Eerbiediging
van het privéleven op het werk
Eerbiediging
van het privéleven op het werk

Vrije visie, eigen stem
INHOUD

I. BESCHERMING VAN PERSOONSGEGEVELS .................................................................................................................................................. 9
   1.1 Begrip persoonsgegevens ........................................................................................................................................................................ 9
   1.2 Toepassingsgebied ................................................................................................................................................................................... 9
   1.3 Begrip verwerking .................................................................................................................................................................................. 9
   1.4 Beginstellen ............................................................................................................................................................................................. 9
   1.5 Recht op inzage in het personeelsdossier ........................................................................................................................................... 11

II. CAMERABEWAKING OP DE ARBEIDSPLAATS ............................................................................................................................... 13
   2.1 Wetgevend kader .................................................................................................................................................................................... 13
   2.2 Toepassingsgebied .................................................................................................................................................................................... 13
   2.3 Respect van de volgende principes ....................................................................................................................................................... 13
   2.4 Vier mogelijke doelstellingen ............................................................................................................................................................... 14
   2.5 Informatieplicht – Bekendmaking ....................................................................................................................................................... 14
   2.6 Rechtspraak ............................................................................................................................................................................................. 15

III. CONTROLE VAN INTERNET- EN E-MAILGEBRUIK (ELEKTRONISCHE COMMUNICATIEGEGEVELS) ON THE WORK: CYBERSURVEILLANCE ...................................................................................................................................................... 17
   3.1 Wetgevend kader .................................................................................................................................................................................... 17
   3.2 Doelstellingen ........................................................................................................................................................................................... 17
   3.3 Begrip elektronische communicatiegegevens .................................................................................................................................. 17
   3.4 Respect van de volgende principes ..................................................................................................................................................... 18
   3.5 Individualisering van de elektronische communicatiegegevens .................................................................................................. 20
   3.6 Procedure van directe individualisering .......................................................................................................................................... 21
   3.7 Procedure van indirecte individualisering ........................................................................................................................................ 21
   3.8 Rechtspraak ............................................................................................................................................................................................. 22
   3.9 Preventief optreden door de werkgever .............................................................................................................................................. 24
   3.10 Geheim van elektronische communicatie ....................................................................................................................................... 26
   3.11 Uitzonderingen op het verbod van kennisname en registratie door de werkgever van elektronische communicatie ....................... 26
   3.12 Sancties ................................................................................................................................................................................................. 27
   3.13 Aanbevelingen en adviezen van de Privacycommissie ............................................................................................................... 27
   3.14 Monitoring door de werkgever van een e-mailprogramma ........................................................................................................ 29

IV. CONTROLE VIA SOCIALE MEDIA ....................................................................................................................................................... 31
   4.1 Algemeen ................................................................................................................................................................................................. 31
   4.2 Rechtspraak ............................................................................................................................................................................................. 31
   4.3 Laster ........................................................................................................................................................................................................ 32
   4.4 Sociale media-beleid ............................................................................................................................................................................... 33
V. CONTROLE VIA GEOLOCALISATIESYSTEEM .......................................................................................................................... 35
  5.1 Wetgevend kader ........................................................................................................................................................................ 35
  5.2 Begrip ........................................................................................................................................................................................................ 35
  5.3 Respect van de volgende principes ............................................................................................................................................... 36
  5.4 Toestemming door de werknemer ............................................................................................................................................... 37
  5.5 Privacycommissie ................................................................................................................................................................................ 37
  5.6 Rechtspraak .................................................................................................................................................................................................. 38
  5.7 Mogelijkheid activeren – desactiveren van het systeem ................................................................................................................. 38

VI. BEROEP DOOR DE WERKGEVER OP EEN PRIVÉ-DETECTIVE ........................................................................................................ 41
  6.1 Wetgevend kader .................................................................................................................................................................................. 41
  6.2 Beginselen .................................................................................................................................................................................................. 41
  6.3 Beperkingen van het optreden van privé-detective .............................................................................................................................. 42
  6.4 Schending van de privacy – gevolg inzake geldigheid bewijsstukken ............................................................................................... 42

VII. TOEGANGS- EN UITGANGSCONTROLE VAN WERKNEMERS (FOUILLERING) ........................................................................... 43
  7.1 Wetgevend kader .................................................................................................................................................................................. 43
  7.2 Beginsel .................................................................................................................................................................................................. 43
  7.3 Uitzonderingen op het verbod .............................................................................................................................................................. 43
  7.4 Principe van proportionaliteit naar aanleiding van de controle ........................................................................................................... 44
  7.5 Modaliteiten van de controle ............................................................................................................................................................... 44
  7.6 Weigering van de controle door de werknemer ................................................................................................................................. 44
  7.7 Informatieverplichting ............................................................................................................................................................................. 44
  7.8 Toegelaten vormen van controle ...................................................................................................................................................... 45
  7.9 Toestemming .................................................................................................................................................................................................. 45
  7.10 Gevolgen uitgangscontrole ................................................................................................................................................................. 45
  7.11 Sancties .................................................................................................................................................................................................. 45
  7.12 Rechtspraak .................................................................................................................................................................................................. 45

VIII. CONTROLE VAN DE WERKNEMERS OP HET GEbruIK VAN ALCOHOL EN DRUGS ................................................................. 47
  8.1 Wetgevend kader .................................................................................................................................................................................. 47
  8.2 Begrip .................................................................................................................................................................................................. 47
  8.3 Testen .................................................................................................................................................................................................. 47

IX. BRIEFGEHEIM OP DE ARBEIDSPLAATS ........................................................................................................................................ 49
  9.1 Wetgevend kader .................................................................................................................................................................................. 49
  9.2 Begrip .................................................................................................................................................................................................. 49
X. AFLUISTEREN, REGISTREREN EN OPNEMEN VAN TELEFOONGESPREKKEN ..........................................................51
  10.1 Wetgevend kader ........................................................................................................................................51
  10.2 Begrip ......................................................................................................................................................51
  10.3 Verbod ....................................................................................................................................................51
  10.4 Sanctie ....................................................................................................................................................52
  10.5 Rechtspraak ..........................................................................................................................................52

XI. PRIVACY IN HET KADER VAN EEN SELECTIEPROCEDURE VAN EEN SOLlicitant ..............................53
  11.1 Wetgevend kader ....................................................................................................................................53
  11.2 Principe ................................................................................................................................................53
  11.3 Medisch onderzoek ................................................................................................................................54
Inleiding – basisbeginselen

De bescherming van de privacy, welk geen absoluut recht is, is een grondrecht dat zowel door het Europees Verdrag voor de Rechten van de mens (EVRM), rechtstreeks van toepassing in België, als door de Belgische Grondwet (GW) wordt beschermd.

Ieder individu heeft recht op eerbiediging van zijn privéleven, ook op de arbeidsplaats.


Beide partijen zijn elkaar respect en eerbied verschuldigd. De werknemer moet zijn werk zorgvuldig, eerlijk en nauwkeurig verrichten en handelen volgens de bevelen en instructies van zijn werkgever.

Een beperking aan dit grondrecht is slechts mogelijk indien het bij wet is voorzien en tevens met respect van de volgende principes die steeds terugkeren in ieder behandeld thema:

- **Legaliteitsbeginsel**: de inbreuk op het recht op privacy moet in overeenstemming zijn met een bepaalde, duidelijke en toegankelijke norm.
- **Finaliteitsbeginsel**: het nastreven van een gewettigd doel. De inperking van het recht op privacy is relevant of geschikt om het gerechtvaardigde belang veilig te stellen en een fundamenteel recht te beschermen.
- **Proportionaliteitsbeginsel**: de inmenging in de privacy en de daarvoor gebruikte middelen moeten in verhouding staan tot het nagestreefde doel. Recht op eerbiediging van het privéleven kan worden afgewogen zowel tegenover andere fundamentele rechten als tegenover de economische belangen van de werkgever.
- **Transparantiebeginsel**: de werknemer moet op de juiste manier geïnformeerd worden.

Er is een grens tussen de gewettigde controle door de werkgever en de ongeoorloofde inmenging in het privéleven van de werknemer.

Het recht op bescherming van de privacy is een functioneel recht en mag echter niet gebruikt worden om te ontsnappen aan de gevolgen van gepleegde misdrijven of onrechtmatig gedrag.
De wet van 8 december 1992 voor de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens bevat de dwingende basisverplichtingen en is de onderbouw van elke persoonsgegevensverwerking. (Privacywet) Ze is een transversale wetgeving die ook toegepast moet worden in het raam van de arbeidsrelaties. Ze is verschillende keren gewijzigd, een eerste maal door de omzetting van de Europese Privacyrichtlijn¹.

¹ Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, L. 281, 23 november 1995.
I. Bescherming van persoonsgegevens

De Privacywet is van toepassing t.a.v. de verantwoordelijken voor de verwerking van persoonsgegevens, m.a.w. alle werkgevers, zowel uit de publieke als de privé-sector.

Ze bepaalt de voorwaarden inzake verwerking van persoonsgegevens, de vormverplichtingen, de procedures en te bereiken doelstellingen.

1.1 Begrip persoonsgegevens
Dit is iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van één of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.
Zo zijn de - al dan niet van professionele aard – gepersonaliseerde professionele e-mailadressen, de elektronische communicatiegegevens en de inhoud van de op een dergelijk adres ontvangen of verstuurde e-mails persoonsgegevens.

1.2 Toepassingsgebied
- Al dan niet volledig geautomatiseerde verwerking van persoonsgegevens.
- Iedere niet-geautomatiseerde verwerking van persoonsgegevens die bewaard worden of bestemd zijn om bewaard te worden in een bestand.

1.3 Begrip verwerking
‘Elke bewerking of elk geheel van bewerkingen m.b.t. persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van persoonsgegevens.’

1.4 Beginselen
Vanaf de opzet van de verwerking moet iedere gegevensverwerking één of meerdere specifieke en welbepaalde doeleinden nastreven die bovendien rechtmatig moeten zijn. Mogelijke doelstellingen zijn:

- Het verzekeren van de continuïteit van de geleverde diensten ingeval van afwezigheid, overlijden of vertrek van de werknemer;
Het bewaren van documenten als bewijsstukken;
Controle op de werknemers (gerechtvaardigd door de uitvoering van de arbeidsovereenkomst).

De gegevensverwerking moet noodzakelijk zijn voor de behartiging van een gerechtvaardigd belang van de werkgever.

De verwerking moet proportioneel zijn. Het specifiek doel dat de werkgever bij dit toezicht nastreeft, moet gerechtvaardigd kunnen worden door de behoefte van de onderneming of door de ondernemingsregels of voortvloeien uit de aard van de arbeidsovereenkomst of van de uit te voeren taak. De opgezette verwerking moet noodzakelijk blijken te zijn om die doelstelling te bereiken.

