van misbruik van de aan de werknemer terbeschikkinggestelde informaticamiddelen voorhanden zijn, moet de werkgever binnen redelijke termijn beslissen wat hij daarmee zal aangevangen. Controle van of andere (naar gelang de omstandigheden meer gepaste) maatregelen. Een permanente controle brengt trouwens eveneens de bescherming van het communicatiegeheim van de deelnemer aan de communicatie ernstig in het gedrang. Dat doet niets af aan de vereisten van noodzakelijkheid en proportionaliteit. Ook bij permanente controle moeten de vereisten van noodzakelijkheid en proportionaliteit nageleefd worden.

Controle van de inhoud

74. De CAO nr. 81 gaat uit van een getrapte controle naarmate de urgentie van de controle. Daarbij geldt dat controle van de inhoud in beginsel niet toegelaten is, tenzij de werknemer ermee akkoord gaat.[79]

Alleen als laatste resort kan de werkgever overgaan tot individualisering. Allereerst moet de controle zich toespitsen op het karakter (omvang en frequentie) van de berichten. Slechts wanneer na opmerkingen en waarschuwing van de werkgever het misbruik toch blijft duren, kunnen de verzamelde telecommunicatiegegevens aan een welbepaalde werknemer gelinkt worden. Het individualiseringsproces kan dus pas worden uitgevoerd wanneer de werknemers voorafgaand aan deze gerichte controle worden onderworpen (art. 16 CAO nr. 81).[80] Individualisering van de telecommunicatiegegevens van de werknemer houdt dus niet in dat de werkgever de

[77] Commissie voor de bescherming van de persoonlijke levenssfeer, Advies uit eigen beweging nr. 10/2000 van 3 april 2000 betreffende het toezicht door de werkgever op het gebruik van het informaticasysteem op de werkplaats, www.privacycommission/beslissingen.

[78] Dat staat in verband met de controle die erop gericht is om de elektronische communicatiegegevens die door de werkgever met toepassing van de spelregels van de CAO nr. 81 werden verzameld te kunnen toeschrijven aan een welbepaalde werknemer (art. 12 CAO nr. 81). De reden is dat de goede werking van de onderneming moet gewaarborgd blijven.

[79] Verslag bij de CAO nr. 81, 8. Daarbij moet zowel rekening worden gehouden met de wet bescherming persoonsgegevens en de bescherming van het communicatiegeheim zoals gewaarborgd door artikel 124 van de wet van 13 juni 2005 betreffende de elektronische communicatie. Kort gezegd komt het erop neer dat zelf met toestemming van de betrokkene de controle van de inhoud van de privécommunicatie een welomschreven en legitiem doeleinde moet nastreven, noodzakelijk moet zijn en ook de toestemming van de andere deelnemer(s) moet verkregen worden. Anders Brussel 22 november 2005. In deze zaak oordeelde het Brussels arbeidshof dat de werkgever binnen de grenzen van de noodzakelijkheid en proportionaliteit, zoals bepaald in het tweede lid van art. 8 EVRM, het recht heeft om de interne post en in zekere mate de inhoud van de berichten te controleren, Brussel 22 november 2005, *JTT* 2006, afl. 947, 218.

[80] Wanneer de werknemer e-mailberichten met ongeoorloofde inhoud krijgt *toegezonden*, kan de werknemer op basis van deze loutere handeling van derden niet ongeoorloofd gebruik van het internet aangerekend worden. De ontvangst van door anderen toegezonden informatie is geen handeling of gedrag die aan de werknemer kan verweten worden, Antwerpen 15 november 2005.

inhoud van e-mailberichten mag lezen. Maar doorgaans staat de rechtspraak welwillend tegenover een controle van de inhoud van elektroniche berichten. Dat heeft vooral te maken met een cruciaal element in rechtszaken, zijnde de bewijsvoering. Vaak zal de rechter op basis van de inhoud van de correspondentie zijn oordeel over het dispuut kunnen vormen.[81]

75. Het proportionaliteitsbeginsel brengt bijgevolg met zich mee dat de controle niet op de inhoud van de communicatie dient toegespitst te worden.[82] Dat is ook de visie van de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL).[83] Aanvankelijk was de CBPL streng in de beoordeling van de controle van de telecommunicatie van de werknemers. In eerdere adviezen had de CBPL gezegd dat de werkgever, zonder de toestemming van *alle* deelnemers (waaronder ook niet-medewerkers van de werkgever die de controle installeert) geen wettelijke controlebevoegdheid had om zowel de professionele als de privécommunicatie te controleren. In een advies van 2 mei 2012 herziet de CBPL haar vroegere adviezen. Er wordt nu onderscheid gemaakt tussen e-mails met een al dan niet beroepsmatig karakter.[84] Op die manier versoepelt de CBPL haar houding ten aanzien van de controle op de inhoud. Volgens de CBPL kan onder omstandigheden ook privécommunicatie door de werkgever gecontroleerd worden. De voorwaarde is dat er redelijke vermoeden van misbruik van door de werkgever ter beschikking gestelde communicatiemiddelen voorhanden.[85] Jammer dat het advies geen aandacht besteedt aan de problematiek van het gebruik en de controle van sociale media op de werkplaats. Dat is wellicht te verklaren door het ontbreken aan rechtspraak.

2.3 BESCHERMING DOOR STRAFWETTEN

2.3.1 Algemeen

76. Naast de hiervoor besproken rechtsinstrumenten wordt de (tele)communicatie nog door strafwetten beschermd. Een bijzonder plaats in het privacyconcept wordt ingenomen door het communicatiegeheim. Net als privacygevoelige persoonsgegevens (zoals medische gegevens) wordt het communicatiegeheim als een risico voor de privacybescherming beschouwd.[86] Onwettige intrusies van het communicatiegeheim worden daarom strafbaar gesteld (artikelen 259*bis* t.a.v. overheidspersoneel en 314*bis* Sw). Tegelijk worden toelaatbare interventies van het communicatiegeheim aan strenge regels onderworpen. Zo vereist het onderscheppen van communicatie de tussenkomst van de onderzoeksrechter (art. 90*ter* Sv). Daarnaast wordt, zonder toestemming

[81] Zie voor een (kort) overzicht uit de rechtspraak 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* 2009-09, afl. 18, 730-744.

[82] P. DE HERT, P. DE HERT, 'C.A.O. nr. 81 en Advies nr. 10/2000 over de controle van internet en e-mail', *l.c.*, 1281 en 1291.

[83] Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL), Advies uit eigen beweging nr. 10/2000 van 3 april 2000 betreffende het toezicht door de werkgever op het gebruik van het informaticasysteem op de werkplaats, sub II, 3.

[84] CBPL, Aanbeveling nr. 08/1012 van 2 mei 2012 betreffende de controle door de werkgever op het gebruik van elektronische communicatie-instrumenten op de werkvloer, www.privacycommission.be/beslissingen. Zo stelt de CBPL voor om twee afzonderlijke account aan de werknemer ter beschikking te stellen: een account waarop de werknemer privégesprekken kan voeren en een account voor louter professionele communicatie. Het gebruik van gescheiden e-mailaccount.

[85] R. SAELENS, 'Privacycommissie versoepelt houding bij e-mailcontrole op de werkplaats', *De Juristenkrant* 2012, afl. 256, 1. Merken we op de aanbeveling het resultaat is van een publieke consultatie dat omtrent deze problematiek door de CBPL in 2012 werd uitgeschreven. Het werkdocument werd op een studiedag van 16 december 2012 voorgelegd en werd zowel van werkgeverszijde als van werknemerszijde verwelkomd.

