BELGISCHE SENAAT

Zitting 2012-2013

22 april 2013

SENAAT Schriftelijke vraag nr. 5-8832

de Nele Lijnen (Open Vld)

aan de minister van Werk

Personeel - Federale administratie - Monitoring - Controle e-mails en surfgedrag - Afluisteren telefoongesprekken - Privacy - Klachten - Evaluatie

22/4/2013	Verzending vraag
11/6/2013	Antwoord

Ook gesteld aan : schriftelijke vraag 5-8822
Ook gesteld aan : schriftelijke vraag 5-8823
Ook gesteld aan : schriftelijke vraag 5-8824
Ook gesteld aan : schriftelijke vraag 5-8825
Ook gesteld aan : schriftelijke vraag 5-8826
Ook gesteld aan : schriftelijke vraag 5-8827
Ook gesteld aan : schriftelijke vraag 5-8828
Ook gesteld aan : schriftelijke vraag 5-8829
Ook gesteld aan : schriftelijke vraag 5-8830
Ook gesteld aan : schriftelijke vraag 5-8831
Ook gesteld aan : schriftelijke vraag 5-8833
Ook gesteld aan : schriftelijke vraag 5-8834
Ook gesteld aan : schriftelijke vraag 5-8835
Ook gesteld aan : schriftelijke vraag 5-8836
Ook gesteld aan : schriftelijke vraag 5-8837
Ook gesteld aan : schriftelijke vraag 5-8838
Ook gesteld aan : schriftelijke vraag 5-8839
Ook gesteld aan : schriftelijke vraag 5-8840

SENAAT Schriftelijke vraag nr. 5-8832 d.d. 22 april 2013 : (Vraag gesteld in het Nederlands)

Onlangs werd bericht dat bedrijfsleiders steeds vaker de activiteiten van hun personeel op de computer controleren. Zo zou, volgens een steekproef van 413 deelnemers, een op drie bazen de mails van personeelsleden controleren, de helft controleert het surfgedrag en 5 % luistert zelfs telefoongesprekken af. In bepaalde sectoren wordt de mailaccount van een personeelslid gekoppeld aan een alias. Daardoor kan een overste alle e-mails meelezen.

Graag wil ik u volgende vragen stellen:

1) Hoe evalueert u die berichtgeving? Vindt u het wenselijk dat een overste in staat is om bijvoorbeeld de e-mails of het surfgedrag van

een personeelslid te controleren? Vindt u dat een inbreuk op de privacy, of toelaatbaar omdat de controle in een professionele omgeving gebeurt? Vindt u het toelaatbaar indien de werknemer duidelijk weet dat hij of zij gecontroleerd kan worden?

2) Zijn er reeds klachten geweest van personeelsleden over zulke praktijken? Hebben er dus al mensen geklaagd dat hun privacy op zulk een manier geschonden werd? Kunt u dat toelichten met cijfers als die beschikbaar zijn?

3) Zelfs al hebt u geen weet van dergelijke controlepraktijken, weet u of de apparatuur of de IT van uw Federale Overheidsdienst het mogelijk maakt om het surfgedrag te controleren? Worden de mailbox of het mailverkeer gemonitord of actief gecontroleerd? Kan hij toelichten?

4) Is het mogelijk om mee te luisteren naar telefoongesprekken? Indien ja, kunt u toelichten?

5) Worden uw werknemers ingelicht over mogelijke controles en hun privacy? Weten zij aldus wat al dan niet gecontroleerd kan worden? Kunt u toelichten?

6) Kan een werknemer op het internet alle websites bezoeken, of zijn bepaalde websites geblokkeerd? Zo ja, waarom? Kunt u toelichten?

7) Kan bij een evaluatie van de prestaties van een werknemer het resultaat van een dergelijke controle (mails, internet, telefoon, enz.) gebruikt worden? Kunt u toelichten?

Antwoord ontvangen op 11 juni 2013 :

Mevrouw, hieronder vindt u het antwoord op uw vragen.