De verwerkte gegevens moeten toereikend, ter zake dienend en niet overmatig zijn, uitgaande van de doeleinden waarvoor de gegevens worden verkregen en verwerkt.

Bovendien mogen gegevens alleen verwerkt worden indien dit noodzakelijk is voor een bepaalde rechtmatige doelstelling (relevantieprincipe) of mits de ondubbelzinnige toestemming van de betrokkene.

Hun bewaringstermijn mag de termijn niet overschrijden die noodzakelijk is voor het verwennenlijken van de doeleinden waarvoor zij werden verkregen of waarvoor zij verder worden verwerkt.

De verantwoordelijke voor de verwerking moet zich ervan verzekeren dat de gegevens nauwkeurig zijn en zo nodig worden bijgewerkt.

Het transparantiebeginsel legt de verplichting op aan de verantwoordelijke voor de verwerking om aan de betrokken werknemers bepaalde informatie te verstrekken, onder meer m.b.t. het doel. einde van de verwerking.

De werknemers moeten goed geïnformeerd worden over wat er met hun persoonsgegevens gebeurt. (finaliteitsprincipe)

De werkgever heeft de verplichting de verwerking vooraf aan te geven aan de Privacycommissie.

De verantwoordelijke van de verwerkingen uitgevoerd n.a.v. een controle of toezicht, moet alle nodige maatregelen nemen om zich ervan te verzekeren dat de rechten van de betrokken werknemers geëerbiedigd worden of kunnen worden uitgeefend en dat de veiligheid van de verwerking verzekerd is. Dit houdt o.a. in dat de toegang tot de gegevens en de verwerkingsmogelijkheden beperkt worden tot wat zij nodig hebben voor het uitoefenen van hun functie of noodzakelijk is voor de verwerking van de dienst.
1.5 Recht op inzage in het personeelsdossier

Iedere werknemer heeft recht van toegang tot en inzage van de gegevens die over hemzelf verwerkt worden. Dit gebeurt op éérvoudig verzoek bij de werkgever die dit niet kan weigeren.
II. Camerabewaking op de arbeidsplaats

2.1 Wetgevend kader

- Wet van 8 december 1992 voor de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.\(^2\)
- Cao nr. 68 van 16 juni 1998 afgesloten in de Nationale Arbeidsraad betreffende de bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de camerabewaking op de werkplaats.

2.2 Toepassingsgebied

Het betreft het opnemen en onmiddellijk weergeven van beelden met of zonder het oog op diens bewaring.

De camerabewaking moet ‘op afstand’ gebeuren. Enkel op de werkplaats kan een vorm van bewaking plaatsvinden. Bijgevolg mag de werkgever de camera’s niet installeren bij de werknemer thuis, ook al werkt deze in het kader van telewerk. De camera’s mogen ook niet geïnstalleerd worden op plaatsen binnen het bedrijf waar de werknemer geen arbeidsprestaties verricht zoals het sanitair, de cafetaria en de kleedruimtes.\(^3\)

2.3 Respect van de volgende principes

Een inmenging in de privacy van de werknemer is toegelaten op voorwaarde dat de volgende principes gerespecteerd worden:

- **Finaliteit**: de werkgever moet een welbepaald, duidelijk omschreven doel voor ogen hebben om de controle via camera te rechtvaardigen en dit expliciet omschrijven (zie doelstellingen).
- **Proportionaliteit**: controle in verhouding tot het te bereiken doel (een verantwoord, niet overmatig gebruik van camera’s). Het is enkel mogelijk indien de werkgever de doelstellingen niet op een andere manier kan bekomen. Met andere woorden, de werkgever moet de middelen gebruiken die het minst binnendringen in de privacy van de werknemers.
- **Transparantie**: voor de werknemer moet het duidelijk zijn wat de werkgever wil bereiken en hoe hij dit gaat bereiken. De werkgever moet melding maken van de aanwezigheid van camera’s (zie informatievereiste).

---

\(^2\) BS 18 maart 1993.
In principe mag geen afbreuk gedaan worden aan het privéleven van de werknemer. Wanneer dit toch het geval is, moet de ondernemingsraad of het comité voor preventie en bescherming bij ontstentenis van ondernemingsraad geraadpleegd worden om te onderzoeken hoe deze inbreuk tot een minimum beperkt kan worden.

2.4 Vier mogelijke doelstellingen
- Controle van veiligheid en gezondheid van de werknemer;
- Bescherming van de goederen van de onderneming;
- Controle van het productieproces, om de goede werking van de machines te controleren of om de organisatie van het werk te evalueren en te verbeteren;
- Controle van het werk van de werknemer.

De werkgever moet de verkregen beelden ter goeder trouw en in overeenstemming met het eraan gegeven doeleinde verwerken.

Voortdurende camerabewaking is enkel toegelaten voor de eerste drie doeleinden. Voor de controle van het productieproces kan het echter enkel betrekking hebben op de machines.

Voortdurende camerabewaking van een werknemer is niet toegelaten. Voortdurende camerabewaking van machines is enkel toegelaten in de mate dat het niet de bedoeling is om de werknemer te viseren.

2.5 Informatieplicht – Bekendmaking
Vooraleer de werkgever overgaat tot het plaatsen van camera’s en op het moment dat het systeem effectief van start gaat, moet hij de werknemers op de hoogte brengen. Hij verschaft informatie over alle aspecten van de camerabewaking (de reden, de periode, de locatie, het eventueel opslaan en bewaren van beelden) aan:

- de ondernemingsraad;
- indien er geen ondernemingsraad is aan het comité voor preventie en bescherming;
- indien er geen comité voor preventie en bescherming is via de vakbondsdelegatie;
- indien er geen vakbondsdelegatie is rechtstreeks aan de werknemers.

In bepaalde gevallen moet de werkgever een consultatieprocedure voeren.

Het principe van de camerabewaking moet vastgelegd worden in het arbeidsreglement en aangegeven worden bij de Privacycommissie.

In geval van geheime camerabewaking gelden de bepalingen van het Strafwetboek. Deze vorm van bewaking kan enkel in overeenstemming met de voorschriften van het Wetboek van Strafvordering.
2.6 Rechtspraak

In de praktijk stelt zich dikwijls de vraag wat het lot is van door de werkgever onrechtmatig verkregen bewijs en bijgevolg welke waarde de rechter hieraan kan geven.

Binnen de rechtspraak heersten twee tegengestelde strekkingen.

Vóór het Cassatiearrest (Antigoonarrest) van 14 oktober 2003⁴, dat wordt besproken in het volgende hoofdstuk, oordeelden de arbeidsgerechten bijna altijd dat elk bewijsstuk dat verkregen werd op een wijze waarbij het recht op privacy van de werknemer werd geschonden, moest worden geweerd. Zo oordeelde het Arbeidshof te Antwerpen dat het onrechtmatig verkregen videobewijs niet kon worden gebruikt bij het beoordelen van de zaak.⁵

Dit is de strekking volgens de welke bewijsstukken ter staving van een overtreding door de werknemer niet geldig zijn indien de vaststelling op onregelmatige wijze gebeurd is.

Het Hof van Cassatie (Manonarrest) aanvaardde echter dat in een geval van geheim cameratoezicht de door een werkgever in strijd met de cao nr. 68 verkregen videobeelden, geldig bewijs vormden. De rechter is niet gehouden het onrechtmatig verkregen bewijs buiten beschouwing te laten indien de volgende drie voorwaarden vervuld zijn:

• De bepaling die miskend werd door de werkgever is niet voorgeschreven op straffe van nietigheid;
• De onrechtmatigheid tast het recht op een eerlijk proces niet aan;
• De onrechtmatigheid tast de betrouwbaarheid van het bewijs niet aan⁶.

Volgens deze strekking zou de werknemer zich niet meer kunnen beroepen op zijn recht op privacy wanneer hij bvb een diefstal pleegt die duidelijk is vastgelegd op camerabeelden.

Het Hof van Cassatie stelt dat het recht op eerbiediging van het privéleven geen absoluut recht is. De werkgever kan, op grond van een gewettigd vermoeden van betrokkenheid van zijn werknemer bij te zijnen nadele gepleegde misdrijven, maatregelen nemen om via camerabewaking, in een door hem uitgebate, en voor het publiek toegankelijke winkelruimte, nieuwe strafbare feiten te voorkomen of vast te stellen. Voor zover deze maatregel de aangifte van de feiten bij de overheid tot doel heeft en toereikend, ter zake dienend en niet overmatig is, is er geen sprake van

inmenging in de uitoefening van het privacyrecht. Bovendien moet deze maatregel niet vooraf worden aangekondigd.⁷

In recente rechtspraak oordeelde het Arbeidshof van Brussel dat in het kader van een ontslag om dringende reden het bewijs van de termijn van drie werkdagen en van de feiten die aanleiding geven tot dit ontslag niet geleverd wordt door camerabeelden die werden verkregen door het gebruik van een verborgen camera.⁸

---

III. Controle van internet- en e-mailgebruik (elektronische communicatiegegevens) op het werk: Cybersurveillance

3.1 Wetgevend kader
- Wet van 8 december 1992 voor de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.9
- Richtlijn 2002/58/EG van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie
- Cao nr. 81 van 26 april 2002 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische onlinecommunicatiegegevens
- Wet van 13 juni 2005 betreffende de elektronische communicatie.10

3.2 Doelstellingen
Er zijn twee doelstellingen:

- aan de werkgever de mogelijkheid bieden binnen bepaalde grenzen controle uit te oefenen op het gebruik van het informatica-instrument dat ter beschikking van de werknemers wordt gesteld;
- voor de werknemer het recht op bescherming van het privéleven waarborgen door regels te bepalen volgens de welke de werkgever zich daarin kan mengen.

3.3 Begrip elektronische communicatiegegevens
Het gaat over de interne en externe elektronische communicatiegegevens met een privé karakter die via het netwerk worden overgebracht in de ruime zin ongeacht de drager (e-mails, SMS en MMS). De volgende gegevens kunnen gecontroleerd worden: de identiteit van de verzender en de bestemmeling, het onderwerp van de mededeling, adressen van bezochte websites, uur van verzending/ontvangst of verbinding en ook de aard en de omvang van een eventueel aanhangsel aan de communicatie met uitzondering van de inhoud.
De toegang tot elektronische communicatie of internetgegevens betreft zowel het toezicht door de werkgever als het bewaren van de elektronische briefwisseling (archivering).

9 BS 18 maart 1993.
10 BS 20 juni 2005.
3.4 Respect van de volgende principes

Legitimité
Het verwerken van persoonsgegevens is slechts toegelaten in welbepaalde gevallen o.m.:

- Bij uitdrukkelijke toestemming van de betrokkene;
- Wanneer de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is;
- Wanneer de verwerking noodzakelijk is voor de behartiging van een gerechtvaardigd belang van de verantwoordelijke voor de verwerking;
- Mits het belang of de fundamentele rechten en vrijheden van de betrokkene niet zwaarder doorwegen.