[86] Dat is vooral gelegen is het feit dat het communicatiegeheim vandaag tot de privacybescherming wordt gerekend. We hebben hiervoor gezien dat, in tegenstelling dat art. 22 GW, artikel 8 EVRM naast de bescherming van het privéleven ook de communicatie beschermt.

van alle deelnemers, het louter kennis nemen van het *bestaan* van telecommunicatie reeds strafbaar gesteld (art. 124 WEC *juncto* 145 WEC).[87]

Voorbeeld:

A is bezig op zijn persoonlijke computer. Wanneer B zonder toestemming van A nagaat of A berichten in zijn postvak heeft ontvangen, is sprake van kennis nemen van het "bestaan" van telecommunicatie. Daarvoor is het niet vereist dat B de berichten ook daadwerkelijk opent en leest.

Voorbeeld:

De Facebookpagina van A staat zichtbaar open op het computerscherm. Zonder toestemming van A klikt B op de link "vrienden". Ook hier is sprake van kennis nemen van het bestaan van telecommunicatie.

Hierna bespreken we achtereenvolgens artikel *314bis* Sw van de wet van 30 juni 1994 op het afluisterverbod, artikel 124 de wet van 13 juni 2005 betreffende de bescherming van telecommunicatie (WEC) en artikel 550*bis* Sw van de wet van 28 november 2000 inzake de bescherming tegen onwettige intrusie van informaticasystemen.

2.3.2 Afluisterverbod

77. Art. 314*bis* Sw beschermt de communicatie tegen onwettig afluisteren, kennisnemen en opnemen van de *inhoud* van privécommunicatie. Deze strafbepaling viseert zowel telecommunicatie als gewone gesprekken. Ook wordt er in principe geen onderscheid gemaakt naar de karakter van de communicatie, of dat nu zakelijk of niet-zakelijk is. Om op een wettige manier communicatie te kunnen onderscheppen, er kennis van nemen of op te nemen is de toestemming van alle partijen nodig die aan de communicatie deelnemen. Het toepassingsgebied van artikel 314*bis* Sw is evenwel onderworpen aan twee beperkingen: de bescherming geldt alleen *tijdens de overbrenging* van de communicatie en voor zover de interceptie gebeurt met behulp van een toestel.

78. De voorwaarde dat de interceptie van de communicatie zich moet afspelen "tijdens de overbrenging" zorgt vandaag voor heel wat onduidelijkheid. In de rechtspraak noch in de rechtsleer is er overeenstemming over het precieze moment waarop de overbrenging van de communicatie is beëindigd. In de hypothese dat de werkgever via een derde – als "vriend" – de gesprekken op een SNS volgt: wanneer bevindt de communicatie zich in de fase van overbrenging?[88]

Voorbeeld:

Een werknemer had tijdens de werkuren het de toegang tot het internet gebruikt voor het verhandelen van aandelen en surfen naar sekssites een aanverwante sites. Als verweer op zijn onmiddellijk ontslag om dringende reden voerde de werknemer aan dat de werkgever artikel 314bis Sw had geschonden (afluisterverbod). De rechter oordeelde dat deze strafbepaling niet van toepassing is wanneer de controle wordt uitgevoerd na het beëindigen van de communicatie en dus niet tijdens het verhandelen van de aandelen of surfen op het internet.[89]

---

[87] Wet van 13 juni 2005 op de elektronische communicatie.

[88] Art. 314*bis* Sw bestraft ook de handeling waarbij een derde wordt aangezet om communicatie af te luisteren, er kennis van te nemen of te nemen.

[89] Gent 9 mei 2005, *Computerr.* 2006, afl. 44, 107.

Voorbeeld:

De werkgever controleert de e-mailberichten van een werknemer. Op dat ogenblik had de werknemer deze e-mailberichten nog niet gelezen. De rechter oordeelt dat de werkgever zich schuldig maakt aan kennis nemen "tijdens de overbrenging" van communicatie omdat de werknemer de e-mailberichten nog niet zelf had opgehaald.[90]

Deze voorbeelden illustreren dat het vooraf moeilijk te zeggen is wanneer communicatie onderweg is en in welke gevallen dat niet zo is.

2.3.3 Kennis nemen van het bestaan van telecommunicatie

79. Wellicht biedt artikel 124 WEC meer perspectieven. Deze bepaling verbiedt het kennisnemen en registreren van *tele*communicatie waaraan men niet deelneemt. Alleen de toestemming van alle indirecte of direct betrokken personen kan de kennisneming of registreren van de communicatie van anderen wettigen. Het gaat om communicatie van alle aard en is bijgevolg niet beperkt tot gesprekken. Ook beelden en muziek bijvoorbeeld worden beschermd. Ook de toevallig (en dus zonder opzet) verkregen informatie mag niet zonder de toestemming van alle partijen aan de communicatie worden gebruikt.

80. De bescherming van artikel 124 WEC wijkt op een aantal punten af van de bescherming geboden door artikel 314*bis* Sw en is ruimer dan artikel 314*bis* Sw.

Zo is reeds het *bestaan* van telecommunicatie beschermd. Daaronder wordt niet alleen de inhoud van communicatie begrepen, ook andere communicatiegegevens zoals, namen van de deelnemers, tijdstip en duur van de communicatie wordt beschermd. Bovendien is het toepassingsgebied van de bescherming niet beperkt tot de transportfase (tijdens de overbrenging van de communicatie) en kan kennis nemen van het bestaan van telecommunicatie ook betrekking hebben op de inhoud van de communicatie.

Voorbeeld:

Toepassing art. 124 WEC

Een werkgever vermoedt dat zijn werknemer (tijdens de werkuren) gesprekken voert op Facebook. Wanneer de werkgever via een eenvoudige muisklik vaststelt dat de werknemer bepaalde sociale netwerksites heeft bezocht, is er reeds sprake van het "bestaan" van communicatie, zonder dat de werkgever kennisneemt van de inhoud van de gesprekken. In dat geval is artikel 124 WEC van toepassing: verbod kennis te nemen van het bestaan van telecommunicatie, tenzij met toestemming van alle deelnemers.

Voorbeeld:

X is een beursgenoteerde onderneming. De bedrijfsleiding stelt vast dat een kaderlid buiten de werkuren zich op zijn 'prikbord" op zijn facebookpagina zeer kritisch uitlaat over de koers dat het bedrijf aanhoudt. Daarop wordt het kaderlid om dringende reden ontslagen. Volgens het arbeidshof te Brussel heeft het bedrijf artikel 124

[90] Corr. Leuven 4 december 2007, met noot I. CEULEMANS, 'De kennisname van e-mails "tijdens de overbrenging ervan", een verduidelijking van het telecommunicatiegeheim?', *TStrafr.* 2008, afl. 3, 207-215.

WEC geschonden doordat ze met opzet heeft kennis genomen van de informatie op de facebookpagina van haar werknemer.[91]

Voorbeeld:

Toepassing art. 314bis Sw

Een werkgever vermoedt dat zijn werknemer tijdens de werkuren gesprekken voert op Facebook. Wanneer de werkgever op slinkse wijze de communicatie tussen zijn werknemer en anderen op Facebook volgt, is hij strafbaar wegens schending van het afluisterverbod.[92]

---

81. Het door de wetgever gemaakt onderscheid tussen het kennisnemen van het bestaan en inhoud van communicatie is overigens niet in alle gevallen vol te houden. Zo zal iemand die kennis neemt van de inhoud van communicatie ook kennis nemen van het bestaan van deze communicatie.[93]

Voorbeeld:

A profileert zich op slinkse wijze als "vriend" van B en C op Fasebook. Op die manier neemt hij kennis van de gesprekken tussen (hemzelf,) B en C. Doordat A kennis neemt van de gesprekken (inhoud) tussen B en C, neemt A onvermijdelijk ook kennis van het bestaan van de communicatie (gesprekken).

Als gevolg zal in dergelijke gevallen sprake zijn van zowel een strafbare handeling onder de wet op het afluisterverbod als de WEC.

