Aanbeveling nr. 08/2012 van 2 mei 2012

Betreft: aanbeveling uit eigen beweging betreffende de controle door de werkgever op het gebruik van elektronische communicatie-instrumenten op de werkvloer (CO-AR-2010-002)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 29;

Gelet op de publieke consultatie;

Gelet op het verslag van de ondervoorzitter;

Brengt op 02/05/2012 de volgende aanbeveling uit:

I. INLEIDING

I.1. CONTEXT VAN DE AANBEVELING

1. Het toezicht of de controle door werkgevers van de informaticatools die gebruikt worden door hun werknemers en vooral van de informatie die er doorgevoerd of opgeslagen wordt, is een complex, terugkerend probleem dat actueel blijft.

2. De zeer talrijke vragen om informatie die in dit opzicht zowel door de werkgevers als door de vertegenwoordigers van de werknemers aan de Commissie gericht worden, alsook de klachten die zij regelmatig ontvangt, getuigen hiervan.

3. De aandacht in deze aanbeveling werd vooral geconcentreerd op de kennisname van elektronische communicaties, ongeacht of het gaat om de invoering van procedures of methoden met het oog op het uitoefenen van toezicht op wat er gebeurt met de informaticatools of het netwerk van de werkgever of om gerichte controles die plaatsvinden via toegang tot informatie die opgeslagen is op de informaticatools.

4. Men stelt vast dat de persoonlijke handelingen en gedragingen van de werknemers (privé of zonder verband met het professioneel kader) die steeds vaker verband houden met het internet en virtuele producten en diensten, zich verderzetten in het raam van hun werk of via het gebruik van de werkinstrumenten. Deze uitbreiding is onder meer te wijten aan de globale toegang tot het world wide web. De werknemers communiceren, informeren zich of ontspannen zich dankzij het werkinstrument van hun werkgever. Deze uitbreiding is ook te wijten aan het ter beschikking stellen van draagbare toestellen (zoals laptops) die de werknemer privé gebruikt buiten de werkuren al dan niet met de toelating of getolereerd door de werkgever (te vergelijken met de ter beschikking stelling van een dienstvoertuig).

5. Er dient echter vooraf te worden vastgesteld dat toegang tot elektronische communicatie of internetgegevens niet enkel een kwestie van toezicht betreft -nagaan of het personeel niet overdrijft met het gebruik van internet en e-mail van de werkgever voor privé-doeleinden- maar eveneens het beheer en de organisatie van de activiteiten van de werkgever aanbelangt: het gaat onder meer over het verzekeren van de bewaring van de elektronische briefwisseling (archivering), maar eveneens om het verzekeren van de continuïteit van de dienstverlening ingeval van afwezigheid, vertrek of overlijden van de werknemer (toegang krijgen tot de professionele e-mails die een werknemer ontvangt tijdens zijn afwezigheid om de goede werking van de onderneming/het openbaar bestuur te kunnen blijven verzekeren).

6. Immers, in uitvoering van zijn arbeidscontract of zijn statuut communiceert de werknemer elektronisch met derden via het informaticasysteem dat beheerd wordt door zijn werkgever of op zijn minst in naam van zijn werkgever.

7. De werkgever heeft een rechtmatig belang om toegang te hebben tot deze informatie. Het resultaat van het geleverde werk moet in beginsel aan de werkgever worden afgeleverd overeenkomstig de door hem bepaalde regels. Dit kan onder meer het geval zijn wanneer deze informaties de inhoud vormen van communicaties (elektronische of andere), of inlichtingen verschaffen over communicaties (duur, ontvanger, …) die verricht werden in functie van het afgesproken werk en in naam van de werkgever (uitdrukkelijk of niet indien de tussenkomst van de werknemers ondubbelzinnig is voor zijn correspondent en voor hemzelf). De werkgever zou deze informatie moeten kunnen ontvangen en verkrijgen of, bij ontstentenis, deze moeten kunnen opzoeken teneinde er kennis van te nemen. Een kennisneming van deze informatie zonder tussenkomst van de werknemer mag echter niet beschouwd worden als de gebruikelijke wijze om het resultaat van het geleverde werk te bekomen. In principe wordt dit afgeleverd door de werknemer zelf.

8. Ongeacht de omstandigheden blijft de vraag dezelfde: kan de werknemer de WVP of andere wettelijke bepalingen inroepen om de werkgever te beletten toegang te verkrijgen tot deze informatie om bijvoorbeeld de kwaliteit van zijn werk te controleren en aldus elk toezicht of controle te beletten van de handelingen die hij uitvoert via de hem ter beschikking gestelde werkinstrumenten?

9. Het antwoord op deze vraag blijft omstreden. Getuige hiervan zijn de disparate rechtspraak, de twijfel van vaak gespecialiseerde vaklui en het onbehagen bij rechtstreeks betrokken partijen.

10. Deze complexiteit is te wijten aan de verschillende wettelijke bepalingen die moeten toegepast worden wanneer het gaat over de kennisneming van elektronische communicaties en communicatiegegevens op de werkplek.

I.2. INHOUD EN BESTEMMELINGEN VAN DE AANBEVELING

11. De Commissie wenst de werkgevers en werknemers, alsook de sociale partners en de overlegorganen die zij vormen, te informeren over procedures die toelaten de regels inzake bescherming van de persoonsgegevens van de werknemers te eerbiedigen naar aanleiding van de invoering van verwerkingen die betrekking hebben op het beheer en de controle van het gebruik van de informaticatools door de werknemers.

12. Zij zal haar overwegingen beperken tot de elektronische communicaties die gevormd worden door e-mail en internetverbindingen en zal zich dus niet uitspreken over de problematiek die gevormd wordt door andere communicatiemiddelen dan e-mail en internet, zoals onder andere de telefonische communicaties, sms of geolocatie[1].

13. De Commissie is zich bewust dat deze scope (e-mail en internetgebruik via de kantoorpc ter beschikking gesteld door de werkgever) als beperkend kan worden ervaren. Het gebruik van mobiele toestellen bijvoorbeeld voegt een extra dimensie toe aan de problematiek van werkgeverstoezicht, omdat het gebruik van dergelijke toestellen zich dan niet beperkt binnen de bedrijfsmuren en/of de kantooruren en dus meer vragen oproept, onder andere inzake beveiliging van de professionele gegevens erop. Dit is a fortiori het geval indien deze mobiele devices niet de eigendom zijn van de werkgever. Dit laatste maakt dat een element dat mede de grondslag kan vormen voor patronale controle (artikel 544 burgerlijk wetboek) dan alvast niet voorhanden is. In dat geval is er sowieso sprake van inherent gemengd gebruik (zowel voor professionele als voor privédoeleinden) door de werknemer. De Commissie is echter van oordeel dat zij de reikwijdte van haar aanbeveling dient te beperken tot wat inhoudelijk werd aangeboden in publieke consultatie (zie randnummer 18). Over die andere kwesties kan de Commissie desgevallend nog aparte aanbevelingen uitbrengen[2].

14. Er zal worden verwezen naar de communicaties zelf (namelijk de inhoud van een e-mail of een bezochte webpagina) en naar de elektronische communicatiegegevens (adressen van verzenders en ontvangers, uur van verzending/ontvangst of verbinding, adressen van bezochte websites).

15. De meerderheid van gegevens die gegenereerd worden door de elektronische werkinstrumenten ter beschikking gesteld van de werknemers worden bewaard of zelfs gekopieerd op een andere drager voor back-updoeleinden. Dit is niet alleen het geval voor documenten maar eveneens voor elektronische communicatiegegevens.

16. De Commissie wil de voorwaarden onderzoeken waaronder deze gegevens aldus voor bepaalde doeleinden kunnen bewaard worden, alsook de voorwaarden waaronder er toegang wordt toe

---

[1] Inzake andere communicatiemiddelen op de werkplek bestaan er overigens al een aantal adviezen:

-geolocalisatie via bedrijfsvoertuig: advies van nr. 12/2005 van 7 september 2005;

-opname van telefoongesprekken in het kader van bankdiensten: aanbeveling nr. 01/2002 van 22 augustus 2002;

-registratie van telefonische oproepen van en naar politiecommissariaten en ziekenhuizen: aanbeveling nr. 07/2011 van 21 december 2011;

-in advies nr. 32/2011 van 30 november 2011 beveelt de Commissie aan ten aanzien van de werkgever om inzake het gebruik van de GSM (voor professionele en privé-doeleinden) twee opties (split billing of verklaring op eer om de professionele GSM niet voor privé-doeleinden te gebruiken) te voorzien voor werknemers.

[2] Zo is er momenteel een aanbeveling met betrekking tot fleetloggers in de maak.

verkregen, hetzij in het raam van toezicht of controle of voor een ander doeleinde. De Commissie zal hierna het concept toegang gebruiken, niet alleen om te verwijzen naar toegang tot gegevens betreffende de werknemer, maar eveneens tot de verschillende daaropvolgende verrichtingen die kaderen in de verwerking (zoals de raadpleging van gegevens en hun gebruik (afdruk op papieren drager, doorzending aan een andere bestemmeling, enz.)), en dit ongeacht het beoogde doeleinde. Deze toegang is mogelijk zowel via een werkstation dat gebruikt wordt door de werknemers, als via andere dragers waarop de gegevens worden bewaard (servers, opslagmedia, enz.).

17. De Commissie zal herinneren aan de toepasselijke wettelijke bepalingen. Zij wil met deze aanbeveling eerder ingenomen standpunten[3] opnieuw onderzoeken door de toepassing van alle relevante normen, waaronder de dwingende bepalingen van het arbeidsrecht, te beoordelen in het licht van de bepalingen van de WVP (cf. punt II) en zij zal eveneens de kwestie aansnijden van de regelmatigheid van bewijzen die verzameld werden in weerwil van de toepasselijke bepalingen (cf. punt III) gelet op de jurisprudentiële omwenteling die zich met betrekking tot dit leerstuk heeft voorgedaan. Zij zal, tot slot, onder de vorm van juridische en technische aanbevelingen, een aantal gedragsregels formuleren die voorbeelden of middelen vormen om rekening te houden met de WVP in het raam van een patronale toegang tot elektronische communicatiemiddelen en waarvan zij meent dat deze conflicten tussen de belangen van de werkgevers en de bescherming van de rechten van de werknemers kunnen vermijden (cf. punt IV).

I.3. PROCEDURE

18. Deze aanbeveling werd vooraf onderworpen aan een publieke consultatie die liep tussen 15 juli 2011 en 30 november 2011, teneinde aan de verantwoordelijken voor de verwerking en aan de betrokken personen toe te laten hun observaties, bemerkingen of kritieken te uiten, en dit met het oog op het richten aan de sociale partners, aan de overlegorganen die ze instelden en, op algemene wijze, aan alle werkgevers, van aanbevelingen die beogen de patronale prerogatieven en de bescherming van persoonsgegevens van werknemers of derden te verzoenen tijdens het gebruik,

[3] De Commissie heeft zich reeds verschillende malen uitgesproken over het vraagstuk van de controle op elektronische communicatie op het werk, met andere woorden, de controle die de werkgever uitoefent op het gebruik van e-mail en internet door zijn personeel, met name bijvoorbeeld in het advies n° 10/2000 uit eigen beweging *betreffende het toezicht door de werkgever op het gebruik van het informaticasysteem op de werkplaats*, het advies n° 39/2001 uit eigen beweging van 8 oktober 2001 *betreffende het voorstel van wet 2-891/1 van 29 augustus 2001 betreffende het reglementeren van het gebruik van telecommunicatiemiddelen op de werkplaats*, het advies n° 13/2003 van 27 februari 2003 *inzake de controle door de werkgever van de communicatiegegevens van een van zijn werknemers*, het advies n° 47/2003 van 18 december 2003 *over de gedragscode voor de personeelsleden van het Ministerie van de Vlaamse Gemeenschap*, het advies n° 18/2005 van 9 november 2005 *met betrekking tot een ontwerpbesluit van de Regering van de Franse Gemeenschap houdende de gedragscode voor gebruikers van informaticasystemen, e-mail en internet binnen de diensten van de Regering van de Franse Gemeenschap, en de instellingen van openbaar nut die onder het Comité van Sector XVII ressorteren* en het advies n° 21/2006 van 12 juli 2006 *met betrekking tot de deontologische code van de Federale Overheidsdienst Economie, KMO, Middenstand & Energie voor het gebruik van informaticamiddelen en elektronische gegevensverwerking.*

het toezicht en de controle van de informatica- en de elektronische communicatiemiddelen in het kader van de arbeidsrelatie.

19. Uit de tientallen reacties[4] die ter zake werden overgemaakt, bleek eigenlijk vooral een nood aan verduidelijking of precisering bij bepaalde passages. Bijkomend was er het pleidooi voor een verruiming van het toepassingsgebied van de teksten (andere communicatievormen op de werkplek en de modaliteiten van patronale controle erop, met inbegrip van de controle op mobiele werknemers en zelfs op de telewerker, cf. randnummer 13). Hoewel de Commissie niet onverschillig staat tegenover deze opmerking, zou het tegemoetkomen aan die opmerking het toevoegen impliceren van nieuwe inhoudelijke topics die niet het voorwerp hebben uitgemaakt van de eigenlijke procedure van openbare consulatie. Het voordeel dat deze aanbeveling enkel internet en e-mailgebruik vanuit een computer van de werkgever behandelt, is dat de focus komt te liggen op de basisregels en principes van de WVP die vanzelfsprekend ook zullen gelden voor die andere meer specifieke situaties. De voorschriften van de WVP, die in de problematiek van cybersurveillance hoe dan ook de maat aangeven, bieden inderdaad een passende en soepele oplossing om de handhaving of ontwikkeling van bepaalde praktijken in verband met het controleren en kennisnemen door de werkgever van andere elektronische communicatiegegevens dan internetgegevens en e-mailgegevens toe te laten en tegelijk misbruiken op dat vlak te sanctioneren.

II. JURIDISCH KADER

20. Hierna volgt een uiteenzetting van de wetgeving (in brede zin) die het controlerecht van een werkgever op het gebruik van de elektronische communicatiemiddelen van de werknemers op het werk beheerst. Allereerst zullen de internationale rechtsbronnen besproken worden, waarbij art. 8 van het EVRM het belangrijkste is. Vervolgens wordt de Belgische wetgeving bestudeerd waarbij de knelpunten voor het controlerecht van de werkgever nader zullen onderzocht worden.

II.1. INTERNATIONALE NORMEN

[4] Deze reacties kwamen uit diverse middens: Verbond Belgische Ondernemingen, de werkgroep arbeidsrecht van het ACV, de bediendenvakbond LBC-NVK, advocatenkantoren Lydian en Claeys & Engels, de Vlaamse overheid (e-government en ICT-beheer), de werkgroep GTSI, afdeling POL (informatieveiligheidsbeleid) met daarin vertegenwoordigers van publieke organismen uit het Waals Gewest, de Franse Gemeenschap en de Duitstalige Gemeenschap (zoals ETNIC, FOREM,..), Beltug, LSEC, de federale politie, politiezone Lebbeke-Buggenhout en Febetra. Deze reacties hebben mee bijgedragen tot het eindresultaat dat nu voorligt.

21. Verschillende (internationale) bepalingen regelen het recht op privacy van een werknemer op het werk en de bescherming van de telecommunicatie van de werknemer (op het werk). Hier hangt ook het controlerecht van de werkgever mee samen.

22. De voor het onderwerp belangrijkste internationale norm is vervat in artikel 8 van het EVRM, dat het recht op bescherming van het privéleven, het gezinsleven, de woning en de correspondentie verzekert, en bepaalt:

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

23. Het Europees Hof voor de Rechten van de Mens bevestigde al in enkele arresten dat de bescherming van de privacy, zoals bepaald in art. 8 van het EVRM, ook geldt binnen een onderneming[5]. Belangwekkend is het arrest *Copland*[6] tegen het Verenigd Koninkrijk. Het arrest behandelt de klacht van een lerares van wie de telefoon werd afgeluisterd en het e-mail- en internetgebruik werd gecontroleerd door haar werkgever, zonder enige voorafgaande toestemming van haar. Het Hof oordeelde dat telefonische oproepen vanuit beroepslokalen op het eerste gezicht gedekt zijn door de begrippen "privéleven" en "briefwisseling" in de zin van artikel 8 EVRM. Hetzelfde geldt voor e-mails of informatie betreffende websites geraadpleegd door een werknemer. Hieruit volgt dat, bij gebrek aan een waarschuwing betreffende de controle waarvan hij het voorwerp kon uitmaken, de werknemer een gewettigd vertrouwen mag hebben betreffende het privékarakter van deze gegevens, zodanig dat de verzameling en de behandeling van genoemde gegevens een inmenging uitmaakt in de rechten die artikel 8 EVRM waarborgt. De omstandigheid dat deze controle beperkt zou zijn tot een overzicht van de data en uren van de gemaakte oproepen, alsook tot de identificatie van de gevormde nummers, heeft, nog altijd volgens het Hof, weinig belang. Hier oordeelt het Hof dat dit in strijd is met het EVRM, onder meer omdat er geen wetgeving was die dergelijke praktijken reguleerde, maar voegt eraan toe dat indien een dergelijke wetgeving had bestaan, controle wel toegelaten zou zijn geweest indien ze noodzakelijk zou zijn in een democratische samenleving en dit "in bepaalde situaties". In ieder geval is met het arrest

[5] Zie Niemitz t. Duitsland, 23 november 1992, *Serie A*, vol. 251/B, § 30 en Halford t./Verenigd Koninkrijk 27 mei 1997, *Recueil* 1997-III, § 44.