Finaliteit
Het/De doeleinde(n) van een toegang tot of controle van de elektronische communicatie van de werknemer moet(en) gerechtvaardigd zijn.

Er moet op voorhand duidelijk gemaakt worden waarvoor de controle dient, alsook hoe de eventuele verwerkte gegevens later kunnen gebruikt worden. Dit belet niet dat de verkregen gegevens kunnen worden aangewend voor een ander doel dan hetwelk was aangekondigd, voor zover die aanwending niet onverenigbaar is met het oorspronkelijke doel.

De gegevens moeten steeds eerlijk worden verwerkt. De gegevensverwerking moet dus plaatsvinden in overeenstemming met het of de aangekondigde doeleind(en).

De controle van elektronische communicatiegegevens is maar toegestaan indien één of meer van de vier volgende doeleinden worden nagestreefd welke op uitdrukkelijke wijze moeten gedefinieerd worden door de werkgever:

- Het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of de waardigheid van een andere persoon kunnen schaden. Het Arbeidshof te Antwerpen argumenteerde dat het moet gaan om het raadplegen van de bedoelde sites, hetgeen duidelijk een actieve inbreng van de gebruiker veronderstelt. ¹¹

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

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

- Het ter goeder trouw naleven van de in de onderneming geldende beginselen en regels voor het gebruik van onlinetechnologieën.

Proportionaliteit
De controle van globale gegevens mag niet bovenmatig zijn en geen inmenging in het privéleven van de werknemer meebrengen. Iedere beperking van de privacy van de werknemer moet tot een minimum beperkt worden.
Ze moet een passend en relevant karakter hebben m.b.t. de nagestreefde doeleinden. Enkel globale gegevens mogen worden verzameld.
Er geldt een verbod tot voorafgaande individualisering van de elektronische communicatiegegevens. Pas nadat alle preventiemaatregelen onvoldoende blijken te zijn, kan de werkgever het bestaan van enig misbruik vaststellen.
Inzake internet kan de werkgever gegevens verzamelen over de duur van de aansluiting per werkpost, zonder de bezochte sites te individualiseren. Inzake e-mail kan de werkgever gegevens verzamelen over het aantal per werkpost uitgaande berichten en het volume ervan zonder identificatiemogelijkheid van de werknemer die ze verstuurd heeft.

Transparantie
Dubbele informatieplicht op collectief en individueel niveau:

- Collectieve informatie: de werkgever die een systeem voor controle op elektronische onlinecommunicatiegegevens wil installeren, licht de ondernemingsraad (of het comité voor preventie en bescherming op het werk of bij ontstentenis, de vakbondsafvaardiging, of bij ontstentenis de werknemers) mondeling en bij voorkeur schriftelijk in over alle aspecten van de controle met name:
  - het controlebeleid en de prerogatieven van de werkgever en het toezichthoudend personeel;
  - de nagestreefelde doelstellingen;
  - het feit of persoonsgegevens al dan niet worden bewaard, de plaats en de duur van bewaring;
  - het al dan niet permanente karakter van de controle.
• Individuele informatie: naast de hierboven aangehaalde gegevens meegedeeld aan de ondernemingsraad deelt de werkgever bij de installatie van een controlesysteem aan de werknemer individueel de volgende elementen mee:
  • Het gebruik van instrumenten die de werknemer voor de uitvoering van zijn werk ter beschikking worden gesteld, inclusief de beperkingen wat het gebruik in het kader van de functie betreft;
  • De rechten, plichten, verplichtingen van de werknemers en de eventuele verboden inzake het gebruik van de elektronische onlinecommunicatiemiddelen van de onderneming;
  • De in het arbeidsreglement bepaalde straffen wanneer de regels niet in acht worden genomen.

De werkgever kiest zelf op welke manier deze informatie gebeurt: algemene instructies (cirkulaire, aanplakking,..), het arbeidsreglement, de individuele arbeidsovereenkomst, instructies bij het gebruik.

De werkgever is verplicht te voorzien in het arbeidsreglement in verplichte vermeldingen zoals straffen die kunnen worden toegepast bij een inbreuk van de werknemer.

**Evaluatie**

De geïnstalleerde controlesystemen moeten regelmatig geëvalueerd worden, met het oog op hun aanpassing aan de technologische ontwikkelingen.

Deze evaluatie gebeurt in de ondernemingsraad (bij ontstentenis van ondernemingsraad in het comité voor preventie en bescherming op het werk of, bij ontstentenis, aan de vakbondsafvaarding of, bij ontstentenis, aan de werknemers).

De bedoeling van deze evaluatie is na te gaan of het mogelijk is om de doelstelling van niet- of minimale inmenging in de privacy van de werknemers beter te bereiken.

3.5 **Individualisering van de elektronische communicatiegegevens**

Dit is de handeling die tot doel heeft de gegevens die tijdens een controle werden verzameld te verwerken om ze aan een geïdentificeerde of identificeerbare werknemer toe te schrijven.

Ook hier geldt het respect van de beginselen finaliteit, proportionaliteit en transparantie.

Indien beroepsmatig karakter mag individualisering van de gegevens zonder dat de procedure moet worden nageleefd.
De individualisering van persoonlijke communicatiegegevens is in normale omstandigheden overmatig en bijgevolg mag de werkgever er geen kennis van nemen. Vanaf het ogenblik echter dat ze de goede uitvoering van de arbeidsovereenkomst of het statuut van de betrokkene in het gedrang brengen, mag de werkgever kennis nemen van hun bestaan en niet van hun inhoud.

Afhankelijk van de doelstellingen die door de werkgever worden nagestreefd, zal bij de individualisering een directe of een indirecte procedure worden gevolgd.

### 3.6 Procedure van directe individualisering

Wanneer de werkgever één van de drie eerste doelstellingen nastreeft (zie pagina 18, Finaliteit) en dus wanneer hij een onregelmatigheid vaststelt, mag de individualisering onmiddellijk gebeuren zonder enige andere formaliteit.

Hij beslist tevens over de gevolgen die hij geeft aan deze individualisering.

### 3.7 Procedure van indirecte individualisering

De controle in het kader van de vierde doelstelling (nagaan of de gedragsregels die aan de werknemers worden opgelegd in het kader van het gebruik van de nieuwe technologieën te goeder trouw worden nageleefd) vereist een specifieke procedure.

Alarmbelfase (voorafgaande voorlichtingsfase): de werkgever moet eerst de werknemers op de hoogte brengen van het feit dat op de arbeidsplaats onregelmatigheden werden vastgesteld in het gebruik van de nieuwe technologieën en dat, in geval van herhaling, zal worden overgegaan tot een individualisering van de werknemer die verantwoordelijk is voor de onregelmatigheid. De werkgever moet hierbij de in de onderneming geldende beginselen en regels in herinnering brengen of preciseren, zodat een nieuwe onregelmatigheid van dezelfde aard wordt voorkomen.

Indien een nieuwe onregelmatigheid wordt vastgesteld, zal de werkgever de verdachte werknemer kunnen identificeren. In dit geval moet de geïdentificeerde werknemer uitgenodigd worden voor een persoonlijk gesprek met de werkgever, uitgezonderd ingeval van schorsing van de overeenkomst om welke reden ook. Dit gesprek moet plaatsvinden vóór iedere beslissing of evaluatie die de werknemer individueel kan raken.

Tijdens een gesprek krijgt de werknemer de kans een verklaring te geven voor het gebruik van de elektronische onlinecommunicatiemiddelen waarover hij beschikt. De werknemer kan bezwaren uiten m.b.t. de voorgenomen beslissing of evaluatie. Hij mag zich laten bijstaan door een vakbondsafgevaardigde.

Zoals uit de procedure blijkt, mag de werkgever niet op directe en rechtstreekse wijze kennis nemen van de inhoud van elektronische communicatie.
3.8 Rechtspraak

Internetgebruik

gsm-gebruik
Een werkneemster werd ontslagen nadat de werkgever vaststelde dat ze systematisch belde naar astrolijnen met de gsm die haar door de werkgever ter beschikking gesteld werd. In eerste aanleg werd het ontslag aanvaard door de arbeidsrechter. In beroep werd aandacht besteed aan ‘de redelijke privacyverwachting’ zonder het nodig te achten verder te bekijken of het recht op privacy geschonden was. De werkgever mocht beslissen waarvoor de gsm gebruikt wordt en had eveneens het recht het gsm-gebruik te controleren. Het feit dat hij traag en te weinig daadkrachtig had opgetreden, vormde geen bezwaar.13

E-mailgebruik
De rechter meent dat er geen voldoende zwaarwichtige reden is om tot ontslag over te gaan. In casu stuurde een werknemer, een informaticaverantwoordelijke van een kantoor van gerechtsdeurwaarders, de hele dag via intranet privéberichten naar een collega, hetgeen een negatieve weerslag had op zijn werk. Bijgevolg had de werkgever zijn online tijdverdrijf gecontroleerd. Het overmatig gebruik van e-mail voor private doeleinden houdt een lichte, maar geen zwaarwichtige fout in aangezien volgens het oordeel van de rechter de werkgever eerder had kunnen en moeten ingrijpen. De rechter vond het niet nodig dat de precieze inhoud van de e-mails werd gecontroleerd.14

Onrechtmatig bekomen bewijsmateriaal:
Het Hof van Cassatie is het beginsel volgens welke onrechtmatig verkregen bewijs uit de debatten wordt geweerd, beginnen te nuanceren in strafzaken. De kentering was definitief met het Cassatiearrest van 14 oktober 2003 (Antigoon-arrest).

In dit arrest oordeelt Het Hof van Cassatie dat een onrechtmatig bekomen bewijs enkel verworpen moet worden wanneer bepaalde vormvereisten voorgeschreven zijn op straffe van nietigheid, wanneer de begane onregelmatigheid de betrouwbaarheid van het bewijs heeft aangetast of wanneer het bewijs in strijd is met het recht op een eerlijk proces. Daarin komt het Hof tot een omkering van de tot dan toe gekende bewijsuitsluitingsregel. Dit mijlpaalarrest uit het strafrecht wordt doorgewerkt naar het burgerlijk/sociaal recht en in 2015 naar het fiscaal recht.

Zo herhaalt het Hof dat het aan de rechter is om de toelaatbaarheid van onrechtmatig verkregen bewijs te beoordelen rekening houdend met de elementen van de zaak in haar geheel genomen, met inbegrip van de wijze waarop het bewijs verkregen werd en de omstandigheden waarin de onregelmatigheid werd begaan.