2.3.4 Hacking

82. Een andere vorm van inbreuk op het communicatiegeheim, die zich onderscheidt van de bovenstaande besproken strafbare handelingen, is hacking.[94] Hacking kan omschreven worden als het ongeoorloofd binnendringen in of toegang tot een informaticasysteem.[95] Onder het begrip "informaticasysteem" wordt verstaan alle systemen voor opslag, verwerking of overdracht van data.[96] De ruime omschrijving van "informaticasysteem" brengt met zich met dat, naast computers en webmailprogramma's (zoals G-mail en MSN Hotmail) en smart-phones ook sociale netwerksites (zoal Facebook en Netlog) onder deze term worden begrepen.[97] Hacking kan twee vormen aannemen: externe hacking en interne hacking. Het onderscheid tussen beide strafbare handelingen is gelegen in het al dan niet beschikken over een (zekere mate van) toegangsbevoegdheid. Wie zich toegang verschaft tot een informaticasysteem terwijl hij daartoe geen toegangsbevoegdheid heeft, maakt zich schuldig aan

[91] Brussel 3 september 2013, *onuitg*.

[92] Met op "slinkse" wij wordt gedoeld op de omstandigheid dat de werkgever met een andere identiteit of door gebruik te maken van een tussenpersoon zich als "vriend" bij zijn werknemer A aanmeldt om op die manier de communicatie van werknemer A te controleren.

[93] Cass. 1 oktober 2009, C.08.0064.N, www.cass.be.

[94] Wet van 28 november 2000 inzake informaticacriminaliteit, *BS* februari 2001. Zie uitgebreid over deze wet P. DE HERT, 'De wet van 28 november 2000 inzake informaticacriminaliteit en het materieel strafrecht. Een wet die te laat komt of een wet die er nooit had moeten komen?', *T.Strafr*. 2001, 286-334;

[95] Memorie van toelichting bij het wetsontwerp inzake informaticacriminaliteit, *Parl. St*. Kamer 1999-2000, nr. 0214/1. De term' hacking' wordt in de wet niet gebruikt.

[96] Memorie van toelichting bij het wetsontwerp inzake informaticacriminaliteit, *Parl. St*. Kamer 1999-2000, nr. 0214/1, 12-13.

[97] J. KERKHOFS en P. VAN LINTHOUT, 'Cybercriminaliteit doorgelicht', *T.Strafr.* 2010, 181

externe hacking. Loutere nieuwsgierigheid is voldoende om deze strafbare handeling te stellen. Wie daarentegen wel toegangsbevoegdheid heeft, maar deze bevoegdheid overschrijdt, maakt zich schuldig aan interne hacking. Bijkomende voorwaarde is dat de handeling gebeurt met bedrieglijk opzet of met het oogmerk te schaden.[98] Wie precies over toegangsbevoegdheid beschikt, heeft de wetgever overgelaten aan de eigenaar van het informaticasysteem.

83. De eigenaar zou het best geplaatst zijn om te bepalen wie toegangsbevoegdheid verkrijgt en binnen welke grenzen.[99] In de onderneming zal de werkgever de eigenaar zijn van de ter beschikking gestelde elektronische communicatiemiddelen. Het is ook de werkgever die de toegang tot het internet faciliteert. In het kader van de controle naar het gebruik van SNS stelt zich bijgevolg de vraag in welke mate de sprake is van externe of interne hacking wanneer de werkgever het internet- en e-mailgebruik van zijn werknemers onwettig controleert.

Voorbeeld:

In de onderneming is de toegang tot het internet niet verboden. Uit loutere nieuwsgierigheid controleert de werkgever op de aan de werknemer ter beschikking gestelde computer het gebruik van SNS door deze werknemer in de onderneming. In dat geval is er geen sprake van externe hacking nu de werkgever de computer aan de werknemer ter beschikking heeft gesteld.

De werkgever zou zich wel aan interne hacking kunnen schuldig maken wanneer wordt aangenomen dat de werkgever door de ongeoorloofde controle zijn toegangsbevoegdheid overschrijdt met bedrieglijk opzet of om de werknemer te schaden. De vraag die zich opdringt is, of de werkgever, in de context van controle op het ongeoorloofd gebruik van internet in de onderneming, zijn toegangsbevoegdheid overschrijdt wanneer hij de principes van de besproken CAO nr. 81 niet heeft nageleefd. En zo ja, of dat gebeurde met bedrieglijk opzet of om de werknemer te schaden. Hierop is geen eenvoudig antwoord te geven. Voorzichtigheid is geboden. Het is afwachten hoe de rechtspraak zal reageren.

Ten aanzien van externe hacking zijn de voorwaarden niet zo streng. Bedrieglijk opzet of oogmerk om te schaden is niet vereist. Algemeen opzet, zoals loutere nieuwsgierigheid, is voldoende om de strafbare handeling te stellen. Maar ook hier maken we voorbehoud. Het volgend voorbeeld kan dit illustreren

---

Voorbeeld:

We nemen het geval dat de werkgever zich op slinkse wijze toegang verschaft tot de communicatie van zijn werknemer op een SNS. In dat geval verschaft hij zich toegang tot een informaticasysteem waartoe hij niet gerechtigd is. Er zou kunnen sprake zijn van externe hacking nu het motief van de handeling geen rol speelt. Zich louter toegang verschaffen tot het systeem is in principe strafbaar. Kennis nemen van de communicatie is niet vereist.

---

[98] Art. 550*bis* Sw.

[99] Arbitragehof 24 maart 2004, nr. 51/2004, www.const-court.be.

3 DEEL III: ENKELE KNELPUNTEN

3.1 ALGEMEEN

84. De term 'informationeel beschikkingsrecht' houdt in dat de burger (een zekere mate van) zeggenschap heeft over het gebruik van zijn persoonsgegevens. Zoals gezegd is de bescherming van persoonsgegevens in de Europese Unie ondertussen tot een zelfstandig grondrecht verheven. [100] Dat informationeel zelfbeschikkingsrecht houdt in dat het individu principieel zelf bepaalt wie, wat en hoe met zijn persoonsgegevens wordt omgegaan. Maar net zoals het recht op privacy, is ook de bescherming van persoonsgegevens niet absoluut. Zowel publieke als private belangen kunnen het principiële zeggenschap over de verwerking van onze persoonsgegevens beperken. Denken we bijvoorbeeld aan het inwinnen en opslag van informatie in het kader van een strafonderzoek en de verplichte verwerking van persoonsgegevens voor sociaalrechtelijke doeleinden. In dit deel worden enkele knelpunten besproken die vaak opduiken in de discussie over de rechtmatigheid van een controle over het internet- en e-mailgebruik.

85. Uit bovenstaande zou onterecht de indruk kunnen gewekt worden dat de controle van het internet en e-mailgebruik alleen zou afspelen binnen de arbeidsrelatie. Zelfs de opsporingsdiensten zijn niet meteen de koplopers van de cybersurveillance. Het zelfbeschikkingsrecht wordt daarentegen het vaakst miskend binnen de context van het gebruik van internet in de private sfeer. Daarbij worden vaak zoekmachines op het internet en sociale netwerksites als boosdoeners aangeduid. De verzamelde informatie wordt aan participerende bedrijven verkocht voor het gebruik van marketingdoeleinden, zoals het aanleggen van profielen van de gebruiker. In deze gevallen worden de persoonsgegevens verder gebruikt voor een ander doeleinde dan ze oorspronkelijk werden verkregen. Wanneer de betrokkene voor deze verdere verwerking niet zijn vrije en op duidelijke informatie berustende toestemming heeft gegeven, is deze verwerking in principe onwettig.

