Ius Laboris BELGIUM
CLAEYS & ENGELS

‘Cybersurveillance’: nieuwe aanbevelingen van de Privacycommissie over de werkgeverscontrole op het e-mail en internetgebruik van werknemers

NEWSLETTER, 4 JULI 2012

INHOUD:

Overvloedige regelgeving	2
Sancties	4
Nieuw advies Privacycommissie	4
Flexibiliteit, proportionaliteit en legaliteit	5
Praktische aanbevelingen	6
Wat brengt de toekomst?	8
Conclusie	8

E-mail en internet zijn belangrijke werkinstrumenten geworden voor werknemers in ondernemingen. Tegelijkertijd vormen zij echter ook een aantrekkelijke bron van ontspanning. Werkgevers hebben er daarom alle belang bij om zich te beschermen tegen bepaalde risico's zoals virussen, netwerkproblemen, misbruik van arbeidstijd, nieuwe vormen van pesten, imagoschade, enz. Verder kan het voor het beheer en de organisatie van de activiteiten van de onderneming van belang zijn dat de werkgever toegang heeft tot de mailbox van de werknemers.

De controle die de werkgever uitoefent op het e-mail- en internetgebruik van de werknemers, evenals de toegang tot de mailbox van de werknemers, kan echter in conflict komen met het recht op privacy van de werknemers.

Cybersurveillance wordt door de Europese en Belgische regelgeving dan ook onderworpen aan strenge eisen met betrekking tot de privacy van de werknemers.

In deze *newsletter* zetten we voor u alles op een rijtje.

Veel leesplezier!

Meer info:
www.claeysengels.be
info@claeysengels.be

1 Overvloedige regelgeving

De regelgeving op "cybersurveillance" is zeer uitgebreid, gaande van internationale rechtsbronnen tot Belgische wetgeving.

Er moet rekening worden gehouden met het **recht op privacy** van elke werknemer, dat beschermd wordt door het artikel 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens, door Europese richtlijnen en door het interne Belgische recht. Meer specifiek zal er in België rekening moeten worden gehouden met volgende regelgeving:

1.1 het artikel 314*bis* van het Strafwetboek

Deze bepaling stelt het afluisteren, kennisnemen of opnemen van privécommunicatie tijdens de overbrenging ervan strafbaar. Bijgevolg kan een werkgever die kennis neemt van de inhoud van e-mails gezonden of ontvangen door diens werknemers strafbaar worden gesteld.

Aangezien een controle van de mailbox van de werknemer veelal niet wordt uitgevoerd "tijdens de overbrenging" van de communicatie wordt door een bepaalde rechtspraak aangenomen dat artikel 314*bis* een dergelijke controle niet verhindert. Verder kan geargumenteerd worden dat de controle op internetgebruik waarbij website adressen worden geregistreerd, niet onder deze bepaling valt.

Er is geen sprake van een inbreuk op artikel 314*bis* van het Strafwetboek indien de wet het toelaat of indien alle deelnemers aan de elektronische communicatie daarmee instemmen.

1.2 het artikel 124 van de Wet Elektronische Communicatie

Overeenkomstig deze bepaling is het niet toegelaten om:

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

Al deze handelingen zijn strafrechtelijk gesanctioneerd. Een werkgever die het e-mail- of internetgebruik van de werknemers controleert, valt onder deze bepalingen.

Ook hier is er geen sprake van een inbreuk indien de wet het toelaat of indien de toestemming tot kennisname van alle deelnemers aan de elektronische communicatie wordt bekomen.

1.3 de Wet Verwerking Persoonsgegevens van 8 december 1992 (hierna "WVP")

Deze wet vormt de Belgische omzetting van de Europese Richtlijn nr. 95/46 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens.

De WVP omschrijft het begrip "persoonsgegevens" als "*iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon*". Informatie met betrekking tot het gebruik van e-mail en internet valt binnen deze begripsomschrijving, aangezien loginnaam, e-mailadres, PC-nummer, en dergelijke meer in verband kunnen worden gebracht met een individuele persoon.

Het verwerken van persoonsgegevens is slechts toegelaten mits naleving van volgende beginselen:

- het finaliteitsbeginsel: de verwerking gebeurt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden;
- het proportionaliteitsbeginsel: de verwerkte gegevens moeten toereikend, ter zake dienend en niet overmatig zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt;
- het transparantiebeginsel: de verplichting om aan de betrokken werknemers bepaalde informatie te verstrekken, onder meer met betrekking tot het doel van de verwerking.

