Question Michel Zadory/Charles Brönnimann **QA 3084.07**

Des fonctionnaires surfent sur des sites douteux !

Question

Lors de la communication à la presse, TJ le vendredi 5 octobre 2007 / le journal «La Liberté» du 6 octobre 2007, de la décision administrative prise à l'encontre du policier qui avait roulé à 229 km/h, le Conseiller d'Etat Erwin Jutzet a terminé son information en disant que le policier ne s'était pas installé dans une routine délictueuse comme certains fonctionnaires qui consacrent, chaque jour, une heure à surfer sur des sites douteux à leur place de travail, a-t-il ajouté. Nous approuvons hautement la déclaration sans équivoque du Conseiller d'Etat Erwin Jutzet, sur le comportement intolérable de certains fonctionnaires. Cette allégation est très importante, car elle atteste que des fonctionnaires surfent chaque jour sur des sites douteux ! Il n'est pas nécessaire de décrire ce qu'on entend par sites douteux ! Ce comportement de certains fonctionnaires n'est pas acceptable et il doit être sanctionné tant pour des raisons d'éthique que pour des raisons de coûts supportés par la collectivité. Par hypothèse, s'il y a cinq cents fonctionnaires qui surfent une heure par jour, cela représente tout de même un montant qu'on ne saurait minimiser sans oublier que durant le surf le travail ne se fait pas !

En conséquence, nous voudrions interpeller le Conseil d'Etat en posant les questions suivantes :

a) Puisque le phénomène est avéré, le Conseil d'Etat peut-il définir son ampleur ou dire quel pourcentage du personnel se permet un tel comportement ?

b) Le Conseil d'Etat peut-il chiffrer le coût que cette indiscipline représente pour la caisse de l'Etat ?

c) Lors de cas reconnus des mesures disciplinaires sont-elles prises et si oui lesquelles ?

d) Le Conseil d'Etat envisage-t-il de prendre des mesures techniques – si cela est possible – sur le plan de son système informatique afin d'empêcher l'accès à ces sites ?

e) Le réseau informatique de l'Etat englobe-t-il tous les services de l'Etat y compris l'enseignement ou y a-t-il des services qui sont indépendants et si oui lesquels ?

Le 10 octobre 2007

Réponse du Conseil d'Etat

Avant de répondre précisément aux questions posées par les députés Michel Zadory et Charles Brönnimann, le Conseil d'Etat estime nécessaire de rappeler l'historique et le contexte légal dans lequel se situe l'utilisation d'Internet par le personnel de l'Etat.

1. Historique

En parallèle avec le développement d'Internet au plan mondial au début des années 2000, un nombre toujours plus important de collaborateurs et de collaboratrices ont obtenu un accès à Internet, y compris au courrier électronique, à leur place de travail. Ces outils de travail permettent un accès rapide à de multiples sources d'informations nécessaires à l'exercice des tâches, le transfert rapide de fichiers informatiques et, par conséquent, un gain de temps et une plus grande efficacité dans l'exercice de la fonction. Toutefois, l'utilisation d'Internet à la place de travail a très vite nécessité la mise en place d'une réglementation qui en fixe les limites, pour les motifs suivants :

- Selon l'article 58 al. 1 de la loi du 17 octobre 2001 sur le personnel de l'Etat (LPers, RSF 122.70.1), le personnel doit consacrer tout le temps de travail à l'exercice de sa fonction. L'utilisation d'Internet à des fins autres que professionnelles, comme d'ailleurs toute autre activité privée pendant le temps de travail, constitue dès lors une violation claire de ce devoir de service.