Ook internet service providers (ISP) worden met de vinger gewezen. Zo zouden ISP's gebruik maken van *Deep packet inspection* (DPI). DPI is een techniek waarbij bijvoorbeeld bepaalde woorden uit het e-mailverkeer worden gedetecteerd en in verband gebracht met andere gegevens om op die manier het internetgedrag van de gebruiker te kunnen bepalen met het oog op commerciële doeleinden. In dat geval is de gebruiker van het internet onwetend van deze verwerking en is het zeer gevaarlijk voor de bescherming van de persoonlijke levenssfeer.[101]

86. De rechtspraak inzake de controle op het gebruik van SNS op de werkplaats is (zeer) schaars. Daarentegen is de rechtspraak met de betrekking tot de controle op het gebruik van internet en e-mail ruim voorhanden. Aan de hand van analyse van een greep voorbeelden uit deze rechtspraak kan een mogelijke relatie met de controle op het gebruik van SNS op de werkplaats geconstrueerd worden. Daarbij zal aandacht besteed worden aan het onderscheid tussen professionele en privécommunicatie, de waarde van de toestemming en de bescherming van de deelnemer aan de communicatie.

[100] Artikel 8 van het Handvest van de Europese grondrechten luidt als volgt:
"1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.
2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet.
Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.
3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels".

[101] Zie over DPI, Commissie voor de bescherming van de persoonlijke levenssfeer, Aanbeveling nr. 05/2012 van 11 april 2012 over neutraliteit, deep packet inspection en bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, www.privacycommission.be/beslissingen.

3.2 PROFESSIONELE VERSUS PRIVÉCOMMUNICATIE

87. Volgens sommige rechtspraak is het onderscheid tussen communicatie met een beroepsmatig karakter en privécommunicatie nagenoeg onmogelijk te maken.[102] Andere rechtspraak oordeelt dan weer dat de communicatie tussen de klant en de bediener van de helpdesk een beroepsmatig karakter heeft.[103] Bij een eventuele controle van de communicatie is het onderscheid tussen zakelijke communicatie en privécommunicatie echter moeilijk zo niet onmogelijk te maken. Hoogstens kan het onderscheid *post factum* wordt gemaakt waarbij tevens het probleem rijst van de bescherming van het communicatiegeheim van de andere correspondent. Maar daarmee is nog niet gezegd dat de controle van de privécommunicatie dan per definitie onrechtmatig is. Immers, uit de besproken rechtspraak volgt dat wanneer het internet buitensporig wordt gebruikt voor privédoeleinden ontslag om dringende reden kan worden aanvaard.

3.3 TOESTEMMING

88. De arbeidsrelatie betekent niet dat de werknemer zomaar afstand doet van zijn grondrechten. In het persoonsgegevensbeschermingsrecht neemt de toestemming een centrale plaats in. Onder de toestemming verstaan, elke vrije, specifieke en op informatie berustende wilsuiting. Volgens de Artikel 29 Groep moet met de toestemming binnen dienstverband omzichtig worden omgesprongen.[104] Het knelpunt is of er binnen het kader van de arbeidsrelatie wel kan sprake kan zijn van een echte vrije keuze, zonder nadeel voor de betrokkene.

89. Uit de meerderheid van de rechtspraak blijkt dat weinig belang aan deze voorwaarde wordt gehecht. Slechts in een minderheid van de rechtspraak zien dat de rechter niet snel aanvaardt dat de toestemming van de werknemer vooraf en op geïnformeerde wijze door de werkgever werd verkregen. Zo blijkt uit het louter onderschrijven van een ICT-policy niet dat de werknemer zijn onvoorwaardelijke toestemming voor de controle van de inhoud van e-mailberichten heeft verstrekt.[105]

Voorbeeld:

Bij of na de ondertekening van de arbeidsovereenkomst wordt aan de werknemer een document voor gelegd waarbij hij zijn toestemming heeft voor controle van zijn gebruik van SNS. De werknemer ondertekent (noodgedwongen) een document dat moet doorgaan als een privacy policy. Het document vermeldt echter niet onder welke voorwaarden en omstandigheden de controle kan plaatsvinden. Zo'n voorafgaande en algemene toestemming wordt niet aanvaard.

[102] Arbh. Antwerpen 15 december 2004, *SRK* 2006, 146. In deze zaak wordt het kennisnemen van het bestaan en de inhoud van de gevoerde elektronische correspondentie via de computerapparatuur op het bedrijf onderzocht in het licht van de toepassing van de hiervoor besproken CAO nr. 81. De rechter oordeelt dat de CAO niet in overeenstemming is met de Europese rechtspraak die zegt dat de bescherming van artikel 8 EVRM ook van toepassing is op zakelijke communicatie.

[103] Gent 9 mei 2005, met noot P. VAN EECKE en B. OOMS, 'De controle van e-mail- en internetgebruik door de werkgever in België: ambiguïteit in de rechtspraak, *Computerrecht* 2006, afl. 45, 107-120.

[104] In het advies WP 55 van 29 mei 2002 in verband met de controle op elektronische communicatie op het werk stelt de Groep zich op het standpunt dat "wanneer een werkgever als noodzakelijk en onvermijdelijk gevolg van de arbeidsverhouding persoonsgegevens moet verwerken, het *misleidend is indien hij deze verwerking door middel van toestemming tracht te wettigen* (onze cursivering). Zich baseren op de toestemming moet worden beperkt tot gevallen waarin de werknemer een echte vrije keuze heeft en nadien de mogelijkheid heeft om de toestemming zonder nadeel in te trekken".

[105] Brussel 3 april 2003, *SRK* 2005, 208; Arbh. Antwerpen 15 december 2004, *SRK* 2006, 146.

90. Ook wanneer er in het bedrijf geen reglement op het gebruik van internet voorhanden is of bestaande wet- en regelgeving niet werd nageleefd, kan met de toestemming *post factum* geen rekening worden gehouden.[106]

Voorbeeld:

Een werknemer heeft zich ziek gemeld. Tijdens zijn afwezigheid op het werk gaat de werkgever over tot controle van het internetgebruik. De werknemer is niet op de hoogte van de controle. Wanneer de werknemer na de ziekteperiode zich opnieuw op het werk aanmeldt, wordt hij door de werkgever geconfronteerd met de resultaten van de internetcontrole. Op dat ogenblik wordt de werknemer een document voorgelegd waarop hij toestemming heeft voor de uitgevoerde controle. Dergelijke toestemming is in principe ongeldig.

91. De toestemming kan ook impliciet worden gegeven. In dat geval blijkt de toestemming niet uit een ICT-protocol, privacyreglement of arbeidsovereenkomst. De impliciet toestemming wordt afgeleid uit de feitelijke omstandigheden.

Voorbeeld:

Werknemer A verstrekt het paswoord van de bedrijfscomputer aan collega B op het werk. Tijdens de afwezigheid van A neemt B kennis van de e-mailberichten van A. B heeft daarbij gebruik moeten maken van het paswoord dat hij van A heeft gekregen. Uit enkele e-mailberichten blijkt dat A buitensporig gebruik maakt van de computer voor privédoeleinden. B meldt deze bevinding aan de werkgever. Als gevolg wordt werknemer A ontslagen. De rechter beschouwt de doorgifte van het paswoord als een impliciete toestemming om de e-mailberichten van A te lezen.[107]

3.4 BESCHERMING DEELNEMER/ONTVANGER

92. 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? Ondanks dat de ontvanger niet het voorwerp van een controle uitmaakt, wordt zijn toestemming voor een mogelijke controle van de communicatie impliciet gegeven. Deze impliciet toestemming wordt doorgaans aangenomen wanneer de communicatie niet wordt aangemerkt dat ze privéberichten zijn.[108]

In de besproken CAO nr. 81 wordt trouwens 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 problematiek van de andere deelnemers aan de communicatie niet of onvoldoende belicht.[109] Zoals reeds opgemerkt wordt door de Privacycommissie aanbevolen dat bij de communicatie in dienstverband zou onderscheid gemaakt worden tussen e-mails met een al dan niet beroepsmatig karakter. De inhoud van de e-mailberichten met een beroepsmatig karakter zouden dan het voorwerp kunnen uitmaken van een inhoudelijke controle. Telkens

[106] Brussel 13 september 2005, *Computerrecht* 2006, afl. 43, 100; Arbh. Hasselt 21 oktober 2002, *SRK* 2003, 197.