[6] Copland t/ The United Kingdom, 3 april 2007, te raadplegen op *http://www.echr.coe.int*.

Copland duidelijk dat de stelling dat er van privacybescherming geen sprake meer is zodra men zich op de werkplek bevindt en gebruikmaakt van de apparatuur van de werkgever, niet verdedigbaar.

24. Het Europees Hof verduidelijkte al in het arrest *Copland* dat een beperking onder bepaalde voorwaarden wel kan. Uit de tekst van artikel 8 EVRM kan met name worden afgeleid dat een inbreuk op het recht op privacy toegelaten is wanneer volgende voorwaarden vervuld zijn:

-de inbreuk is in overeenstemming met een bestaande, duidelijke en toegankelijke norm (*legaliteitsbeginsel*);
-de werkgever moet een legitieme doelstelling hebben, met name de noodzaak om een fundamenteel recht te beschermen (*finaliteitsbeginsel*);
-de inbreuk moet proportioneel zijn (*proportionaliteitsbeginsel*): een inbreuk op het recht op privacy is enkel toegelaten indien deze in verhouding is tot de doelstellingen waarvoor zij wordt gesteld. In het raam van deze proportionaliteitscontrole kan het recht op eerbiediging van het privéleven niet alleen worden afgewogen tegenover andere fundamentele rechten maar eveneens tegenover de economische belangen van de werkgever[7].

25. Ook de Europese richtlijn nr. 95/46 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*[8] moet vermeld worden. Die richtlijn werd in België omgezet (de WVP, zoals gewijzigd door de wet van 11 december 1998), zodat als dusdanig hier niet verder wordt ingegaan op die Richtlijn.

26. Er kan eveneens verwezen worden naar een verzameling van praktische richtlijnen van de Internationale Arbeidsorganisatie (IAO) betreffende de bescherming van de persoonsgegevens van de werknemers, aangenomen tijdens de 267e zitting in november 1996[9].

27. Tot slot kan nog naar de volgende internationale normen verwezen worden die bepalingen bevatten die het recht op privacy beschermen (maar waar in de Belgische rechtsleer en rechtspraak nauwelijks naar verwezen wordt):

- art. 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten (BUPO-verdrag);
- art. 12 van de Universele Verklaring voor de Rechten van de Mens;

---

[7] Zie bijvoorbeeld F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, p. 45 en J.-F. NEVEN, « Les principes généraux : les dispositions internationales et constitutionnelles », in ss dir. J.-F. LECLERCQ, Vie privée du travailleur et prérogatives patronales, Bruxelles, EJBB, pp. 30-32.

[8] *PB. L*281 van 23 november 1995, 31.

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

- art. 7 en 8 van het Europees Handvest van de Grondrechten;
- EU-richtlijn 2002/58 inzake elektronische communicatie (deze richtlijn werd in België omgezet door de wet van 13 juni 2005 *betreffende de elektronische communicatie*) en EU-richtlijn 2009/136 inzake elektronische communicatie;
- Conventie nr. 108 en aanvullend protocol nr. 181 van de Raad van Europa.

II.2. BELGISCHE BESCHERMING VAN PRIVACY

1. Grondrecht vervat in artikel 22 G.W.

28. Artikel 22 G.W. bepaalt:

"*Ieder heeft recht op eerbiediging van zijn privé-leven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald. De wet, het decreet of de in artikel 134 bedoelde regel waarborgen de bescherming van dat recht*".

29. Artikel 22 G.W. moet worden uitgelegd in het licht van art. 8 EVRM. Uit de parlementaire voorbereiding blijkt dat het de bedoeling was dat artikel 22 G.W. de verwoording zou zijn van artikel 8 E.V.R.M. Bovendien wordt het recht verder ingevuld door de wettelijke bepalingen zoals hierna uiteengezet.

2. Geheim van elektronische communicatie

a) Artikel 314*bis* van het Strafwetboek

30. Artikel 314*bis* van het Strafwetboek stelt het afluisteren, kennisnemen of opnemen van privé-(tele) communicatie tijdens de overbrenging ervan strafbaar:

"*§1. Met gevangenisstraf van zes maanden tot één jaar en met geldboete van tweehonderd euro tot tienduizend euro of met een van die straffen alleen wordt gestraft hij die :*
1° ofwel, opzettelijk, met behulp van enig toestel privé-communicatie of -telecommunicatie, waaraan hij niet deelneemt, tijdens de overbrenging ervan, afluistert of doet afluisteren, er kennis van neemt of doet van nemen, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die communicatie of telecommunicatie;
2° ofwel, met het opzet een van de hierboven omschreven misdrijven te plegen, enig toestel opstelt of doet opstellen.

§ 2. Met gevangenisstraf van zes maanden tot twee jaar en met geldboete van vijfhonderd euro tot twintigduizend euro of met een van die straffen alleen wordt gestraft hij, die wetens, de inhoud van privé-communicatie of -telecommunicatie die onwettig afgeluisterd of opgenomen is of waarvan onwettig kennis genomen is, onder zich houdt, aan een andere persoon onthult of verspreidt, of wetens enig gebruik maakt van een op die manier verkregen inlichting.

Met dezelfde straffen wordt gestraft hij die, met bedrieglijk opzet of met het oogmerk te schaden, gebruik maakt van een wettig gemaakte opname van privé-communicatie of –telecommunicatie (…).″ (eigen onderstreping)

31. Hierbij gaat het duidelijk om de inhoud van de communicatie. Ook professionele communicatie zoals een e-mail, die niet bestemd is om gehoord of gelezen te worden door andere personen dan de correspondenten, is beschermd door deze bepaling. Bijgevolg kan een werkgever die kennis neemt van de inhoud van gezonden of ontvangen e-mails die niet voor hem bestemd zijn of waarvan hij niet de afzender is via tussenkomst van een werknemer in principe strafbaar worden gesteld.

32. Evenwel moet opgemerkt worden dat artikel 314*bis* Strafwetboek volgens bepaalde auteurs niet verhindert dat een werkgever de mailbox van een werknemer controleert, aangezien een dergelijke controle niet wordt uitgevoerd "tijdens de overbrenging" van de communicatie[10].

33. Een meerderheid van de rechtspraak lijkt ook uit te gaan van een strikte interpretatie van art. 314*bis* van het Strafwetboek zodat die bepaling geen toepassing kan vinden op het inkijken van een e-mail van een werknemer aangezien dit dan niet meer "tijdens de overbrenging" van de e-mail gebeurt[11].

34. Verder kan geargumenteerd worden dat de controle op internetgebruik waarbij website adressen worden geregistreerd (het zogenaamd "loggen") niet onder deze bepaling valt[12].

35. Artikel 314*bis* Sw. vereist dat met opzet wordt gehandeld, d.i. het wetens en willens handelen. Een louter toevallige ontdekking zal dus niet strafbaar zijn onder art. 314*bis* Sw.

---

[10] Zie o.m. F. HENDRICKX, Privacy en arbeidsrecht, Brugge, die Keure, 1999, 188-190; P. VAN EECKE en J. DUMORTIER, "Bescherming van privécommunicatie op het internet", in S. PARMENTIER (red.), De rechten van de mens op het internet, Antwerpen, Maklu, 2000, 85.

[11] Zie o.m. Arbh. Gent 12 december 2007, onuitg. en Arbh. Gent 13 maart 2006, onuitg. zoals aangehaald in P. WATERSCHOOT, "Bespreking van enkele arresten van het Arbeidshof te Gent in verband met het gebruik en misbruik van e-mail en internet op de werkplaats en het controlerecht van de werkgever daarop", R.W. 2008-2009, 730 -744; Arbh. Gent 9 mei 2005, Soc.Kron. 2006, afl. 3, 158.

[12] Zie Arbh. Gent 4 april 2001, *J.T.T.* 2002, 49.

36. De Commissie beschouwt de raadpleging door een werkgever van gegevens aangaande e-mails die opgeslagen zijn op de harde schijf van de werknemer of op een bestand dat beheerd wordt door de persoon die belast is met de controle als zijnde uitgevoerd na de overbrenging van de communicatie, en valt dus, in die veronderstelling, niet onder artikel 314*bis* Sw[13].

b) Artikel 124 van de Wet Elektronische Communicatie

37. Artikel 124 van de wet *betreffende de elektronische communicatie van 13 juni 2005*[14] *(hierna: Wet Elektronische* Communicatie) bepaalt dat "*Indien men daartoe geen toestemming heeft gekregen van alle andere, direct of indirect betrokken personen, mag niemand :*

1. met opzet kennis nemen van het bestaan van informatie van alle aard die via elektronische weg is verstuurd en die niet persoonlijk voor hem bestemd is;
2. met opzet de personen identificeren die bij de overzending van de informatie en de inhoud ervan betrokken zijn;
3. onverminderd de toepassing van de artikelen 122 en 123, met opzet kennisnemen van gegevens inzake elektronische communicatie en met betrekking tot een andere persoon;
4. de informatie, identificatie of gegevens die met of zonder opzet werden verkregen, wijzigen, schrappen, kenbaar maken, opslaan of er enig gebruik van maken.".

38. Die bepaling betreft het kennisnemen van het bestaan van de elektronische communicatie.

39. Al deze handelingen zijn strafrechtelijk gesanctioneerd met een geldboete van 50 tot 50.000 euro (art. 145 Wet Elektronische Communicatie).

40. Van belang is dat het wijzigen, schrappen, kenbaar maken, opslaan of op enige wijze gebruik maken van informatie, identificatie of gegevens zonder dat hier enig opzet mee gemoeid is, in principe strafbaar is.

---

[13] "*Het precieze tijdstip van de voltooiing van het overbrengen van een communicatie* (…)*, kan afhangen van het soort verleende elektronische-communicatiedienst. Voor een spraaktelefonieoproep bijvoorbeeld is het 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 dienstenaanbieder.*", cf. Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 *betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie* (richtlijn betreffende privacy en elektronische communicatie).

[14] B.S. 20 juni 2005.

41. In zijn arrest van 1 oktober 2009 herhaalde het Hof van Cassatie nog eens dat de opzettelijke kennisname van het bestaan van een e-mail, alsook het gebruik van die kennis of van de informatie die zodoende met of zonder opzet werd verkregen, is uitgesloten voor wie niet vooraf de nodige toestemmingen heeft gekregen (art. 124, 1° en 4° Wet Elektronische Communicatie)[15].

42. Belangrijker is dat het Hof besliste dat het kennisnemen van de inhoud van een e-mail samengaat met de kennisname en gebruik ervan. In de rechtsleer werd geopperd dat art. 124 van de Wet Elektronische Communicatie geen betrekking had op de kennisname van de inhoud van een e-mail. Dit zou enkel bestraft kunnen worden via art. 314*bis* Sw. Aangezien die laatste strafbepaling enkel betrekking zou hebben op de kennisname van een e-mail *tijdens de overbrenging van het bericht* en opzet vereist was, werd ervan uitgegaan dat bij kennisname van de inhoud van een e-mail door de werkgever, er ook geen overtreding was van art. 314*bis* Strafwetboek. Uit het arrest van het Hof van Cassatie van 1 oktober 2009 (waar het niet ging om een arbeidsrechtelijke zaak) zou kunnen afgeleid worden dat een werkgever die een e-mail gebruikt (bijv. in het kader van een ontslag wegens dringende reden) in principe strafbaar is, zelfs wanneer hij toevallig kennis neemt van die e-mail.

43. De Commissie is van oordeel dat er slechts interactie is met artikel 124 Wet Elektronische Communicatie in zoverre men aanneemt dat de werkgever nooit een medebestemmeling is van de elektronische communicatie van een werknemer (wat volgens sommigen niet het geval is als de werknemer digitale rechtshandelingen stelt in naam en voor rekening van zijn werkgever[16]) of in zoverre men aanneemt dat de verbodsbepaling van artikel 124 Wet Elektronische Communicatie zich uitstrekt tot na de overbrenging van de boodschap (wat volgens sommigen niet het geval is[17]).

---

[15] Cass., 1 oktober 2009, RG C.08.0064.N.

[16] In die zin bv. R. BLANPAIN, M. VAN GESTEL, Gebruik en controle van e-mail, intranet en internet in de onderneming, Praktijken Recht, Brugge, Die Keure, 2003, nr. 252 en 254.

[17] In die zin bv. RAAD VOOR DE MEDEDINGING in de zaak MEDE-I/O-04/0063 en MEDE-I/O-06/0032: Staalplaatradiatoren, beslissing nr. 2010-I/O-11 van 20 mei 2010. In deze zaak wordt nagegaan door deze RAAD of het gebruik van kopies van mobiele telefoonfacturen in het kader van een onderzoek naar restrictieve mededingingspraktijken te kwalificeren is als kennisname en gebruik in de zin van artikel 124 WEC. De RAAD is van oordeel dat de bescherming van het geheim van elektronische communicatie enkel geldt tijdens de elektronische communicatie:

"*83. De Raad is van oordeel dat de wettelijke bepaling die door Caradon wordt aangehaald in werkelijkheid ziet op de kennisname van informatie (inhoud) die via elektronische weg wordt verstuurd en informatie betreffende het versturen via elektronische weg tijdens de transmissie. Met andere woorden, de bescherming van het geheim van elektronische communicatie ziet op de bescherming tijdens de elektronische communicatie.*

De aard van de uitzonderingen die voorzien zijn in artikel 125 (zie hierna) toont dit aan : er is bijvoorbeeld sprake van afluisteren, gebruikmaken van de communicatie voor interventies van hulpdiensten, het uitvoeren van controle door het BIPT.

Ook de bijzondere regelingen inzake afluisteren die voorzien zijn in het strafrecht en die door Caradon worden geciteerd, tonen dit aan. Het afluisteren of opnemen van gesprekken tijdens transmissie is een maatregel met een ingrijpend karakter waardoor het geheim van de communicatie kan worden geschonden.

84. Van dergelijke maatregelen is hier geen sprake want het gaat om kennisname achteraf van gegevens betreffende elektronische communicatie middels kennisname van de schriftelijke weerslag in een factuur.

85. De Raad is van oordeel dat hier ook relevant is dat het gaat om telefoonfacturen die zijn opgemaakt door de operator aan de abonnee of gebruiker van de diensten van die operator. Er is dus geen gebruik van informatie die zich nog op het netwerk

c) Uitzonderingen op het wettelijk verbod

44. Het recht op privacy is niet absoluut[18] en de bijzondere situatie van de gezagsverhouding tussen werkgever en werknemer dient in acht te worden genomen[19].

45. Bovendien mag de werknemer zich niet op zijn privacy beroepen enkel en alleen om aan de gevolgen van zijn frauduleus gedrag te ontsnappen[20].

46. Ook DE CORTE stelt dat *"een individu slechts de rechtsbescherming komende uit de privacyregeling kan inroepen in die omstandigheden waarin hij zich effectief beroept op de door het recht beschermingswaardige omgeving tot zelfrealisering"*. Volgens DE CORTE moet de rechter ervoor zorgen dat het recht op privacy wordt uitgeoefend binnen het 'normdoel' van het rechtsstelsel. Privacy mag niet gebruikt worden om te ontsnappen aan de gevolgen van gepleegde misdrijven of onrechtmatig gedrag[21]. Het recht op bescherming van de privacy is een functioneel recht.

47. Ook HENDRICKX vermeldt *"het beginsel dat men geen misbruik kan maken van zijn recht op privacy om een andere burger schade te berokkenen, zodat men zijn rechtmatige aanspraak op bescherming verliest"*[22]. Er moet met andere woorden getracht worden beide rechten met elkaar te verzoenen. Art. 8 EVRM laat hiervoor ook de nodige ruimte. Ook de Belgische wetgeving staat toe dat beide rechten met elkaar verzoend worden.

---

bevindt maar slechts het gebruik van de schriftelijke neerslag van de contractuele relatie die bestaat tussen de operator en de gebruiker, namelijk via de factuur. Die factuur omvat de beschrijving van de geleverde diensten, met name de gevoerde gesprekken met vermelding van bestemmeling (nummers), de duur en het tijdstip. Het gaat dus om een afgeleide van de communicatie zelf in de vorm van een factuur achteraf.

Ook om die reden is de Raad van oordeel dat het gebruik van de facturen niet valt onder het geheim van de elektronische communicatie in de zin van artikel 124 WEC.

86. Bovendien moet er op worden gewezen dat de interpretatie die aan deze bepaling wordt gegeven door Caradon, meer bepaald ten aanzien van het vereiste van toestemming, onwerkbaar zou zijn in de praktijk en niet in lijn is met de bedoeling van de wetgever.

De vermelding van het vereiste van toestemming ondersteunt de hierboven vermelde interpretatie : het is alleen zinvol te spreken over toestemming wanneer het gaat om een ingrijpen tijdens de transmissie. De stelling dat elke betrokkene bij een elektronische communicatie toestemming zou moeten geven wanneer in een later stadium kopies worden gebruikt van een factuur, bijvoorbeeld ook door één van de betrokkenen zelf, is in de praktijk ondenkbaar." Zie http://economie.fgov.be/fr/binaries/11_2010IO11_Staalplaatradiatoren_pub_tcm326-104598.pdf.