Het Hof van Cassatie vernietigde de beslissing van het Arbeidshof die geoordeeld had de beslissing van de RVA te vernietigen omdat deze genomen was op basis van een onrechtmatig verkregen proces-verbaal. Het Hof van Cassatie oordeelde echter dat een rechter een bewijs niet mag afwijzen enkel en alleen op basis van de vaststelling dat het onrechtmatig verkregen is. De rechter dient over de toelaatbaarheid van het bewijsmiddel te oordelen en het bewijs mag enkel geweerd worden in geval van een miskening van een op straffe van nietigheid voorgeschreven vormvereiste en wanneer de manier waarop het verkregen is, de betrouwbaarheid van het bewijs aantast of het recht op een eerlijk proces in het gedrang brengt.

Door dit arrest wordt de gevestigde rechtspraak in strafzaken naar burgerrechtelijke zaken uitgebreid.

Zo kan de arbeidsrechtbank het voorgelegde bewijs aannemen wanneer de ernst van de inbreuk van de werknemer de onregelmatigheid begaan door de werkgever ruimschoots overtreft.

Zo vonniste de arbeidsrechtbank te Gent dat de e-mails die de werknemer had verzonden en waarmee een concurrerende activiteit werd opgezet, toch mochten gebruikt worden om het ont-

---

slag wegens dringende reden te aanvaarden hoewel de controle niet werd aangekondigd.\textsuperscript{18} Het Arbeidshof te Antwerpen paste dezelfde principes toe.\textsuperscript{19}

De wet heeft dit verankerd in het Wetboek van Strafvordering op 24 oktober 2013, met inwerkingtreding op 22 november 2013 door de rechtpraak ‘Antigoon’ om te zetten in onze wetgeving. Slechts in drie gevallen zal er sprake zijn van nietigheid.

Dat is het geval als de wetgever uitdrukkelijk heeft bepaald dat het bewijs nietig is als een bepaalde vormvoorwaarde niet wordt gevolgd. Het gaat dus om de vormvoorwaarden die op straffe van nietigheid zijn voorgeschreven. Dat is bijvoorbeeld het geval bij de procedurele voorwaarden rond telefoontap, inkijkoperaties en briefgeheim.

Ook wanneer de onregelmatigheid de betrouwbaarheid van het bewijs aantast, is het onregelmatig verkregen bewijs nietig. Dat is bijvoorbeeld het geval bij een verklaring die onder foltering is gegeven.

Tot slot is het onregelmatig verkregen bewijs ook nietig als het gebruik ervan in strijd is met het recht op een eerlijk proces.

In alle andere gevallen buiten deze drie is het onregelmatig verkregen bewijsorganisme niet nietig. Het kan dus wel dienen om een misdrijf te bewijzen.

In het tweede en derde geval moet de rechter – alvorens hij besluit dat het bewijs nietig is – zelf in concreto en in het licht van de zaak nagaan of de betrouwbaarheid van het bewijs wel daadwerkelijk werd aangetast en of het gebruik van het bewijs de eerlijkheid van het proces effectief zou aantasten. En voor dat laatste geval heeft het Hof van Cassatie in zijn rechtspraak een aantal subcriteria aangereikt, zoals:

- het al dan niet opzettelijk karakter van de vormfout;
- de ernst van het misdrijf;
- het feit of de onregelmatigheid al dan niet een invloed heeft op de schuldvraag.

Buiten deze aangehaalde situaties is de Privacycommissie van mening dat de rechter steeds de afweging moet maken tussen de begane inbreuk en de aantasting van het recht op privacy.

Naast de uitsluiting van het bewijs (al dan niet na een belangenafweging door de feitenrechter) kan de werkgever ook strafrechtelijk veroordeeld worden in geval van schending van de privacyregels.

\textbf{3.9 Preventief optreden door de werkgever}

De cao nr. 81 heeft geen betrekking op de regels voor de toegang tot en/of het gebruik van de elektronisch onlinecommunicatiegegevens, welke het prerogatief van de werkgever zijn.
Bijgevolg kan de werkgever anticiperen en de regels omtrent het gebruik van deze communicatiemiddelen vastleggen in een richtlijn. Dit kan hetzij afzonderlijk hetzij naast de bestaande richtlijnen.

Wat de inhoud van het beleid betreft, is het aan te raden om zich op alle aspecten van gebruik van elektronische communicatiemiddelen te focussen.

Belangrijk aandachtspunt is het verduidelijken van het toepassingsgebied (op het werk en/of daarbuiten) en het benadrukken van het vertrouwelijk karakter van de informatie.

Dit kan onder de vorm van een gedragscode waarin de werkgever de communicatiemiddelen bepaalt die ter beschikking staan van de werknemers, de personen die er gebruik kunnen van maken en de gebruiksvoorwaarden voor deze werktuigen.

In het algemeen kunnen, op basis van de afdwingbaarheid, drie vormen van beleid inzake het gebruik van elektronische communicatiemiddelen onderscheiden worden:

- Opname in de arbeidsovereenkomst;
- Opname in het arbeidsreglement;
- Eenzijdig opstellen van richtlijnen.

Het staat de werkgever vrij het internet en e-mailgebruik van zijn werknemers te beperken. Hij kan bijvoorbeeld de toegang tot bepaalde websites blokkeren.

In de gedragscode moet de werkgever de volgende informatie opnemen:

- De controlemiddelen die worden gebruikt om na te gaan of de gebruiksvoorwaarden worden gerespecteerd;
- De personen die belast zijn met de veiligheid van en het toezicht op het informaticawerktuig en meer bepaald de elektronische online communicaties;
- De doelstelling van de controle op het gebruik van de online technologieën;
- De controlemaatregelen voor het gebruik van internet en de elektronische mail;
- De maatregelen voor de individualisering van de gegevens die worden verzameld tijdens een controle;
- De eventuele sancties die de werknemer riskeert wanneer hij de opgelegde regels niet respecteert.

Deze policy zal van toepassing zijn op alle ICT-middelen, ICT-infrastructuur en elektronische communicatiemiddelen alsook op alle gegevens die door die systemen van de werkgever worden verzonden of erin worden opgeslagen.
Aangezien de mailbox steeds niet-professionele informatie kan bevatten, kan het best gewerkt worden met een intermediaire vertrouwenspersoon, zelfs wanneer de mailboxen zich op een server van de werkgever bevinden. De tussenkomst van deze persoon kan vermijden dat de werkgever a priori op individueel gebruikersniveau controleert op ongewenst, onrechtmatig of strafbaar misbruik van onlinecommunicatiemiddelen. Hij mag enkel informatie selecteren en overmaken aan de werkgever die werkelijk noodzakelijk is.

3.10 Geheim van elektronische communicatie

Zonder toestemming van alle rechtstreeks of onrechtstreeks betrokken personen mag niemand zelf of door toedoen van een derde:

- Met opzet kennis nemen van het bestaan en de inhoud van informatie van alle aard die via elektronische weg is verstuurd en die niet persoonlijk voor hem bestemd is;
- Met opzet de personen identificeren die bij de overzending van de informatie en de inhoud ervan betrokken zijn;
- Met opzet kennis nemen van gegevens inzake elektronische communicatie en m.b.t. een andere persoon;
- De informatie, identificatie of gegevens die met of zonder opzet werden verkregen, wijzigen, schrappen, kenbaar maken, opslaan of er enig gebruik van maken.

De inhoud van de privécommunicatie is beschermd.

Het EHRM besliste dat het kennisnemen van de inhoud van een e-mail samengaat met de kennisname en het gebruik ervan.

3.11 Uitzonderingen op het verbod van kennisname en registratie door de werkgever van elektronische communicatie

In volgende gevallen mag de werkgever kennis nemen van de gegevens aangaande de telecommunicatie, alsook van diens inhoud:

- mits akkoord van alle rechtstreeks of onrechtstreeks bij de informatie, identificatie of gegevens betrokken personen. Deze toestemming kan niet op voorhand gegeven worden. Een clausule in die zin is in strijd met de Arbeidsovereenkomstenwet.
- Wanneer de wet het stellen van bedoelde handelingen toestaat of oplegt;
- Wanneer ze uitgevoerd worden met als enig doel de goede werking van het netwerk na te gaan en de goede communicatie te verzekeren;
- Wanneer de handeling wordt uitgevoerd om een tussenkomst van de hulp- of spoeddiensten toe te laten in antwoord op een vraag om bijstand;
- De registratie van elektronische communicatie ten bewijze van een commerciële transactie of van een andere zakelijke communicatie mits voorafgaande inlichting van de registratie;
De kennisname en registratie van elektronische communicatie met als enig doel de kwaliteit van de dienstverlening in callcenters te controleren mits voorafgaande inlichting van mogelijkheid tot kennisname en registratie.

3.12 Sancties

De persoon die zich met bedrieglijk opzet of met het oogmerk om te schaden, toegang verschafft tot een informaticasysteem terwijl hij bewust is van het feit dat hij daartoe niet gerechtigd is, is strafbaar.

Dit is ook van toepassing voor de volgende drie gevallen:

- diegene die de gegevens die worden opgeslagen, verwerkt of overgedragen d.m.v. het informaticasysteem, op enige manier overneemt;
- diegene die enig gebruik maakt van een informaticasysteem van een derde of zich bedient van het informaticasysteem om toegang te verkrijgen tot een informaticasysteem van een derde;
- diegene die enige schade, zelfs onopzettelijk, veroorzaakt aan het informaticasysteem of aan de gegevens die d.m.v. het informaticasysteem worden opgeslagen, verwerkt of overgedragen of aan een informaticasysteem van een derde of aan de gegevens die d.m.v. dit informaticasysteem worden opgeslagen, verwerkt of overgedragen.

De sanctie(s) is/zijn een gevangenisisstraf van drie maanden tot één jaar en/of een geldboete van 26 euro tot 25 000 euro.

3.13 Aanbevelingen en adviezen van de Privacycommissie

In haar aanbeveling van 2 mei 2012 heeft de Privacycommissie zich beperkt tot de elektronische communicaties die gevormd worden door e-mail en internetverbindingen op de werkvloer. Deze basisregels zullen bij uitbreiding ook gelden voor andere meer specifieke situaties.20

De Commissie beschouwt de cao nr. 81 als een document met een juist evenwicht tussen de conflicterende belangen. Ze acht de bestaande wetgeving voldoende om te bepalen in welke mate de werkgever over een controlerecht beschikt.

Wanneer het onderwerp en de inhoud van de elektronische onlinecommunicatiegegevens een beroepsmatig karakter hebben dat door de werknemer niet in twijfel wordt getrokken, zal de werk-

gever zonder enige procedure en relatief vrijelijk kennis kunnen nemen van deze gegevens. De goede werking van de onderneming moet gewaarborgd blijven.