[107] Antwerpen 28 mei 2003, *onuitg.* Vgl. Antwerpen 8 januari 2003, *RW* 2005-2006, 391.

[108] Anders Gent 22 oktober 2001, waar het arbeidshof oordeelde dat het doelbewust installeren van specifieke software die op zoek gaat naar privédocumenten van de werknemer niet alleen diens privacy schendt maar ook de privacy van de andere deelnemer aan de communicatie schendt wanneer dat gebeurt zonder de toestemming van deze persoon.

[109] CBPL, Aanbeveling nr. 08/1012 van 2 mei 2012 betreffende de controle door de werkgever op het gebruik van elektronische communicatie-instrumenten op de werkvloer, www.privacycommission.be/beslissingen.

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. Of de ondernemingen de aanbevelingen van de Privacycommissie effectief in de praktijk gaan omzetten valt nog af te wachten.

3.5 SNS BUITEN DE WERKUREN

93. De werkgever kan het gebruik van sociale netwerken buiten de werkuren niet verbieden. Zijn gezag reikt niet zo ver dat hij het doen en laten van zijn medewerkers mag controleren. Hiervoor hebben we evenwel aangetoond dat de communicatievrijheid van de werknemer niet zo ver reikt dat hij onfatsoenlijke zaken ten opzichte van de werkgever kan uiten. Zaken die betrekking hebben op de persoonlijke levenssfeer kunnen negatieve gevolgen hebben voor de arbeidsrelatie.

Voorbeelden:

Een ogenschijnlijke zieke werknemer heeft het relaas van een leuke winkelnamiddag op Facebook gedeeld.

In een andere zaak had een werknemer van Ford een foto van het nieuwe model enkele uren voor de officiële aankondiging op Facebook gezet. In beide gevallen kan ontslag tot gevolg hebben.

Voorbeeld:

X is een beursgenoteerde onderneming. De bedrijfsleiding stelt vast dat een kaderlid buiten de werkuren zich op zijn 'prikbord op zijn facebookpagina zeer kritisch uitlaat over de koers dat het bedrijf aanhoudt. Daarop wordt het kaderlid om dringende reden ontslagen. Volgens het arbeidshof te Brussel heeft het bedrijf artikel 124 WEC geschonden doordat ze met opzet heeft kennis genomen van de informatie op de facebookpagina van haar werknemer.[110]

94. Het zijn voorbeelden waarbij de werknemers onbezonnen informatie op sociale netwerken delen waarbij zelden worden gedacht aan de gevolgen van hun handelingen.[111] 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. Dergelijk gedrag kan ontslag op staande voet (en dus zonder opzegvergoeding) tot gevolg hebben. Er zij opgemerkt dat de werkgever deze informatie niet zelden verkrijgt via personen die met de betrokkene communiceren. 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.[112]

[110] Brussel 3 september 2013, *onuitg*.

[111] Deze voorbeelden zijn een weergave van vragen die gesteld werden op Jobat, www.jobat.be.

[112] Zie onder meer Brussel 3 september 2013, *onuitg*.

3.6 ZIJN SNS PUBLIEKE RUIMTEN?

95. Voorgaande voorbeelden vormen de aanzet tot de complexe vraag of sociale netwerken als publieke ruimten moeten worden beschouwd. Uit het zeer recent arrest van het Brussels arbeidshof van 3 september 2013 blijkt dat de gebruiker een redelijke privacyverwachting kan doen gelden wanneer gebruiker de toegang tot de informatie beperkt tot een welbepaalde kring, *i. c* 'vrienden'. Zelfs als zou aangenomen worden dat SNS publieke ruimten zijn, betekent dat niet dat de communicatie geen besloten karakter zou kunnen hebben. Uit Europese rechtspraak blijkt namelijk dat het recht op privacy ook geldt in publieke ruimten. Communicatie in een publieke ruimte ontneemt niet noodzakelijk het besloten (privé) karakter van de communicatie. Een en ander hangt mede af van de intentie van de deelnemers aan de communicatie en de context waarin het gesprek plaatsvindt. Is het de intentie van de partijen dat het gesprek in een besloten kring wordt gevoerd of wordt het gesprek niet afgeschermd en toegankelijk voor een onbepaalde groep mensen?[113]

Voorbeeld:

Een werknemersvertegenwoordiger had op Facebook deelgenomen aan een voor iedereen toegankelijk debat. Behalve kritiek over de werkgever, had de werknemer ook dreigende taal geuit aan het adres van de werkgever en aan aantal collega's op het werk. De rechter oordeelde dat de discussie een publiek karakter had.[114]

Voorbeeld:

Een manager van een beursgenoteerde onderneming had de negatieve resultaten van de onderneming besproken op zijn publiek prikbord de 'wall'van zijn Facebookpagina. Zijn Facebook-profiel was voor iedereen toegankelijk. De Leuvense arbeidsrechtbank oordeelde dat er geen sprake was van schending van zijn privacy omdat de informatie niet afgeschermd was voor derden.[115]

3.7 DE BESCHERMENDE WERKING VAN DE WVP

96. In weerwil over de onduidelijke toepassing van de CAO nr. 81 en de discussie over de reikwijdte inzake toepassing van de strafwetbepalingen betreffende de bescherming van de telecommunicatie op de werkplaats, kan de wet verwerking persoonsgegevens (WVP) bescherming bieden tegen de onrechtmatige verwerking van persoonsgegevens. In het kader van deze bijdrage zou de inzet betrekking kunnen hebben op onrechtmatige controle van communicatie op SNS (met het oog op sanctionering van de werknemer). Het volgen van het gedrag van werknemers op internet valt immers onder de WVP indien kan worden nagegaan welke werknemers het precies betreft.[116]

[113] Deze redenering wordt ook gevolgd met betrekking tot de vraag of degene die het gesprek afluistert (opneemt) kan aannemen dat het gesprek ook voor hem bestemd is. Ook hier zijn de bedoelingen van de deelnemers aan het gesprek een belangrijk uitgangspunt bij de vraag of er sprake is van schending van het communicatiegeheim.

[114] Brussel 4 maart 2010, aangehaald door S. COCKX, *l.c.*, 15.

[115] Arbrb. Leuven 17 november 2011, aangehaald door S. COCKX, *l.c.*, 15.

[116] Brussel 8 april 2003, *SRK* 2005, 208; F. HENDRICKX, *Privacy en arbeidsrecht*, die Keure 1999, 186; J. DUMORTIER, 'Little brother is watching you: mag de werkgever het internetgebruik van de werknemer controleren?' in Liber Amicorum R. Blanpain, die Keure 1998, 249. Zie voor een interessante zaak waarin voor het eerst toepassing wordt gemaakt van artikel 14 WVP dat de verwijdering van onrechtmatig verwerkte persoonsgegevens mogelijk maakt, R. SAELENS, 'Kan de Wet Verwerking Persoonsgegevens de Antigoonleer buitenspel zetten?', noot onder Gent 16 juni 2001, *RW* 2012-13, afl. 31, 1221-1226.