[18] Zie o.m. Cass. 7 oktober 1981, *Arr. Cass.* 1981-82, 1983; Cass. 27 februari 2001, *R.W.* 2001-2002, 1171.

[19] Cass. 27 februari 2001, *A.J.T.* 2000-01, 949, noot I. VERHELST.

[20] Zie bv. Arbrb. Brussel 22 juni 2000, *Computerrecht* 2001, 311.

[21] R. DE CORTE, "De achterkant van de privacy – Kan het beroep op privacy leiden tot straffeloosheid?", *NJW.*, p. 808.

[22] F. HENDRICKX, *Privacy en arbeidsrecht*, nr. 1 van de Bijzondere reeks ICA, Brugge, die Keure, 1999, 200.

48. Het spreekt evenwel voor zich dat de privacyverwachtingen van de werknemers op het werk minder groot zijn. De privacyverwachtingen kunnen dan worden gedefinieerd als de verwachtingen die iemand redelijkerwijze heeft omtrent de mate van inmenging in zijn privéleven[23]. Ook de privacyverwachtingen van de werknemer omtrent de gegevens waarvan hij zelf aangeeft dat hij die niet als persoonlijke informatie beschouwt, zijn duidelijk minder groot.

49. Onverminderd het bepaalde in randnummer 43, worden hierna de specifieke uitzonderingen behandeld op de bepalingen van artikel 124 van de Wet Elektronische Communicatie en artikel 314*bis* van het Strafwetboek.

1° De toestemming van alle personen betrokken bij de elektronische communicatie

50. Er is geen inbreuk op de artikelen 314*bis* Sw. en 124 van de Wet Elektronische Communicatie wanneer de werkgever de toestemming tot kennisname bekomt van alle deelnemers aan de elektronische communicatie.

51. Wat het gebruik van internet betreft, zou het desgevallend voldoende kunnen zijn dat de toestemming van de werknemers wordt bekomen. Evenwel is de rechtsleer verdeeld over de vraag in welke mate de werknemer een dergelijke toestemming kan geven. Voor bepaalde auteurs volstaat het om een algemene bepaling dienaangaande op te nemen in het arbeidsreglement, in de arbeidsovereenkomst of in een e-mail- en internetpolicy. Anderen stellen, met verwijzing naar de parlementaire voorbereidingen, dat de werknemer telkens opnieuw toestemming moet verlenen. Dit laatste zou kunnen bekomen worden door bij het opstarten van de internet browser een tekstscherm te laten verschijnen, waarbij de werknemer op "akkoord" moet drukken om verder te gaan.

52. Met betrekking tot de controle op het gebruik van e-mail kan het bekomen van toestemming een praktisch probleem vormen aangezien alle partijen betrokken bij de communicatie hun toestemming moeten geven. Het is duidelijk dat het moeilijk is om de toestemming te bekomen van deelnemers die geen werknemers zijn van de onderneming.

53. Hoewel een werkgever zich in theorie zou kunnen baseren op de toestemming van de werknemer, stelt zich eigenlijk een probleem met de kwaliteit van die toestemming. Bij een arbeidsovereenkomst is er geen sprake van een evenwicht tussen de aanwezige partijen (in die mate zelfs dat het arbeidsrecht overigens dit gebrek aan evenwicht compenseert door een veelheid aan beschermende maatregelen ten gunste van de werknemer), zodat de toestemming van de

[23] Zie F. HEYNDRICKX, *Privacy en arbeidsrecht*, Brugge, die Keure, 1999, 51.

werknemer moeilijk kan beschouwd worden als "vrij" in de zin zoals dit vereist is door de wet[24]. In het specifieke domein van gegevensbescherming kan enkel een vrije en bewuste keuze van het gegevenssubject de verwerking van zijn persoonsgegevens wettig maken op grond van artikel 5 a) WVP. Indien het vrije karakter van de toestemming niet gewaarborgd is, zoals in een arbeidsrelatie, zal dit immers elk relevant en beschermend effect van deze toelaatbaarheidsgrond om persoonsgegevens te verwerken teniet doen. Als een werkgever data verwerkt in het kader van controle op het gebruik van de patronale communicatiemiddelen is de toestemming van de werknemer dus niet de juiste rechtvaardigingsgrond. De verwerking is dan het noodzakelijk en onvermijdbaar gevolg van de arbeidsverhouding. Het is in dat geval zelfs misleidend de verwerking door middel van de toestemming van de werknemer te wettigen[25]. Vermits de beoogde verwerking inherent is aan het werkgeverstoezicht kan de werknemer zich evident niet aan de verwerking onttrekken door het enkele feit zijn toestemming niet te geven of een gegeven toestemming later in te trekken. Een eventuele toestemming van de werknemer of het gebrek eraan voegt nl. niets toe of doet niets af aan het principiële recht van de werkgever om het gebruik door werknemers van de ter beschikking gestelde online communicatiemiddelen te controleren, kennis te nemen van hun online communicatiegegevens en deze persoonsgegevens te verwerken, wanneer die verwerkingen noodzakelijk zijn met het oog op de uitvoering van de specifieke verplichtingen en rechten van de werkgever met betrekking tot het arbeidsrecht. In plaats van te focussen op de zogenaamde onontbeerlijke toestemming van de werknemer ingevolge de telecomwetgeving (en waardoor hoogstens een kunstmatig systeem van rechtvaardiging voor de verwerking zal worden gecreëerd), kunnen de privacybelangen van een individuele werknemer die onder gezag staat volgens de Commissie beter op een andere wijze worden beschermd:

-vooreerst door gebruik te maken van de in het kader van het sociaal recht uitgewerkte onderhandelings- en overleginstrumenten tussen werkgevers en werknemers die juist het milderen van de gevolgen van deze ongelijke relatie tot doel hebben;

-voorts door het gevoerde patronaal toezichtsbeleid 'voorzienbaar' te maken voor de personeelsleden zelf in de zin zoals vereist door artikel 8 EVRM, met name door dit beleid te verbijzonderen in een policy die rekening houdt met het geheel van de in deze materie toepasselijke normen (WVP, arbeidsreglementenwet, desgevallend CAO nr. 81…).

---

[24] "*Onder toestemming van de betrokkene, wordt elke vrije, specifieke en op informatie berustende wilsuiting verstaan, waarmee de betrokkene of zijn wettelijke vertegenwoordiger aanvaardt dat persoonsgegevens betreffende de betrokkene worden verwerkt*" (artikel 1, § 8 WVP). In Richtlijn 2002/58/EG (omgezet in de Wet Elektronische Communicatie), dient "toestemming van een gebruiker of abonnee", ongeacht of deze laatste een natuurlijke of rechtspersoon is, dezelfde betekenis te hebben als "toestemming van de betrokkene" zoals gedefinieerd en nader bepaald in Richtlijn 95/46/EG (zie overweging 17 Richtlijn 2002/58/EG).

[25] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48nl_sum.pdf. Het gaat om een samenvatting van een advies van de Werkgroep "artikel 29" *betreffende de verwerking van persoonsgegevens in het kader van de arbeidsverhouding*. De Groep 29 is de Europese instantie die de controleautoriteiten en autoriteiten voor gegevensbescherming van alle lidstaten van de Europese Unie groepeert.

54. Toch moet worden vastgesteld dat in de rechtspraak toch enig belang wordt gehecht aan het voorhanden zijn van een geldige toestemming van de werknemer. Zo besliste de Arbeidsrechtbank te Brussel dat de aangetroffen e-mails niet mochten gebruikt worden in het kader van een procedure over het ontslag wegens dringende reden van een werknemer. De werkgever kon namelijk niet aantonen dat hij de toestemming tot kennisname van die e-mails van de werknemer had gekregen en dat de kennisname onopzettelijk gebeurde[26].

2° Technische uitzonderingen

55. Artikel 125, 2° van de Wet Elektronische Communicatie laat de handelingen bedoeld in artikel 124 toe wanneer zij worden gesteld met als enig doel de goede werking van het netwerk na te gaan en de goede uitvoering van een elektronische communicatiedienst te garanderen.

56. Sommige auteurs hebben de bedoelde uitzondering geïnterpreteerd als een toelating voor het uitvoeren van vereiste tussenkomsten in het netwerk van de onderneming[27].

57. Artikel 128 van de Wet Elektronische Communicatie laat volgende handelingen toe (mits naleving van de WVP):

-de registratie van elektronische communicatie en de ermee verband houdende verkeersgegevens uitgevoerd in het legale zakelijke verkeer ten bewijze van een commerciële transactie of van een andere zakelijke communicatie, op voorwaarde dat de bij de communicatie betrokken partijen vóór de registratie op de hoogte worden gebracht van de registratie, van de precieze doeleinden ervan en van de duur van de opslag van de registratie (waarbij de gegevens uiterlijk gewist worden op het einde van de periode waarbinnen de transactie in rechte kan worden aangevochten);

-de kennisname en registratie van elektronische communicatie en de verkeersgegevens met als enig doel de kwaliteit van de dienstverlening in callcenters te controleren, op voorwaarde dat de personen die werkzaam zijn in het callcenter op voorhand op de hoogte gebracht worden van de mogelijkheid tot kennisnemen en registreren, het precieze doel ervan en de duur van bewaring van de geregistreerde communicatie en gegevens (de gegevens mogen ten hoogste gedurende één maand worden bewaard).

---

[26] Arbrb. Brussel 4 december 2007, *J.T.T.* 2008, afl. 1005, 179.

[27] O. RIJCKAERT, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, 2005, n°35, p. 51-52 ; H. BARTH, « Contrôle de l'employeur de l'utilisation « privée » que font ses travailleurs des nouvelles technologies de l'information et de communication au lieu de travail », *J.T.T.*, 2002, p. 173.

58. Deze twee laatste uitzonderingen lijken onvoldoende mogelijkheden te bieden aan de werkgever om er een algemene controle op het e-mail- en internetgebruik in de onderneming op te baseren. Echter, ook al is de draagwijdte van deze specifieke wettelijke uitzonderingen voor reguliere werkgevers beperkt, dit neemt niet weg dat dit artikel eigenlijk illustreert dat de werkgever communicatiegegevens van werknemers met een beroepsmatig karakter uiteindelijk soepeler moet kunnen verwerken dan communicatiegegevens van werknemers met een privékarakter. Of omgekeerd, dat communicatiegegevens van werknemers met een persoonlijk karakter enkel kunnen worden verwerkt als er meer waarborgen worden geboden. Deze redenering lijkt bijvoorbeeld ten grondslag te liggen van CAO nr. 81 (zie hierna).

59. Bovendien mag niet vergeten worden dat deze specifieke wettelijke uitzonderingen slaan op de kennisname van de inhoud tijdens de transmissie van de communicatie -een maatregel met een bijzonder ingrijpend karakter waardoor het geheim van de communicatie kan worden geschonden- terwijl reguliere werkgevers zich er 'slechts' van willen vergewissen of voltooide persoonlijke communicatie de uitvoering van de arbeidsovereenkomst van de betrokkene niet in het gedrang brengt (door kennis te nemen van de verkeersgegevens) of enkel toegang willen krijgen tot de inhoud van professionele elektronische communicatie die een werknemer reeds heeft ontvangen tijdens zijn afwezigheid om de dienstverlening te kunnen verderzetten tijdens die afwezigheid. Deze nuance is niet onbelangrijk.

3° Wettelijke toelating

60. Artikel 125, § 1, 1°, van de Wet Elektronische Communicatie voorziet dat het verbod ook niet geldt wanneer "*de wet het stellen van de bedoelde handelingen toestaat of oplegt*" (handelingen bedoeld in artikel 124[28]).

61. De vraag die zich stelt, is of de bepalingen van de Arbeidsovereenkomstenwet van 3 juli 1978 een voldoende wettelijke basis hiervoor vormt. De arbeid wordt door de werknemer uitgevoerd in het kader van een arbeidsovereenkomst of in een gelijkaardige situatie waarbij gewerkt wordt onder gezag. Gezag houdt de mogelijkheid in om leiding en toezicht uit te oefenen op een werknemer (art. 2, 3, 4 en 5 van de Arbeidsovereenkomstenwet). Het is in het kader van die bevoegdheid om leiding en toezicht uit te oefenen dat zich het controlerecht van de werkgever situeert. Hetzelfde geldt uiteraard ook voor ambtenaren die onder gezag werken krachtens een statuut.

[28] In dat geval zijn de artikelen 259*bis* en 314*bis* van het Strafwetboek evenmin van toepassing.

62. Artikel 16 van de Arbeidsovereenkomstenwet bepaalt bovendien dat werkgever en werknemer elkander eerbied en achting verschuldigd zijn en zij gedurende de uitvoering van de overeenkomst de welvoeglijkheid en de goede zeden in acht nemen en doen in acht nemen.

63. Artikel 17 Arbeidsovereenkomstenwet voorziet verder dat "*de werknemer verplicht is:*

1° zijn werk zorgvuldig, eerlijk en nauwkeurig te verrichten, op tijd, plaats en wijze zoals is overeengekomen;
2° te handelen volgens de bevelen en de instructies die hem worden gegeven door de werkgever, zijn lasthebbers of zijn aangestelden met het oog op de uitvoering van de overeenkomst; (…)*".*

64. De rechtspraak lijkt van oordeel te zijn dat die bepalingen de vereiste wettelijke uitzondering kunnen vormen[29].

65. De Commissie is eveneens van oordeel dat dit het geval is en wijst er meteen op dat dit ook geldt voor de gelijkaardige wettelijke bepalingen die, net zoals de arbeidsovereenkomstenwet, het gezag verwoorden van werkgevers uit de openbare sector, zoals bv. art. 120 en 124 van de wet van 7 december 1998 *tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus* en art. 7 § 1 van het Koninklijk besluit van 2 oktober 1937 *houdende het statuut van het rijkspersoneel*.

66. Elke werkgever heeft een algemene wettelijke opdracht inzake toezicht en controle op zijn personeelsleden, en dus ook op het gebruik dat werknemers maken van de ter beschikking gestelde (online)communicatiemiddelen. Het gevoerde patronaal toezichtsbeleid moet uiteraard verder 'voorzienbaar' worden gemaakt voor de personeelsleden, met name door dit beleid te verbijzonderen in een policy. Ook zal de werkgever zijn gezagsrecht steeds moeten uitoefenen binnen de perken van de uitzonderingen en de waarborgen die o.a. in de WVP zijn beschreven. Dit betekent echter nog niet dat de algemeen geformuleerde gezagsbepaling in bv. de arbeidsovereenkomstenwet op zich onvoldoende zou zijn.

---

[29] Zo besliste het Arbh. Bergen in een arrest van 25 november 2009 (RDTI 2010, 81, noot K. ROSIER) alvast dat art. 16 en 17 Arbeidsovereenkomstenwet wel wetsbepalingen zijn die, in de zin van art. 109*ter*E, § 1, 1 van de wet van 21 maart 1991 *betreffende de hervorming van sommige economische overheidsbedrijven*, de kennisname van internetverbindingsgegevens van een werknemer toelaten. Het Arbeidshof wees bovendien op het risico op verspreiding van een virus in het informaticasysteem van de werkgever. Het Arbeidshof te Gent besliste ook dat de werkgever tot controle gemachtigd wordt door de bepalingen van de arbeidsovereenkomstenwet die de werknemer verplichten om gedurende de uitvoering van de arbeidsovereenkomst de welvoeglijkheid en de goede zeden in acht te nemen (art. 16), het werk zorgvuldig, eerlijk en nauwkeurig te verrichten op tijd, plaats en wijze zoals overeengekomen (art. 17, 1°) en te handelen volgens de bevelen en de instructies van de werkgever (art. 17, 2°) (Arbh. Gent 9 mei 2005, *Soc. Kron.* 2006, 158). In een vonnis van 22 juni 2000 oordeelde de Arbeidsrechtbank te Brussel (*Computerr*. (NL) 2001, 311) dat een werkgever artikel 16 van de Arbeidsovereenkomstenwet kan inroepen als wettelijke toelating om een e-mail van een werknemer te kunnen gebruiken. De betrokken werknemer, die een pornografische afbeelding per e-mail had verstuurd naar een vrouwelijke collega, mocht van de rechtbank dan ook wegens dringende reden ontslagen worden en de desbetreffende e-mail mocht voorgelegd worden.

67. Zoals reeds aangehaald is er voor bepaalde patronale bewakingsmethoden, zoals het systematisch afluisteren of opnemen van communicatie tijdens transmissie (bv. volledige telefoonconversaties) een specifieke wettelijke inbedding gekomen voor bepaalde arbeidsmilieus. Zo is de wettelijke basis in de sector van beurs/beleggingen/callcenters, om systematisch realtime telefoongesprekken van personeelsleden mee te beluisteren specifiek in de Wet Elektronische Communicatie opgenomen (artikel 128). Gezien het hier duidelijk gaat om een verregaandere "inmenging" werd op dat punt dus een bijzondere wettelijke uitzondering beschreven voor deze werkomgevingen in de Wet Elektronische Communicatie zelf. De algemene legitimiteit van dergelijke controlehandelingen in bedoelde milieus werd dus erkend in de Wet Elektronische Communicatie zelf en kan dus niet zonder meer op basis van bv. artikel 4 WVP als disproportioneel worden aangemerkt. Dergelijke handelingen, indien systematisch van aard, zijn voor reguliere werkgevers daarentegen niet te verantwoorden louter op basis van hun algemene opdracht inzake toezicht en controle op hun werknemers (en indien wel zouden ze in ieder geval nog steeds als disproportioneel kunnen beschouwd worden). Dit betekent echter *a contrario* dat de wetgever eveneens van oordeel moet zijn geweest dat voor minder ingrijpende handelingen in de zin van artikel 124 Wet Elektronische Communicatie, zoals het vaststellen en kennisnemen van voltooide telecommunicatie, de algemene wettelijke toezichtsbepaling waarover elke werkgever beschikt in principe wel toereikend is, zoals bijvoorbeeld de controle en toegang tot de e-mailberichten in een mailbox van een gebruiker.