- En tant qu'agents ou agentes des services publics, les collaborateurs et les collaboratrices de l'Etat ont des obligations spécifiques tant auprès des citoyens destinataires des prestations étatiques qu'auprès de l'Etat, leur employeur. Le personnel étatique est ainsi tenu, en particulier, d'adopter un comportement qui donne ou renforce la confiance qu'est en droit d'avoir le citoyen à l'égard de l'Etat et que celui-ci doit posséder à l'égard de ses agents et agentes. Or, l'utilisation abusive d'Internet à des fins autres que professionnelles peut porter une atteinte grave à l'image de l'Etat ainsi qu'à ses agents et agentes; elle est donc de nature à entamer le lien de confiance qui doit exister entre les citoyens et l'administration.

- L'utilisation d'Internet présente des risques de surcharge des systèmes d'information et des risques pour la sécurité informatique (transmission de virus). Il importe donc de limiter aux seules fins professionnelles le recours à cet outil informatique.

Pour les motifs précités, en 2001, sur demande du Centre informatique de l'Etat de Fribourg (CIEF, actuellement le Service de l'informatique et des télécommunications, SITel), un groupe de travail, chargé de préparer une réglementation, a été constitué.

En mars-avril 2002, un avant-projet d'ordonnance relative à la surveillance de l'utilisation d'Internet par le personnel de l'Etat a été mis en consultation auprès des Directions, services, établissements et associations de personnel. A la suite de cette consultation, le Conseil d'Etat a adopté l'ordonnance du 20 août 2002 relative à la surveillance de l'utilisation d'Internet par le personnel de l'Etat (RSF 122.70.17). Cette ordonnance, entrée en vigueur le 1er octobre 2002, et son commentaire explicatif, se trouvent sur le site Internet du SPO, sous la rubrique « Actualités », actualité no 27 du 7 octobre 2002, lien : http://www.fr.ch/spo/news/2002/.

2. Contenu de l'ordonnance du 20 août 2002

2.1. Principes d'utilisation

Ces principes sont régis par l'article 4 de l'ordonnance.

En tant qu'outil professionnel destiné à améliorer l'efficacité au travail, l'utilisation d'Internet est réservée à des fins professionnelles. L'alinéa 1er de cet article pose donc ce principe.

Une exception figure à l'alinéa 2. Compte tenu de l'ampleur prise par l'Internet dans tous les domaines d'activités, une interdiction absolue d'utilisation d'Internet à des fins privées est difficilement acceptable et applicable. C'est la raison pour laquelle une utilisation occasionnelle d'Internet à des fins privées est tolérée comme le prévoient par ailleurs d'autres employeurs privés et publics. Il ne s'agit toutefois pas d'une autorisation d'utiliser Internet à des fins privées mais bien d'une tolérance limitée, qui doit rester compatible avec l'obligation de consacrer tout son temps à son travail (art. 58 al. 1 LPers). En conséquence, cette utilisation ne peut être qu'occasionnelle et n'est admise que dans des conditions restrictives. Bien que l'ordonnance ne contienne pas de critères précis pour délimiter ce qui peut être considéré comme occasionnel et que l'autorité jouisse de ce fait d'une marge d'appréciation, il est évident que l'utilisation d'Internet à des fins privées, quotidiennement ou plusieurs heures par semaine, ne peut en aucun cas être qualifiée d'occasionnelle. Cela étant, le caractère occasionnel de la consultation doit à chaque fois se déterminer en fonction des situations particulières. L'appréciation d'une utilisation non professionnelle d'Internet sera aussi différenciée, selon que cette utilisation est en rapport, entre autres, avec l'exercice d'une charge publique ou d'une activité accessoire autorisée. Dans ces cas, une requête préalable de l'utilisation d'Internet à des fins privées devra être déposée ; le cas échéant, l'autorisation sera assortie de conditions précises.

Dans tous les cas et quelles que soient les circonstances, sont interdites à des fins privées, sans aucune marge de tolérance, l'utilisation de médias interactifs (« chat »), les transactions financières (notamment le « telebanking ») ou les sites payants, la visite de sites Internet à caractère érotique, violent ou raciste (art. 4 al. 3 de l'ordonnance).