Verder moeten de persoonsgegevens nauwkeurig zijn, en zo nodig, worden bijgewerkt, en mogen ze niet langer worden bewaard dan noodzakelijk voor de verwezenlijking van de doeleinden. Ook zal de werkgever bepaalde verplichtingen moeten naleven met betrekking tot confidentialiteit en veiligheid van de verwerkte gegevens. Tot slot moet, vooraleer de verwerking een aanvang neemt, een aangifte van de verwerking worden verricht bij de Privacycommissie.

1.4 de CAO nr. 81

Deze CAO, gesloten in de Nationale Arbeidsraad, concretiseert de beginselen uit de WVP en voorziet in een geleidelijke en trapsgewijze controle door de werkgever op het e-mail en internetgebruik aan de hand van de 3 gekende beginselen:

(a) Finaliteitsbeginsel:

De CAO nr. 81 voorziet 4 mogelijke gerechtvaardigde doeleinden:

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;
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;
4. het te goeder trouw naleven van de in de onderneming geldende beginselen en regels voor het gebruik van on-line technologieën.

(b) Transparantiebeginsel:

Voorafgaand aan de installatie van een controlesysteem, moet de werkgever de ondernemingsraad inlichten over alle aspecten van deze controle. Bij de installatie van het controlesysteem, zal bovendien bepaalde informatie moeten worden verstrekt aan de individuele werknemers.

(c) Proportionaliteitsbeginsel—een trapsgewijze controle:

Teneinde een eventuele inmenging in de persoonlijke levenssfeer van de werknemers tot een minimum te beperken voorziet de CAO nr. 81 in een trapsgewijze controle. In eerste instantie is enkel een globale controle mogelijk, en is een identificatie van de individuele werknemers niet toegelaten. Pas in een volgende fase mogen de elektronische online communicatiegegevens worden verwerkt om ze toe te schrijven aan een geïdentificeerde of identificeerbare persoon. Indien de doelstelling van de cybersurveillance er in bestaat om de naleving te controleren van de in de onderneming geldende beginselen en regels voor het gebruik van on-line technologieën, zal voorafgaand aan de individualisering een voorlichtingsfase in acht moeten worden genomen.

Anderzijds zijn er ook de **werkgeversrechten en –belangen** (recht op gezagsuitoefening, tuchtrecht, eigendomsrecht, aansprakelijkheidsrecht, …) die mee in de balans moeten genomen worden. Het recht op privacy is immers niet absoluut en de bijzondere situatie van de gezagsrelatie tussen werkgever en werknemer zal in acht moeten worden genomen. De redelijke privacyverwachtingen (verwachtingen die iemand redelijkerwijze heeft omtrent de mate van inmenging in zijn privéleven) van de werknemers zijn om die reden minder groot op het werk dan buiten de arbeidsrelatie.

****

De draagwijdte en de interventie van de diverse bepalingen is niet altijd even duidelijk en zij worden vaak verschillend geïnterpreteerd door de rechtsleer en de rechtspraak. Werkgevers die het e-mail- en internetgebruik van hun werknemers controleren, moeten bijgevolg voorzichtig zijn aangezien zij zich in een “grijze zone” bevinden.

2 Sancties

De mogelijke sancties in geval van niet-naleving van de bepalingen die hierboven werden besproken zijn de volgende:

- *Strafsancties:* Werkgevers die een inbreuk plegen op de meeste van deze bepalingen kunnen strafrechtelijk worden gesanctioneerd (bv. in geval van een klacht door een (ex-)werknemer). Noteer wel dat in de praktijk strafrechtelijke vervolging eerder uitzonderlijk is.
- *Schadevergoeding:* De werknemer zou desgevallend ook een schadevergoeding kunnen vorderen wegens inbreuk op zijn privacy.
- *Weren van bewijsmateriaal:* Bewijzen die werden bekomen in strijd met één of meer van hierboven besproken bepalingen, kunnen door het bevoegde arbeidsgerecht terzijde worden geschoven (bijvoorbeeld in het kader van het bewijs van feiten voor een ontslag om dringende reden). Ingevolge recente rechtspraak kan dit evenwel nog slechts:
  - wanneer een op straffe van nietigheid voorgeschreven vorm werd miskend - wat in casu niet het geval kan zijn aangezien de bepalingen van de CAO nr. 81 of van de WVP niet op straffe van nietigheid zijn voorgeschreven;
  - wanneer de bewijsverkrijging is aangetast door een gebrek waardoor de betrouwbaarheid ervan wegvalt; of
  - wanneer het recht op een eerlijk proces erdoor in gevaar wordt gebracht.

