ROYAUME DE BELGIQUE

COMMISSION DE LA PROTECTION DE LA VIE PRIVEE

Bruxelles, le

Adresse : Rue Haute, 139, B-1000 Bruxelles
Tél.: +32(0)2/213.85.40 E-mail : commission@privacycommission.b
Fax.: +32(0)2/213.85.65 http://www.privacy.fgov.be/

AVIS N° 18 / 2005 du 9 novembre 2005

N. Réf. : SA2 / A / 2005 /019

OBJET : Avis relatif à un projet d'arrêté du Gouvernement de la Communauté française *relatif au code de bonne conduite des usagers des systèmes informatiques, du courrier électronique et d'Internet au sein des services du Gouvernement de la Communauté française, et des organismes d'intérêt public relevant du comité de secteur XVII*.

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*, en particulier l'article 29 ;

Vu la demande d'avis du 16 septembre 2005 du Ministre de la Fonction publique et des Sports ;

Vu le rapport de Monsieur F. ROBBEN;

Emet, le 9 novembre 2005, l'avis suivant :

I. OBJET DE LA DEMANDE

---

1. Le Ministre de la Fonction publique et des Sports demande à la Commission d'émettre un avis à propos d'un projet d'arrêté du Gouvernement de la Communauté française *relatif au code de bonne conduite des usagers des systèmes informatiques, du courrier électronique et d'internet au sein des services du Gouvernement de la Communauté française, et des organismes d'intérêt public relevant du comité de secteur XVII*.

II. DISCUSSION GENERALE

---

2. En guise de remarque préliminaire, la Commission souhaite souligner que l'on ne peut bien entendu qu'applaudir l'initiative consistant à consigner dans un code les règles de conduite que doivent respecter les membres du personnel des services de la Communauté française si leur employeur met à leur disposition des outils de travail numérique : en effet, les membres du personnel en question doivent savoir ce qui est permis ou défendu en matière d'utilisation d'Internet et du courrier électronique sur le lieu de travail et avoir connaissance des restrictions et limites imposées dans le cadre de l'usage toléré, de même qu'ils doivent être informés de l'existence et des modalités d'un contrôle exercé par l'employeur.[1] Il faudra donc que les services de la Communauté française aient soin de faire connaître le code de conduite à leur personnel.

De façon générale, la Commission constate que le Code en question ne contrevient pas aux dispositions légales en matière de protection de la vie privée et de protection des télécommunications telles que relevées par la Commission dans son avis 10/2000 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail.
La Commission renverra de façon ponctuelle à cet avis dans le cadre de l'examen de certains articles du Code de conduite.

Ici, la Commission ne s'est pas seulement laissé guider par la protection de la vie privée des utilisateurs des systèmes informatiques. En effet, la Commission estime qu'il faut garder à l'esprit la vie privée du citoyen, dont des données à caractère personnel sont traitées dans ces systèmes informatiques. Et ceci peut, dans certains cas, exiger que les responsables puissent vérifier si les utilisateurs du système ont travaillé conformément à cette dernière exigence. La réglementation doit par conséquent chercher à atteindre un équilibre entre d'une part la protection juridique de l'utilisateur et d'autre part la protection des données à caractère personnel qui sont traitées par les utilisateurs.

---

[1] « *Le dialogue entre employeur et employés devra permettre d'établir de façon suffisamment détaillée, conformément à l'article 9 de la loi du 8 décembre 1992, les différentes caractéristiques de la politique de contrôle de l'employeur. Celles-ci devront notamment viser :*
- les modalités d'utilisation du courrier électronique et de l'Internet qui sont permises, tolérées ou interdites ;
- les finalités et modalités du contrôle de cette utilisation (nature des données collectées, étendue et circonstances des contrôles, personnes ou catégories de personnes sujettes aux procédures de contrôle) ;
- l'existence d'un stockage des données de télécommunication et la durée de ce stockage, par exemple sur un serveur central, dans le cadre de la gestion technique du réseau, et les éventuels systèmes de cryptage existants ;
- les décisions pouvant être prises par l'employeur à l'endroit de l'employé sur la base du traitement des données collectées à l'occasion d'un contrôle ;
- le droit d'accès de l'employé aux données à caractère personnel le concernant. » (cf. l'avis d'initiative *relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail* émis par la Commission le 3 avril 2000).