Ook professionele e-mails bevatten persoonsgegevens en zijn dus niet zomaar controleerbaar en verwerkbaar volgens de Privacywet. De werkgever moet bij controle dus steeds de basisprincipes van de Privacywet respecteren: een welbepaald doel voor ogen hebben, niet systematisch alles controleren en de werknemer informeren over mogelijke controle. Blijft er sprake van een gemengd gebruik, worden er het best afspraken gemaakt tussen werkgever en werknemer en dient de procedure van cao nr. 81 gevolgd te worden.

Wanneer privécommunicatie wordt toegestaan, moeten de regels van de cao nr. 81 strikt nageleefd worden.

Onder toestemming van alle personen betrokken bij de elektronische communicatie wordt verstaan ‘elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene of zijn wettelijke vertegenwoordiger aanvaardt dat persoonsgegevens betreffende de betrokkene worden verwerkt’.

Bij gebruik van internet is de toestemming van de werknemers voldoende door opname in het arbeidsreglement, in de arbeidsovereenkomst of in een e-mail - en internetpolicy.

Bij gebruik van e-mail is het moeilijk om toestemming te bekomen van deelnemers die geen werknemers zijn van de onderneming.

In de rechtspraak wordt er enig belang gehecht aan het aanwezig zijn van een geldige toestemming van de werknemer. De arbeidsrechter besliste dat de aangetroffen e-mails niet mochten gebruikt worden in het kader van een procedure inzake het ontslag wegens dringende reden van een werknemer. De werkgever kon immers niet aantonen dat hij de toestemming van de werknemer had gekregen om kennis te nemen van de e-mails noch dat de kennisname onopzettelijk gebeurde.21

De Privacycommissie is voorstander van een voorzienbaar patronaal toezichtsbeleid, verwerkt in een policy.

Aangezien de werkgever aansprakelijk is voor de schade aangericht door de werknemer aan een derde door misbruik van het computersysteem, moet hiertegenover een zeker controlerecht van de werkgever staan.

De Privacycommissie raadt werknemers af het e-mailsysteem op het werk ook voor privézaken te gebruiken. Hierbij stelt ze verschillende acties voor. Zo is het aangewezen om zoveel mogelijk een

onderscheid te maken tussen professionele en privé e-mails door voor deze laatste communicatiebron een ander adres te gebruiken. Indien een afzonderlijk privé e-mailadres niet mogelijk is, maakt de gebruiker minstens een onderscheid door het privé-karakter (‘vertrouwelijk’) te vermelden bij het versturen van e-mails.

3.14 Monitoring door de werkgever van een e-mailprogramma

Hierover heeft het EHRM uitspraak gedaan naar aanleiding van een vermeende schending van de privacy door een Roemeense werkgever.

Een Roemeense werkgever in de private sector vraagt aan zijn werknemer, een ingenieur in een commerciële functie, een ‘Yahoo Messenger’-account te creëren om met klanten van het bedrijf te kunnen communiceren. Hierbij wordt in de interne policy uitdrukkelijk verboden om dit voor persoonlijke doeleinden te gebruiken. Gedurende een week monitort de werkgever het e-mailprogramma van de werknemer (zonder andere gegevens en documenten op diens computer te onderzoeken). Uit deze controle blijkt dat de werknemer deze regelmatig voor persoonlijke doeleinden heeft gebruikt. De werknemer wordt ontslagen. Hij vecht het ontslag aan, maar de Roemeense rechter oordeelt, zowel in eerste aanleg als in hoger beroep, dat de werkgever het recht heeft na te gaan of de regels die in zijn onderneming bestaan, worden nageleefd. De werknemer daagt Roemenië voor het EHRM waarbij hij aanvoert dat zijn recht op privacy werd geschonden. Het EHRM is van oordeel dat het recht op eerbiediging van het privéleven niet geschonden is. Het monitoren van de werknemer was redelijk in het kader van een tuchtprocedure. In casu werd enkel de vraag gesteld of de werkgever de communicatie van zijn werknemers mag monitoren gedurende de arbeidstijd. Volgens het EHRM treedt de werkgever enkel op binnen zijn disciplinaire bevoegdheid. Belangrijke opmerking is dus het feit dat haar beslissing geen betrekking heeft op de kennisneming door de werkgever van de inhoud van de persoonlijke communicatie (geen controle op de inhoud van de e-mails), noch op de bekendmaking ervan. De werkgever controleerde de professionele account in de veronderstelling dat er alleen professionele berichten werden verstuurd. Bovendien was de controle proportioneel. In casu heeft de werkgever vastgesteld dat er sprake was van privé-communicatie, ten gevolge van een algemene monitoring. Volgens de interne richtlijn van het bedrijf, in overeenstemming met de nationale reglementering, was dit niet toegestaan.

22 EHRM 12 januari 2016, nr. 61496/08 (Barbulescu v. Romania).
iv. Controle via sociale media

4.1 Algemeen

De vraag stelt zich hier of de werkgever gebruik mag maken van de informatie die een werknemer/sollicitant (zie hoofdstuk XI) op een sociaal netwerk publiceert. Deze vraag kan opduiken bij een wervingsprocedure, maar ook in de loop van de uitvoering van de arbeidsovereenkomst.

De werknemer die sociale media zoals Facebook gebruikt, moet er zich bewust van zijn dat naast zijn ‘vrienden’ de werkgever kan meelezen. Als de gebruiker van Facebook, zonder de veiligheidsparameters in te stellen, informatie post die bijgevolg toegankelijk is voor alle deelnemers, kan hij niet verwachten dat dit vertrouwelijk is. We stellen vast dat de scheidingslijn tussen privé en professioneel vervaagt. Er bestaat beperkte rechtspraak over het gebruik van sociale media. Momenteel zijn de rechtsleer en de rechtspraak veeleer van mening dat informatie die via de sociale media op het internet wordt geplaatst over het algemeen zelden strikt privé is. Hierbij wordt steeds rekening gehouden met de concrete omstandigheden van de zaak.

Volgende elementen spelen mee bij een concrete beoordeling:

• Het type van het sociaal netwerk;
• De openbare aard van de kritiek;
• De agressieve of beledigende aard van de kritiek;
• De bedoeling van de werknemer op het ogenblik dat hij een bericht plaatst;
• De functie van de werknemer;
• De sociale sfeer in de onderneming;
• Het gegeven of collega’s van de betrokken werknemer tot de mogelijke ontvangers van het bericht behoren.

4.2 Rechtspraak

De arbeidsrechter te Namen beantwoordde de vraag of een betwiste e-post een strikt persoonlijk en vertrouwelijk karakter bekleedt negatief. Hij oordeelde dat de uitwisseling van de berichten op Facebook, open en toegankelijk voor deelnemers en bestemmelingen die personeelsleden zijn van de onderneming, niet als vertrouwelijk kunnen bestempeld worden. In casu werd een werkneemster ontslagen voor zware fout ingevolge racistische en beledigende bewoordingen geuit tegenover een andere werknemer op een Facebookpagina waarop tal van werknemers van
het bedrijf actief zijn. Bij de feitenanalyse blijkt dat de bewoordingen in hun context moeten geplaatst worden en dat ze moeten genuanceerd worden gelet op een ruimer conflict binnen de onderneming. Volgens de opinie van de rechter mochten de bewoordingen niet zonder reactie blijven maar was een ontslag voor een zware fout niet gerechtvaardigd rekening houdend met de gespannen en botsende relatie tussen de twee werknemers die de agressie in de uitzettingen kon verklaren.

De rechter oordeelde in een andere zaak dat de controle door de werkgever van het gebruik van de uitzettingen op Facebook wettig en geoorloofd is en niet als misbruik kan bestempeld worden. In casu nam een werkneemster op Facebook deel aan een gesprek op een prikbord waarvan ze de vertrouwelijkheidsparameters en dus de openbaarheid niet beheerste. Men kan hieruit niet besluiten dat deze uitzettingen in de louter privéfeer zijn gebleven.

Het Arbeidshof te Brussel bevestigde het vonnis van de arbeidsrechtbank te Leuven en oordeelde dat de werknemer, lid van het CPBW, terecht ontslagen was wegens een dringende reden. Het kaderlid van een beursgenoteerd bedrijf had zich op zijn publiek toegankelijk Facebook-prikbord kritisch en sceptisch uitgelaten over het beleid van zijn werkgever toen het bedrijf zijn halfjaarlijkse resultaten bekendmaakte. Aangezien het profiel van de werknemer openbaar ingesteld stond, vond de rechter dat er geen schending van de privacy (de redelijke privacyverwachtingen) was.

Er bestaat ook rechtspraak die ingaat tegen de gangbare koers. In casu was het Arbeidshof te Brussel van mening dat het niet om beledigingen gaat die een fout uitmaken omdat de werknemer niet kon vermoeden dat de Facebookpagina waarop hij zijn kritiek had gepost openbaar was en omdat zijn uitzettingen slechts een uiting waren van een diepe malaise en een zekere machteloosheid tegenover een situatie die hij als onrechtvaardig en onverdraaglijk ervoer. De beschermde werknemer had dreigende en agressieve kritiek geuit over zijn werkgever op een Facebookpagina die aangemaakt was door een groep van werknemers van de onderneming waarop de naam en het logo van de onderneming voorkwam.

## 4.3 Laster

Bovengenoemde arresten zijn voorbeelden van lasterlijke uitzettingen. Deze kunnen geuit worden in een arbeidsrechtelijk kader en dus zowel t.a.v. een werknemer als t.a.v. de werkgever. Het gevaar van dergelijke ’e-beledigingen’ is dat ze de reputatie van de onderneming of de goede verstandhouding tussen collega’s kan schaden.

---

In dat geval ontstaat er een conflict tussen de vrijheid van meningsuiting van de werknemer enerzijds en de plicht tot loyaliteit van de werknemer t.a.v. zijn werkgever anderzijds.

Het recht van de werknemer om kritiek te leveren moet op redelijke wijze uitgeoefend worden. Verzwarend element bij de beoordeling kan zijn indien de naam en het logo van de onderneming zichtbaar is op Facebook.

4.4 Sociale media-beleid
Hier verwijzen we naar de ‘gedragscode’ opgesteld in het kader van de controle van de elektronische communicatiemiddelen.
Er wordt de nadruk gelegd op het feit dat de werkgever goed opgestelde policies inzake het gebruik van sociale media bekendmaakt met afbakening van het toepassingsgebied (al dan niet tijdens de werkuren). Aangezien de e-mail- en internetpolicies niet altijd toepasbaar zijn op sociale media, wordt aangeraden de regels inzake sociale mediagebruik te integreren in de gedragscode inzake het gebruik van elektronische communicatiemiddelen.
Het is met name belangrijk dat de werkgever hieromtrent duidelijke richtlijnen heeft gegeven en bovendien heeft medegedeeld welke sancties er zijn bij overtreding van de policy. Op die manier worden de werknemers geïnformeerd over hun privacyverwachtingen.
v. Controle via geolocalisatiesysteem

5.1 Wetgevend kader

- Cao nr. 81 van 26 april 2002 tot bescherming van de persoonlijke levenssfeer van de werkne-mers ten opzichte van de controle op de elektronische onlinecommunicatiegegevens
- Wet van 13 juni 2005 betreffende de elektronische communicatie.28

Het gebruik van geolocalisatiesystemen wordt niet duidelijk omkaderd door een specifieke wet of een cao. De algemene beginselen van cao nr. 81 kunnen toegepast worden.