2.2. Règles de comportement

Selon l'article 6 de l'ordonnance, le collaborateur ou la collaboratrice doit adopter un comportement digne de la confiance et de la considération que sa fonction exige. En particulier, il ou elle doit respecter les convenances ainsi que les règles sur la protection des données personnelles et sur la sécurité des données et celles sur le droit d'auteur. Ces règles sont d'ailleurs également applicables à l'Etat-employeur.

Volontairement, cette disposition a été rédigée de manière positive et dans le sens d'une sensibilisation à l'utilisation d'Internet. Dans son comportement en tant qu'utilisateur ou utilisatrice d'Internet, l'agent ou l'agente des services publics ne doit pas seulement respecter son devoir de service de consacrer tout son temps à son travail, mais il ou elle doit surtout avoir un comportement digne de la confiance et de la considération que sa fonction exige. La formulation de l'article 6 tient compte de l'importance que la LPers attache à la spécificité de la fonction d'agent-e des services publics et aux règles de comportement qui en découlent (art. 1er et 56 al. 3 LPers).

2.3. Contrôles globaux

L'article 7 de l'ordonnance prévoit :

Art. 7 *Contrôles globaux*

[1] Par contrôles globaux de l'utilisation d'Internet, on entend l'établissement de statistiques anonymes (effectuées de manière telle qu'elles ne permettent pas l'identification de l'utilisateur ou de l'utilisatrice) sur les sites les plus fréquemment visités, sur le nombre de connexions, sur le temps total passé à visiter des sites Internet ainsi que sur le volume du courrier électronique.

[2] Le Service (SITel) effectue régulièrement des contrôles globaux, dans le respect des dispositions de la législation sur la protection des données. Pour les secteurs de l'Etat qui ne sont pas sous le contrôle du Service, les contrôles globaux sont réalisés par les organes informatiques compétents, qui mandatent au besoin le Service.

[3] Les résultats des contrôles globaux sont communiqués trimestriellement à la Direction et au/à la chef-fe de l'unité administrative.

A la lumière de cette disposition, le Conseil d'Etat observe que les Directions et les unités administratives sont à même, sur la base des résultats des contrôles globaux, de détecter les indices d'abus de l'utilisation d'Internet.

2.4. Contrôles personnalisés

Les articles 8 à 10 de l'ordonnance sont consacrés aux contrôles personnalisés et en décrivent très précisément le déroulement :

Art. 8 *Contrôles personnalisés*
a) Principes

[1] Lorsque les contrôles globaux, ou d'autres constatations, mettent en évidence des indices d'abus dans l'utilisation d'Internet, des contrôles personnalisés peuvent être effectués.
[2] Par indices d'abus dans l'utilisation d'Internet, on entend, notamment, un temps anormalement élevé d'utilisation par rapport aux tâches à effectuer, la visite fréquente de sites Internet paraissant ne pas avoir de lien avec la fonction ou la visite de sites interdits.
[3] En ce qui concerne le courrier électronique, le contrôle se limite au nombre de messages envoyés et reçus, aux éléments d'adressage, aux types et volumes de fichiers attachés. Il ne porte pas sur le contenu des messages.

Art. 9 *b) Instances compétentes*

[1] Les contrôles personnalisés sont ordonnés par la Direction ou par le/la chef-fe de l'unité administrative.
[2] Ils sont effectués par le Service ou l'unité informatique compétente.

Art. 10 *c) Mesures en cas d'abus*

Après avoir entendu le collaborateur ou la collaboratrice et s'il s'avère que l'utilisation d'Internet constitue une violation des devoirs de service, le/la chef-fe de l'unité administrative, ou au besoin la Direction, prend les mesures appropriées conformément à la législation sur le personnel de l'Etat.

Pour rappel, la visite de sites interdits (comme, par exemple, les sites érotiques et pornographiques) est toujours un indice d'abus.