III. DISCUSSION ARTICLE PAR ARTICLE

---

3. Dans les lignes qui suivent, un certain nombre de suggestions sont formulées à propos de quelques articles du projet d'arrêté qui ont un rapport avec la protection de la vie privée ou la sécurisation du système d'information de la Communauté française, et donc avec la protection de la vie privée des individus dont la Communauté française traite les données à caractère personnel.

4. Les articles 3 à 7 inclus du projet d'arrêté déterminent les règles d'utilisation de l'équipement numérique de l'employeur : le mode d'utilisation, l'usage autorisé, les limites de celui-ci et l'usage interdit.

En principe, les membres du personnel doivent utiliser le courrier électronique et consulter Internet afin d'accomplir les missions qui leur sont confiées par l'employeur. C'est à cette fin que ces moyens de communication sont mis à leur disposition.

Il est cependant admis qu'à titre exceptionnel, les membres du personnel utilisent le courrier électronique et Internet à des fins privées, sans autorisation préalable, à condition que cet usage soit occasionnel, qu'il n'entrave en rien l'exécution des tâches confiées aux membres du personnel, qu'il ne nuise d'aucune manière à leur productivité et qu'il ne constitue pas une infraction aux dispositions du projet d'arrêté, en particulier à l'article 3, § 1 de celui-ci, ainsi qu'à d'autres dispositions légales ou statutaires en vigueur.

Ce faisant, le projet d'arrêté se conforme à ce que la Commission affirmait dans son avis du 3 avril 2004, par référence à la jurisprudence de la Cour européenne des Droits de l'Homme[2] : le lieu de travail étant le lieu le plus propice pour entretenir des contacts avec des collègues et même des personnes extérieures, les employeurs doivent faire preuve d'une certaine tolérance quant aux communications privées passées par les membres de leur personnel à l'aide de leurs moyens de communication.

5. L'article 4, § 2, du projet d'arrêté stipule que « [l]*es membres du personnel ont droit au respect de leur vie privée pendant le temps et sur le lieu de travail. En application de ce principe, en aucun cas, les services de la Communauté ne prennent connaissance du contenu des messages émis ou reçus par les membres du personnel sur leur adresse électronique nominative*. »

La Commission prend acte de cette disposition et constate qu'elle est formulée de façon très absolue.

Elle rappelle qu'une prise de connaissance du contenu des télécommunications est soumise aux conditions de l'article 124 de la loi du 13 juin 2005, qui prévoit notamment l'obtention du consentement libre et spécifique « de toutes les personnes directement ou indirectement concernées » par la communication[3].

En ce qui concerne la collecte de données de communication, et notamment d'éventuels loggings, la Commission rappelle par ailleurs que le principe de confidentialité des données de télécommunication s'applique sans préjudice de la nécessaire adoption de mesures de sécurité techniques et organisationnelles telles que prévues à l'article 16 de la loi, destinées à sécuriser l'accès aux réseaux et à assurer de façon globale la protection des données à caractère personnel. L'enregistrement de loggings dans cette perspective est admissible et même

---

[2] Avis *relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail,* émis d'initiative par la Commission le 3 avril 2000.

[3] La Commission a dans sa recommandation 1/2002 du 2 août 2002 précisé les modalités à respecter lorsqu'une telle prise de connaissance est envisagée sur le lieu de travail (notamment à des fins de preuves de transactions effectuées dans un contexte professionnel). La convention collective de travail n°81, bien que non applicable au secteur public, constitue également un instrument de référence.

souhaitable, mais il doit être effectué dans une perspective de protection des données, sans détournement de finalité et réutilisation à des fins de contrôle permanent des employés.

6. L'article 6, § 1, du projet d'arrêté indique que « [*l*]*ors de la connexion au réseau ou à toute autre ressource informatique chacun doit utiliser son propre login et son mot de passe.*»

La Commission estime que le recours à un « *login* » et à un mot de passe ne suffit pas pour toutes les applications. L'utilisation de certaines applications et surtout l'accès via Internet à l'infrastructure de la Communauté française requièrent des moyens d'authentification plus « pointus », comme le recours à une carte électronique avec certificat d'authentification utilisable moyennant l'introduction d'un « code PIN ». En d'autres termes, les moyens d'identification et d'authentification devraient être adaptés aux normes de sécurité établies en fonction de la nature de l'application et des canaux d'accès. Dès lors, la Commission juge préférable de formuler l'article 6, § 1 du projet d'arrêté en des termes plus généraux et d'y parler de « moyens d'authentification » plutôt que du « *login* » et du « mot de passe ».

