

SÉNAT DE BELGIQUE

Session 2012-2013

22 avril 2013

SÉNAT Question écrite n° 5-8832

de Nele Lijnen (Open Vld)

à la ministre de l'Emploi

Personnel - Administration fédérale - Surveillance - Contrôle du courriel et de l'utilisation du web - Écoutes de conversations téléphoniques - Vie privée - Plaintes - Évaluation

22/4/2013 Envoi question

11/6/2013 Réponse

Aussi posée à : question écrite 5-8822
Aussi posée à : question écrite 5-8823
Aussi posée à : question écrite 5-8824
Aussi posée à : question écrite 5-8825
Aussi posée à : question écrite 5-8826
Aussi posée à : question écrite 5-8827
Aussi posée à : question écrite 5-8828
Aussi posée à : question écrite 5-8829
Aussi posée à : question écrite 5-8830
Aussi posée à : question écrite 5-8831
Aussi posée à : question écrite 5-8833
Aussi posée à : question écrite 5-8834
Aussi posée à : question écrite 5-8835
Aussi posée à : question écrite 5-8836
Aussi posée à : question écrite 5-8837
Aussi posée à : question écrite 5-8838
Aussi posée à : question écrite 5-8839
Aussi posée à : question écrite 5-8840

SÉNAT Question écrite n° 5-8832 du 22 avril 2013 : (Question posée en néerlandais)

On a appris récemment que les dirigeants d'entreprise contrôlaient de plus en plus souvent les activités sur ordinateur de leur personnel. Ainsi, dans un échantillon de 413 personnes, un patron sur trois contrôlerait les courriels des membres de son personnel, la moitié contrôlerait l'usage du web et cinq pour cent écouterait même les conversations téléphoniques. Dans certains secteurs, le compte de courrier électronique d'un membre du personnel est lié à un alias, de sorte qu'un supérieur peut lire tous ses messages.

J'aimerais vous poser les questions suivantes :

1) Comment évaluez-vous cette information ? Estimez-vous souhaitable qu'un supérieur puisse contrôler, par exemple, les courriels ou

l'utilisation du web d'un membre du personnel ? Considérez-vous que ce soit une violation de la vie privée ou trouvez-vous cela acceptable puisque ce contrôle se produit dans un cadre professionnel ? Trouvez-vous cela acceptable si le travailleur est clairement au courant qu'il peut être contrôlé ?

2) Y a-t-il déjà eu des plaintes de membres du personnels à propos de pareilles pratiques ? Des personnes se sont-elles donc déjà plaintes d'une violation de leur vie privé à cause de ces pratiques ? Pouvez-vous étayer votre réponse de données chiffrées pour autant que vous en disposiez ?

3) Même si vous n'êtes au courant d'aucune pratique de contrôle de ce genre, savez-vous si le matériel ou le système informatique de votre Service public fédéral pourrait permettre de contrôler l'utilisation du web ? Les boîtes de courriels ou le trafic de courriels sont-ils surveillés ou activement contrôlés ? Pouvez-vous expliquer ce qu'il en est dans votre SPF ?

4) Est-il possible d'écouter les conversations téléphoniques ? Si c'est possible, pouvez-vous vous en expliquer ?

5) Vos travailleurs sont-ils informés sur les contrôles possibles et sur le respect de leur vie privée ? Savent-ils donc ce qui peut ou ne peut pas être contrôlé ? Pouvez-vous expliquer la situation ?

6) Un travailleur peut-il visiter tous les sites sur le web, ou certains sites sont-ils bloqués ? S'il y a blocage, pourquoi ? Pouvez-vous expliquer la situation ?

7) Le résultat de pareils contrôles (courriels, internet, téléphone, etc.) peut-il être utilisés lors d'une évaluation des prestations d'un travailleur ? Pouvez-vous expliquer la situation ?

Réponse reçue le 11 juin 2013 :

Vous voudrez bien trouver ci-dessous les éléments de réponse à la question posée.

1. le désir de contrôle par l'employeur de la productivité des travailleurs n'est pas neuf et des outils permettant de superviser les agents qui utilisent des ordinateurs et des logiciels pour l'exécution de leurs tâches existent sur le marché depuis de nombreuses années déjà.

Il a toujours existé un point de tension entre le droit de contrôle de l'employeur et le droit au respect de la vie privée (privacy) revendiqué par l'employé. Pour l'employeur, le droit de contrôler les activités de ses employés fait intégralement partie de ses prérogatives.

Pour éviter les abus, le droit social s'est doté de plusieurs conventions collectives de travail qui reposent sur des principes de base importants pour baliser ce domaine : le principe de proportionnalité et le principe de transparence. En outre, tout contrôle doit avoir une justification avérée et s'exécuter strictement dans les limites autorisées par les dispositions légales en matière de respect de la vie privée. Il est donc important de sensibiliser les employeurs à cette problématique avant qu'ils utilisent des techniques spécifiques de contrôle.

Des contrôles sont acceptables s'ils sont conformes aux dispositions légales et exécutés dans le respect des droits fondamentaux des travailleurs ;

2. pas de plainte enregistrée, pas de rapport chiffré à communiquer ;

3. le service d'encadrement Technologies de l'information et de la communication du département dispose d'outils permettant d'analyser les traces laissées par les agents qui utilisent Internet.

Une intervention sur les courriels et le contenu d'une boîte email n'est réalisée que dans des cas très précis et toujours en accord avec son propriétaire.

Ces différents instruments ne sont pas exploités à des fins de contrôle mais sont utilisés comme instruments de dépannage et servent à appuyer des messages de mise en garde contre les spam, les virus, etc. On se situe ici plus dans de l'information et de la prévention ;

4. non, nos installations ne le permettent pas ;

5. les activités des agents du département ne sont pas expressément contrôlées sauf dans des cas nécessitant une analyse poussée de leurs consultations, des sites qu'ils ont visités, des échanges de mails qu'ils ont entretenus et ce, et c'est rare, dans le cas d'une recherche menée en vue de déterminer comment un nouveau virus a tenté de proliférer au sein du système informatique.

Les agents sont parfaitement au courant des règles de déontologie et de prudence élémentaires à adopter au quotidien dans leurs activités. Une charte pour le bon usage de l'Internet et une charte pour le bon usage du mail sont deux documents qui leur rappellent les règles de déontologie de base et les consignes de sécurité élémentaires à absolument observer.

L'accès à certaines applications est sévèrement protégé et contrôlé. Les connexions aux banques de données sensibles développées dans un certain nombre d'institutions de sécurité sociale sont analysées et les demandes de renseignement qui leur sont adressées font l'objet d'un traçage systématique et d'un examen attentif. Les agents concernés dans leurs activités par le traitement de ces données sensibles ont reçu une information précise quant à la manière de conserver le caractère confidentiel des renseignements obtenus ;

6. il existe un système de blocage des accès aux sites présentant des contenus dangereux, illicites, pornographiques ;
7. des outils informatiques permettent d'établir, par travailleur, un profil basé sur une analyse de ses mails, de l'utilisation qu'il fait d'Internet, de l'utilisation du téléphone, etc. Le Service public fédéral (SPF) ne pratique pas ce type d'analyse et respecte la réglementation en matière de protection de la vie privée.