3. Information du personnel

Au moment de l'adoption de l'ordonnance, le 20 août 2002, celle-ci, ainsi que son commentaire explicatif, ont été distribués à chaque membre du personnel. De même, la réglementation a fait l'objet d'une actualité, publiée sur le site Internet du Service du personnel et d'organisation (SPO), sous « Actualités », actualité no 27 du 7 octobre 2002, lien : http://www.fr.ch/spo/news/2002/. Enfin, cette réglementation a fait l'objet d'articles dans les médias.

En outre, à chaque démarrage de son ordinateur, l'utilisateur est averti par un message qui fait référence à l'ordonnance du 20 août 2002 relative à la surveillance de l'utilisation d'Internet par le personnel de l'Etat (RSF 122.70.17).

Enfin, depuis son ordinateur personnel, à partir du portail Intranet de l'Etat de Fribourg, lorsque le collaborateur ou la collaboratrice veut accéder à un site Internet externe, la page suivante du SITel s'affiche une fois par mois sur son écran :

POLITIQUE D'ACCES À INTERNET DE L'ETAT DE FRIBOURG

L'utilisation d'Internet est réservée à des fins professionnelles. Toutefois, l'utilisation occasionnelle d'Internet à des fins privées est tolérée, dans les limites résultant de l'obligation de service de consacrer tout son temps à son travail et sous certaines conditions :

- Elle doit être limitée et peu fréquente;
- Elle ne doit pas compromettre l'activité professionnelle;
- Elle ne doit pas entraver l'activité de l'Etat de Fribourg;
- Elle ne doit pas nuire aux intérêts de l'Etat de Fribourg.

Le collaborateur ou la collaboratrice doit adopter un comportement digne de la confiance et de la considération que sa fonction exige.

«Ordonnance du 20 août 2002 relative à la surveillance de l'utilisation d'internet par le personnel de l'Etat de Fribourg».(lien qui donne accès à l'ordonnance)

Cliquez ici si vous avez lu la politique de sécurité et que vous l'acceptez

Le collaborateur ou la collaboratrice est ainsi régulièrement rappelé à ses devoirs de fonction. Il n'ignore pas l'existence des contrôles globaux périodiques et le fait qu'il peut être soumis en tout temps à un contrôle personnalisé en cas de soupçon d'abus.

4. Réponses aux questions posées

Le Conseil d'Etat répond maintenant comme suit aux questions posées :

a) Puisque *le phénomène est avéré, le Conseil d'Etat peut-il définir son ampleur ou dire quel pourcentage du personnel se permet un tel comportement ?*

En ce qui concerne le réseau informatique géré par le SITel (cf. ci-dessous, tableau, ad question e), les statistiques anonymes de l'utilisation d'Internet sont établies tous les mois par le Responsable de la Sécurité des Systèmes d'information (RSSI) du SITel et communiquées aux secrétaires généraux trimestriellement. A noter qu'afin d'assurer une meilleure lisibilité, ces statistiques sont produites mensuellement, alors que l'ordonnance spécifie une périodicité trimestrielle.

En ce qui concerne le réseau fri-tic (cf. ci-dessous, tableau, ad question e), les contrôles globaux sont effectués mensuellement par les organes responsables; selon les cas détectés, sur requête des écoles concernées, il est procédé à des contrôles personnalisés. Pour ce qui est du réseau universitaire (Switch ; cf. ci-dessous, tableau, ad question e), des contrôles personnalisés sont effectués sur requête des services et en cas de soupçon d'abus.

Lorsque les contrôles globaux, ou d'autres constatations, mettent en évidence des indices d'abus dans l'utilisation d'Internet, des contrôles personnalisés peuvent alors être effectués par le RSSI, mais seulement sur demande de la Direction représentée par son secrétaire général ou par le/la chef-fe de l'unité administrative. Cette demande est adressée au Directeur et/ou au RSSI du SITel.