De Privacycommissie merkt op dat de feitenrechter bij de afweging of het eerlijk proces al dan niet in het gedrang is gebracht, een afweging moet maken tussen de ernst van de inbreuk door de werknemer begaan (en desgevallend aan het licht gekomen ingevolge een cybersurveillance) en de aantasting van het recht op privacy. Indien de werknemer een inbreuk op de wet heeft gepleegd (bv. diefstal, fraude, oneerlijke concurrentie, …), kan het niet naleven van procedureregels niet rechtvaardigen dat bepaalde bewijsstukken worden geweerd. Indien de werknemer louter de interne regels niet heeft gerespecteerd (bv. te veelvuldig privé e-mails heeft gestuurd), oordeelt de Commissie dat de werkgever zelf ook de procedureregels moet hebben nageleefd.

3 Nieuw advies van de Privacycommissie

De Commissie voor de Bescherming van de Persoonlijke Levenssfeer (hierna “Privacycommissie”) is zich blijkbaar bewust van de vele interpretatieproblemen, en heeft daarom een nieuw rapport gepubliceerd in verband met cybersurveillance, waarbij zij haar eerder ingenomen standpunten terug in vraag stelt.

Een advies van de Privacycommissie is juridisch niet bindend en heeft in principe dus slechts een morele waarde. Toch kan dit advies als richtlijn door de arbeidsrechtbanken en -hoven worden gebruikt om na te gaan of een specifieke controlemethode in overeenstemming is met de diverse hierboven opgesomde regels ter bescherming van het recht op privacy.

Hoewel de Privacycommissie nog steeds van oordeel is dat de werkgever zijn informaticastructuur niet op buitensporige wijze mag gebruiken als elektronisch controlemiddel van werknemers, neemt zij in haar recent gepubliceerde rapport een meer genuanceerde houding aan. Vanuit deze houding meent de Privacycommissie dat werkgevers voor de organisatie en het beheer van hun professionele activiteiten in beginsel toegang hebben tot de inhoud van alle professionele communicatie van hun werknemers. Ook bepaalde privé communicatiebewegingen in de arbeidscontext kunnen door de werkgever worden gecontroleerd, maar enkel bij vermoedens van misbruik door de werknemer.

Toegang tot elektronische communicatie of internetgegevens van werknemers betreft dus niet enkel een kwestie van toezicht, maar kan ook belangrijk zijn voor het beheer en de organisatie van de activiteiten van de werkgever: het gaat daarbij onder meer over het verzekeren van de bewaring van de correspondentie (archivering) maar ook om het verzekeren van de continuïteit ingeval van afwezigheid, overlijden of vertrek van de werknemer.

Alhoewel het privacyrecht klassiek een uitzondering voorziet voor inbreuken op de privacy indien dit gebeurt met de uitdrukkelijke toestemming van de betrokkene, stelt de Commissie in haar advies dat de toestemming van de werknemer in het kader van een arbeidsrelatie geen geldige rechtvaardiging kan vormen om kennis te nemen van privé e-mail of internetgebruik.

Een werknemer zou volgens de Commissie dus geen vrije toestemming kunnen geven, wat toch wel vragen kan doen rijzen. De Commissie loopt hiermee alvast vooruit op de nieuwe verwachte Europese verordening betreffende de verwerking van persoonsgegevens (zie hierna).

Niettemin benadrukt de Commissie in haar advies dat het zeer belangrijk is voor de werkgever om de regels aangaande het toezichtsbeleid transparant te maken in een e-mail en internetpolicy, die bij voorkeur deel uitmaakt van het arbeidsreglement. Hierbij moet worden opgemerkt dat de rechtspraak eerder - ons inziens terecht - wel waarde hechtte aan de door de werknemer gegeven instemming met de controle van zijn e-mail en internetgebruik.

4 Finaliteit, proportionaliteit en legaliteit

Belangrijk is wel dat, ongeacht het doel van de patronale toegang (controle of beheer) en ongeacht de aard van de gegevens die het voorwerp uitmaken van die toegang (privé of professioneel), steeds de hierboven opgesomde basisbeginselen van het Belgische en Europese privacyrecht en de Wet Verwerking Persoonsgegevens moeten worden gerespecteerd.