68. Uiteraard kan dit algemeen geformuleerd gezagsrecht van de werkgever slechts als een wettelijk grondslag dienen om bepaalde controlehandelingen te stellen, voor zover die dan gebeuren conform de normaal gangbare bedrijfsvoering (als een redelijk en voorzichtige werkgever[30]) en conform andere toepasselijke relevante wettelijke (zoals de WVP en de wet van 8 april 1965 *tot instelling van de arbeidsreglementen*[31]), reglementaire bepalingen (zoals het Koninklijk Besluit van 27 augustus 1993 *betreffende het werken met beeldschermapparatuur*[32]) en bepalingen uit bepaalde collectieve arbeidsovereenkomsten (zoals CAO nr. 81 *tot bescherming van de persoonlijke levenssfeer van de*

---

[30] Zoals wettelijk vereist door o.a. artikel 1134 lid 3 BW. (goede trouw), artikel 1382 BW. (zorgvuldigheidsplicht). Ook de naleving van de algemene beginselen van behoorlijk bestuur die van toepassing zijn op een werkgever uit het openbaar ambt beletten dat deze niet zou handelen als een normale bedachtzame werkgever.

[31] Ook de wet van 8 april 1965 voorziet en bekrachtigt eveneens het toezicht op het werk. Maar zij verplicht vooral dat de controle en het toezicht dat de werkgever zou kunnen uitoefenen, alsook de eventuele gevolgen hiervan voor de werknemer, gereglementeerd worden in de schoot van de onderneming/bestuur.

[32] Het KB van 1993 schrijft in zijn bijlage voor dat zonder medeweten van de werknemers geen gebruik mag worden gemaakt van een kwantitatief of kwalitatief controlemechanisme. A contrario laat dit KB werkgevers dus met medeweten van de werknemers toe gebruik te maken van een kwantitatief of kwalitatief controlemechanisme. Dit zal enkel kunnen door registratie en/of kennisname van bepaalde gegevens, dus via een verwerking van persoonsgegevens. Van een toestemming van werknemers is in dit KB bijvoorbeeld geen sprake. Deze reglementaire tekst illustreert dat controlehandelingen op het digitaal optreden van werknemers die door de werkgever worden gesteld in het kader van zijn algemene opdracht van toezicht in principe wettig zijn.

werknemers ten opzichte van de controle op de elektronische online-communicatiegegevens, CAO nr. 9 van 9 maart 1972 *houdende ordening van de in de Nationale Arbeidsraad gesloten nationale akkoorden en collectieve arbeidsovereenkomsten betreffende de ondernemingsraden* en CAO nr. 39 van 13 december 1983 *betreffende de voorlichting en het overleg inzake de sociale gevolgen van de invoering van nieuwe technologieën*).

69. Bovendien moet ook rekening gehouden worden met de verantwoordelijkheid, zelfs aansprakelijkheid van de werkgever tegenover derden. Artikel 1384, derde lid, B.W., bepaalt dienaangaande:
"*Men is aansprakelijk niet alleen voor de schade welke men veroorzaakt door zijn eigen daad maar ook voor die welke veroorzaakt wordt door de daad van personen voor wie men moet instaan, of van zaken die men onder zijn bewaring heeft.*
(…)
De meesters en zij die anderen aanstellen, voor de schade door hun dienstboden en aangestelden veroorzaakt in de bediening waartoe zij hen gebezigd hebben".

70. De vereiste dat het moet gaan om schade veroorzaakt in de bediening waartoe de aangestelden gebezigd worden, wordt door de rechtspraak ruim geïnterpreteerd. Het volstaat dat het schadeverwekkend feit werd verricht tijdens de bediening en ermee verband hield, zelfs al is dat verband onrechtstreeks en occasioneel[33]. Het feit dat de aangestelde heeft gehandeld op de arbeidsplaats en tijdens de normale diensturen wordt daarbij als doorslaggevend beschouwd[34]. Die ruime interpretatie heeft tot gevolg dat de aansteller ook aansprakelijk is bij misbruik van functie[35] en de aansteller ook aansprakelijk gesteld wordt voor de schade veroorzaakt door een misdrijf van de aangestelde[36].

71. Van belang is te onderstrepen dat het hier gaat om een objectieve, foutloze aansprakelijkheid. Wanneer een werknemer door misbruik van het computersysteem schade aanricht aan een derde, kan de werkgever hiervoor dus aansprakelijk gesteld worden. Hiertegenover moet een zeker controlerecht van de werkgever staan.

3. CAO nr. 81 van 26 april 2002

---

[33] Zie o.m. Cass. 24 december 1980, *R.W.* 1981-1982, 2739; Cass. 12 december 1960, *RGAR* 1962, nr. 6874; Cass. 27 maart 1944, *Pas.* 1944, I, 275.

[34] Zie o.m. H. VANDENBERGHE, M. VAN QUICKENBORNE en P. HAMELINK, "Overzicht van rechtspraak (1964-1978), *TPR* 1980, 1336.

[35] L. CORNELIS, *Beginselen van het Belgisch buitencontractuele aansprakelijkheidsrecht*, Antwerpen, Maklu, 1989, 231-232; A. VAN OEVELEN, "De civielrechtelijke aansprakelijkheid van de werknemer en de werkgever voor onrechtmatige daden van de werknemer in het raam van de uitvoering van de arbeidsovereenkomst", *R.W.* 1987-1988, 1202.

[36] Zie Cass. 9 februari 1982, *Arr. Cass.* 1981-1982, 741.

72. Ook de sociale partners hebben zich over de problematiek gebogen en in de Nationale Arbeidsraad werd op 26 april 2002 de *CAO nr. 81 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische onlinecommunicatiegegevens* gesloten.

73. Gelet op de hiërarchie van de rechtsnormen moet er rekening mee gehouden worden dat die CAO geen afbreuk kan en mag doen aan de bovenstaande wetten en internationale normen. Dat wordt ook zo vermeld in de toelichting die de CAO voorafgaat. De bedoeling van de CAO nr. 81 is dan ook "*de bestaande rechtsnormen te verduidelijken en toch de nodige soepelheid te bieden om zo goed mogelijk in te spelen op de feitelijke situatie van de werkgevers, de werknemers en/of hun vertegenwoordigers*".

74. Voor de toepassing van de CAO nr. 81 wordt onder elektronische onlinecommunicatiegegevens verstaan, "*de elektronische onlinecommunicatiegegevens in de brede betekenis van het woord, ongeacht de drager via welke een en ander door een werknemer wordt overgebracht of ontvangen in het kader van de dienstbetrekking*".

75. Luidens de commentaar bij de CAO nr. 81 wil de CAO "*een kader vaststellen dat ruim genoeg is om alle onlinetechnologieën te omvatten, rekening houdend met de toenemende verwevenheid en de snelle ontwikkeling van deze technologieën en de drager die wordt gebruikt. Zij is dan ook van toepassing ongeacht deze drager. Zij viseert bovendien de elektronische onlinecommunicatie, zowel intern als extern*".

76. Met elektronische onlinecommunicatiegegevens worden volgens het arbeidshof te Brussel ook de opgeslagen e-mailberichten bedoeld[37].

77. De CAO nr. 81 heeft geen betrekking op de regels voor de toegang tot en/of het gebruik van de elektronische onlinecommunicatiemiddelen van de onderneming, welke het prerogatief van de werkgever zijn. Het staat dus de werkgever vrij het internet en e-mailgebruik van zijn werknemers te beperken. Dit hangt samen met zijn gezagsuitoefening en met het eigendomsrecht van de werkgever.

78. Hoewel de werkgever dus bijv. de toegang tot bepaalde websites kan blokkeren, moet, in het licht van de hoger aangehaalde rechtspraak van het Europees Hof van de Rechten van de Mens toch

---

[37] Arbh. Brussel 13 september 2005, *Computerr. (Ned.)* 2006, afl. 2, 100.

de vraag gesteld worden of ieder privégebruik kan verboden worden. Bovendien kan zelfs het feit dat de werkgever ieder persoonlijk gebruik van de online communicatiemiddelen verbood, geen vrijgeleide zijn om toegang te verkrijgen tot de communicatiegegevens van de betrokken werknemer. In een van voor de totstandkoming van de CAO nr. 81 daterend arrest bevestigde het arbeidshof te Gent dit beginsel.

79. De globale controle op de elektronische onlinecommunicatiegegevens wordt door de CAO nr. 81 slechts toegestaan voor zover voldaan wordt aan:

-het finaliteitsbeginsel;
-het proportionaliteitsbeginsel;
-het transparantiebeginsel.

a) Doeleinden van de controle (finaliteitsbeginsel)

80. De werkgever kan het gebruik van e-mail en internet slechts controleren indien hij één of meer van de hiernavolgende doelstellingen nastreeft, die duidelijk en expliciet moeten omschreven worden:

1° 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 interpreteerde die bepaling restrictief. Volgens het Arbeidshof moest het gaan om het *raadplegen* van de bedoelde sites wat duidelijk een actieve inbreng van de gebruiker veronderstelt, bestaande in het verrichten van handelingen die erop gericht zijn dergelijke sites te bezoeken en te raadplegen. De ontvangst van door anderen toegezonden e-mails is voor het arbeidshof geen handeling die als zodanig aan de geadresseerde ervan kan worden toegeschreven of verweten en laat de werkgever bijgevolg niet toe om controle te verrichten[38].

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

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

[38] Arbh. Antwerpen (afd. Hasselt) 15 november 2005, *Soc. Kron.* 2006, 153.

4° het te goeder trouw naleven van de in de onderneming geldende beginselen en regels voor het gebruik van onlinetechnologieën.

Het Arbeidshof te Luik oordeelde dat de werkgever die toevallig in het interne berichtenverkeer van de onderneming een uitwisseling van e-mails ontdekt tussen twee werknemers die toegang hebben tot het systeem, waarin de mogelijkheid wordt geopperd om een virus in het systeem te introduceren, het recht heeft om zich toegang te verschaffen tot de e-mails van deze werknemers om controle te verrichten op de tussen beiden uitgewisselde gegevens[39]. Het Arbeidshof lijkt daarbij wel uit het oog te verliezen dat de CAO nr. 81 slechts betrekking heeft op de controle van elektronische onlinecommunicatiegegevens en niet op de inhoud ervan.

b) Informatie (transparantiebeginsel)

81. De werkgever die een controlesysteem wil installeren, moet de ondernemingsraad (als er geen ondernemingsraad is, wordt deze informatie verstrekt aan het preventiecomité of, bij ontstentenis, aan de vakbondsafvaardiging of, bij ontstentenis, aan de werknemers) inlichten over alle aspecten van deze controle en dit vooraleer het controlesysteem wordt geïnstalleerd. De informatie moet betrekking hebben op:

-het controlebeleid en de prerogatieven van de werkgever en het toezichthoudend personeel;
-de nagestreefde doelstelling(en);
-het feit of persoonsgegevens al dan niet worden bewaard, de plaats en de duur van de bewaring;
-het al dan niet permanente karakter van de controle.

82. Bovendien moet de werkgever bij de installatie van een controlesysteem de individuele werknemers inlichten over alle aspecten van de controle. De informatie moet betrekking hebben op de hierboven aangehaalde elementen van de collectieve informatie, alsmede op volgende punten:

-het gebruik van de 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.

---

[39] Arbh. Luik 20 maart 2006, R.R.D. 2006, afl. 118, 89, noot K. ROSIER en S. GILSON.

83. De werkgever kan zelf kiezen welke middelen hij gebruikt om de werknemers te informeren: algemene instructies (circulaires, aanplakking, …), het arbeidsreglement, de individuele arbeidsovereenkomst, instructies bij het gebruik (boodschappen op het scherm wanneer de werkpost wordt aangezet en/of bepaalde programma's worden geactiveerd). Het is dus niet zo dat dit volgens de CAO nr. 81 moet opgenomen worden in het arbeidsreglement. Dit is enkel het geval wanneer de controle zou gebeuren met het oog op het meten van de arbeid, of de bevoegdheden van het toezichthoudend personeel zou betreffen (artikel 6, § 1, 5° van de Arbeidsreglementenwet) of wanneer er disciplinaire sancties zouden worden opgelegd. Gelet op de inspraak die werknemers bij de totstandkoming en aanpassing van het arbeidsreglement hebben, biedt een arbeidsreglement wel de meeste waarborgen. Desgevallend kan geopteerd worden voor een gelijkaardige mogelijkheid voor de werknemers om hun opmerkingen mee te delen in een register.

c) Legitimiteit

84. Het verwerken van persoonsgegevens is slechts toegelaten in welbepaalde gevallen, onder meer wanneer de betrokkene uitdrukkelijk toestemming verleent, wanneer de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of wanneer de verwerking noodzakelijk is voor de behartiging van het gerechtvaardigd belang van de verantwoordelijke voor de verwerking, mits het belang of de fundamentele rechten en vrijheden van de betrokkene niet zwaarder doorwegen.

d) Evaluatie

85. De geïnstalleerde controlesystemen moeten regelmatig geëvalueerd worden, met het oog op voorstellen om ze aan te passen aan de technologische ontwikkelingen. Deze evaluatie gebeurt in de ondernemingsraad (als er geen ondernemingsraad is, wordt deze informatie verstrekt aan het preventiecomité of, bij ontstentenis, aan de vakbondsafvaardiging 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.

e) Controle (proportionaliteitsbeginsel)

86. De controle op de elektronische online communicatiegegevens mag geen inmenging in de persoonlijke levenssfeer van de werknemers tot gevolg hebben. Als de controle tot dergelijke inmenging zou leiden, dient deze inmenging tot een minimum te worden beperkt (proportionaliteitsbeginsel).

87. De commentaar bij de CAO nr. 81 verduidelijkt dat enkel de elektronische online communicatiegegevens die noodzakelijk zijn voor de controle mogen worden verwerkt en verzameld, dit wil zeggen de gegevens die gezien het doel van de controle een zo gering mogelijke inmenging in de persoonlijke levenssfeer van de werknemers tot gevolg hebben.

88. In deze fase mogen enkel globale gegevens worden verzameld en is een identificatie van de individuele werknemers niet toegelaten:
-internet: de werkgever kan gegevens verzamelen over de duur van de aansluiting per werkpost, maar kan de bezochte sites niet individualiseren;
-e-mail: de werkgever kan gegevens verzamelen over het aantal per werkpost uitgaande berichten en het volume ervan, maar kan de werknemer die ze heeft verstuurd niet identificeren.

89. De CAO nr. 81 verduidelijkt niet op welke manier een dergelijke globale controle zonder individualisering van de werknemers dient te gebeuren. Een mogelijke interpretatie is dat op basis van de informatie die zich op de server bevindt in eerste instantie lijsten met globale gegevens mogen opgesteld worden, op grond waarvan het niet mogelijk is individuele werknemers te identificeren. Wanneer op basis van die algemene lijsten onregelmatigheden vermoed worden, kan overgegaan worden tot identificatie van de individuele werknemers op basis van de overige gegevens die werden verzameld en zich op de server bevinden (zie volgend punt inzake de individualiseringsprocedure).

f) Individualisering van de elektronische online communicatiegegevens

90. De CAO nr. 81 bevat specifieke regels inzake individualisering, zijnde "*de handeling die tot doel heeft elektronische on-line communicatiegegevens die tijdens een door de werkgever geïnstalleerde controle werden verzameld, te verwerken om ze aan een geïdentificeerde of identificeerbare persoon toe te schrijven*".

91. De individualisering moet te goeder trouw gebeuren en overeenkomstig de door de controle nagestreefde doelstelling. Enkel de gegevens die noodzakelijk zijn voor de door de controle nagestreefde doelstelling mogen worden geïndividualiseerd. Ze dienen uitgaande van deze doelstelling toereikend, ter zake dienend en niet overmatig te zijn.

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

g) Directe procedure

93. Een directe individualisering is toegelaten wanneer de werkgever één of meer van de in punt 80, 1°-3° opgesomde doelstellingen nastreeft.

94. De werkgever die bij het nastreven van één van deze doeleinden een onregelmatigheid vaststelt, in het licht van de algemene gegevens waarover hij beschikt, mag direct overgaan tot individualisering.

95. Eventuele onregelmatigheden kunnen bv. worden geconstateerd door de statistische gegevens geregeld te raadplegen of door gebruik te maken van elke andere informatiebron.

h) Indirecte procedure

96. Indien de werkgever de doelstelling nastreeft vermeld onder punt 80, nr. 4°, moet een specifieke procedure gevolgd worden vooraleer tot individualisering kan worden overgegaan.