5.2 Begrip

Dit is een systeem dat toelaat personen te lokaliseren door gebruik te maken van een combinatie van de gsm- en gsm-technologie.

Het belangrijkste gegeven dat door dit systeem wordt verwerkt, betreft de positie of plaats van een voertuig op een welbepaald ogenblik die desgevallend op een kaart wordt aangeduid of elektronisch weergegeven. Dit gegeven kan in verband gebracht worden met andere gegevens, zoals de route die gevolgd wordt door de bestuurder, de stoptijden, de gemiddelde snelheid,...

Deze controle kan onder verschillende vormen bestaan zoals gsm, gsm/Galileo (satelliet), wifi, IP-adres (gegevensbank), toegangskaarten, biometrische identificatie- en legalisatietoestellen, chip, prikklok, bewakingscamera’s, ...

Toepassingen in het kader van bewaking zijn firmawagens, dienstwagens, gsm, smartphone, pc’s, intern netwerk onderneming, ...

Het doel van deze verwerking van gegevens is het identificeren van een voertuig, een machine, koopwaar, een persoon (op een gegeven ogenblik en een gegeven plaats).

Het is noodzakelijk om veiligheidsmaatregelen te voorzien die de toegang tot deze gegevens beperken tot hiertoe gerechtigde personen.

De afgevaardigden van het personeel en de werknemers moeten hierover vooraf geïnformeerd en geconsulteerd worden.

28 BS 20 juni 2005.
5.3 Respect van de volgende principes

Finaliteit
De doeleinden moeten eerst duidelijk en vooraf omschreven worden. Het systeem laat de verwerking van persoonsgegevens toe op voorwaarde dat ze beantwoordt aan welbepaalde en gerechtvaardigde doeleinden zoals:

- de veiligheid van de werknemer, bijvoorbeeld bewakingsagenten die omwille van hun eigen veiligheid, bij de uitvoering van hun taken, in verbinding moeten staan met een oproepcentrale van een bewakingsonderneming of van de interne bewakingsdienst van de plaats waar ze werkzaam zijn;
- de bescherming van de dienstwagen, bijvoorbeeld het verstrekken van interventieondersteunende informatie aan de politie- en hulpdiensten bij diefstal van het voertuig;
- professionele behoeften aangaande transport en logistiek, bijvoorbeeld wagenparkmanagement;
- het uitoefenen van controle op de arbeid van de werknemer.

Proportionaliteit
Uitgaande van de doelstellingen dienen de verwerking op zich, evenals de verwerkte gegevens, toereikend, ter zake dienend en niet overmatig te zijn. De verwerking op zich van de gegevens, evenals ieder verwerkt gegeven wordt op zijn proportionaliteit getoetst.
Indien het systeem geïnstalleerd is met het oog op de controle van de uitvoering van de taken die aan de werknemers toevertrouwd zijn, moet dit een gerichte controle zijn en gerechtvaardigd door aanwijzingen die een overtreding of misbruik door bepaalde werknemers doen vermoeden. Dit kan gebeuren na een voorafgaande collectieve waarschuwing.
De verwerking van geolocalisatiegegevens moet zich beperken tot de bestuurders van dienstvoertuigen en de verplaatsingen hiermee tijdens de arbeidsduur of de prestaties zelf.
Een permanente controle is uitgesloten tenzij dit gebeurt uit veiligheidsoverwegingen zoals bv. een nucleair transport of een geldtransport.
Regelmatigere controle is gerechtvaardigd indien er een rechtstreeks verband is met de aard van de te vervullen taken door de werknemer en in het bijzonder met het oog op de optimalisatie van het beheer van de verplaatsingen van de professionele voertuigen. In deze optiek kan de werkgever de hele werkdag controles uitvoeren, zonder dat de voertuigen continu gevolgd worden.

Transparantie
Dit houdt een uitgebreide kennisgeving in ten behoeve van de werknemers wiens gegevens verwerkt worden, in het bijzonder:

- wie aan controle onderworpen is;
- de aard van de misbruiken die aanleiding geven tot controle;
- de duur van de controles;
- de ná de controle gevolgde procedure.

Een verborgen gegevensverwerking, zonder dat de werknemer op de hoogte is gebracht, is in elk geval verboden.

5.4 Toestemming door de werknemer
De werkgever moet beschikken over een gekwalificeerde en ondubbelzinnige toestemming van de werknemer. Deze toestemming dient aan de volgende voorwaarden te beantwoorden:

- Individueel: d.w.z. door de betrokkene zelf;
- Goed ingelicht: de werknemer dient de draagwijdte van de toestemming te kunnen inschatten;
- Vrij: d.w.z. niet onder dwang;
- Voorafgaand: vóór de inmenging in de privacy;
- Bijzonder: voor elke nieuwe invoering van het systeem moet een nieuwe toestemming gegeven worden;
- Herroepbaar: de werknemer kan steeds terugkomen op de gegeven toestemming.

Deze toestemming kan de vorm aannemen van een afzonderlijk ondertekend document.

5.5 Privacycommissie
De Privacycommissie heeft zich gunstig uitgesproken in zijn advies van 7 september 2005 betreffende het wetsvoorstel tot regeling van het toezicht op werknemers door middel van een monitoringsysteem verbonden met het gps-navigatiesysteem van dienstwagens.

Het wetsvoorstel waarvoor het advies is gevraagd, heeft niet tot een wet geleid. Naast de individuele toestemming van de werknemers wordt geadviseerd de instemming van de vakbonden te bekomen. Tevens wordt aangestuurd op het vermelden van het doeleinde waarvoor de bewaking gebeurt.

Een permanente controle via een lokalisatiesysteem waarbij er een systematische lezing is van de geregistreerde gegevens wordt in principe als overmatig beschouwd. Een regelmatige controle kan gerechtvaardigd zijn om het beheer van de verplaatsingen van professionele voertuigen te optimaliseren waarbij de werknemer het systeem kan activeren en desactiveren naargelang de behoeften van zijn lokalisatie.
Bovendien moet voorzien worden in een uitgebreide kennisgeving ten behoeve van de personen van wie de gegevens verwerkt worden.

5.6 **Rechtspraak**

Door de afwezigheid van een specifiek wettelijk kader vervult de rechtspraak de rol bij het bepalen van de voorwaarden waarbinnen het geolocalisatiesysteem in een voertuig geplaatst kan worden. De heersende strekking in de rechtspraak keert zich eerder gunstig ten aanzien van de werkgever tijdens diens uitoefening van zijn toezichtsbevoegdheid tegenover het recht van de werknemer op eerbiediging van zijn privéleven. In het vonnis van het Arbeidshof te Brussel sprak de rechter zich niet uit over de vraag van de geoorloofdheid van een gps in een arbeidsrelatie. Er werd geoordeeld dat het gps-systeem, geïnstalleerd door een taxibedrijf geen schending inhield van het privéleven, maar een normale handelwijze in het beheer om het voertuig dat zich het dichtst bij de cliënt bevond, te lokaliseren. Het principe van de proportionaliteit was geëerbiedigd.30

Het Arbeidshof te Gent, bevestiging van de uitspraak in eerste aanleg, heeft de bestaande strekking genuanceerd. Ze oordeelt dat het recht op het privéleven van de werknemer geschonden is, waarbij voor de eerste keer uitdrukkelijk de toepasbaarheid van de Privacywet en het EHRM werd ingeroepen. In casu was een voertuig van een handelsvertegenwoordiger permanent, met inbegrip van ‘s nachts en tijdens het weekend, uitgerust met een geolocalisatiesysteem. Hoewel het bestaan van deze gps in het arbeidsreglement opgenomen was, oordeelde het Hof dat de werknemer, die betwistte dat hij over deze vorm van bewaking ingelicht was, niet exact wist met welke doeleinden de gps geïnstalleerd was.31

5.7 **Activeren – desactiveren van het systeem**

De werknemer kan naargelang de behoeften van zijn lokalisatie het systeem gericht activeren en desactiveren bijvoorbeeld bij aankomst en vertrek van elke plaats van bestemming. In elk geval diert het systeem gedesactiveerd te worden bij gebruik van het voertuig buiten de werkuren, zoals tijdens het weekend, tijdens de middagpauze en in geval van afwezigheid wegens arbeidsongeschiktheid.

Er is een interessant arrest geveld bij het gebruik van een Track and Trace-systeem waarbij de rechter zich moest uitspreken over de vraag of de privacy geschonden werd. De arbeidsrechter heeft geoordeeld dat er inderdaad een schending van de privacy is bij de aanwezigheid van een ‘Track and Trace systeem’ in het voertuig van een handelsvertegenwoordiger om verschillende redenen. De werkgever kan in de eerste plaats niet bewijzen dat dit systeem kon uitgeschakeld worden. Bovendien heeft hij ook tijdens de privé-uren en tijdens de weekends controles van de verplaatsingen laten uitvoeren. Naar het oordeel van de arbeidsrechtbank heeft

---

de werknemer als gevolg hiervan morele schade geleden. De bewaking d.m.v. een monitoringsysteem gekoppeld aan een gps-navigatiesysteem in dienstvoertuigen van werknemers is alleen toegestaan mits respect voor de finaliteits-, proportionaliteit-, transparantie- en toelaatbaarheidsbeginselen van de Privacywet.32

VI. Beroep door de werkgever op een privé-detective

6.1 Wetgevend kader

- Wet van 19 juli 1991 tot regeling van het beroep van privé-detective.33

6.2 Beginselen

De wet op zich volstaat niet om de geoorloofdheid van het beroep op een privé-detective te waarborgen. De drie principes dienen afgetoetst te worden.

Finaliteit
De inmenging moet noodzakelijk zijn met het oog op het nastreven van een bepaald doel zoals bijvoorbeeld in geval van verdenkingen van diefstal, fraude of van oneerlijke concurrentie.

Proportionaliteit
Dit houdt een afweging in van het nagestreefde doel en de aangewende middelen. De aangehaalde motieven moeten relevant en afdoende zijn.

Dit principe vormt een doorslaggevend criterium in de beslissingen van de hoven en rechtbanken inzake de inmenging van de werkgever in het privéleven van de werknemer.

Transparantie
Deze informatieverplichting moet genuanceerd worden.

Het rapport van de privé-detective kan een verwerking van persoonlijke gegevens inhouden.