- Finaliteitsbeginsel: de werkgever moet een gerechtvaardigd doel voor ogen hebben, zoals het opvolgen van professionele correspondentie, het verzekeren van de continuïteit van de geleverde diensten ingeval van afwezigheid, overlijden of vertrek van de werknemer, het bewaren van documenten als bewijsstukken, controle op de naleving van de e-mail- en internetpolicy.
- Proportionaliteitsbeginsel: de werkgever moet het toezicht beperken tot het strikt noodzakelijke. Dit betekent bijvoorbeeld:
  - Indien een e-mail bestemd is voor de personeelsdienst, is het niet de bedoeling dat andere diensten hiervan kennis kunnen nemen.
  - Indien er een vermoeden rijst dat een bepaalde werknemer misbruik maakt van de elektronische communicatiemiddelen, bijvoorbeeld om zijn werkgever te beconcurreren, kan gezocht worden op bepaalde trefwoorden, data of de identiteit van de ontvangers of verzenders van berichten, in plaats van de inhoud van het hele elektronische communicatieverkeer van de werknemer te onderzoeken. In geval van oneerlijke concurrentie, zou de werkgever bijvoorbeeld kunnen zoeken op de namen van zijn concurrenten.
- Transparantiebeginsel: de werknemer moet op de hoogte zijn van het eventuele elektronische toezicht en de manier waarop het uitgevoerd wordt. Daarom is het aan te bevelen het ICT-beleid vast te leggen in een e-mail- en internetpolicy, die door de werknemers ondertekend wordt voor ontvangst of - bij voorkeur - voor akkoord.

5 Praktische aanbevelingen

Op basis van bovenstaande analyse formuleert de Privacycommissie een aantal praktische aanbevelingen over hoe om te gaan met privacyregels bij elektronisch toezicht en het opvolgen van de professionele e-mails van werknemers.

5.1 Professionele en privécommunicatie scheiden

Wanneer de werknemer het e-mailsysteem van de werkgever zowel voor professionele als voor privécommunicatie gebruikt, kunnen er bij elektronisch toezicht privacyproblemen opduiken. In dat geval zal de werkgever immers, ook al ligt het enkel in zijn bedoeling kennis te krijgen van de inhoud van de 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 werknemer raken. De werkgever 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 mogelijk is na het volgen van de geleidelijke aanpak van CAO nr. 81 (eerst een globale anonieme controle en pas daarna een geïndividualiseerde controle).

Een eerste oplossing die de Privacycommissie voorstelt, bestaat erin om aan de werknemer te vragen in de gemengde mailbox (die zowel voor professionele als voor privécommunicatie gebruikt wordt) de verstuurde en ontvangen e-mails te classificeren als 'privé' en 'professioneel' in twee verschillende mappen. In dat geval zal enkel voor de map met als 'privé' geclassificeerde e-mails, de gefaseerde aanpak van CAO nr. 81 moeten worden gevolgd. De professionele e-mails kunnen volgens de Privacycommissie worden gecontroleerd, weliswaar mits naleving van de principes van de Wet Verwerking Persoonsgegevens. De Privacycommissie raadt aan om de privé map van de werknemer op te slaan op een gedeelte van de harde schijf waarvan geen gecentraliseerde en systematische veiligheidskopieën (back-ups) worden gemaakt, maar dit lijkt ons niet in alle netwerkomgevingen even evident.

Privé communicatie kan ook van professionele communicatie gescheiden worden door de werknemers te verplichten om in privé berichten de vermelding “PERSOONLIJK” of “VERTROUWELIJK” toe te voegen, maar de Privacycommissie geeft zelf aan dat deze oplossing niet ideaal is aangezien het moeilijk is om deze discipline te eisen vanwege derden die een boodschap sturen aan het bedrijf.

Een verdergaande oplossing die de Privacycommissie voorstelt, is het vermijden van dubbel gebruik (zowel professioneel als privé) van het professionele e-mailsysteem: de werknemer verstuurt met andere woorden geen privéberichten vanaf het e-mailadres dat hem door zijn werkgever toegewezen is. Dit impliceert dan wel dat de werkgever toelaat dat de werknemer een eigen mailadres (genre Hotmail, Gmail, …) of een tweede mailaccount toegekend door de werkgever (bijvoorbeeld met een andere naam of domeinnaam) kan en mag gebruiken. Als de werkgever de werknemer hierover duidelijk informeert (bijvoorbeeld in de ICT-policy), dan mag hij er in principe van uit gaan dat de e-mails in de professionele mailbox enkel een beroepsmatig karakter hebben, zeker ten aanzien van de verzonden berichten. In dat geval heeft de werkgever in principe rechtstreekse toegang tot de professionele mailbox, zonder dat daarbij de gefaseerde aanpak van de CAO nr. 81 moet worden gevolgd. Wel zal de werkgever hierbij nog steeds het finaliteits-, proportionaliteits- en transparantiebeginsel van de Wet Verwerking Persoonsgegevens moeten naleven.

