Date de dépôt : 12 décembre 2012

Réponse du Conseil d'Etat

à la question écrite urgente de M. Jean-Louis Fazio : Quelle sécurité informatique apportée au Télétravail exécuté par des fonctionnaires genevois depuis leur lieu de domicile – notamment depuis la France ?

Mesdames et
Messieurs les députés,

En date du 30 novembre 2012, le Grand Conseil a renvoyé au Conseil d'Etat une question écrite urgente qui a la teneur suivante :

Il est avéré que certains fonctionnaires, notamment du département de l'urbanisme (office des bâtiments) pratiquent le télétravail depuis leur lieu de domicile, notamment en France.

Particulièrement préoccupé par la confidentialité des données de l'Etat, cette manière de procéder soulève plusieurs questions relatives entre autres, à la sécurité et à la délocalisation à l'étranger de travail administratif.

En effet, il serait important de connaître quel type de documents sont élaborés et transmis par ce biais, quelle confidentialité depuis le poste de travail de l'émetteur peut être garantie et surtout quel type de sécurité informatique est appliquée au système de transmission afin d'éviter des fuites ou piratages.

Cette crainte par rapport à la sécurité est renforcée, dans le cas du DU et pourrait l'être d'autant plus en ce qui concerne le département de la sécurité, voire le pouvoir judiciaire - où il est reconnu que certains greffiers utilisent ce mode de travail - par deux éléments. Premièrement, les cas de télétravail sont particulièrement sensibles s'ils touchent des cadres ayant des responsabilités élevées. Ces personnes ont dès lors accès à un grand nombre de documents confidentiels. Deuxièmement, les personnes qui habitent en France passent la frontière. Les cas, certes différents car touchant le

domaine privé, des banquiers, nous apprennent qu'emmener des documents confidentiels à l'étranger peut augmenter les risques de fuites.

Dès lors pour répondre à ces craintes légitimes, voici mes six questions :

1. *Pourquoi le Conseil d'Etat prend-il le risque de recourir au télétravail ?*
2. *Combien de fonctionnaires/employé-e-s de l'Etat utilisent le télétravail, et combien depuis la France ?*
3. *Quels départements ont recours au télétravail ?*
4. *Quelles mesures sont prises afin d'assurer la sécurité des données emportées à leur lieu de domicile ?*
5. *Quels types de documents sont transmis par ce biais ?*
6. *Quel système ou application sont mis en place afin de sécuriser la transmission des données informatiques et éviter ainsi toutes cyberattaques ?*

RÉPONSE DU CONSEIL D'ÉTAT

1. Les technologies de l'information permettent aujourd'hui de créer des places de travail indépendamment de leur implantation géographique. Cette évolution a contribué au développement du télétravail dans de nombreux pays, dont la Suisse.

Dans son plan de mesures de 2006, le Conseil d'Etat a exprimé sa volonté *« d'encourager et favoriser les possibilités de travailler à domicile »*.

La préparation du plan de continuité des activités de l'Etat employeur en vue de la grippe pandémique de 2009 a accéléré la recherche de solutions de travail à distance sur les plans technique, organisationnel et législatif.

De nombreux avantages sont habituellement associés au télétravail : il permet une meilleure articulation entre vie privée et vie professionnelle et se traduit généralement par des gains de concentration et d'efficacité, une diminution des temps de déplacement et donc du stress et de la fatigue qui en découlent, une motivation renforcée et une réduction de l'absentéisme. Il offre en outre une solution favorable pour les travailleurs à mobilité réduite permanente ou temporaire.

Tous ces éléments ont favorisé la mise en place d'un concept qui a conduit à la promulgation du règlement sur le télétravail (B 5 05.13), du 30 juin 2010.

2. L'entrée en vigueur du règlement a été suivie d'une phase pilote qui a débuté en février 2011 avec un triple objectif :

– Evaluer la solution technique proposée.
– Déterminer avec plus de précision les activités qui se prêtent au télétravail et les règles à respecter afin qu'il soit utilisé à l'avantage de l'employé, de l'employeur et des usagers.
– Ajuster, le cas échéant, le règlement.

Dans ce contexte, 55 accès à distance ont été accordés (CHA : 1 / DF : 16 / DIP : 4 / DS : 4 / DU : 10 / DIME : 10 / DSE : 3 / DARES : 7). Certains ont été octroyés à usage de test uniquement. Parmi les personnes ayant participé à la phase pilote de télétravail, cinq sont domiciliées en France.

3. Tous les départements et la Chancellerie ont recours au télétravail.

4. La question de la confidentialité et de la protection des données est pour le Conseil d'Etat une préoccupation majeure.

Dans ce contexte, l'accent a été mis sur les conditions cadres associées à la procédure d'autorisation d'accès à distance :

– Le règlement B 5 05.13 contient des dispositions strictes relatives aux responsabilités des télétravailleurs et de leur hiérarchie en matière de secret de fonction et de sécurité absolue (art. 18A et 19).
– A l'issue de la phase pilote, le règlement a encore été renforcé : « Aucune autorisation ne peut désormais être accordée pour le traitement de données sensibles, telles que les données fiscales, les données relatives à des élèves ou à des mineurs, ainsi qu'aux données relatives au personnel » (art. 18). Le télétravail depuis un lieu public (par exemple un café Internet) est en outre interdit (art. 18A).
– Toute autorisation de télétravail fait préalablement l'objet d'un entretien entre le candidat et sa hiérarchie, à l'issue duquel une convention rappelant les principes de confidentialité absolue est signée.

Enfin, le télétravail concerne exclusivement les tâches effectuées par l'intermédiaire des systèmes d'information. Le traitement de dossiers physiques est soumis à des règles aussi strictes de protection des données.

5. Les documents traités par les télétravailleurs sont liés à l'activité courante de ces derniers. Sont le plus souvent concernées les tâches de rédaction, d'analyse de dossiers, de conception de projets, de gestion administrative, de programmation.

6. Sur le plan technique, la direction générale des systèmes d'information a mis en place pour les télétravailleurs un outil d'accès à distance, sécurisé notamment via un canal de communication crypté. Dénommé « PAD », cet outil offre à ses utilisatrices et utilisateurs un niveau de sécurité similaire à celui en vigueur dans l'administration cantonale. La sécurité absolue n'existe toutefois pas. Des organisations disposant de moyens de sécurité sans commune mesure avec ceux de l'Etat de Genève en font régulièrement les frais, comme le ministère de la défense américain lors de l'affaire WikiLeaks. Il est par exemple possible pour un membre du personnel de copier au bureau des documents sensibles sur une clef USB, voire de les envoyer par messagerie électronique, afin de les traiter ensuite depuis son domicile ou un cybercafé. Sauf à interdire les moyens informatiques ou les brider au point de leur faire perdre tout intérêt, le risque de fuite ne peut donc que marginalement être atténué par des solutions techniques. Les bonnes pratiques en la matière reposent avant tout sur des mesures managériales, combinant des actions de sensibilisation à la sécurité de l'information avec des normes contraignantes, à l'instar des articles 18 et 19 du règlement sur le télétravail, suivies en cas de violation par les sanctions disciplinaires, voire pénales, prévues dans les dispositions statutaires (art. 9A LPAC).

Au bénéfice de ces explications, le Conseil d'Etat vous invite, Mesdames et Messieurs les Députés, à prendre acte de la présente réponse.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :	Le président :
Anja WYDEN GUELPA	Charles BEER