97. Vooreerst moet de werkgever een voorafgaande voorlichtingsfase in acht nemen, die tot doel heeft de werknemers op een duidelijke en begrijpelijke wijze in te lichten over het bestaan van een onregelmatigheid en over het feit dat de elektronische onlinecommunicatiegegevens zullen geïndividualiseerd worden wanneer opnieuw een dergelijke onregelmatigheid wordt vastgesteld. 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.

98. Wanneer vervolgens een individuele werknemer verantwoordelijk wordt geacht voor een (nieuwe) onregelmatigheid, dient hij of zij door de werkgever te worden uitgenodigd voor een persoonlijk gesprek. Dit gesprek moet plaatsgrijpen vóór iedere beslissing of evaluatie met betrekking tot de werknemer. Het gesprek heeft tot doel de werknemer de kans te bieden bezwaren te uiten met betrekking tot de voorgenomen beslissing of evaluatie en het gebruik van de ter beschikking gestelde elektronische onlinecommunicatiemiddelen te rechtvaardigen.

99. Wat de interactie betreft tussen deze CAO en een aantal hogere rechtsnormen, kan herhaald worden dat de wettelijke fundering voor de patronale ingreep op de privacy, de persoonsgegevens en de elektronische communicatie(gegevens) van werknemers wordt geleverd door de dwingende wettelijke bepalingen met betrekking tot het werkgeversgezag (zie hoger) zoals toegelaten op basis van artikel 125, § 1, 1° Wet Elektronische Communicatie ("als de wet het toelaat of oplegt"). De werkgever beschikt over het tuchtrecht/disciplinaire macht in zijn onderneming/bestuur en de

controle op digitale handelingen van werknemers gebeurt primair voor deze finaliteit die duidelijk binnen het arbeidsrecht valt. De patronale controle op e-mail- en internetgegevens op de werkplek, moet daarbij wel passend en noodzakelijk zijn, voor legitieme doeleinden geschieden en transparant zijn. Deze basisverplichtingen vloeien nl. voort uit de WVP –de onderbouw van elke persoonsgegevensverwerking- en deze plichten worden, specifiek wat de controle op onlinecommunicatie op de werkplek betreft, verbijzonderd door CAO nr. 81[40]. Dit maakt ook dat de wezenlijke bepalingen uit die CAO, hoewel een CAO formeel niet van toepassing op de publieke sector, door werkgevers uit die sector niet zomaar naast zich neer kunnen worden gelegd. De belangrijkste verbijzondering in de CAO is het opleggen van een gelaagde controle op persoonlijke elektronische communicatiegegevens in toepassing van artikel 4, § 1, 3° WVP: er moet nl. een ongewenst, onrechtmatig of strafbaar privégebruik zijn vastgesteld naar aanleiding van een globale controle, alvorens die persoonlijke communicatiegegevens mogen toegeschreven worden (al dan niet via een directe procedure) aan een specifieke werknemer en in principe beperkt de individualisering zich tot de telecomgegevens zelf en niet tot de inhoud ervan. Het is dan ook niet denkbaar dat in de publieke sector controle van persoonlijke elektronische communicatiegegevens die aan een bepaalde werknemer kunnen worden toegeschreven a priori zou gebeuren, laat staan dat de inhoud van dergelijke persoonlijke gegevens systematisch zou worden geïndividualiseerd. De niet naleving van dit evenredigheidsprincipe in het openbaar ambt zou immers niet alleen in strijd zijn met de WVP, doch ook in strijd met artikelen 1134, lid 3 BW (goede trouw), artikel 1382 BW (zorgvuldigheidsplicht) en met de algemene beginselen van behoorlijk bestuur die eveneens beletten dat een publieke werkgever zou handelen als een onzorgvuldige werkgever.

100. Het onderscheid die de CAO maakt tussen communicatiegegevens die betrekking hebben op een werknemer (en zijn correspondent) en tot stand komen in uitvoering van diens arbeidsovereenkomst en de persoonlijke gegevens die betrekking hebben op een werknemer (en zijn correspondent) en tot stand komen (nl. ontvangen en verstuurd worden) in de beleving van de

---

[40] Antwoord van de vice-eerste minister en minister van Werkgelegenheid op de vraag om uitleg van de heer Vincent Van Quickenborne (nr. 2-788), over «de rechtsgeldigheid van de CAO nr. 81 die beoogt de persoonlijke levenssfeer van de werknemers te beschermen ten aanzien van de controle op de elektronische on line-communicatiegegevens», Belgische Senaat, Handelingen, 23 mei 2002 : " (…) *On ne fixe pas des règles nouvelles ou supplémentaires pour garantir la protection de la vie privée. Les règles existantes sont simplement précisées et concrètement appliquées pour le cas où l'employeur voudrait contrôler et traiter l'utilisation des données sur le lieu de travail. En réponse à votre première question, je peux vous dire que la CCT nº 81 est compatible avec l'article 22 de la Constitution, étant donné que la protection du droit au respect de la vie privée et familiale n'est pas le moins du monde réglée, mais simplement précisée. Pour cela, une loi au sens formel du terme n'est pas nécessaire. Vous m'avez demandé si la convention sera rendue obligatoire. Elle sera traitée comme toutes les autres conventions collectives de travail. Le contenu fera tout d'abord l'objet d'un contrôle afin de déterminer s'il est conforme aux normes nationales, européennes et internationales valables en la matière. Si, au terme d'un tel contrôle, aucune objection n'est émise et aucun problème n'est décelé, la convention sera rendue obligatoire. Enfin, je ne peux actuellement pas vous donner une réponse définitive à votre troisième question. On doit auparavant déterminer s'il est utile et opportun de créer, à côté de la législation déjà existante, un nouveau texte de loi distinct, relatif aux droits et devoirs des employeurs et des travailleurs en ce qui concerne les e-mails et l'utilisation d'internet au travail en général. Je souhaite encore une fois insister sur le fait que la CCT nº 81 consiste seulement en une précision de la réglementation déjà existante, qui est applicable tant aux entreprises privées qu'aux institutions publiques*".

persoonlijke levenssfeer van betrokkene op de werkplek ("Niemitz"), steunt op het relevantiebeginsel uit de WVP[41]. Op beide categorieën gegevens moet uiteraard de WVP worden toegepast[42], want beiden zijn persoonsgegevens. De graad van bescherming onder de WVP is immers dezelfde voor alle gegevens (persoonlijke gegevens zowel als professionele gegevens), ermee rekening houdend dat deze equivalente bescherming toelaat dat een aantal gegevens wettig en rechtmatig zullen kunnen worden verwerkt door de werkgever (door de patronale kennisname ervan) en andere gegevens eventueel niet. In dat opzicht zijn gegevens die tot stand komen in uitvoering van de arbeidsovereenkomst op zich relevant voor de werkgever, ook ten aanzien van hun inhoud. Enkel toegang tot de inhoud van een zakelijk elektronisch bericht kan ervoor zorgen dat de werkgever zijn doel realiseert (bv. de verderzetting van de zakelijke correspondentie in afwezigheid van een werknemer). Persoonlijke communicatiegegevens zijn daarentegen in normale omstandigheden overmatig en mogen dus niet ter kennis komen van de werkgever. Zij worden slechts relevant voor de werkgever, in eerste instantie wat hun bestaan betreft, in de mate dat zij de goede uitvoering van de arbeidsovereenkomst of het statuut van de betrokkene in het gedrang brengen (met name in geval van strafbare, onrechtmatige of ongeoorloofde persoonlijke communicatie). Zo niet blijft de werkgever verwerkingsonbevoegd en mogen geïndividualiseerde persoonlijke communicatiegegevens hem niet ter kennis komen.

101. Hoewel de omvang van de toegang tot persoonlijke elektronische on-linecommunicatiegegevens in vergelijking met deze tot beroepsmatige elektronische on-linecommunicatiegegevens beperkter is (van de inhoud mag in principe geen kennis worden genomen), wordt dergelijke toegang ingevolge het evenredigheidsbeginsel dus met meer waarborgen omringd voor de betrokkene (toepassing van een gelaagde controle en pas individualiseren wanneer naar aanleiding van een algemene controle misbruiken of onregelmatigheden werden vastgesteld), net omdat dergelijke toegang controle impliceert van private communicatiebewegingen die bij uitstek binnen de bescherming van de persoonlijke levenssfeer van de werknemer worden beleefd. De striktere toegangsregeling tot dit type van elektronische communicatie(gegevens) houdt daarmee gelijke tred met de toename van de privacyrisico's voor de betrokkene.

---

[41] Een en ander impliceert dat een werknemer reeds een actieve stap heeft gezet door te specificeren dat de bedoelde e-mail van professionele aard is (of net niet).

[42] Artikel 11, derde lid, van de CAO stelt dat ten aanzien van deze categorie gegevens, de individualiseringsregels van de CAO niet gelden, maar niet dat de WVP niet van toepassing zou zijn. Het is vermoedelijk het verslag bij de CAO dat op dat punt wat ambigu is geformuleerd: "*Tegen deze achtergrond en wanneer het onderwerp en de inhoud van de elektronische on-linecommunicatiegegevens een beroepsmatig karakter hebben dat door de werknemer niet in twijfel wordt getrokken, zal de werkgever* ***zonder enige procedure*** *kennis kunnen nemen van deze gegevens*".

102. Dit impliceert ook dat een werkgever niet op directe en rechtstreekse wijze kennis kan nemen van de inhoud van elektronische communicatie. Rekening houdend met het feit dat een mailbox steeds niet-professionele informatie kan bevatten, kan best gewerkt worden met een intermediaire vertrouwenspersoon, zelfs wanneer de mailboxen zich op een server van de werkgever bevinden: een menselijke 'firewall' tussen werkgever en werknemer die het gerechtvaardigd vertrouwen geniet van de twee partijen, met voldoende onafhankelijkheid ten aanzien van de werkgever en alert voor 'bevoegdheidsoverschrijding' in hoofde van beide partijen. De tussenkomst van deze persoon kan bijvoorbeeld vermijden dat de werkgever reeds a priori op individueel gebruikersniveau controleert op ongewenst, onrechtmatig of strafbaar misbruik van de onlinemiddelen in strijd met de principes van CAO nr. 81. Deze vertrouwenspersoon, bv. een aangestelde voor de gegevensbescherming, mag nl. zonder legitieme reden geen geïndividualiseerde communicatiegegevens over werknemers aan het management overmaken ingevolge zijn discretieplicht. De tussenkomst van deze persoon vermijdt bv. ook dat een werkgever, die zich in het kader van zijn legitieme zoektocht naar bepaalde professionele elektronische berichten, toegang verschaft tot de mailbox van een (afwezig) personeelslid, terloops ook de inhoud van diens persoonlijke berichten gaat nalezen. Deze persoon zou tenslotte ook kunnen nagaan of het label 'privé' dat werd aangebracht door een werknemer in de subjectline van een bepaald e-mailbericht, wel te goeder trouw gebeurde (in het kader van rechtmatige beleving van het recht op privacy) dan wel onder het mom ervan teneinde op onrechtmatige of strafbare wijze de belangen te schaden van de werkgever. In het ene geval blijft de nagetrokken mail confidentieel ten aanzien van management en in het andere geval wordt ze wel overgemaakt aan het management voor verder gevolg. Kortom, deze vertrouwenspersoon zou enkel die informatie mogen selecteren en overmaken aan de werkgever die a priori werkelijk noodzakelijk is.

4. Art. 550*bis* van het Strafwetboek

103. Artikel 550*bis*, § 1, van het Strafwetboek bestraft met een gevangenisstraf van 3 maanden tot 1 jaar en/of met een geldboete van 26 euro tot 25.000 euro (excl. opdeciemen), diegene die, "*terwijl hij weet dat hij daar toe niet gerechtigd is, zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft*". Wanneer sprake is van bedrieglijk opzet bedraagt de gevangenisstraf 6 maanden tot 2 jaar.

104. Die bepalingen gelden voor het van buitenuit hacken van het computersysteem. Hiervan zal bij een controle door de werkgever meestal geen sprake zijn.

105. Voor het zich "intern" toegang verschaffen tot een informaticasysteem door "*met bedrieglijk opzet of met het oogmerk om te schaden, zijn toegangsbevoegdheid tot een informaticasysteem te*

overschrijden", voorziet artikel 550*bis*, § 2, van het Strafwetboek, een gevangenisstraf van zes maanden tot twee jaar en/of een geldboete van zesentwintig euro tot vijfentwintigduizend euro.

106. In die gevallen is ook diegene die :
" 1° hetzij de gegevens die worden opgeslagen, verwerkt of overgedragen door middel van het informaticasysteem op enige manier overneemt;
2° hetzij 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;
3° hetzij enige schade, zelfs onopzettelijk, veroorzaakt aan het informaticasysteem of aan de gegevens die door middel van het informaticasysteem worden opgeslagen, verwerkt of overgedragen of aan een informaticasysteem van een derde of aan de gegevens die door middel van het laatstgenoemde informaticasysteem worden opgeslagen, verwerkt of overgedragen;"
strafbaar (met een gevangenisstraf van een jaar tot drie jaar en/of met geldboete van zesentwintig euro tot vijftigduizend euro).

107. Of het kennisnemen van elektronische communicatie door de werkgever onder artikel 550*bis* van het Strafwetboek strafbaar is, zal dus afhankelijk zijn van de vraag of de werkgever zijn toegangsbevoegdheid heeft overschreden. Die vraag zal dan moeten worden beantwoord worden aan de hand van de andere besproken wetgeving.

108. Bovendien is voor een strafbaarstelling ook vereist dat er sprake is van opzet.

5. De bescherming van persoonsgegevens: de WVP

109. De Commissie wenst nadrukkelijk te herinneren aan de toepassing van de WVP waarvan de dwingende bepalingen opgelegd worden aan de verantwoordelijken voor de verwerking, in dit geval alle werkgevers, ongeacht of zij hun activiteiten ontplooien in de openbare- dan wel de privésector: vormverplichtingen, procedures, te bereiken doelstellingen. Deze verplichtingen kunnen niet omzeild noch terzijde geschoven worden. De Commissie is niet op de hoogte van enig argument dat toelaat te besluiten dat deze verplichtingen een hinderpaal zouden vormen voor de ontwikkeling van de economische activiteit of de uitoefening van het openbaar bestuur.

110. De WVP is een transversale wetgeving die dient toegepast te worden, ook in het raam van de arbeidsrelaties. De WVP bepaalt de voorwaarden waaronder een verantwoordelijke voor een verwerking persoonsgegevens mag verwerken.

111. Artikel 1, § 1 van de WVP definieert persoonsgegevens als "*iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon", hierna "betrokkene" genoemd"* en verduidelijkt dat *"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*".

112. De WVP beoogt dus de bescherming van alle persoonsgegevens, ongeacht hun gevoeligheidsgraad en ongeacht of zij al dan niet verband houden met het privéleven van de betrokkene. Vanuit dit oogpunt genieten de gegevens van de werknemer, ook op de werkplek, van de bescherming door de WVP. De gepersonaliseerde professionele e-mailadressen, de elektronische communicatiegegevens (ongeacht of het gaat om e-mails of internetverbindingen en al dan niet van professionele aard), de inhoud van de op een dergelijk adres ontvangen of verstuurde e-mails (al dan niet met een professioneel karakter) zijn persoonsgegevens aangezien zij betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon.

113. De WVP is van toepassing op elke al dan niet volledig geautomatiseerde verwerking van persoonsgegevens alsook op iedere niet-geautomatiseerde verwerking van persoonsgegevens die bewaard worden in, of bestemd zijn om bewaard te worden in een bestand. Onder "verwerking" wordt verstaan "*elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van persoonsgegevens*" (artikel 1, § 2 WVP).

114. Zo veronderstelt de controle of de rechtmatige kennisneming van informatie die gegenereerd wordt door informatica- of elektronische communicatie-instrumenten die door de werknemer gebruikt worden in het raam van zijn arbeidsrelatie, in het algemeen een verwerking van persoonsgegevens.

115. Bij dergelijke verwerkingen dienen de bepalingen van de WVP dus nageleefd te worden en dienen zij de tussenkomst van de verschillende verantwoordelijken en interveniënten te omkaderen, hetzij om te voorkomen dat de persoonsgegevens onrechtmatig, overmatig of onder het mom van een klaarblijkelijke automatie worden aangewend in de marge van een andere interventie voor andere doeleinden, hetzij om ervoor te zorgen dat een *a priori* rechtmatige en wettige verwerking

van dergelijke gegevens geen afbreuk doet aan de fundamentele rechten en vrijheden van de betrokkenen.

116. De WVP legt aan de verantwoordelijken voor de verwerking van persoonsgegevens een aantal verplichtingen op onder de vorm van te bereiken doeleinden, doch verleent hen eveneens een zekere vrijheid en autonomie en dus verantwoordelijkheid wat betreft de te nemen maatregelen om aan hun verplichtingen te voldoen en wat betreft de aard van de relevante elementen die toelaten hun beslissingen te rechtvaardigen.

117. Iedere gegevensverwerking moet aldus vanaf de opzet van de verwerking **een of meerdere specifieke en welbepaalde doeleinden** nastreven. De WVP verbiedt, behalve in uitzonderlijke gevallen voorzien door de wet[43], het hergebruik van gegevens voor doeleinden die niet verenigbaar zijn met de oorspronkelijk doeleinden.