Het blijft nog maar de vraag of de rechtspraak de stelling zal volgen dat bij een scheiding tussen privé en professionele communicatie het de werkgever inderdaad toegelaten wordt om kennis te nemen van alle e-mails die geacht worden professioneel te zijn. Eerder werd in de rechtspraak immers geoordeeld dat het niet voldoende is om het privégebruik eenvoudig te verbieden.

5.2 Maatregelen in geval van afwezigheid of uitdiensttreding

In geval van afwezigheid van werknemers (wegens ziekte, vakantie, enz.) kan het noodzakelijk zijn dat de werkgever toegang heeft tot de mailbox van deze werknemers om de opvolging van de professionele e-mails te verzekeren. Dit is tevens het geval wanneer een werknemer de onderneming heeft verlaten en het e-mailadres van deze ex-werknemer nog operationeel is. Het is van belang om voor deze situaties functioneringsregels af te spreken.

De Privacycommissie reikt een aantal oplossingen aan die kunnen toelaten de opvolging van de e-mails van afwezige werknemers te verzekeren en de inmenging in de privacy van de werknemers zoveel mogelijk te beperken.

(a) Oplossing 1: 'out-of-office' - bericht

Volgens de Privacycommissie kan de werkgever in de e-mail- en internetpolicy een verplichting opnemen voor de werknemer tot het instellen van een 'out of office'-bericht in geval van voorziene afwezigheid om te verwittigen dat hij/zij gedurende een bepaalde periode de ontvangen e-mails niet kan beantwoorden. In dit automatisch antwoord aan de afzender dient dan vermeld te worden aan welke persoon de boodschap gericht kan worden ter opvolging, indien deze niet kan wachten tot bij de terugkeer van de afwezige werknemer. Volgens ons kan de werknemer in de e-mail- en internetpolicy de werkgever tevens de toestemming geven om dit 'out of office'-bericht in te stellen in geval van *onvoorziene* afwezigheid (bv. ziekte).

Dit heeft als voordeel dat de werkgever de mailbox van zijn werknemers niet meer zal moeten consulteren, aangezien de afzender ervan verwittigd wordt dat de werknemer in kwestie afwezig is en dat hij zijn bericht opnieuw dient te versturen naar een werknemer die de zaken opvolgt.

(b) Oplossing 2: kennisname van e-mails door een vertrouwenspersoon

Indien de werkgever toch kennis wenst te nemen van de inhoud van een mailbox van een afwezige werknemer, adviseert de Privacycommissie te werken met een vertrouwenspersoon die gemachtigd wordt om toegang te hebben tot de mailbox van de afwezige werknemer.

Deze vertrouwenspersoon zou onafhankelijk van het management moeten opereren en moeten filteren wat door de werkgever gelezen mag worden.

In geval van voorziene afwezigheid moet de werknemer volgens de Privacycommissie zelf de mogelijkheid krijgen om een vertrouwenspersoon te machtigen en in geval van onvoorziene afwezigheid zou deze vertrouwenspersoon bijvoorbeeld kunnen worden aangeduid in onderling akkoord tussen de werkgever en een vakbondsafgevaardigde. Het lijkt ons praktischer om met de werknemer in kwestie vooraf overeen te komen wie die vertrouwenspersoon kan zijn.

(c) Quid toestemming werknemer en afzender van de berichten?

De Privacycommissie oordeelt dat noch de toelating van de werknemer noch de toelating van de afzender van een e-mail aan de werknemer nodig zijn om kennis te nemen van e-mails nu een dergelijke kennisname volgt uit het recht van leiding en toezicht van de werkgever.

Een voorzichtige werkgever doet er o.i. best aan om aan werknemers alsnog de toelating te vragen tot de eventuele kennisname van e-mails (al dan niet door een vertrouwenspersoon). Wij zouden tevens in alle gevallen een 'out of office' bericht verzenden met een disclaimer waarin de geadresseerde op de hoogte wordt gebracht van de kennisname en de mogelijkheid wordt geboden te protesteren indien hij niet akkoord zou gaan.