Le nombre de contrôles personnalisés réalisés par le SITel dans le courant de l'année 2007, à la demande des secrétaires généraux ou chef-fe-s d'unité administrative, s'élève à une vingtaine. Le SITel, en tant que fournisseur d'informations statistiques, ignore si le contrôle personnalisé a permis de prouver l'existence d'un abus et quelles ont été les mesures

individuelles prises. Toutefois, il constate que quasi systématiquement après les contrôles personnalisés, les sites indicatifs d'abus ont disparu des listes de sites figurant dans le contrôle global suivant.

Le nombre de contrôles personnalisés réalisés dans les autres réseaux s'élève, depuis l'entrée en vigueur de l'ordonnance du 20 août 2002, à 3. A l'instar du SITel, les responsables des autres réseaux ont constaté lors des contrôles globaux suivants la disparition des sites indicatifs d'abus éventuels.

En conséquence, selon les statistiques périodiques et sur la base des enquêtes demandées par les Directions et/ou chef-fe-s d'unité administrative, le Conseil d'Etat peut conclure que seule une très petite fraction de pourcent du personnel utilise Internet de manière à provoquer un soupçon d'abus en relation avec la fréquentation de sites interdits selon l'ordonnance du 20 août 2002. Les statistiques mettent cependant régulièrement en évidence des visites sur des sites non interdits mais qui n'ont pas nécessairement un caractère professionnel. Ces visites se situent dans la très grande majorité des cas dans les zones de tolérance admissibles, en particulier en ce qui concerne leur fréquence et leur durée.

b) Le Conseil d'Etat peut-il chiffrer le coût que cette indiscipline représente pour la caisse de l'Etat ?

Les pertes de productivités liées à l'utilisation non professionnelle d'Internet sont très difficilement chiffrables. En effet, d'une part, l'ordonnance tolère une utilisation occasionnelle d'Internet dans les limites résultant de l'obligation de consacrer tout son temps à son travail et, d'autre part, l'utilisation d'Internet à des fins privées en dehors des heures de travail n'est pas interdite explicitement. Ainsi, sur le plan pratique, distinguer une utilisation privée non abusive à partir des statistiques, ou établir une corrélation entre les heures privées et l'utilisation d'Internet, relève du défi.

Cela étant, pour tous les cas d'abus avérés, la question du temps consacré à la visite de sites non professionnels est analysée. En principe, le collaborateur ou la collaboratrice concerné-e est tenu de rattraper les heures de travail injustement comptées, ou peut être tenu-e de les rembourser.

c) Lors de cas reconnus des mesures disciplinaires sont-elles prises et si oui lesquelles ?

La LPers ne contient plus de droit disciplinaire ; les infractions aux devoirs de service sont traitées comme des manquements aux obligations contractuelles découlant du contrat d'engagement. Selon leur gravité, elles peuvent entraîner des mesures telles qu'un avertissement, une modification du cahier des charges avec une modification consécutive du traitement (transfert), une résiliation ordinaire des rapports de service ou encore un renvoi pour de justes motifs. La consultation abusive d'Internet, constituant clairement une infraction aux devoirs de service, doit donc entraîner la prise de mesures. Celles-ci sont de la compétence de l'autorité d'engagement, soit, sauf exceptions, les Directions du Conseil d'Etat et les établissements personnalisés. Les chef-fes des unités administratives sont compétents également pour adresser des avertissements. Etant donné la sensibilisation permanente effectuée sur la question de l'utilisation d'Internet, le Conseil d'Etat peut assurer que les autorités et organes concernés prennent les mesures adéquates à l'égard des collaborateurs et collaboratrices qui ont commis des abus dans ce domaine. En vertu du principe de la proportionnalité, selon la gravité de l'infraction (nature du site, durée, fonction exercée, etc.), les mesures telles qu'un avertissement ou un renvoi pour de justes motifs ont été prises. Ces décisions ont permis dans tous les cas de mettre un terme aux abus constatés.

d) Le Conseil d'Etat envisage-t-il de prendre des mesures techniques – si cela est possible – sur le plan de son système informatique afin d'empêcher l'accès à ces sites ?