118. Als voorbeelden uit de praktijk met betrekking tot de doelstellingen die een werkgever zou kunnen nastreven indien hij wenst toegang te verkrijgen of kennis te nemen van elektronische communicaties of communicatiegegevens, zou men kunnen stellen dat het gaat om het verzekeren van de continuïteit van de geleverde diensten ingeval van afwezigheid, overlijden of vertrek van de werknemer, het bewaren van documenten als bewijsstukken of nog voor controle. Wat de controleverrichtingen betreft kan men verwijzen naar de doelstellingen vervat in artikel 5 van de CAO nr. 81.

119. Deze **doeleinden** moeten bovendien **rechtmatig** zijn. Artikel 5 van de WVP somt zes gevallen op waarin het doeleinde *a priori* rechtmatig is en de verantwoordelijke voor de verwerking moet kunnen aantonen dat de gegevensverwerking ten minste kadert in een van deze zes limitatief opgesomde gevallen.

120. In dit opzicht meent de Commissie dat een gegevensverwerking die uitgevoerd wordt in het raam van een controle op de werknemers, in voorkomend geval gerechtvaardigd zou kunnen worden door de uitvoering van de arbeidsovereenkomsten, gelet op de aard van deze overeenkomst (art. 5, b van de WVP) of door de uitvoering van een gelijkaardige verplichting die door de wet wordt opgelegd aan de werkgevers van de openbare sector (art. 5, c van de WVP). Bovendien moet rekening gehouden worden met de mogelijkheid dat deze gegevensverwerking noodzakelijk is voor de behartiging van een gerechtvaardigd belang van de werkgever (art. 5, f van de WVP).

---

[43] Artikel 4, § 1, 2° van de WVP.

121. Zoals reeds gezegd meent de Commissie dat de instemming van de werknemer(s) echter niet de wettelijke basis kan vormen voor de uitoefening van een patronale controle op de digitale handelingen die uitgevoerd worden in het raam van de arbeidsovereenkomst of aan de hand van de werkinstrumenten. Gelet op de tussen partijen bestaande machtsverhoudingen zou een individuele instemming van de betrokken werknemers niet als werkelijk vrij kunnen beschouwd worden.

122. Het koninklijk besluit van 13 februari 2001 heeft trouwens de conclusies getrokken uit deze bijzondere situatie door te stellen: "*Indien de verwerking van persoonsgegevens bedoeld in de artikelen 6 en 7 van de wet uitsluitend is toegestaan op grond van de schriftelijke toestemming van de betrokken persoon, is die verwerking verboden indien de verantwoordelijke voor de verwerking de huidige of potentiële werkgever van betrokkene is of indien de betrokken persoon zich ten aanzien van de verantwoordelijke voor de verwerking in een afhankelijke positie bevindt, wat hem belet vrij zijn toestemming te verlenen. Dit verbod wordt opgeheven wanneer de verwerking erop gericht is de betrokken persoon een voordeel te verstrekken".*[44]

123. In dezelfde zin concludeerde de Groep 29 dat: "*wanneer een werkgever als noodzakelijk en onvermijdbaar gevolg van de arbeidsverhouding persoonsgegevens moet verwerken, het misleidend is indien hij deze verwerking door middel van toestemming tracht te wettigen. Zich baseren op toestemming moet worden beperkt tot gevallen waarin de werknemer een echte vrije keuze heeft en nadien de mogelijkheid heeft om de toestemming zonder nadeel in te trekken".*[45]

124. De verwerking moet eveneens **proportioneel** zijn. Het volstaat niet dat het toezicht kan gerechtvaardigd worden door de uitvoering van de arbeidsovereenkomst of de administratieve taak (bijv. controleren of de werknemer de instructies naleeft) en eventueel daarenboven op de verwezenlijking van het gerechtvaardigd belang dat de werkgever nastreeft (bijv. de werking en de prestaties van de onderneming monitoren). Dan nog moet het specifiek doel dat de werkgever bij dit toezicht nastreeft, gerechtvaardigd kunnen worden door de behoeften van de onderneming of door de ondernemingsregels of voortvloeien uit de aard van de arbeidsovereenkomst of van de uit te voeren taak en moet de opgezette verwerking noodzakelijk blijken te zijn om die doelstelling te bereiken.

---

[44] Koninklijk besluit van 13 februari 2001 *ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens*.

[45] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48nl_sum.pdf. Het gaat om een samenvatting van een advies van de Werkgroep "artikel 29" *betreffende de verwerking van persoonsgegevens in het kader van de arbeidsverhouding*. De Groep 29 is de Europese instantie die de controleautoriteiten en autoriteiten voor gegevensbescherming van alle lidstaten van de Europese Unie groepeert.

125. Overigens moeten de hierbij verwerkte gegevens toereikend zijn, ter zake dienend en niet overmatig, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt. Hun bewaringstermijn mag de termijn niet overschrijden die noodzakelijk is voor het verwezenlijken van de doeleinden waarvoor zij werden verkregen of waarvoor zij verder worden verwerkt (artikel 4, § 1, 5° van de WVP).

126. De verantwoordelijke voor de verwerking moet zich ervan verzekeren dat de gegevens nauwkeurig zijn en zo nodig worden bijgewerkt (artikel 4, § 1, 4° van de WVP).

127. Artikel 12*bis* van de WVP verbiedt dat een besluit waaraan voor een persoon rechtsgevolgen verbonden zijn of dat hem in aanmerkelijke mate treft, louter genomen wordt op grond van een geautomatiseerde gegevensverwerking die bestemd is om bepaalde aspecten van zijn persoonlijkheid te evalueren. Indien dit verbod niet van toepassing is (wanneer het besluit wordt genomen in het kader van een overeenkomst of zijn grondslag vindt in een bepaling voorgeschreven door of krachtens een wet, decreet of ordonnantie) wordt vereist dat in die overeenkomst of in die bepaling passende maatregelen zijn genomen ter bescherming van de gerechtvaardigde belangen van de betrokkene. Minstens moet hem de mogelijkheid geboden worden om op nuttige wijze zijn standpunt naar voor te brengen.

128. Tenslotte legt artikel 4, § 1, 1° een loyauteitsbeginsel vast bij de verwerking van persoonsgegevens. Een toepassing van dit beginsel vindt men trouwens terug in de **transparantievereiste** die aan de verantwoordelijke voor de verwerking wordt opgelegd en die zich vertaalt in de verplichting om aan de betrokken werknemers bepaalde informatie te verstrekken, onder meer met betrekking tot het doeleinde van de verwerking (artikel 9 WVP). Indien er wordt gecontroleerd voor legitieme doeleinden en met medeweten van de betrokken gebruikers kan er niet gesproken worden van het gebruik van 'spy'ware in hoofde van de werkgever. Zie in dat verband overigens het Koninklijk Besluit van 27 augustus 1993 *betreffende het werken met beeldschermapparatuur* dat voorschrijft dat met medeweten van de werknemers gebruik mag worden gemaakt van een kwantitatief of kwalitatief controlemechanisme. Ten slotte is er de plicht de verwerking vooraf aan te geven bij de Commissie[46]. Hoewel er uitzonderingen bestaan op deze twee verplichtingen is de Commissie van oordeel dat deze in onderhavig geval *a priori* niet van toepassing zijn[47].

[46] Zie in dit verband de artikelen 9 en 17 van de WVP.

[47] Zie in dit verband de uitzonderingen op deze verplichtingen respectievelijk enerzijds in artikel 9, § 2 en anderzijds in de artikelen 17 WVP en 51 t.e.m. 62 van het Koninklijk besluit van 13 februari 2001.

129. Overigens moet de verantwoordelijke van de verwerkingen die uitgevoerd worden ter gelegenheid van een controle of toezicht, alle nodige maatregelen nemen om zich ervan te verzekeren dat **de rechten van de betrokken werknemers worden geëerbiedigd of kunnen worden uitgeoefend**[48] en dat de **veiligheid van de verwerking verzekerd is**[49], onder andere bij onderaanneming van bepaalde onderdelen van verwerkingen, teneinde een ongeoorloofd later hergebruik van de ingezamelde informatie te voorkomen. Deze verplichtingen houden onder meer in dat de verantwoordelijke voor de verwerking erover waakt dat voor de personen die optreden onder zijn gezag, 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 werking van de dienst (artikel 16, § 2, 2°) en dat hij de personen die optreden onder zijn gezag informeert over de bepalingen van de WVP en haar uitvoeringsbesluiten, alsook over elk relevant voorschrift met betrekking tot de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (artikel 16, § 2, 3°).

130. Hij zal zich eveneens moeten schikken naar alle overige verplichtingen die opgelegd worden door de WVP.

II.3. BESLUIT

131. Er wordt uitdrukkelijk erkend dat werknemers ook op het werk recht hebben op de bescherming van hun privacy. Maar de arbeidsrelatie heeft een belangrijke impact op de uitoefening van de grondrechten door de werknemer. Op het werk oefent de werkgever namelijk gezag uit, wat inhoudt dat hij leiding en toezicht heeft op het werk van zijn werknemers en dus ook op hun digitale handelingen. Op het werk is de privacyverwachting van de werknemer bijgevolg minder groot dan wanneer de werknemer zelfde handelingen stelt in de familiekring.

132. Het gezagsrecht van de werkgever houdt in dat de werkgever vrij is om het internet en e-mailgebruik op het werk toe te laten of te verbieden.

133. De artikelen 2, 3, 4 et 5 van de Arbeidsovereenkomstenwet voorzien het gezag van de werkgever (met andere woorden zijn bevoegdheid inzake instructie en toezicht) als een wezenlijk element van het contract.

134. Artikel 16 van de Arbeidsovereenkomstenwet voorziet verder dat de beide partijen elkaar respect en eerbied verschuldigd zijn. Artikel 17 van de Arbeidsovereenkomstenwet bepaalt dat de

[48] Het gaat om het recht op toegang, verbetering en verzet zoals beschreven in de artikelen 10, 11 en 12 van de WVP.

[49] Zie in dit verband de verplichtingen die beschreven zijn in artikel 16 van de WVP.

werknemer zijn werk zorgvuldig, eerlijk en nauwkeurig moet verrichten en dat hij moet handelen volgens de bevelen en instructies van zijn werkgever.

135. De Commissie is van oordeel dat die bepalingen, of gelijkluidende bepalingen in het openbaar ambt, samen met de richtsnoeren zoals vastgelegd in de WVP en de CAO nr. 81, voldoende duidelijk zijn om te bepalen in welke mate de werkgever over enig controlerecht beschikt. Die bepalingen vormen, samen gelezen, voor de Commissie een wettelijke toelating in de zin van artikel 125, § 1, 1° van de Wet Elektronische Communicatie, waardoor er geen sprake kan zijn van een inbreuk op artikel 124 van de Wet Elektronische Communicatie, voor zover de werkgever rekening houdt met de 3 basisbeginselen uit deze wetgevingen, waarvan de naleving essentieel wordt geacht voor de bescherming van de persoonlijke levenssfeer van werknemers bij de verwerking van hun persoonsgegevens: het finaliteitsbeginsel, het proportionaliteitsbeginsel en het transparantiebeginsel.

136. In dat geval kan ook geen sprake zijn van bedrieglijk opzet zoals vereist in art. 550*bis* Strafwetboek. Het gaat ook niet om een kennisname van de inhoud van een e-mail tijdens de overbrenging van de communicatie, zoals vereist om strafbaar te zijn in toepassing van art. 314*bis* Strafwetboek.

137. De Commissie meent dat de toestemming van de betrokken werknemer(s) niet de wettelijke basis kan vormen welke een patronale controle van de digitale handelingen van de werknemers verwezenlijkt in het kader van de arbeidsrelatie of aan de hand van de werkinstrumenten toelaat. Omwille van de bestaande machtsverhoudingen tussen de partijen zou een individuele toestemming van de betrokken werknemers niet kunnen worden aanzien als werkelijk vrij.

138. De Commissie geeft hierna de voornoemde basisprincipes aan waar de werkgever zich bij de uitoefening van zijn controlerecht moet aan houden.

Principe 1: Finaliteitsbeginsel

139. Het finaliteitsbeginsel houdt in de eerste plaats in dat de doeleinden van een toegang tot of controle van de elektronische communicatie van de werknemer gerechtvaardigd moeten zijn.

140. Voor elke inmenging in dat grondrecht moet een gerechtvaardigd doeleinde kunnen worden aangetoond. De controle moet t.o.v. de finaliteit van de verwerking toereikend, ter zake dienend en niet overmatig zijn, zodat de gekozen persoonsgegevens volgens de vooropgestelde finaliteit moeten worden geëvalueerd. De doeleinden waarvoor men enige controle doorvoert mogen niet vaag en

onbepaald omschreven worden. Er moet op voorhand duidelijk gemaakt worden waarvoor de controle dient, alsook hoe de eventuele verwerkte gegevens later kunnen/zullen gebruikt worden. Daaraan staat echter niet in de weg dat de verkregen gegevens kunnen worden aangewend voor een ander doel dan was aangekondigd, voor zover die aanwending niet onverenigbaar is met het oorspronkelijke doel.

141. De gegevens moeten steeds eerlijk worden verwerkt (de werknemer mag niet in de val worden gelokt), of het nu gaat om een controle of voor een ander doeleinde, voor doeleinden die niet onverenigbaar zijn met de redelijke verwachtingen van de betrokken werknemers. De gegevensverwerking moet dus plaatsvinden in overeenstemming met het of de aangekondigde doeleinden. Indien de verwerking plaatsvindt in het raam van een ander doeleinde, dan moet dit verenigbaar zijn met het oorspronkelijke doeleinde en moet de werkgever de nodige maatregelen nemen om vergissingen bij de interpretatie van de resultaten van de verrichting te vermijden. Het feit dat de werkgever gegevens bewaart voor bewijsdoeleinden of voor de continuïteit van zijn activiteiten, volstaat niet om een controle van deze gegevens te rechtvaardigen (hierbij wordt in het bijzonder informatie geviseerd die via een netwerk wordt vermenigvuldigd, opgeslagen en gearchiveerd (back-ups)).

Principe 2: Transparantiebeginsel

142. De werkgever dient duidelijk aan zijn werknemers aan te geven in welke mate het internet- en e-mailgebruik binnen de onderneming wordt toegelaten en op welke wijze hier toegang tot of controle zal worden uitgeoefend.

Principe 3: Proportionaliteitsbeginsel

143. Iedere beperking van de privacy van de werknemer moet zoveel mogelijk beperkt worden. Het is pas nadat alle preventiemaatregelen onvoldoende blijken te zijn dat de werkgever het bestaan kan vaststellen van enig misbruik. Bij de controle waarbij enige inbreuk wordt gepleegd op het recht op privacy van de werknemer wordt die inbreuk zo veel mogelijk beperkt door het volgen van een stappenplan zoals omschreven in de CAO nr. 81. Het is pas als dat alles onvoldoende zou zijn om het vermoede misbruik vast te stellen dat de werkgever kennis kan nemen van de inhoud van communicatie waar de werknemer aan deelgenomen heeft.

III. **GEBRUIK VAN HET (ONRECHTMATIG VERKREGEN) BEWIJS**

144. Hoewel de werkgever er baat bij heeft de bovenstaande wettelijke voorwaarden, procedures en waarborgen op correcte wijze te implementeren en na te leven, aangezien de bewijsmiddelen naar aanleiding van de door hem gevoerde controles dan normaliter als rechtsgeldig zullen worden aanzien, oordeelde het Hof van Cassatie in het zogenaamde "Antigoon-arrest" van 14 oktober 2003 dat onrechtmatig verkregen bewijs slechts tot uitsluiting moet leiden indien de naleving van bepaalde vormvereisten voorgeschreven is op straffe van nietigheid, indien de onrechtmatigheid de betrouwbaarheid van het bewijs heeft aangetast of het gebruik van het bewijs in strijd is met het recht op een eerlijk proces[50]. In het arrest van 23 maart 2004 herhaalde het Hof van Cassatie dit en voegde eraan *toe "dat het de rechter staat de toelaatbaarheid van onrechtmatig verkregen bewijs te beoordelen in het licht van de artikelen 6 EVRM of 14 IVBPR, rekening houdende met de elementen van de zaak in haar geheel genomen, inbegrepen de wijze waarop het bewijs verkregen werd en de omstandigheden waarin de onrechtmatigheid werd begaan"*[51].

145. Het Europees Hof voor de Rechten van de Mens keurde die rechtspraak ook al goed[52].

146. In het Chocolatier Manonarrest van 2 maart 2005 aanvaardde het Hof van Cassatie dat de rechter rekening hield met videobeelden, die een werkgever in strijd met de CAO nr. 68 van 16 juni 1998 *betreffende de bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de camerabewaking op de arbeidsplaats* had verkregen. Het Hof overweegt dat, aangezien de miskenning van de informatieverplichting uit de CAO nr. 68 niet met nietigheid wordt bestraft, het de rechter toekomt de gevolgen van die miskenning te bepalen op de toelaatbaarheid van de bewijsmiddelen die op onregelmatige wijze werden verkregen[53].