5.3 Internetgebruik reguleren

De werkgever kan preventief risicovolle handelingen uitsluiten door de toegang tot bepaalde websites of elektronische adressen die bekend staan als gevaarlijk, te blokkeren. Verder kan de werkgever ook waarschuwingen programmeren bestemd voor de gebruiker ingeval van twijfelachtige handelingen.

De Privacycommissie geeft aan dat ook voor internetcommunicatie twee of meer gebruikersaccounts kunnen worden toegekend om misbruiken te vermijden. Indien de werknemer voor privé doeleinden wil surfen, zal hij moeten inloggen op een andere account dan diegene die hij voor zijn professionele activiteiten gebruikt.

Indien bepaalde diensten of gedeelten van een netwerk een bijzondere gevoeligheid vertonen (bijvoorbeeld het lokaal voor het beheer van systemen en netwerken, de dienst human resources), kan het volgens de Privacyommissie bovendien gewettigd zijn om elke privé activiteit op deze werkstations te verbieden om deze permanent en strikt te kunnen controleren. In dat geval raadt de Commissie aan om andere werkstations ter beschikking te stellen voor minder gevoelige of privé activiteiten.

6 Wat brengt de toekomst?

Op Europees niveau werd een voorstel tot verordening betreffende gegevensbescherming gelanceerd. De ontwerp tekst van deze verordening voorziet dat de toestemming van de werknemer in het kader van een arbeidsrelatie geen geldige grondslag kan vormen voor een verwerking van persoonsgegevens, dit in de lijn van het standpunt dat de Privacycommissie vandaag reeds hanteert.

De nieuw te verwachten Europese regels voorzien verder in een administratieve vereenvoudiging van de verplichtingen van de werkgever, met waarschijnlijk een schrapping van de verplichting tot voorafgaandelijke aangifte van gegevensverwerking bij de Privacycommissie.

Indien het voorstel wordt aangenomen, zal in grote ondernemingen bovendien verplicht een 'Data Protection Officer' (functionaris voor de gegevensbescherming) moeten worden aangesteld.

Dit voorstel wordt momenteel onderzocht door het Europees Parlement en de Europese Raad. Van zodra de verordening wordt aangenomen, zal deze rechtstreeks toepasselijk zijn in alle lidstaten van de Europese Unie, met een wijziging van de Wet Verwerking Persoonsgegevens tot gevolg.

Wij houden u uiteraard op de hoogte van deze ontwikkelingen.

7 Conclusie

Cybersurveillance wordt geregeld door een amalgaam aan regels die niet altijd met elkaar in overeenstemming zijn en waarover bovendien in rechtsleer en rechtspraak geen eenduidige interpretatie bestaat. De nieuwe aanbeveling van de Privacycommissie heeft als verdienste dat ze het fundamenteel controlerecht van de werkgever bevestigt en een aantal praktische oplossingen formuleert.

Deze aanbeveling is echter niet bindend. Het valt dus af te wachten of de rechtspraak deze interpretaties steeds zal volgen.

In de toekomst zal tevens rekening moeten worden gehouden met een nieuwe Europese verordening die de toestemming van de werknemer voor een verwerking van zijn/haar persoonsgegevens waarschijnlijk verder zal bemoeilijken.

Het belang van een duidelijke e-mail en internetpolicy wordt meermaals bevestigd door de Commissie. We raden werkgevers dan ook aan om bestaande e-mail en internetpolicies te updaten in het licht van deze nieuwe aanbevelingen. Claeys & Engels kan daarbij uiteraard graag assisteren.

Ius Laboris BELGIUM
CLAEYS & ENGELS

Brussel
Vorstlaan 280
1160 Brussel
Tel.: 02 761 46 00
Fax: 02 761 47 00

Luik
boulevard Frère Orban 25
4000 Luik
Tel.: 04 229 80 11
Fax: 04 229 80 22

Antwerpen
Commodity House
Generaal Lemanstraat 74
2600 Antwerpen
Tel.: 03 285 97 80
Fax: 03 285 97 90

Gent
Ferdinand Lousbergkaai 103 bus 4-5
9000 Gent
Tel.: 09 261 50 00
Fax: 09 261 55 00

Kortrijk
Ring Bedrijvenpark
Brugsesteenweg 255
8500 Kortrijk
Tel.: 056 26 08 60
Fax: 056 26 08 70

Hasselt
Luikersteenweg 227
3500 Hasselt
Tel.: 011 24 79 10
Fax: 011 24 79 11

Partners with you.