3.7.1 Verwijdering en vernietiging van persoonsgegevens

97. De werknemer kan een niet onbelangrijke gerechtelijke actie nemen die het lot kan bezegelen van de over hem opgeslagen informatie. Hij kan namelijk voorkomen dat een derde (werkgever) zijn persoonsgegevens zou kunnen gebruiken (als bewijsmiddel). De vraag is op welke manier hij dat kan doen. Welnu, de WVP kent aan de persoon van wie zijn of haar persoonsgegevens worden verwerkt een aantal subjectieve rechten toe. Het zijn subjectieve rechten die een evenwicht moeten bieden tegenover de verwerkingsbevoegdheid van de persoon die de persoonsgegevens verwerkt. Naast het recht op toegang tot de persoonsgegevens (art. 10, § 1 WVP), verbetering en verzet (art. 12, § 1 WVP) kan de burger bij de voorzitter van de rechtbank van eerste aanleg ook de verwijdering van onrechtmatig verwerkte persoonsgegevens vorderen. En dat is nu precies wat de werknemer kan beogen: verwijdering van door een derde op onrechtmatige manier verwerkte persoonsgegevens. Want persoonsgegevens worden onrechtmatig verwerkt wanneer de randvoorwaarden van de WVP niet worden nageleefd.[117]

98. Hoe moet de werknemer tewerk gaan? De werknemer moet de zaak voorleggen aan de voorzitter van de rechtbank in eerste aanleg.[118] Deze rechter behandelt zaken over betwistingen omtrent verwerkingen van persoonsgegevens. Wat kan degene die meent dat zijn persoonsgegevens onwettig verwerkt worden aan de rechter vragen:

- Dat zijn persoonsgegevens correct worden verwerkt;

Voorbeeld:

Op een SNS staat te lezen dat u overleden bent. Maar dat berust op een vergissing. U kan deze rechtzetting desnoods afdwingen voor de rechtbank

- Dat u toegang kan krijgen tot de persoonsgegevens die over u verwerkt worden;

Voorbeeld:

U wenst uw gegevens die de werkgever in het personeelsdossier bijhoudt, inzien. Maar de werkgever weigert u inzage te verlenen.

[117] En bovendien strafbaar met geldboeten (art. 39 WVP). Denken we maar aan de geldboete van 150.000 dat Google diende te slikken voor het (onbewust) registreren van telecommunicatiegegevens bij het verzamelen gegevens voor Google Streetview.

[118] Art. 14, § 1 WVP luidt als volgt. "De voorzitter van de rechtbank van eerste aanleg, zitting houdend zoals in kort geding, neemt kennis van de vorderingen betreffende het door of krachtens de wet verleende recht om kennis te krijgen van persoonsgegevens, alsook van de vorderingen tot verbetering, tot verwijdering of tot het verbieden van de aanwending van onjuiste persoonsgegevens of die gelet op het doel van de verwerking onvolledig of niet ter zake dienend zijn, dan wel waarvan de registratie, de mededeling of de bewaring verboden is, tegen de verwerking waarvan de betrokkene zich heeft verzet of die langer bewaard werden dan de toegestane duur". Het is daarbij van belang om op te merken dat art. 14 WVP moet worden gelezen in samenhang met art. 10 (toegang tot de persoonsgegevens) en 12 (verzet en verwijdering van persoonsgegevens) WVP. Bepaalde overheden en organisaties zijn namelijk van deze verplichtingen vrijgesteld. Dat is onder meer het geval voor de politie en de gerechtelijke overheid. Als gevolg hiervan kan de vordering tot toegang tot de persoonsgegevens, tot verzet, tot verwijdering en tot verbod van het gebruik van de opgeslagen persoonsgegevens niet worden ingeroepen tegen de gerechtelijke overheid en de politie, in zoverre zij hun respectieve opdrachten van gerechtelijke en bestuurlijke politie uitvoeren (art. 3, § 5,1° en 2° WVP). Een van de redenen is dat het principe van het geheim van het strafonderzoek ondergraven zou worden. De betrokkene zou er anders van op de hoogte zijn dat tegen hem een strafonderzoek loopt.

U richt een verzoek om toegang tot uw gegevens aan een administratief orgaan van de overheid. De overheid antwoordt niet binnen de 45 dagen op uw verzoek. Dat is de termijn waarbinnen antwoord op uw verzoek moet volgen.[119]

- Dat uw gegevens uit het bestand of dossier verwijderd worden;

Voorbeeld:

Op een SNS wordt over u gepraat, zonder dat u zelf aan de gesprekken deelneemt noch gebruik maakt van een SNS noch hebt u toestemming gegeven om uw persoonsgegevens te verwerken. U kan de rechter vragen dat het beveelt dat uw persoonsgegevens verwijderd worden.

- Dat de gegevens moeten verwijderd en niet mogen gebruikt worden;

Voorbeeld:

In een zaak diende het Gentse hof van beroep zich uit te spreken over de rechtmatigheid van de verwerking door een werkgever van de persoonsgegevens van zijn werknemer in het raam van een uitgevoerde e-mailcontrole op de werkplaats. Volgens de werknemer was de emailcontrole strijdig met zowel de wet van 8 december1992 betreffende de verwerking van persoonsgegevens als de CAO nr. 81. In deze zaak voert de eiser concreet aan dat de werkgever persoonsgegevens heeft verwerkt in strijd met het finaliteits- en proportionaliteitsprincipe.

Het Gentse hof van beroep besluit dat de controle van het e-mailverkeer werd uitgevoerd op basis van een onbepaald doeleinde. De werkgever had namelijk nagelaten de doelstelling van de controle uiterlijk ten laatste op het ogenblik van de controle precies en duidelijk aan de werknemer mede te delen. Dat het gonsde van geruchten dat de werknemer zijn e-mailaccount gebruikte om concurrerende activiteiten op te zetten, is in de ogen van het Gentse Hof onvoldoende. Een gerechtvaardigde e-mailcontrole vereist duidelijke aanwijzingen dat de professionele communicatiemiddelen worden misbruikt. Op die manier is de verwerking strijdig met het finaliteitsprincipe en tevens disproportioneel, omdat de controle verder is gegaan dan de CAO nr. 81 toelaat. Er is met andere woorden geen plaats voor arbitraire verwerkingen van persoonsgegevens.

---

99. Uit bovenstaande volgt dat de gebruiker (werknemer) van sociale media niet verstoken is van grondrechtelijke bescherming van zijn privacy en persoonsgegevens. De WVP biedt de betrokkene (gebruiker) de nodige instrumenten om een dam op te werpen tegen een onwettige of ongebreidelde verwerking van zijn persoonsgegevens. Via de rechter kan de betrokkene (gebruiker) zijn controlerechten afdwingen en (verdere) negatieve gevolgen voor zijn persoon verhinderen of stopzetten. Voorwaarde is dat deze wet op een correcte manier in stelling wordt gebracht. Via de besproken procedure zou de werknemer dus kunnen voorkomen dat de werkgever informatie over de werknemer, die op sociale netwerken wordt uitgewisseld, bijhoudt voor later gebruik. Dat kan het geval zijn wanneer de werkgever bijvoorbeeld zich op slinkse wijze als “vriend” of “vrienden van” toegang krijgt tot informatie over de werknemer, zonder diens medeweten. Van belang daarbij is of de werknemer kon verwachten dat het gebruik van SNS op of na het werk kon gecontroleerd worden.

[119] Uit het cassatiearrest van 14 februari 2013 volgt dat de verantwoordelijke voor de verwerking alleen aan zijn informatieplicht heeft voldaan wanneer hij de categorieën van gegevens en de persoonsgegevens die zijn verwerkt aan de verzoeker worden medegedeeld (Cass. 14 februari 2013, C.11.0777.F, www.cass.be.