De informatieverplichting heeft betrekking op de naam, het adres van de verantwoordelijke van de verwerking, de doeleinden van de verwerking, het bestaan van een recht om zich hiertegen te verzetten. Ze rust op de verantwoordelijke van de verwerking t.a.v. de betrokken persoon en moet plaatsvinden vóór de verzameling van de informatie verkregen bij de betrokken persoon.

33 BS 2 oktober 1991.
6.3 *Beperkingen van het optreden van privé-detective*

Het is verboden om in het kader van zijn opdracht ‘gevoelige’ informatie te verzamelen, zoals geloofs-, filosofische- en vakbondsovertuigingen alsook informatie over de seksuele geaardheid en over de gezondheid in de ruime zin.

6.4 *Schending van de privacy – gevolg inzake geldigheid bewijsstukken*

Deze ‘gevoelige’ informatie maakt het voorwerp uit van de bijzondere bescherming van de Privacy-wet. In geval van overtreding zal het verslag van de privé-detective een onregelmatig bewijs zijn.

Wanneer de werkgever bijvoorbeeld opdracht gegeven heeft aan een privé-detective teneinde te weten of de werknemer zijn beroepsvoertuig voor privé-doeleinden gebruikt, vormen het bespioneren gedurende zeven dagen op zeven van de werknemer en zijn familie en bijgevolg eveneens buiten de werkuren, het nemen van foto’s van de werknemer en het verhoor van de werknemer, ongeoorloofde bewijsmiddelen. In dit geval is er sprake van schending van het privéleven en zal het verslag van de privé-detective verworpen worden. Dit houdt immers een inmenging in het privéleven van de werknemer die niet evenredig is met de belangen van de werkgever. In deze belangenafweging moet er tevens rekening gehouden worden met de eerbiediging van het gebruik van materiaal dat toekomt aan de werkgever.

Het Arbeidshof te Luik heeft beslist om geen rekening te houden met een verslag van een privé-detective, bestaande uit onder meer drie films die zonder medeweten van de werknemer werden genomen. In casu was een bediende slachtoffer van een arbeidsongeval. De privé-detective vervulde zijn opdracht zonder medeweten van de werknemer en stelde vast dat de werknemer niet arbeidsongeschikt was. De rechtsverzekeraar die de conclusie van de gerechtelijke expert m.b.t. de vaststelling van de graad van blijvende ongeschiktheid betwiste, legde een verslag van een privé-detective neer. De bewijslevering gebeurde in dit geval in strijd met de informatieverplichting, opgelegd door de Privacywet aan de verantwoordelijke voor de verwerking van de persoonsgegevens, die stelt dat de betrokkene op voorhand van de verwerking van zijn persoonsgegevens op de hoogte gebracht moet worden. Bijgevolg is hier sprake van schending van één van de essentiële voorwaarden om zich rechtmatig op betrokken bewijs te beroepen. Het bewijs (verslag van de privé-detective) werd uit de debatten geweerd.34

---

34 Arbh. Luik 6 februari 2015, JTT 10 september 2015, nr. 1223, 298.
VII. Toegangs- en uitgangscontrole van werknemers (fouillering)

7.1 Wetgevend kader
- Wet van 10 april 1990 tot regeling van de private en de bijzondere veiligheid: zowel betrekking op toegangs- als op uitgangscontroles, zowel t.o.v. personen in het algemeen als t.o.v. werknemers.35
- Cao nr. 89 betreffende de diefstalpreventie en de uitgangscontrole van werknemers bij het verlaten van de onderneming of de werkplaats: enkel betrekking op uitgangscontroles van werknemers.

7.2 Beginsel
Het principe is het verbod van controle van de kledij of van de persoonlijke goederen.

7.3 Uitzonderingen op het verbod
Toegelaten zijn activiteiten in een voor het publiek toegankelijke plaats mits voorafgaandelijke toestemming van de bevoegde burgemeester.

Toegangscontrole door bewakingsagenten:
Dit is geoorloofd indien het uitsluitend gericht is op het opsporen van wapens of gevaarlijke voorwerpen waarvan het binnenbrengen in een plaats het goede verloop van het evenement kan verstoren of de veiligheid van de aanwezigen in het gedrang kan brengen.

Cumulatieve voorwaarden:

- enkel in het kader van een controle op personen;
- enkel door bewakingsagenten van hetzelfde geslacht als de gecontroleerde persoon;
- enkel indien de betrokken persoon zich vrijwillig onderwerpt aan de controle;
- enkel een oppervlakkige betasting van de kledij van de persoon en de controle van de door hem voorgelegde goederen die hij op zich of in zijn handbagage draagt;
- enkel goederen relevant in het licht van hun wettelijk doel;

35 BS 29 mei 1990.
enkel indien er op grond van de gedragingen van de betrokken, van materiële aanwijzingen of van de omstandigheden redelijke gronden zijn om te denken dat deze persoon een wapen of een gevaarlijk voorwerp kan dragen.

De toegang wordt geweigerd aan eenieder die zich tegen de controle verzet of bij wie is vastgesteld dat hij of zij in het bezit is van een wapen of een ander gevaarlijk voorwerp.

Uitgangscontrole door bewakingsagenten:

Dit is geoorloofd in twee gevallen:

- controle uitsluitend gericht op het vaststellen van de ontvreemding van goederen in een winkelruimte t.o.v. klanten;
- controle uitsluitend gericht op het voorkomen of vaststellen van de ontvreemding van goederen in de onderneming of op de werkplaats t.o.v. werknemers.

### 7.4 Principe van proportionaliteit naar aanleiding van de controle

De controle kan niet op een wijze die onverenigbaar is met het uitdrukkelijk omschreven doelende en moet toereikend, ter zake dienend en niet overmatig zijn. Men moet eerst de controlemaatregel aanwenden die het minst het recht van elk individu op de eerbiediging van zijn persoonlijke levenssfeer schaadt.

### 7.5 Modaliteiten van de controle

Enkel indien de betrokken werknemer zich vrijwillig aan de controle onderwerpt, is fouillering toegestaan.

Er is enkel nazicht mogelijk van de door de gecontroleerde werknemer aan de bewakingsagent voorgelegde goederen die hij op zich draagt of in zijn handbagage draagt en/of die zich in zijn of een door hem gebruikt voertuig bevinden.

### 7.6 Weigering van de controle door de werknemer

Indien de werknemer de controle van zijn goederen weigert, mag de bewakingsagent geen dwang uitoefenen. Hij mag evenmin de werknemer verplichten zijn goederen voor te leggen of hem vasthouden in de ondernemingslokalen. In dit geval moet hij de hulp van de bevoegde oderdiensten inroepen.

Indien de werknemer weigert zich te laten controleren, omdat de controle niet volgens de voorzchriften van de cao nr. 89 gebeurt, gaat het niet om een zware fout. Wanneer de werknemer verdacht wordt van diefstal, mag de controle enkel uitgevoerd worden nadat de werknemer zich hiermee akkoord verklaard heeft.\(^\text{36}\)

---

\(^{36}\) Arbh. Brussel 21 oktober 2014, JTT 2015, afl. 1210, 86.
7.7 **Informatieverplichting**
De betrokken persoon moet, uiterlijk bij het betreden van de plaats, in kennis gesteld worden dat uitgangscontroles kunnen worden uitgevoerd.
De werkgever moet voorafgaandelijk aan de ondernemingsraad informatie verschaffen over het systeem.

De informatie heeft betrekking op:

- de perimeter van de onderneming of van de werkplaats;
- de diefstalrisico’s in de onderneming of op de werkplaats;
- de maatregelen om die risico’s te voorkomen of te verhelpen.

De controlevoorschriften en de eventuele sancties moeten worden vermeld in het arbeidsreglement.

7.8 **Toegelaten vormen van controle**
- individuele controle door bewakingsagenten indien op grond van gedragingen van de werknemer, van materiële aanwijzingen of van de omstandigheden, redelijke gronden zijn om te denken dat de werknemer goederen in de plaats die hij verlaat, ontvreemd heeft;
- steekproefsgewijze controle ter voorkoming van diefstal: voor alle betrokken werknemers zonder onderscheid;
- systematische controle: enkel toegelaten met elektronische en/of technische detectiesystemen.

7.9 **Toestemming**
Bij ieder controle (zowel bij toegang als uitgang), alsook controle tijdens de uitoefening van het werk, moet de werkgever vooraf de toestemming van de werknemer verkrijgen. De werkgever kan deze toestemming door een clausule in het arbeidsreglement opnemen. Persoonlijke toestemming van de werknemer tot uitgangscontrole en collectieve toestemming voor steekproefsgewijze uitgangscontrole zijn vereist.

7.10 **Gevolgen uitgangscontrole**
De vaststellingen die tegen de werknemer gebruikt kunnen worden, moeten schriftelijk meege-deeld worden aan de werkgever. De werknemer ontvangt hiervan een kopie.

7.11 **Sancties**
Bij het niet-naleven van de procedure, wordt de werkgever geacht geen toestemming van de werknemer verkregen te hebben om controles uit te voeren. De werknemer kan bijgevolg de controle weigeren zonder gesanctioneerd te worden. Het hierbij verkregen bewijs wordt als nietig beschouwd en kan niet gebruikt worden om een dringende reden te bewijzen.
7.12 Rechtspraak

De rechtspraak past de principes van de finaliteit, proportionaliteit en transparantie toe om het al dan niet wettelijk karakter van een fouillering door een werkgever te beoordelen.

Het Arbeidshof oordeelde dat de fouillering van de persoonlijke kleedkamer van een bediende een overmatige inbreuk vormde op de private levenssfeer van de werknemer. Het feit dat enkel de bediende de sleutel had met toelating van de werkgever, toont onweerlegbaar aan dat deze werknemer een privaat en beschermd gebruik van die plaats mocht maken. In casu vond een fouillering plaats door een hiërarchische meerdere en een collega in afwezigheid van betrokken bediende (met vakantie) die niet gewaarschuwd werd over deze fouillering en dus ook haar toestemming niet had gegeven.

De arbeidsrechter van Nijvel vonniste dat het bewijs verkregen door het fouilleren van de persoonlijke tas van een werknemer zonder zijn uitdrukkelijke toestemming gevraagd te hebben onwettig is en niet in acht genomen kan worden bij de beoordeling van een dringende reden (een vermeende diefstal).

VIII. Controle van de werknemers op het gebruik van alcohol en drugs

8.1 Wetgevend kader
- Cao nr. 100 van 1 april 2009 betreffende een preventief alcohol- en drugsbeleid in de onderneming.

8.2 Begrip
Alcohol- en drugstesten mogen enkel worden afgenomen als de onderneming de regels en de procedures hierbij vooraf heeft vastgelegd.
Het arbeidsreglement moet de aard van de testen, de betrokken werknemers, de procedures, de personen die de testen mogen afnemen, het ogenblik waarop een test mag worden afgenomen en de mogelijke gevolgen, uitvoerig beschrijven.