147. Bij arrest van 10 maart 2008[54] aanvaardde het Hof van Cassatie dat dezelfde bewijsuitsluitingsregels van toepassing zijn in een burgerlijke, sociale zaak. Behoudens wanneer de wet uitdrukkelijk anders bepaalt, dient de rechter volgens het Hof van Cassatie de toelaatbaarheid van een onrechtmatig verkregen bewijs te beoordelen in het licht van de artikelen 6 EVRM en 14 internationaal verdrag inzake burgerrechten en politieke rechten, rekening houdende met de elementen van de zaak in haar geheel genomen, inbegrepen de wijze waarop het bewijs verkregen werd en de omstandigheden waarin die onrechtmatigheid werd begaan. Een dergelijk bewijs, behoudens het geval van miskenning van een op straffe van nietigheid voorgeschreven vorm, mag,

---

[50] Cass. 14 okt. 2003, AR P.03.0762.N, met concl. van adv.-gen. DE SWAEF.

[51] Cass. 23 maart 2004, AR P.04.0012.N.

[52] Arrest Lee Davies t. België van 28 juli 2009, *www.echr.coe.int*; F. SCHUERMANS, "Antigoon-rechtspraak nu definitief in de fase van de rustige vastheid", *R.A.B.G.* 2010, 17-24.

[53] Cass. 2 maart 2005, *Arr.Cass.* 2005, afl. 3, 506, concl. VANDERMEERSCH; *Rev.dr.pén.* 2005, afl. 6, 668.

[54] *Pas.* 2008, afl. 3, 652; *RCJB* 2009, afl. 3, 325.

zo besliste het Hof, alleen worden geweerd wanneer de bewijsverkrijging is aangetast door een gebrek waardoor de betrouwbaarheid ervan wegvalt of waardoor het recht op een eerlijk proces in gevaar wordt gebracht. De rechter kan bij deze afweging, onder meer, rekening houden met één of meer van volgende omstandigheden:

- het zuiver formeel karakter van de onregelmatigheid;
- de weerslag op het recht of de vrijheid die door de overschreden norm zijn beschermd;
- de omstandigheid dat de overheid die met de opsporing, het onderzoek en de vervolging van misdrijven is belast, al dan niet de onrechtmatigheid opzettelijk heeft begaan;
- de omstandigheid dat de ernst van de inbreuk veruit de begane onrechtmatigheid overstijgt;
- het feit dat het onrechtmatig verkregen bewijs alleen een materieel element van het bestaan van de inbreuk betreft;
- het feit dat de onregelmatigheid die aan de vaststelling van de inbreuk voorafging of daarmee gepaard ging, volstrekt onevenredig is met de ernst van die inbreuk.

148. Hoewel de zaak betrekking had op de gevolgen van een strafonderzoek op een burgerlijke zaak (de schorsing door de RVA), lijkt het Hof hiermee toch de principes van de Antigoonrechtspraak in het strafrecht door te trekken naar het burgerlijk/sociaal recht.

149. Die principes hebben ook al ingang gevonden bij de arbeidsrechtbank en –hoven. Zo besliste de arbeidsrechtbank te Gent in haar vonnis van 1 september 2008[55] dat de e-mails die de werknemer had verzonden en waarmee een concurrerende activiteit werd opgezet, toch mochten gebruikt worden om het ontslag wegens dringende reden te aanvaarden hoewel de controle niet werd aangekondigd. De arbeidsrechtbank stelde vast dat ondanks die onwettigheid, de betrouwbaarheid van het bewijs niet was aangetast, het recht op een eerlijk proces niet geschonden was en het verkregen bewijs dus toch mocht worden gebruikt. Het arbeidshof te Antwerpen paste dezelfde principes ook toe in zijn arrest van 2 september 2008[56]. Sindsdien hebben meerdere beslissingen toepassing gemaakt van de rechtspraak bij sociale geschillen[57].

150. De Commissie is van mening dat de rechter die niet met een van deze situaties geconfronteerd wordt bij een probleem van cybersurveillance, de afweging zou moeten maken tussen de begane inbreuk en de aantasting van het recht op privacy ("de ernst van de "inbreuk" die de vaststelling mogelijk maakte overstijgt duidelijk de begane onregelmatigheid").

---

[55] *TGR-TWVR,* 2009, afl. 4, 275.

[56] *Or.* 2008, afl. 9, 261.

[57] Zie onder meer C.T. Liège (Sect. Namur), 14 décembre 2010, R.G. n°2009/AN/8.833; Trib. trav. Charleroi, (1ère ch.), 16 juin 2010, *Bull.Ass.*, 2010, n°372, p. 294.

151. Indien de werknemer een inbreuk gepleegd heeft op de wet, zou het feit dat bepaalde procedureregels met betrekking tot de privacy niet werden nageleefd op zich niet kunnen rechtvaardigen dat bewijsstukken worden geweerd.

152. Indien de werknemer de door de werkgever vastgestelde interne regels voor het gebruik van netwerktechnologieën niet heeft nageleefd, zou de Commissie het daarentegen onbillijk vinden dat deze laatste met succes een bewijs voor het gerecht zou kunnen aanvoeren dat strijdig is met zijn eigen professionele verplichtingen ingevolge de wet of zijn eigen arbeidsreglement (zoals zijn werknemers informeren, controleprocedures voorzien en ze naleven, enz.).

153. Tot slot herinnert de Commissie eraan dat schendingen van de WVP ook op een andere wijze gesanctioneerd kunnen worden dan door de uitsluiting (al dan niet na een belangenafweging door de feitenrechter) van het bewijs. De WVP bevat een aantal strafbepalingen (in het bijzonder art. 39 WVP). De werkgever die in strijd met de WVP gegevens verwerkt, stelt zich bijgevolg bloot aan een strafvervolging. Er is al rechtspraak gekend waar het onrechtmatig verkregen bewijs niet uit de debatten werd geweerd, gelet op de zwaarwichtigheid van de feiten die het bewijs aantoonde, maar dat de werkgever tegelijk ook wordt veroordeeld wegens de begane schending van de privacyregels.

IV. AANBEVELINGEN

154. De Commissie zal hierna, onder de vorm van een reeks aanbevelingen, een aantal gedragsregels formuleren die voorbeelden of middelen vormen om rekening te houden met de WVP in het raam van een toegang tot elektronische communicatiemiddelen en waarvan zij meent dat deze conflicten tussen de belangen van de werkgevers en de bescherming van de rechten van de werknemers kunnen vermijden.

155. Deze aanbevelingen zouden in het algemeen en onder voorbehoud van de praktische uitvoering ervan, moeten toelaten een passende bescherming te waarborgen voor de fundamentele rechten en vrijheden van al diegenen van wie de persoonsgegevens worden verwerkt in het raam van een toegang tot elektronische communicatiemiddelen.

156. De Commissie wil echter benadrukken dat deze aanbevelingen geen enkel dwingend of verplichtend karakter hebben. De opgesomde aanbevelingen vormen slechts een leidraad. Er zijn nl. andere voorbeelden/suggesties, wellicht meer aangepast aan de specificiteit van sommige ondernemingen of functies, denkbaar die eveneens de concrete invulling of vertaling kunnen zijn van bepaalde wettelijke regels of verplichtingen die voortvloeien uit de WVP.

157. De Commissie wil zich hier immers niet in de plaats stellen van de werkgevers, die verantwoordelijk zijn voor de verwerkingen van persoonsgegevens die zij verrichten tijdens een controle van of toezicht op hun werknemers, noch van de sociale partners die de macht en bevoegdheid bezitten om regels inzake de organisatie van die controle en dit toezicht te onderhandelen en, in overeenstemming met de dwingende wettelijke voorschriften, akkoorden ter zake af te sluiten.

158. Dit is des te meer het geval, gelet op de diversiteit tussen en binnen besturen en bedrijven. Een interne policy zal uiteindelijk moeten concretiseren op welke (procedurele) wijze het samenstel van waarborgen, neergelegd in onder andere de WVP, in de praktijk door een werkgever zal worden aangeboden en geëerbiedigd, ten einde bij controle/toegang het recht op bescherming van de privacy van werknemers waarin artikel 2 WVP[58] voorziet veilig te stellen.

159. Hierna volgen een aantal **juridische** gedragsregels geformuleerd rond 4 clusters die voorbeelden of middelen vormen om rekening te houden met de WVP bij een patronale toegang tot of controle van elektronische communicaties.

160. Bij wijze van algemene basisaanbeveling dienen preventieve (juridische, managementgerelateerde en technische) regels, alsook procedures (bijvoorbeeld voor klassement van e-mails, documenten, bestanden) maximaal uitgewerkt te worden teneinde de nood aan patronale toegang tot of controle op persoonlijke informatie van werknemers te vermijden.

161. Ter zake is er niet alleen een taak weggelegd voor de werkgever, maar ook voor de betrokkenen zelf. Personeelsleden moeten ook een zorgvuldigheidsplicht aannemen met betrekking tot de eigen persoonsgegevens voorhanden op de werkplek (bv. evaluatiegegevens, weddenfiches,…) en moeten deze dus voldoende afschermen voor derden, zelfs binnen de onderneming/het openbaar bestuur.

162. Dit geldt ook voor privé-e-mailberichten die zij ontvangen of versturen op de werkplek. Werknemers gebruiken het e-mailsysteem van de werkgever inderdaad ook in meerdere of mindere mate voor privédoeleinden, zeker als dat expliciet werd toegelaten door de werkgever.

---

[58] "*Iedere natuurlijke persoon heeft in verband met de verwerking van persoonsgegevens die op hem betrekking hebben, recht op bescherming van zijn fundamentele rechten en vrijheden, inzonderheid op bescherming van zijn persoonlijke levenssfeer.*".

163. Werknemers hebben weliswaar het recht om in beperkte mate op de werkvloer privé-communicatie te voeren, maar om hun privacy te waarborgen is het aan te bevelen om zakelijk mailverkeer zo veel als mogelijk van privé-mailverkeer te scheiden.

164. Private e-mails die tijdens de werkuren wordt ontvangen of verzonden door de werknemer zijn immers niet *a priori* bestemd om door de werkgever te worden vernomen of ontvangen, en al zeker niet ten aanzien van de inhoud ervan[59].

165. Functionele e-mails moeten daarentegen *a priori* kunnen worden behandeld en verwerkt in de normale context van professionele communicatie binnen een bedrijf/bestuur, ook ten aanzien van de inhoud ervan, aangezien ze evident te maken hebben met de uitvoering van de arbeidstaak sensu stricto.

166. Bij dubbel gebruik van het e-mailsysteem zijn de rechten en belangen van de twee partijen echter moeilijk te verzoenen.

167. In dat geval zal de werkgever immers, ook al ligt het enkel in zijn bedoeling kennis te krijgen van de inhoud van e-mails met een beroepsmatig karakter voor doeleinden van beheer en organisatie van zijn activiteiten (en niet om te 'controleren' of er enig misbruik wordt gemaakt van zijn e-mailsysteem), hoe dan ook aan de privacy van de eindgebruiker raken.

168. Hij zal immers onvermijdelijk stoten op niet-beroepsmatige e-mails, terwijl de kennisname van het bestaan van dergelijke e-mails (laat staan de inhoud ervan) eigenlijk alleen maar zou kunnen na het volgen van de geleidelijke aanpak van CAO nr. 81 (eerst een anonieme controle en pas daarna een geïndividualiseerde controle) en mits respect voor de individualiseringsregels waarin CAO nr. 81 voorziet.

169. Tegen een dergelijke achtergrond ligt een oplossing voor de hand: het komt er op aan het dubbel gebruik van het patronaal e-mailsysteem te vermijden en het probleem van de directe toegang tot privé e-mail van werknemers stelt zich dan normalerwijze niet meer.

---

[59] Omdat ze echter tijdens de dienstbetrekking worden gegenereerd, moet de werkgever wel het bestaan van bepaalde private communicatiebewegingen van zijn ondergeschikten kunnen volgen wanneer ze de correcte uitvoering van de arbeidstaak ondermijnen (misbruik van arbeidsuren).

170. Dit kan door aan de werknemers te vragen om private e-mail via een persoonlijk e-mailadres te laten verlopen (genre hotmail), en niet via het e-mailadres dat de werknemer werd ter beschikking gesteld om de professionele activiteiten te kunnen uitvoeren.

171. Indien de werkgever in de ICT-policy heeft opgelegd dat het dubbel gebruik van zijn e-mailsysteem (professioneel en privaat) is verboden, dan mag de werkgever er in principe van uit gaan dat de e-mails een beroepskarakter hebben, zeker ten aanzien van de verzonden berichten[60].

172. Een eventuele rechtstreekse toegang tot dergelijke e-mails van een werknemer kan dan ook worden verantwoord, mits respect voor de grote basisprincipes uit de WVP, nl. een toegang enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden; een toegang die bovendien toereikend, ter zake dienend en niet overmatig is, uitgaande van die doeleinden en mits adequate informatie werd verstrekt over die toegang.

173. Wanneer de werkgever bij een dergelijke rechtstreekse toegang niettemin een private e-mail aantreft, krijgt hij daar dus op een rechtmatige wijze kennis van, aangezien er geen specifieke maatregelen moesten worden genomen om privé-informatie (die er immers in principe niet kon/mocht zijn) te beschermen. Dit betekent nog niet dat een privémail die aldus ter kennis komt van de werkgever nadien voor eender welk doel (bv. een gebruik met bedrieglijk opzet of met het oogmerk de betrokken werknemer of derde te schaden) zou mogen worden gebruikt. Een verder gebruik ervan zal daarentegen moeten beantwoorden aan de vereisten van WVP.

174. Wanneer werkgevers niet kunnen of willen afstappen van het dubbel gebruik van hun e-mailsysteem, zullen zij onvermijdelijk moeten aanvaarden dat een personeelslid een hogere privacyverwachting kan laten gelden over zijn elektronische postbus. Bij gemengd gebruik van het patronaal e-mailsysteem door de werknemer zullen dus wel specifieke maatregelen moeten worden genomen door de werkgever die ertoe strekken om bijvoorbeeld in het kader van de zoektocht naar professionele berichten (waarop de werkgever evident recht heeft), de persoonlijke berichten van de betrokkene zoveel als mogelijk te ontzien en te beschermen.

175. Een dergelijke gemengde elektronische postbus kan dan ook niet in zijn geheel rechtstreeks consulteerbaar zijn voor de werkgever. Er zal daarentegen een bijkomende procedure moeten afgesproken worden om de scheiding te maken tussen beide type berichten, bijvoorbeeld door de werknemer te vragen de verstuurde en ontvangen e-mails te classificeren, waarbij de patronale

[60] Inzake binnenkomende e-mail zal de werkgever voorzichtiger moeten optreden dan ten aanzien van uitgaande mails, vermits de werknemer er de auteur niet van is en allicht bepaalde mails zelfs niet verwachtte.

kennisname van het bestaan van als 'privé geclassificeerde e-mails (laat staan de inhoud ervan) eigenlijk alleen maar zou kunnen na het volgen van de gefaseerde aanpak van en mits respect voor de individualiseringsregels van CAO nr. 81.

176. De hiernavolgende juridische aanbevelingen zijn dan ook vooral, maar niet uitsluitend, van toepassing op werkgevers die het dubbel gebruik van hun e-mailsysteem toelaten of gedogen.

Verzeker u van de naleving van het wettigheidsbeginsel, de voorzienbaarheid van de verwerkingen en van de inmenging in het recht op bescherming van de privacy van de werknemers

-verwerk enkel persoonsgegevens in de door de WVP toegelaten gevallen;

-voorzie inspraak en consultatie van de werknemersvertegenwoordiging;

-stel de werknemers in kennis van de na te leven regels en voorwaarden voor de controle of het toezicht;

-leg het toegangsbeleid tot elektronische communicatie of elektronische communicatiegegevens van werknemers vast in een geschreven document, bijvoorbeeld in het arbeidsreglement.

Beperk de mogelijke inmenging in de privacy van werknemers

-beperk de verwerkingsmogelijkheden van een werkgever met betrekking tot informatie opgeslagen in de eindapparatuur van een eindgebruiker (bijvoorbeeld in een *de facto* "gemengde" professionele mailbox) tot wat hij effectief nodig heeft;

-voer de minst ingrijpende gegevensverwerking uit (die dus de kleinste kans biedt op identificatie van de betrokkenen door het verwerken van zo algemeen mogelijke informatie);

-motiveer iedere aanzienlijkere toegang tot persoonsgegevens van werknemers of een werknemer in het bijzonder door feitelijke elementen;

-responsabiliseer werknemers opdat ze zich zouden houden aan de regels met betrekking tot het internet- en e-mailgebruik op het werk, bv. door de functie "afwezigheidsassistent" van hun mailbox (met vermelding van te contacteren personen) in te stellen zodat enige inbraak op professionele informatiedragers bij hun afwezigheid niet nodig is;

-neem (technische) preventiemaatregelen om misbruik door werknemers te vermijden;

-controleer, indien preventie niet zou volstaan, op misbruik enkel aan de hand van het bestaan van bepaald e-mailverkeer of surfgedrag en dit volgens het stappenplan waarin CAO nr. 81 voorziet;

-controleer, indien het bestaan van bepaald e-mailverkeer of surfgedrag niet volstaat om misbruik vast te stellen, slechts uitzonderlijk door kennisname van de inhoud van communicatie waaraan de werknemer heeft deelgenomen.