7. L'article 7, § 2 du projet d'arrêté précise : « *Seule l'Entreprise des Technologies Nouvelles de l'Information et de la Communication a le droit d'installer des applications sur les ordinateurs des utilisateurs ou d'autoriser autrui à le faire*. »

La Commission s'étonne que l'ETNIC, en tant que sous-traitant, soit la seule à pouvoir installer des applications sur les ordinateurs des membres du personnel et que ce droit soit refusé à la Communauté française, en tant que responsable du traitement. La façon dont l'article 7, § 2 du projet d'arrêté est rédigé semble suggérer que toute décision en la matière est réservée à l'ETNIC. Celle-ci n'est finalement qu'un sous-traitant. Il va de soi que le responsable du traitement n'a pas besoin de l'autorisation du sous-traitant, puisque ce dernier agit sous son autorité et sa responsabilité.

8. L'article 8, 2ème alinéa, du projet d'arrêté stipule : « *Ce contrôle est exercé par L'Entreprise publique des Technologies Nouvelles de l'Information et de la Communication (l'ETNIC), dans le cadre des missions qui lui sont confiées par le décret du 27 mars 2002 et par son contrat de gestion.* »

Selon la Commission, il y a lieu de préciser quels sont les employés de l'ETNIC compétents à cet effet. D'après l'article 12 du projet d'arrêté, il s'agirait des membres du personnel de l'ETNIC désignés dans le contrat de gestion. Cette précision devrait déjà figurer dans l'article 8 du projet d'arrêté.

9. L'article 8, 3ème alinéa, du projet d'arrêté est rédigé comme suit : « *L'ETNIC enregistre et analyse les statistiques des accès à Internet, en tant que sous-traitant au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et dans le respect des dispositions légales et notamment de la loi du 8 décembre 1992 et dans les limites fixées aux articles 11 et 13 du présent arrêté.* »

La Commission souligne que l'ETNIC est un sous-traitant au sens de la loi du 8 décembre 1992 et qu'il doit par conséquent offrir, conformément à l'article 16 de ladite loi, les garanties requises quant à la sécurité dudit traitement.

De plus, il y a lieu qu'une convention réglant les points prévus à l'article 16 de la loi du 8 décembre 1992, notamment la responsabilité du sous-traitant à l'égard du responsable du traitement, soit conclue entre ces derniers.

La Commission souhaite en outre que les membres du personnel de l'ETNIC qui auront accès aux données soient désignés nommément et signent une déclaration relative au caractère confidentiel des données.

Le responsable du traitement devra tenir à la disposition de la Commission le contrat conclu entre lui et le sous-traitant, la liste des employés de ce dernier ayant accès aux données et les

déclarations de confidentialité signées par ceux-ci.

10. L'article 9 du projet d'arrêté stipule : « Les finalités du contrôle sont les suivantes :

- *vérifier et garantir la sécurité et le bon fonctionnement des systèmes informatiques des Services de la Communauté française ;*

- *assurer la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à autrui et d'assurer ou de vérifier qu'aucune ressource ne peut être ou n'est utilisée d'une quelconque manière réprimée par la loi ou susceptible de porter atteinte à autrui ;*

- *contrôler le respect par le personnel des principes et règles énoncées dans le présent arrêté;*

- *contrôler les coûts générés par l'usage des moyens de communication.* »

L'article 9 du projet d'arrêté contient un exposé explicite des finalités déterminées et légitimes du contrôle de l'utilisation du courrier électronique et d'Internet. Ce faisant, il répond aux exigences de l'article 4 de la loi du 8 décembre 1992.