4 DEEL IV: SLOTBESCHOUWINGEN

100. De controle van het internet- en e-mailgebruik zoals geregeld door de bestaande wetgeving lijkt niet probleemloos toepasbaar op sociale media. Het onderscheid is vooral gelegen in de vrijheid van de gebruiker (*user*). Terwijl de e-mail- en internetgebruiker in het algemeen een zekere mate van controle (zelfbeschikkingsrecht) over het vrijgeven van persoonlijke informatie heeft, is dat doorgaans minder het geval op SNS. SNS is vooral gericht op het quasi onbeperkt uitwisselen van persoonlijke informatie waarbij de deelnemers vaak niet beseffen dat de – vaak gevoelige - informatie ook buiten de ogenschijnlijk afgebakende kring wordt verspreid en kenbaar gemaakt. Op die manier kunnen derden, zoals de werkgever, zich "onschuldiger" toegang tot de informatie verschaffen dan het geval is wanneer de communicatie via bijvoorbeeld e-mail of Sms-berichten wordt uitgewisseld. Zo hebben derden doorgaans rechtstreeks toegang tot het profiel van de gebruiker, kunnen ze zich makkelijk (onder andere naam of pseudoniem) voorstellen als "vriend" of "vrienden van" en deelnemer worden aan de communicatie.

101. Op die manier zou de werkgever ongestoord het gedrag van de werknemers kunnen controleren, zowel binnen als buiten de werkuren. Uiteraard is het gezags- en controlerecht van de werkgever begrensd door de werktijd. Na de werkdag hoeft de werknemer geen controle van de werkgever ten aanzien van zijn arbeidsprestaties te verwachten. Een werkgever die de werknemer tijdens zijn vrije uren en dagen controleert, schendt dan ook de privacy van de werknemer en de andere deelnemers aan de interactie. Aan de andere kant mag de werknemer zich zowel binnen als buiten de werkuren niet schuldig maken aan lasterlijke of andere ongeoorloofde uitingen en handelingen jegens de werkgever. Hoewel interactie via SNS uiting geeft aan de vrijheid van meningsuiting, mag deze vrijheid niet ontaarden in het plegen van strafrechtelijke feiten. Hiervoor hebben we immers gezien dat de schaarse rechtspraak vaak betrekking heeft op lasterlijke aantijgingen jegens de werkgever, al dan niet tijdens de werkuren. Een werknemer die na zijn werkuren op een SNS kritiek verspreid over zijn baas zal er rekening moeten mee houden dat de werkgever kan meeluisteren. Kritiek die de eer en de goede naam van de persoon van de werkgever of de onderneming zelf in het gedrang brengt, kan leiden tot ontslag en strafrechtelijke vervolging. Dat geldt eveneens wanneer de werkgever gevoelige bedrijfsinformatie via een SNS op straat gooit.

102. Het besproken onderscheid tussen communicatie met een beroepsmatig karakter privécommunicatie is problematisch. Zo wordt in de Europese rechtspraak en de Belgische wetgeving enerzijds in principe geen onderscheid gemaakt tussen zakelijke en privécommunicatie.[120] Daarentegen is de Belgische rechtspraak op dat vlak verdeeld. Naargelang de feitelijkheden van de zaak wordt de communicatie tijdens de werkuren al dan niet als privé dan wel zakelijk beschouwd. Er zijn geen eenduidige criteria op basis waarvan de betrokkenen het karakter van hun communicatie kunnen inschatten. Maar zo verbazingwekkend is dat niet. Een aanvankelijk "zakelijk gesprek" kan snel ontaarden in of snel evolueren naar een privégesprek. Hoe bepaal je dat onderscheid? Het enige criterium dat de wetgever heeft voorzien is, dat een gesprek "privé" is wanneer het niet bestemd is om door anderen te worden gehoord. Men kan zich onmiddellijk de vraag stellen in welke mate de communicatie tussen werknemers onderling en werknemers en derden niet bestemd is om door de werkgever te worden gehoord of er kennis van te nemen. Hierbij kan de continuïteit van de onderneming een rol spelen.

[120] Zie hierover P. DE HERT, 'C.A.O. nr. 81 en Advies nr. 10/2000 over de controle van internet en e-mail', *l.c.*, 1282. Merken we op dat de besproken wet van 30 juni 1994 met betrekking tot het principiële aftapverbod onder privécommunicatie ook zakelijke communicatie verstaat.

103. Een bijkomend heikel punt is de kwalificatie van de interactie op SNS tijdens en na de werkuren. Op SNS is de communicatie van alle aard. Het gaat niet alleen om opinies die de vrije mening van de deelnemers ventileren, maar ook privégesprekken en andere communicatie zoals foto's en afbeeldingen. Een onderscheid tussen communicatie met een beroepsmatig karakter en privékarakter lijkt dan ook moeilijk, zo niet onmogelijk te maken. Daar komt nog bij dat de informatie op sociale netwerken vaak met meerdere deelnemers wordt gedeeld of dat de andere deelnemers interveniëren zonder dat zich op enigerlei wijze bewust kunnen zijn van het beroepsmatig karakter van de interactie van de andere deelnemer(s). In de rechtspraak en de rechtsleer blijft controverse en discussie over het karakter van sociale media in termen van privacy en persoonsgegevensbescherming. Sommige rechtspraak en rechtsleer wijzen op de verantwoordelijkheid van de werknemer. De gebruiker moet beseffen dat SNS geen vrijplaats is voor privacybescherming in ruime zin. Alles is kenbaar en publiek toegankelijk, is de gedachte. In het beste geval kunnen de privacy-instellingen (bijvoorbeeld: "vrienden") enige soelaas brengen. Deze "privacy-tools" worden echter vaak als een illusie beschouwd. Andere verdedigen een technologie neutraal uitgangspunt. In deze visie ligt de verantwoordelijkheid bij de SNS. De burger mag er van uitgaan dat zijn privacy ook daadwerkelijk wordt beschermd. Daarbij geldt dat niet de privacysettings doorslaggevend zijn maar wel de intentie van de gebruiker. Als de informatie enkel en alleen bestemd is voor welbepaalde personen (of afgebakende groep), dan kan de gebruiker privacybescherming genieten.[121]

104. Deze bijdrage laat zien dat de wetgeving op het vlak van controle op het internetgebruik onduidelijkheden bevat dat en evenmin de rechtspraak hierin te hulp schiet. Dergelijke confusie kan eveneens geconcludeerd voor de bestaande rechtsinstrumenten en rechtspraak over de controle op het gebruik van SNS op het werk. De spelregels inzake het uitwisselen van informatie zijn van andere orde dan het surfen op het internet en het communiceren via e-mail. Het lijkt daarom aanbevolen dat de wetgever en de sociale partners het gebruik en de controle van de elektronische communicatie in het algemeen herbekijken. Daarbij stelt zich de vraag of een bijzondere regeling ten aanzien van het gebruik van en de controle op het gebruik van SNS wel realistisch en gewenst is. Is er nog plaats voor nieuwe en totaal andere communicatiemiddelen en –kanalen in het communicatielandschap? Wellicht wel. Hoe kunnen de wetgever en de sociale partner hierop dan op een adequate manier anticiperen, voor zover dat al mogelijk is?

[121] Zie voor een discussie over beide invalshoeken, J. ROUSSEAU en I. PLETS, 'Sociale media en arbeidsrecht. Een praktische leidraad voor sociale mediarichtlijnen ', 119-156, 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*, Intersentia 2013, 286 p.

5 BIBLIOGRAFIE

L. ASSCHER, *Communicatiegrondrechten.*, Otto Cramwinckel Uitgeverij 2002, 13-26.

W. BRUGGEMAN, 'Naar een nieuw concept sociale media voor de Belgische politie', *Panopticon* 2011, afl. 6, 37-43.

M.K. BULTERMAN en R.A. LAWSON, 'Het EU-grondrechtenhandvest: méér dan een festijn voor juristen', *Int. Spectator* 2000, 423-429.

I. CEULEMANS, 'De kennisname van e-mails "tijdens de overbrenging ervan", een verduidelijking van het telecommunicatiegeheim?', *TStrafr.* 2008, afl. 3, 207-215.