8.3 Testen
De enige toegelaten testen zijn ademtesten en psychomotorische testen (vaardigheidsproeven en eenvoudige reactietesten). Bloed- en urineonderzoek is verboden. De arbeidsgeneesheer mag eventueel bepaalde testen afnemen in het kader van het gezondheidstoezicht.
De werknemer moet voorafgaandelijk zijn toestemming geven.
De testen mogen enkel gebruikt worden met het oog op preventie, met name om na te gaan of een werknemer al dan niet geschikt is om zijn werk uit te voeren. De resultaten van de testen zijn geen bewijsmateriaal dat gebruikt kan worden om een ontslag of een sanctie te rechtvaardigen.
IX. Briefgeheim op de arbeidsplaats

9.1 Wetgevend kader
- de Grondwet
- het Europees Verdrag voor de rechten van de mens.

9.2 Begrip
Het principe van de onschendbaarheid van het briefgeheim geldt zonder dat hierbij onderscheid gemaakt wordt tussen de professionele en de niet-professionele sfeer. Het betreft de bescherming tegen het kennisnemen van de inhoud van brieven.

Dit is van toepassing op de inhoud van brieven, faxen en e-mails, alsook op de briefwisseling die de werknemer op zijn naam in de onderneming ontvangt.

Hier dient een onderscheid gemaakt te worden tussen een professionele of persoonlijke zending, hoewel dit niet steeds duidelijk is.

Indien de brieven gericht zijn aan “de onderneming X, ter attentie van persoon X” is de werkgever de geadresseerde en mag hij bijgevolg deze brieven lezen.

Zendingen waarvan men redelijkerwijze kan vermoeden dat ze een persoonlijk karakter hebben, mogen niet geopend worden. De werkgever is niet de geadresseerde. Dit is briefwisseling met vermeldingen “persoonlijk” of “vertrouwelijk” bij de naam of vermelding van ‘per adres’ bij het adres van het bedrijf.

Teneinde discussies te vermijden, wordt de zending ongeopend aan de geadresseerde bezorgd indien hij aanwezig is. Bij afwezigheid (wegens bvb ziekte) of in geval van ontslag laat men het gezond verstand spreken.
x. Afluisteren, registreren en opnemen van telefoongesprekken

10.1 Wetgevend kader

• Wet van 13 juni 2005 betreffende de elektronische communicatie.39
• Strafwetboek (Wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en openen van privé-communicatie en telecommunicatie).40

10.2 Begrip

Het afluisteren en opnemen van telefoongesprekken heeft tot doel het kennis nemen van de inhoud ervan.

Het registreren van telefoongesprekken strekt ertoe vast te stellen met wie, hoe lang en hoeveel gesprekken een werknemer heeft gevoerd.

De controle door de werkgever op het gebruik door de werknemer van de middelen van telecommunicatie moet beoordeeld worden volgens de vier klassieke criteria, namelijk de legitimiteit, de transparantie, de finaliteit en de proportionaliteit.

Op Europees niveau houdt de bescherming elke vorm en manier van communicatie in.

10.3 Verbod

Het is principieel verboden communicatie waaraan men niet deelneemt, tijdens de overbrenging ervan, via enig toestel af te luisteren, kennis te nemen of op te nemen zonder toestemming van alle deelnemers aan de communicatie.

Dit verbod geldt voor iedereen, in principe ook voor de werkgever.

In tegenstelling tot de cao nr. 81 wordt het beperkt tot de transportfase tussen verzender en ontvanger.

Het precieze tijdstip van het overbrengen van een communicatie kan afhangen van het soort verleende elektronische communicatiedienst. Voor een spraaktelefonieoproep bijvoorbeeld is het

39 BS 20 juni 2005.
40 BS 24 januari 1995.
overbrengen voltooid zodra één van de gebruikers de verbinding beëindigt, voor elektronische post zodra de geadresseerde het bericht ophaalt, meestal van de server of zijn dienstaanbieder. Zo worden niet geraadpleegde mails beschouwd als onderweg en zijn ze slechts ontvangen na openen e-mail én gelezen.

10.4 Sanctie
De werkgever die met behulp van enig toestel zonder toestemming van de werknemer en de andere persoon betrokken bij het gesprek een telefoongesprek afluistert of opneemt waaraan hijzelf niet deelneemt, kan strafrechtelijk vervolgd worden.

10.5 Rechtspraak
Het feit dat de controle door de werkgever inzake het gebruik van de gsm niet beantwoordt aan de vereiste transparantie en proportionaliteit betekent echter niet automatisch dat de voorgelegde bewijsmiddelen dienen geweerd te worden.
Wanneer de begane onregelmatigheid doet twijfelen aan de betrouwbaarheid van het bewijsmateriaal, kan de rechter oordelen om het bewijs niet toe te laten, rekening houdend met alle elementen in de zaak.*

De werkgever die de hem door de telefoonprovider afgeleverde gedetailleerde afrekeningen van de bedrijfsgsm controleert, schendt hiermee geenzins de gerechtvaardigde privacyverwachtingen van de werknemer zodat hij het bekomen bewijs kan aanwenden in rechte. Het Arbeidshof erkende dat de werkgever het gebruik van de ter beschikking gestelde gsm als arbeidsgereedschap kan bepalen en dat de werknemer de gsm in overeenstemming met de goede trouw moet gebruiken. Bijgevolg is het evident dat de werkgever de periodiek door hem betaalde facturen kan controleren om na te gaan in hoeverre het privégebruik binnen de limieten blijft, ongeacht de vraag of het telefoonverkeer deels een privaat karakter heeft.*

---

XI. Privacy in het kader van een selectieprocedure van een sollicitant

11.1 Wetgevend kader

- Cao nr. 38 van 6 december 1983 betreffende de werving en selectie van werknemers
- Wet van 28 januari 2003 betreffende de medische onderzoeken die binnen het kader van de arbeidsverhoudingen worden uitgevoerd
- Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer t.o.v. de verwerking van persoonsgegevens.

11.2 Principe

Zwijgrecht van de werknemer geldt als algemeen principe. Beide partijen moeten tijdens de hele selectieprocedure het principe van de goede trouw en de relevantie naleven. Ze moeten alle informatie geven waarvan ze redelijkerwijs kunnen aannemen dat zij voor de andere partij belangrijk kan zijn.

Vragen over het privéleven zijn slechts verantwoord indien zij relevant zijn wegens de aard en de uitoefeningsvoorwaarden van de functie. Hierbij is het van geen belang of de werkgever de informatie eigen aan de persoon van de sollicitant achterhaald heeft via het CV, dan wel tijdens een persoonlijk onderhoud of op het internet. Zo is het bij wijze van voorbeeld verboden om de sollicitante te vragen of zij zwanger is of plannen in die zin heeft, tenzij deze informatie relevant is omwille van medische reden.

De vraag stelt zich of de sollicitant mag liegen tijdens het interview. Er zijn verschillende strekkingen in rechtspraak en rechtsleer. Vele auteurs, gevolgd door een groot deel van de rechtspraak, zijn van mening dat een soort liegrecht bestaat wanneer de werkgever een vraag stelt die een inbreuk op de privacy betekent. In de rechtspraak wordt er daarentegen aangenomen dat het verzwijgen van informatie tijdens de sollicitatieprocedure nadien een dringende reden tot ontslag kan zijn.

De werkgever mag enkel kennis nemen van een attest van goed gedrag en zeden met toestemming van de sollicitant, indien dit noodzakelijk is voor de verwezenlijking van wettelijke doeleinden en relevant is voor de functie. Dit attest mag enkel gebruikt worden om de kandidatuur te beoordelen en moet nadien onmiddellijk vernietigd worden. De Privacycommissie hanteert hier een gedoogbeleid bij afwezigheid van wettelijke regels.

Op grond van het finaliteitsbeginsel zal de relevantie van de informatie bekeken moeten worden in het licht van de rechtmatige doelstellingen van de werkgever welke afhankelijk zal zijn van de concrete functieweekstallende. De werkgever moet de mogelijkheid hebben om alle informatie te verkrijgen die hem in staat stelt zich een oordeel te vormen over de geschiktheid van de sollicitant.
Er bestaat geen specifieke wetgeving over blogs of sociale netwerken. In dit kader moet er rekening gehouden worden met de vrijheid van meningsuiting en het recht op privacy van de sollicitant. Een beperking hierop is slechts verantwoord mits respect van de beginselen van finaliteit, proportionaliteit en legaliteit. De werkgever kan bijgevolg zonder toestemming van de sollicitant kennisnemen van informatie die de sollicitant bekendmaakt via een sociale netwerksite zonder deze informatie te bewaren want dan is er sprake van verwerking van persoonsgegevens.

Door een profielpagina op een sociale netwerksite aan te maken, kiest de sollicitant er zelf voor om een deel van zijn privacy op te geven. De sollicitant zal zich in dit geval moeilijk op zijn recht op privacy kunnen beroepen indien hij de informatie zelf beschikbaar gemaakt heeft op het internet of op een bepaalde sociale netwerksite.

De sollicitant dient zich er bewust van te zijn en er rekening mee te houden dat de informatie die via sociale media circuleert en geactiveerd blijft, toegankelijk is voor het publiek. Vanaf het ogenblik dat de informatie openbaar wordt, kan de potentiële werkgever hiertoe toegang hebben. De werkgever moet een gelijke behandeling garanderen en mag geen discriminerende maatregelen nemen.

De kandidaat heeft recht op toegang en inzage in de gegevens die over hem verwerkt worden. Hij moet ook op dit recht gewezen worden. Dit recht strekt zich ook uit tot inzage in de verwerkte subjectieve gegevens.

Hij heeft eveneens recht om foutieve objectieve gegevens te laten verbeteren.

Bij het uitvoeren van psychologische tests moet de Privacywet toegepast worden. Een dergelijke test is een inmenging in de privacy en kan alleen mits naleving van alle principes uit de Privacywet. Inzake de verwerking van persoonsgegevens van de sollicitant (zoals van de werknemer) moet de werkgever de Privacywet respecteren. Wanneer hij persoonsgegevens wenst te gebruiken in een sollicitantenbestand, moet dit gebeuren op een eerlijke en rechtmatige wijze en voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze persoonsgegevens moeten relevant zijn voor de functie of voor de inhoud van het werk.

11.3 Medisch onderzoek

Het medisch onderzoek is verplicht bij de aanwerving, vóór de indiensttreding en ten laatste veertien dagen daaropvolgend. De arbeidsgeneesheer mag enkel de geschiktheid voor het uitvoeren van een functie aan een bepaalde arbeidspost controleren. Zijn beroepsgeheim is algemeen en zonder beperking. Hij mag de medische gegevens waarop hij zich baseert niet kenbaar maken.