11. L'article 11, § 2, 4ème alinéa, du projet d'arrêté est libellé comme suit : « *Les règles adoptées par la Communauté française pour assurer la protection de la vie privée des membres du personnel n'entravent pas la recherche des auteurs d'infractions par les autorités judiciaires dans le cadre d'enquêtes menées dans le respect des procédures légales, ni la coopération des membres des services de la Communauté en ce sens.* »

La Commission est d'avis qu'il doit en aller de même en ce qui concerne la compétence d'investigation reconnue à la Commission par l'article 32, §1, de la loi du 8 décembre 1992.[4]

12. L'article 11, §3, 1er et 2ème alinéas, du projet d'arrêté est ainsi formulé : « *Pour l'Internet, sont enregistrés l'ordinateur au départ duquel la consultation est effectuée, la page, les dates et heures d'accès à Internet, y compris le temps de connexion. Sur base de ces éléments, une liste générale et anonyme des sites visités indique la durée et le moment des visites.*

Pour le courrier électronique, sont enregistrés le nombre de messages, la taille et la présence de fichiers joints. »

La Commission constate que des données sont enregistrées quant à l'ordinateur au départ duquel des consultations sont effectuées.

Si seul un contrôle général et anonyme des sites est effectué, comme il semble ressortir de l'article 11, elle ne voit pas l'intérêt de conserver des données quant aux ordinateurs à partir desquels les consultations sont effectuées.

[4] « *Pour l'accomplissement de toutes ses missions, la Commission peut requérir le concours d'experts. Elle peut charger un ou plusieurs de ses membres, éventuellement assistés d'experts, de procéder à un examen sur place.*
Dans ce cas, les membres de la Commission ont la qualité d'officier de police judiciaire, auxiliaire du procureur du Roi.
Ils peuvent notamment exiger communication de tout document pouvant leur être utile dans leur enquête.
Ils peuvent également pénétrer en tous lieux où ils ont un motif raisonnable de supposer que s'exerce une activité en rapport avec l'application de la présente loi. »

S'il devait néanmoins être envisagé d'individualiser les informations, la Commission rappelle les recommandations formulées dans son avis 10/200 selon lesquelles « *le contrôle doit se fonder sur des données objectives restreintes et non sur une prise de connaissance préalable et systématique du contenu de toutes les données de trafic concernant chaque employé. L'employeur pourra à cet effet disposer par exemple d'une liste d'adresses de sites consultés de façon globale sur une certaine période, sans que soient identifiés dans un premier temps les auteurs des consultations. Il pourra sur cette base repérer une durée anormalement élevée de consultation d'Internet ou la mention d'adresses de sites suspects et prendre les mesures de contrôle appropriées. La détection de la consultation de certains sites pourrait également être effectuée de façon automatique grâce à un logiciel spécifique sur la base de mots-clés déterminés* ». S'il devait être envisagé d'individualiser les informations, la Commission suggère que les loggings individuels permettent d'identifier l'utilisateur avec plus de certitude et d'éviter que ne soit suspectée toute personne faisant usage d'un seul et même ordinateur.

La Commission fait remarquer que les données enregistrées dont il est ici question sont des données à caractère personnel au sens de l'article 1 de la loi du 8 décembre 1992 et que les dispositions de ladite loi s'appliquent donc à leur traitement.

13. L'article 13, 1er alinéa, du projet d'arrêté stipule : « *Lorsqu'à l'occasion de l'analyse statistique, l'Entreprise des Technologies Nouvelles de l'Information et de la Communication détecte des indications d'utilisation anormale des ressources réseau, elle en informe immédiatement la Commission de déontologie. Cette dernière peut, en vue de la poursuite de l'une ou de l'ensemble des finalités décrites à l'article 9, demander à l'Entreprise des Technologies Nouvelles de l'Information et de la Communication de procéder à l'individualisation des données de communication électronique mais, elle ne peut en aucun cas, demander à accéder au contenu de celles-ci.* »

La Commission interprète comme suit cette disposition : la seconde phase du contrôle, à savoir l'individualisation des données de télécommunications, ne pourra intervenir qu'après que l'ETNIC aura constaté, à l'occasion d'un contrôle statistique de l'usage fait de l'infrastructure numérique de l'employeur, des anomalies au sens de l'article 12, § 2, 1er et 2ème alinéas, du projet d'arrêté, qu'elle aura porté celles-ci à la connaissance de la Commission de déontologie et que cette dernière lui aura demandé de procéder à la mise en relation des données de télécommunications visées avec un membre du personnel.

D'après la dernière phrase du 1er alinéa de l'article 13 du projet d'arrêté, la Commission de déontologie ne peut en aucun cas demander à l'ETNIC de prendre connaissance du contenu des données de communication électronique.