S. COCKX, 'Sociale media in de arbeidsrelatie: 'vriend' of vijand?', *Or*. 2012, afl. 1, 12-24.

D. DE BOT, *Verwerking van persoonsgegevens*, Kluwer 2001, 403 p.

R. DE CORTE, 'De achterkant van de privacy: kan het beroep op privacy leiden tot straffeloosheid?' noot onder Gent 22 maart 2002, *NJW* 2003, 798-810.

P. DE HERT, 'Het verzamelen en gebruiken van visuele informatie: foto's, videosurveillance en verkeersradar, *Belgisch Politievakblad*, Politeia 1994, 9 oktober.

P. DE HERT, 'C.A.O. nr. 81 en Advies nr. 10/2000 over de controle van internet en e-mail', *RW* 2002-2003, 1281-1294.

P. DE HERT, 'De wet van 28 november 2000 inzake informaticacriminaliteit en het materieel strafrecht. Een wet die te laat komt of een wet die er nooit had moeten komen?', *T.Strafr*. 2001, 286-334.

P. DE HERT, S. GUTWIRTH, Data Protection in de Case Law of Straatsbourg and Luxemburg: Constitutionalisation in action, in S. GUTWIRTH, *Reinvening Data Protection?*, Springer Science+Business Media, 2009, 3-44.

P. DE HERT en S. GUTWIRTH, 'Oude en nieuwe wetgeving op controletechnieken in bedrijven', *SRK* 1995, afl. 3, 108. P. DE HERT en S. GUTWIRTH, 'Controletechnieken op de werkplaats' (Deel 1 & 2), *Or.* 1993, 93-109, 125-147.

P. DE HERT en V. PAPAKONSTANTINOU, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', *Computer law & Security Review* 2012, 130-142.

P. DE HERT en D. PISSOORT 'De wet verwerking van 8 december 1992 met betrekking tot de verwerking van persoonsgegevens', in P. DE HERT (ed.) *Privacy en persoonsgegevens*, Politeia 2005, losbladig, afl. 16, 1-179.

P. DE HERT en A. HOEFMANS, 'Het arrest *Copland* in het kader van de verdieping van de Europese rechtspraak op het gebied van privacybescherming', *EHRC* 2007, afl. 6, 665-674.

D. DEJONGHE, 'Werkgeverscontrole op e-mail- en internetgebruik: C.A.O. nr. 81 schetst de krijtlijnen', *Or* 2002, 225-235.

R. DELARUE, 'Bescherming van de privacy in de onderneming en de begrenzing van de patronale prerogatieven', *SRK* 1992, 133-141.

B. DE SMET, 'Criteria voor de beoordeling van onrechtmatig verkregen bewijs', noot onder Cass. 4 november 2007, *RW* 2008-09, 111-113.

M.A.C. DE WIT, 'Privacy van werknemers in het informatietijdperk', *Arbeid*, 2002, afl. 6, 351.

J. DUMORTIER, 'Little brother is watching you: mag de werkgever het internetgebruik van de werknemer controleren?' in Liber Amicorum R. Blanpain, die Keure 1998, 249.

G. G. FUSTER en S GUTWIRTH, 'Privacy 2.0?', *Privacy en persoonsgegevens*, Politeia 2009, losbl., afl. 27, Titel V, 213-227.

H. GRAUX, 'Privacybescherming op de sociale netwerken: heeft u nog een privéleven?', in P. VALCKE, P.J. VALGAEREN en E. LIEVENS (eds) *Sociale media. Actuele juridische aspecten*, Intersentia 2013, 1-28.

S. GUTWIRTH, *Waarheidsaanspraken in recht en wetenschap*, Antwerpen-Apeldoorn, Maklu-VUBPRESS 1993, 614-656.

F. HENDRICKX, *Privacy en arbeidsrecht*, die Keure 1999.

F. HENDRICKX, *Elektronisch toezicht op het werk: internet en camera's*, Mechelen, Kluwer 2005.

M. HILDEBRANDT, 'Profiling and the Identitty of the European citizen', in M. HILDEBRANDT en S. GUTWIRTH (eds.) *Profiling the European citizen – Cross-disciplinary perspectives*, Dordrecht, Springer Science 2008.

E. HIRSCH BALLIN, 'Het Handvest van de Grondrechten van de Europese Unie: het eerste hoofdstuk van een Europese Constitutie?', *Ars Aequi* 2001, 50, 2, 88- 93.

F. KEFER, 'Antigone et Manon s'invitent en droit social. Qeulqeus propos sur la légalité de la preuve, *RCJB* 2009, 325-352.

F. KEFER, La légalité de la preuve confrontée au droit à la vie privée', in G. DE LEVAL (ed.), *La preuve et la difficile quête de la vérité judiciare*, Luik, Anthémis 2011, 1758.

J. KERKHOFS en P. VAN LINTHOUT, 'Cybercriminaliteit doorgelicht', *T.Strafr.* 2010, 179-199.

K. KILDONCK, 'Privacy werknemers. Onrechtmatig verkregen bewijs op het werk', *NJW* 2010, 181-183.

K. LENAERTS en E. DE SMIJTER 'Een "Bill of Rights" voor de Europese Unie', in *Bijdragen aan een Europese Grondwet* (Staatsrechtconferentie 2000), 107-138.

J. LORRE, , 'Facebook en arbeidsrecht: *mysterium tremendum et fascinans*', *RW* 2010-11, afl. 36,

A. PEIFFER, 'Controle van e-mailverkeer en internetgebruik', in A. PEIFFER, A. MATTHYS, E. VERLINDEN (eds.), *Privacy in de arbeidsrelatie. Gids voor het voeren van een privacybeleid*, Story Publishers 2008, 49-64.

J. ROUSSEAU en I. PLETS, 'Sociale media en arbeidsrecht. Een praktische leidraad voor sociale mediarichtlijnen ', 119-156, 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*, Intersentia 2013.

R. SAELENS, P. DE HERT, S. GUTWIRTH, Openbaarheid van rechtspraak en het verwerken van persoonsgegevens: categorisch denken vermijden', *AM* 2012, afl. 6, 520-523.

R. SAELENS, 'Kan de Wet Verwerking Persoonsgegevens de Antigoonleer buitenspel zetten?', noot onder Gent 16 juni 2001, *RW* 2012-13, afl. 31, 1221-1226.

R. SAELENS en P. DE HERT, *De wet patiëntenrechten en de verwerking van gezondheidsgegevens*, Politeia 2010.

R. SAELENS, 'Privacycommissie versoepelt houding bij e-mailcontrole op de werkplaats', *De Juristenkrant* 2012, afl. 256, 1.

W. STEENBRUGGEN, *Publieke dimensies van privé-communicatie*, Otto Cramwinckel Uitgeverij 2009.

P. VAN EECKE en B. OOMS, 'De controle van het e-mail- en internetgebruik door de werkgever in België: ambiguïteit in de rechtspraak', noot onder Arbrb. 17 oktober 2005, Brussel 13 september 2005 en Gent 9 mei 2005, *Compterr.* 2006, afl. 44, 107-120.

Y.S. VAN DER SYPE, '(Anti)Antigoon in het arbeidsrecht', *P&I* 2013, afl. 4, 198-199.

A.H. VEDDER, 'Privacy tussen ethiek en techniek', in S. NOUWT & W. VOERMANS (eds.) *Privacy in het informatietijdperk*, Den Haag: SDU 1996, 22.

M. VERMEULEN & P. DE HERT, 'Toegang tot sociale media en controle door de politie. Een eerste juridische verkenning vanuit mensenrechtelijke perspectief', *Panopticon* 2012, afl. 33 (2), 259.

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* 2009-09, afl. 18, 730-744.

G-J. ZWENNE, noot bij Europees Hof van Justitie 6 november 2003 (zaak C101/01), *JAVI* 2004/2.