Sur le plan technique, il est tout à fait possible de mettre en œuvre des systèmes qui empêchent l'accès à des sites considérés comme illicites, non conformes à l'éthique ou non professionnels. A cet effet, le SITel a mené une étude en 2005 pour obtenir un aperçu des produits disponibles sur le marché ; un tel système est même opérationnel sur le réseau pédagogique fri-tic.

Pour le réseau de l'administration cantonale et selon la solution choisie, les coûts de mise en œuvre et d'exploitation se situeraient entre 50 000 et 75 000 francs par année. A cela s'ajoute la charge occasionnée au niveau du personnel, charge estimée à environ ¼ EPT, pour maintenir le système. Il convient en effet de signaler que de nombreuses requêtes d'exception devraient être traitées. En effet, vu la diversité des services de l'Etat (police, services médicaux, tribunaux, etc.), un réglage standard et uniformisé du système, pour l'ensemble des services, nécessiterait en permanence le traitement des exceptions par un ajustement continu des réglages du système.

Pour une partie du personnel enseignant (écoles primaires et cycles d'orientation), le réseau fri-tic contient déjà des blocages par rapport aux sites interdits. En effet, cette mesure a été rendue nécessaire en raison de l'accessibilité des ordinateurs situés dans les écoles à de multiples utilisateurs, en particulier les élèves.

En conclusion à cette question, le Conseil d'Etat considère que le nombre très peu important des abus constatés ne justifie pas que l'on généralise les blocages au delà de ce qui existe déjà. Grâce aux contrôles globaux et personnalisés, force est de constater que les moyens préventifs d'abus sont suffisants.

e) Le réseau informatique de l'Etat englobe-t-il tous les services de l'Etat y compris l'enseignement ou y a-t-il des services qui sont indépendants et si oui lesquels ?

L'accès à Internet pour les services de l'Etat et ses différents organes est réalisé par plusieurs réseaux informatiques selon le tableau suivant :

Désignation de l'entité	**Réseau informatique pour accéder à Internet**	**Géré par**
Services de l'Etat y compris les établissements (tels HFR, ECAB, etc.)	Réseau informatique cantonal	SITel
Hautes écoles (HES-SO, Uni), excepté la Haute Ecole Pédagogique qui est reliée au réseau informatique cantonal	Réseau universitaire (Switch)	Switch
Enseignement secondaire 1 (CO) et écoles primaires	Réseau informatique pédagogique fri-tic	fri-tic
Enseignement secondaire 2 et écoles professionnelles	Réseau informatique cantonal mais accès à Internet par fri-tic	SITel / fri-tic

Conclusions

Déjà en 2002, le Conseil d'Etat, en sa qualité d'employeur, conscient des abus que peut entraîner l'utilisation d'Internet par le personnel, a adopté une réglementation sévère qui règle clairement la surveillance de l'utilisation d'Internet par le personnel de l'Etat et sanctionne les abus. Ainsi, depuis l'utilisation généralisée d'Internet au début des années 2000, une réglementation existe et la surveillance de l'utilisation d'Internet est réalisée au moyen de contrôles globaux et personnalisés. Avec de tels outils, de tels contrôles et une politique d'information constante pour le personnel, le Conseil d'Etat a atteint un résultat qui ne peut que rassurer les députés à l'origine de cette question parlementaire : les abus sont prévenus, détectés et sanctionnés. Selon les statistiques résultant des contrôles globaux et personnalisés, le Conseil d'Etat peut ainsi affirmer que l'ensemble du personnel de l'Etat, à l'exception d'une infime minorité, utilise Internet dans un but professionnel, au plus grand profit de son employeur.

Fribourg, le 20 novembre 2007