L'accomplissement des finalités en vue desquelles le contrôle a été institué ne nécessite en principe pas de prendre connaissance du contenu du flux de données : la liste générale des courriels envoyés et/ou reçus ou des sites Web consultés durant une période déterminée contient en principe suffisamment d'éléments révélant que les règles prescrites dans le projet d'arrêté ont été ou non respectées (par exemple : une durée de consultation d'Internet anormalement longue ou la présence d'adresses de sites suspects ; la fréquence importante, le nombre, la taille, ..., des courriels) – tout comme une facture de téléphone peut faire apparaître des montants anormalement élevés. La Commission constate que la disposition est formulée de façon très absolue et qu'aucune exception n'est prévue. Elle renvoie à cet égard aux conditions relatives à la prise de connaissance des données de télécommunication tels que développés dans son avis 10/2000 et dans la recommandation 1/2002, ainsi que, à titre de référence utile, dans la convention collective n°81.

14. Pour conclure quant aux articles 11, § 3, 1er et 2ème alinéas, 12, § 1 et 13, 1er alinéa, du projet d'arrêté, il est permis d'affirmer que le contrôle par étapes qui est (sera) prévu par ces dispositions permet de limiter au maximum l'intrusion dans la vie privée des membres du personnel.

15. L'article 17 du projet d'arrêté précise ce qui suit : « *Les droits dont les membres du personnel disposent, en vertu des articles 9 à 12 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel sont exercés de la façon décrite aux alinéas deux à quatre du présent article.*

Le droit d'accès aux données à caractère personnel les concernant qui ont fait l'objet d'un enregistrement, est exercé par les membres du personnel sur simple demande adressée au responsable de l'Entreprise des Technologies Nouvelles de l'Information et de la Communication désigné à cet effet dans le contrat de gestion.

Le droit de rectification des données inexactes les concernant s'exerce moyennant demande écrite adressée à la Commission de déontologie.

Le droit de suppression des données qui, compte tenu des finalités du traitement, sont inexactes ou dont l'enregistrement, la communication ou la conservation sont légalement interdits ou qui sont conservées au-delà d'une période raisonnable, prenant fin un an après les relations de travail entre les parties, s'exerce également moyennant demande écrite adressée auprès de la Commission de déontologie. »

L'article 17 du projet d'arrêté a pour but d'appliquer les droits dont l'intéressé jouit en vertu des articles 10 à 12 inclus de la loi du 8 décembre 1992 mais ne parle pas des conditions formelles que ces articles imposent pour pouvoir exercer les droits en question, à savoir l'obligation pour le demandeur d'apporter la preuve de son identité. Pareille preuve est indispensable afin d'éviter que quelqu'un ne puisse obtenir communication de données concernant une autre personne. Les modalités de l'exercice des droits visés aux articles 10 et 12 de la loi du 8 décembre 1992 ont été précisées dans les articles 32 et 33 de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992.[5]

PAR CES MOTIFS,

La Commission émet un avis favorable au sujet du projet d'arrêté qui lui a été soumis, à condition qu'il soit tenu compte des remarques formulées plus haut.

L'administrateur,	Le président,
(sé) Jo BARET	(sé) Michel PARISSE

[5] « *Art. 32. Toute personne, justifiant de son identité, a le droit d'obtenir, dans les conditions prévues par la loi, communication de l'information visée à l'article 10 de la loi, en adressant une demande signée et datée qu'elle remet sur place ou qu'elle envoie par la poste, ou par tout moyen de télécommunication :*
** soit au responsable du traitement ou à son représentant en Belgique, ou à l'un de ses mandataires ou préposés;*
** soit au sous-traitant du traitement des données à caractère personnel qui la communique, le cas échéant, à une des personnes mentionnées ci-dessus.*
En cas de remise de la demande sur place, la personne, qui la reçoit, délivre immédiatement un accusé de réception daté et signé à l'auteur de la demande.

Art.33. Les demandes de rectification, de suppression ou d'interdiction des données à caractère personnel, ou la communication d'une opposition, fondée sur l'article 12 de la loi, sont introduites selon la même procédure et auprès des mêmes personnes que celles mentionnées à l'article 32 du présent arrêté. »