1. De wens van de werkgevers om de productiviteit van hun werknemers te controleren is geen nieuw gegeven en op de markt zijn al vele jaren tools voorhanden die het mogelijk maken om de personeelsleden, die voor het uitvoeren van hun taken gebruik maken van computers en software, te superviseren.

De scheidingslijn tussen het recht op controle van de werknemer en het recht op respect van de privésfeer (privacy) geclaimd door de werknemer is altijd een delicaat punt geweest. Het recht om de activiteiten van zijn werknemers te controleren behoort onlosmakelijk tot de voorrechten van de werkgever.

Om misbruiken te voorkomen werden in het kader van het sociaal recht een reeks collectieve arbeidsovereenkomsten uitgewerkt die uitgaan van belangrijke basisbeginselen om dit domein duidelijk af te bakenen : het proportionaliteitsbeginsel en het principe met betrekking tot transparantie. Bovendien moeten alle controles aan de hand van bewijzen worden gerechtvaardigd en strikt worden uitgevoerd binnen de grenzen toegestaan door de wettelijke bepalingen op gebied van het respect van de privésfeer. Het is dus belangrijk om de werkgevers voor deze problematiek te sensibiliseren, en dit vóór ze specifieke controletechnieken gaan gebruiken.

Controles zijn toegestaan wanneer ze conform de wettelijke bepalingen zijn en worden uitgevoerd met naleving van de fundamentele rechten van de werknemers ;

2. Geen klachten geregistreerd, geen cijfergegevens mee te delen ;

3. De Stafdienst Informatie- en communicatietechnologieën van het departement beschikt over tools die het mogelijk maken om de sporen te analyseren van de personeelsleden die het internet gebruiken.

Het emailverkeer en de inhoud van de mailbox wordt enkel in zeer precieze gevallen gecontroleerd en zulks steeds met de instemming van het personeelslid. Deze verschillende tools worden niet gebruikt voor controledoeleinden maar als middelen om problemen uit de wereld te helpen en dienen als ondersteuning voor de berichten die waarschuwen tegen spam, virussen, enz. In deze gevallen gaat het eerder om informatie en preventie ;

4. Neen, onze installaties zijn hiervoor niet geschikt.

5. De activiteiten van de personeelsleden van het departement worden niet uitdrukkelijk gecontroleerd behalve wanneer het noodzakelijk blijkt om een grondige analyse te maken van hun surfgedrag, de sites die ze bezoeken, hun emailverkeer en in zeldzame gevallen, wanneer er onderzocht wordt hoe een nieuw virus getracht heeft om door te dringen in ons informaticasysteem.

De personeelsleden zijn perfect op de hoogte van deze voorschriften inzake deontologie en elementaire voorzichtigheid die ze dagelijks bij hun taken moeten naleven. Een handvest voor goed gebruik van het internet en een handvest voor het correcte gedrag van het e-mailverkeer zijn twee documenten die hen wijzen op de deontologische basisregels en de elementaire veiligheidsvoorschriften die absoluut in acht moeten worden genomen.

De toegang tot bepaalde toepassingen wordt streng beschermd en gecontroleerd. De verbindingen met de gegevensbanken met gevoelige informatie in een aantal instellingen van de sociale zekerheid worden geanalyseerd en de informatieaanvragen die hen worden toegestuurd worden systematisch getraceerd en aandachtig onderzocht. De personeelsleden die via hun taken toegang hebben tot deze

gevoelige informatie, hebben duidelijke richtlijnen gekregen over de wijze waarop het vertrouwelijk karakter van de verkregen informatie gevrijwaard moet blijven ;

6. Er bestaat een systeem waarmee de toegang tot websites met gevaarlijke, onwettige en pornografische inhoud geblokkeerd wordt ;

7. Informaticatools maken het mogelijk om voor elke werknemer een profiel op te stellen op basis van een analyse van zijn e-mailverkeer, het gebruik van het internet, het gebruik van de telefoon, enzovoort. De Federale Overheidsdienst (FOD) past dit type analyses niet toe en respecteert de regelgeving met betrekking tot de bescherming van de privésfeer.