Omkader de toezicht- en controleverrichtingen

-verwerk naar aanleiding van een toegang tot elektronische communicatie of elektronische communicatiegegevens, al dan niet in het raam van een controle, enkel toereikende, ter zake dienende, nauwkeurige, geactualiseerde en voor de verwezenlijking van het doeleinde niet te lang bewaarde persoonsgegevens;

-zorg ervoor dat de persoon die met opzoeking en de inzameling van persoonsgegevens wordt belast een andere persoon is dan degene die daartoe de opdracht geeft;

-zorg ervoor dat de zoeker tewerk gaat op basis van zo nauwkeurig mogelijke instructies van de opdrachtgever en dat hij zich in zijn zoektocht beperkt tot wat hem werd gevraagd;

-zorg ervoor dat de opzoeking zoveel als mogelijk gebeurt op basis van relevante criteria die in een eerste fase toelaten een maximaal aantal gegevens uit de raadpleging te weren;

-zorg ervoor dat de opzoeking vooreerst gebeurt op basis van data, trefwoorden, identiteit van de ontvangers of verzenders van berichten alvorens zich toegang te verschaffen tot de inhoud;

-vaardig speciale regels inzake toegang en gebruik af voor de systeembeheerder in het kader van de uitoefening van zijn functie;

-zorg ervoor dat de persoonsgegevens die door toegang rechtmatig worden opgezocht en ingezameld blijven verder genieten van hun oorspronkelijke bescherming, gelet op hun wettelijk statuut (bv. een personeelsdossier: de persoon die werd aangeduid voor het realiseren van de toegang op vraag van de werkgever is na die toegang gehouden tot dezelfde vertrouwelijkheid als de werknemer die normaal het personeelsdossier beheert) of door het statuut dat er beroepsmatig

aan werd verleend door de titularis van het instrument of een eventuele correspondent (bv. een nog vertrouwelijke onderhandeling met een derde moet dus ook na de toegang even vertrouwelijk blijven);

-neem geen belangrijke beslissing tegen de betrokkene louter op basis van informatie die ingezameld werd naar aanleiding van een verwerking van zijn persoonsgegevens (bijvoorbeeld in het raam van een toezicht of controleverrichting);

-biedt de betrokkene, alvorens enige beslissing jegens hem te nemen, de mogelijkheid zijn standpunt naar voor te brengen, onder andere wat de juistheid en relevantie van de ingezamelde persoonsgegevens betreft.

Waarborg de naleving van de regels en versterk de veiligheid van het toezicht en de controle

-hou alle intrusieverrichtingen in de informatica-instrumenten of in de informatie die deze instrumenten genereren in een geschrift bij (wat werd er bekeken, verzameld en doorgegeven, wanneer, hoe en voor wiens rekening, door wie en aan wie het werd meegedeeld) om enige controle op de naleving door de werkgever op het finaliteitsbeginsel en het proportionaliteitsbeginsel mogelijk te maken;

-zorg ervoor dat indien het beheer en het onderhoud van de instrumenten en netwerken wordt verzekerd door een externe dienstverlener, de interne bedrijfsregels ook gelden voor deze dienstverlener en sluit een verwerkerscontact af met een dergelijke onderaannemer;

-leg de organisatie van de procedures maar ook de effectief geplande toezicht- en controleverrichtingen, en meer in het algemeen alle toegangen tot de informaticatools, indien voorhanden, voor aan de aangestelde voor de gegevensbescherming in de onderneming zodat hij het noodzakelijk en rechtmatig karakter ervan kan beoordelen;

-voorzie ten slotte een opleiding gegevensbescherming welke moet leiden tot responsabilisering van de gecontroleerde en tot goede praktijken in hoofde van het toezichthoudend personeel.

177. Tot slot volgen nog een aantal **praktische** gedragsregels die voorbeelden of middelen vormen om rekening te houden met de WVP bij een patronale toegang tot of controle van elektronische communicaties voor de meest voorkomende problemen. De voorgestelde oplossingen zullen echter nooit blindelings mogen toegepast worden (de toepassing van een bepaalde maatregel kan een

andere maatregel overbodig maken of zelfs onverenigbaar zijn met een andere maatregel). Ieder bedrijf dient de toepasselijkheid ervan te onderzoeken en na te gaan of er geen passender oplossingen zijn.

178. Sommige van de vermelde praktijken lijken veeleer op "kunst en vliegwerk" maar vormen vaak efficiënte oplossingen voor problemen met de eerbiediging van de beginselen van de bescherming van de persoonlijke levenssfeer.

Praktijk nr. 1: Professionele en privé-informatie scheiden

1. Voor informaties, bestanden en documenten

Voorbeeld 1: opslag van privé-informaties

- Aanmaak op het werkstation van een map genaamd "privé-naam gebruiker" voor het opslaan van alle niet-professionele documenten. Deze map mag geen professionele informatie bevatten.
- De privé map wordt opgeslagen op een gedeelte van de harde schijf waarvan geen gecentraliseerde en systematische veiligheidskopieën (back-ups) worden gemaakt.

Voorbeeld 2: opslag van professionele informaties

- De professionele informaties, alle privé-informatie uitgezonderd, wordt verplicht opgeslagen op de harde schijf van een centrale server, in voorkomend geval in aan de gebruiker voorbehouden mappen. De professionele documenten op het werkstation vormen dan louter kopieën die beschouwd worden als van tijdelijke aard en die niet noodzakelijk het voorwerp uitmaken van systematische veiligheidskopieën (deze gebeuren centraal voor de informaties op de server).

2. Voor elektronische boodschappen

Voorbeeld 3: opslag van privé-informaties

- Aanmaak in de mailbox van een map genaamd "privé-naam gebruiker" voor het opslaan van alle niet-professionele boodschappen (verzonden en ontvangen). Deze map mag geen professionele boodschappen bevatten (niet-naleving kan aanleiding geven tot sancties).

Voorbeeld 4: Gebruik van verschillende accounts

- Toekenning van twee (of meer) mailaccounts aan elke gebruiker met verschillende identificatie, één voor de privéboodschappen, de andere voor de professionele boodschappen naargelang de aard van de activiteit. Dit onderscheid kan gemaakt worden aan de hand van de naam (bv. initialen@domein.com voor de professionele en naam.voornaam@domein.com voor de privéboodschappen) of aan de hand van de domeinnaam (bv. naam@domein.com voor de professionele en naam@domein.net voor de privéboodschappen), of nog, aan de hand van een subdomein, genre naam@persoonlijk.domein.com.

3. Voor de internetcommunicatie

Voorbeeld 5: Gebruik van verschillende accounts

- Toekenning van twee (of meer) gebruikersaccounts naargelang de aard activiteit. Een semantische structuur van het identificatiemiddel laat toe de controlefilters hierop af te stemmen (naam0 voor privé, naam, naam1, naam2,… voor het professionele gedeelte).

4. Door het onderscheiden van de werkstations

Bepaalde diensten of gedeelten van een netwerk kunnen een bijzondere gevoeligheid vertonen (bv. lokaal voor het beheer van systemen en netwerken, dienst human resources,…). In die gevallen kan het gewettigd zijn elke privéactiviteit op deze werkstations te verbieden teneinde deze permanent en op strikte wijze te kunnen controleren, doch hierbij andere werkstations ter beschikking te stellen voor minder gevoelige of privéactiviteiten. Een dergelijk onderscheid kan eveneens bijdragen aan de efficiëntie van de technische scheiding van de netwerken zoals de VLAN en VPN.

5. Door het onderscheiden van de handtekeningen

De gestructureerde handtekeningen in de berichten kunnen ook een onderscheidend criterium vormen tussen professioneel en privé.

Voorbeeld 6: Gebruik van verschillende handtekeningen met een standaard disclaimer

- De automatische toevoeging van standaard waarschuwingsclausules bij elektronische berichten die verstuurd worden via de server of een adres van het bedrijf: hetzij een disclaimer waarin gesteld wordt dat het bericht privé verstuurd wordt en niet bindend is voor het bedrijf; hetzij een waarschuwing met betrekking tot het professioneel karakter van het bericht en de mogelijkheid

dat dit, zonder noodzakelijke rechtvaardiging, geraadpleegd of gelezen kan worden door de verantwoordelijken van het bedrijf.

Praktijk nr. 2: Bepaalde risicovolle handelingen uitsluiten

Om de naleving van bepaalde onderrichtingen over het gebruik van informatica-uitrusting te waarborgen en een toezicht te vermijden waardoor de werkgever toegang zou verkrijgen tot nutteloze informatie, kan het opportuun zijn via de uitrusting van het bedrijf bepaalde handelingen uit te sluiten (bv. de toegang blokkeren tot bepaalde websites of elektronische adressen die bekend staan als gevaarlijk) of waarschuwingen te programmeren bestemd voor de gebruiker ingeval van twijfelachtige handelingen. De verschillende functies en lijsten met te verbieden websites en adressen zijn beschikbaar bij specifieke software (internet veiligheidspakketen) en kunnen aangevuld worden op basis van de specifieke behoeften van het bedrijf.

Wanneer men de kostprijs en de efficiëntie vergelijkt van de antivirusprogramma's met de internet veiligheidspakketten kan men de antivirusbescherming als ontoereikend beschouwen ten opzichte van de permanente dreiging die gevormd wordt door internetnetwerken.

Praktijk nr. 3: de toegang tot persoonlijke communicaties vereist een specifieke omkadering

Sommige professionele communicaties kunnen een specifiek persoonlijk karakter hebben (bv. door een vermelding in het onderwerp). Een toegang tot deze communicaties zal slechts met de passende voorzichtigheid kunnen plaatsvinden, zelfs als deze communicaties duidelijk van professionele aard zijn.

Voorbeeld 1:

- Vermelding "PERSOONLIJK" of "VERTROUWELIJK" in het onderwerp van het bericht. Het lijkt evenwel moeilijk om deze discipline te eisen vanwege derden die een boodschap sturen aan het bedrijf.

Voorbeeld 2:

- Gebruik van specifieke mappen in de domeinen die voorbehouden zijn aan de professionele communicaties.

Voorbeeld 3:

- Om berichten te selecteren en hieraan het nodige gevolg voor te behouden, zal men een neutrale vertrouwenspersoon aanduiden die gehouden is tot vertrouwelijkheid en gemachtigd is om de hoedanigheid van het bericht te beoordelen. Een hiërarchische meerdere, een collega of een bestuursassistent kunnen slechts uitzonderlijk als gepaste persoon fungeren.

Voorbeeld 4:

- Wanneer informaties een gevoelig karakter hebben, ze overbrengen in bijgevoegde stukken die op specifieke wijze beschermd kunnen worden.

Voorbeeld 5:

- Wanneer personen vaak informaties met vertrouwelijk karakter behandelen (voorbeelden: medische gegevens, beraadslaging van een jury), de toegang met het oog op controle enkel toelaten aan de personen die gemachtigd zijn toegang te hebben tot deze categorie van gegevens (voorbeeld: een geneesheer voor de medische gegevens).

<u>Praktijk nr. 4: Het toezicht beperken tot de noodzakelijke gegevens en geen hergebruik van ingezamelde gegevens</u>

Aangezien een toegang tot het informatica-instrument of elektronisch communicatiemiddel toelaat om gemakkelijk andere informatie in te zamelen dan deze (toereikend, ter zake dienend en niet overmatig) die bedoeld wordt door het toezichtdoeleinde, zou de toegang tot de gegevens, hun opsporing, inzameling en doorgifte moeten omkaderd worden door beperkingsprocedures.

Voorbeelden:

- Extractie, in real time of zo vlug mogelijk van toezichtgegevens (journalen, logs, sporen) voor een opslag in een beveiligde zone ("silo": specifieke server, gecodeerd bestand,…) waarvan de toegang strikt beperkt is en specifiek wordt afgebakend.
- Verduidelijking in het informatieveiligheidsbeleid van het verbod om toezichtgegevens te gebruiken voor enig ander doeleinde dan deze die bepaald werden in het raam van het toezicht.

<u>Praktijk nr. 5: Onverenigbaarheden invoeren in de toegangsrechten voor eenzelfde persoon</u>

Een gebruiker zou niet in staat mogen zijn om zijn onrechtmatige handelingen te verdoezelen, bijvoorbeeld door de sporen die gegenereerd worden door zijn handelingen te wijzigen. Dergelijke beperkingen zijn thans mogelijk via de beheersinstrumenten voor identiteiten en toegangen.

Praktijk nr. 6: Beheer van de sporen

De procedures voor het natrekken van sporen, hun behandeling, opslag en beveiliging dienen expliciet en voldoende precies te zijn om het nodige vertrouwen te creëren voor een erkenning van ontvankelijkheid en tegenwerpbaarheid door partijen. Het behoort de Commissie niet toe een of andere techniek aan te bevelen dus suggereert zij enkele mogelijkheden:

Voorbeelden:

- Creatie, vóór iedere analyse, van een bestand met gecumuleerde sporen op sequentiële en oplopende wijze waardoor iedere latere aantasting moeilijk zo niet onmogelijk gemaakt wordt.
- Berekening van een afdruk vóór iedere analyse en opgeslagen op beveiligde wijze.
- Auditmogelijkheid van de dagelijkse en praktische naleving van de goede uitvoering van de procedures.
- Tijdens opgespoorde verwerkingen, vergrendeling waardoor desactivering of wijziging van de sporen onmogelijk gemaakt wordt.
- Verzegeling, via passende cryptografische instrumenten, van de sporen in real time waardoor de authenticiteit en integriteit wordt gewaarborgd.

Praktijk nr. 7: De functioneringsregels bepalen in uitzonderlijke gevallen

Het normale gebruik van een informatica-instrument laat toe het toezicht te waarborgen via relatief eenvoudige regels. Talrijke uitzonderlijke situaties veroorzaken echter ernstige moeilijkheden indien zij niet werden voorzien en omkaderd door passende regels.

1. Geplande afwezigheid van een medeweker

Praktische voorbeelden:

- Automatisch antwoord aan de afzender waarmee deze in kennis gesteld wordt van de afwezigheid met vermelding van de geschikte persoon aan wie de boodschap kan gericht worden indien deze niet kan wachten tot bij de terugkeer van de afwezige werknemer (beginsel van de "Out of Office" berichten).

- De persoon spreekt af met een vertrouwenspersoon die gemachtigd wordt om de berichten of professionele bestanden te selecteren ingeval van gerechtvaardigde noodzaak en dringendheid die niet toelaat de terugkeer van de werknemer af te wachten.

2. Niet geplande of toevallige afwezigheid van een werknemer

De procedure voorzien in het raam van het informatieveiligheidsbeleid of in het arbeidsreglement zal de modaliteiten en de criteria moeten bepalen bij de keuze van de vertrouwenspersoon die gemachtigd wordt om toegang te hebben tot de informaties van de werknemer.

Voorbeelden:

- Een vooraf aangeduide en als "wijze" bekend staande persoon wordt gemachtigd om de delicate gevallen te behandelen (bv. in ziekenhuismiddens: de ziekenhuisombudsman).
- Een persoon die geval per geval aangeduid wordt in onderling akkoord tussen de werkgever en een vertegenwoordiger van het personeel.

3. Ontslag of afdanking van een werknemer met of zonder opzeggingstermijn

Ontslagen of afdankingen (al dan niet wegens zware fout) zijn steeds delicaat en oorzaak van moeilijkheden. De procedure moet analoog zijn aan deze die voorzien wordt voor niet geplande afwezigheden. Bovendien zal de procedure moeten verduidelijken welke bestemming moet worden verleend aan de berichten die bestemd zijn voor de ontslagen werknemer en aan de professionele en privébestanden die opgeslagen zijn op zijn werkstation.

Praktische voorbeelden:

- Ingeval van vertrek met opzeggingsperiode een procedure voorzien naar analogie met die voor geplande afwezigheden, in voorkomend geval in overleg met de werknemer op het ogenblik van zijn vertrek.
- Ingeval van vertrek zonder opzeggingsperiode wordt geval per geval een persoon aangeduid in onderling akkoord tussen de werkgever en een vakbondsafgevaardigde; deze persoon wordt gemachtigd om de berichten te beheren die binnenkomen op naam van de werknemer.
- In het informatieveiligheidsbeleid voorzien welk gevolg dient te worden voorbehouden aan professionele berichten (doorgifte aan een andere geschikte werknemer) en aan privéberichten (uitwissing of doorzending naar een privéadres gedurende een beperkte periode van 1 maand). Het is niet altijd aanbevelenswaardig om in het automatisch antwoord aan de afzender te vermelden dat

de werknemer niet langer deel uitmaakt van het personeel van het organisme; een dergelijke vermelding zal dan ook slechts mogelijk zijn mits expliciete en formele toestemming van de werknemer.

- In het informatieveiligheidsbeleid voorzien welk gevolg dient te worden voorbehouden aan privébestanden en –informaties (de professionele bestanden en informaties kunnen door de werkgever aangewend worden conform de interne regels).

4. Verdenking van fraude of kwaadwilligheid vanwege de werknemer

Ook in deze delicate en moeilijke situaties zal de toegang op omzichtige en "progressieve" wijze moeten gebeuren, bijvoorbeeld door selectie op de onderwerpen of andere criteria vooraleer kennis te nemen van de inhoud.

De Wnd. Administrateur, De Voorzitter,

(get.) Patrick Van Wouwe (get.) Willem Debeuckelaere