P.V. ENFPS 15
P.V. ERMCE 14
P.V. FPSA 01

CHAMBRE DES DEPUTES

Session ordinaire 2011-2012

NB/YH

Commission de l'Education nationale, de la Formation professionnelle et des Sports
et
Commission de l'Enseignement supérieur, de la Recherche, des Media, des Communications et de l'Espace
et
Commission de la Fonction publique et de la Simplification administrative

Procès-verbal de la réunion du 17 février 2012

ORDRE DU JOUR :

Echange de vues avec des membres du Gouvernement au sujet de la sécurité informatique au sein des structures informatiques de l'Etat, en général, ainsi que sur l'accès à la base de données du "Centre médico-sportif" et le projet de loi portant sur l'exploitation d'une base de données à caractère personnel relative aux élèves, en particulier
(à la demande du groupe DP et du groupe déi gréng, par lettres du 19 janvier 2012)

*

Présents : M. Claude Adam, Mme Nancy Arendt épouse Kemp, M. André Bauler, M. Eugène Berger, M. Fernand Boden, M. Emile Eicher, M. Ben Fayot, M. Claude Haagen, Mme Josée Lorsché, M. Roger Negri remplaçant M. Fernand Diederich, M. Jean-Paul Schaaf, M. Serge Wilmes, membres de la Commission de l'Education nationale, de la Formation professionnelle et des Sports

M. Claude Adam, Mme Diane Adehm, M. Eugène Berger, Mme Anne Brasseur, Mme Claudia Dall'Agnol, M. Ben Fayot, M. Claude Haagen, M. Norbert Haupert, M. Marcel Oberweis, M. Serge Wilmes, membres de la Commission de l'Enseignement supérieur, de la Recherche, des Media, des Communications et de l'Espace

M. Claude Adam, M. André Bauler, M. Fernand Boden, Mme Claudia Dall'Agnol, M. Fernand Etgen, M. Gast Gibéryen, M. Norbert Haupert, M. Jean-Pierre Klein, M. Paul-Henri Meyers, membres de la Commission de la Fonction publique et de la Simplification administrative

M. François Biltgen, Ministre des Communications et des Médias, Ministre de la Fonction publique et de la Réforme administrative
M. Patrick Houtsch, Ministère d'Etat
M. Michel Lanners, Ministère de l'Education nationale
M. Gérard Lommel, M. Pierre Weimerskirch, Commission Nationale pour la Protection des Données
M. Pierre Zimmer, Centre des Technologies de l'Information de l'Etat
Mme Annik Sax, Centre médico-sportif
Mme Michèle Bram, Service des Médias et des Communications

M. Nicolas Bock, Administration parlementaire

Excusés : Mme Claudia Dall'Agnol, M. Fernand Diederich, M. Fernand Kartheiser, M. Gilles Roth, Mme Tessy Scholtes, membres de la Commission de l'Education nationale, de la Formation professionnelle et des Sports

M. Jean Colombera, Mme Christine Doerner, membres de la Commission de l'Enseignement supérieur, de la Recherche, des Media, des Communications et de l'Espace

M. Fernand Diederich, M. Léon Gloden, M. Gilles Roth, membres de la Commission de la Fonction publique et de la Simplification administrative

*

Présidence : M. Ben Fayot, Président de la Commission de l'Education nationale, de la Formation professionnelle et des Sports
M. Marcel Oberweis, Président de la Commission de l'Enseignement supérieur, de la Recherche, des Media, des Communications et de l'Espace
M. Norbert Haupert, Président de la Commission de la Fonction publique et de la Simplification administrative

*

Echange de vues avec des membres du Gouvernement au sujet de la sécurité informatique au sein des structures informatiques de l'Etat, en général, ainsi que sur l'accès à la base de données du "Centre médico-sportif" et le projet de loi portant sur l'exploitation d'une base de données à caractère personnel relative aux élèves, en particulier
(à la demande du groupe DP et du groupe déi gréng, par lettres du 19 janvier 2012)

Le représentant des Verts précise que son groupe n'a eu connaissance de l'incident au Centre médico-sportif que par la presse et qu'il a convoqué cette réunion pour obtenir des informations supplémentaires et fiables de la part des instances officielles. Il pose ensuite les questions ci-après :

- De quelle façon l'Etat sécurise-t-il ses données informatiques et pour quelle durée ?
- Quelles informations figurent dans la base de données du Centre médico-sportif ? Les Verts trouvent p.ex. étrange que l'origine d'un sportif soit uniquement indiquée s'il s'agit d'un sportif africain.
- Quelles conséquences découleront de l'incident précité ?
- Pourquoi est-il question dans la presse d'une affaire criminelle ?
- Ne faudrait-il pas également mettre en cause le Ministre compétent ou le médecin imprudent ?
- Quelles sont les règles imposées en matière d'utilisation des mots de passe ?

Le représentant du groupe DP remarque de son côté que l'incident montre malheureusement que la structure de protection des données de l'Etat semble peu efficace, se posant ainsi la question de savoir si un incident analogue ne risque pas de se reproduire. Les questions posées au Ministre par le groupe DP sont les suivantes :

- Quelles règles sont appliquées en matière de gestion, de protection et de contrôle des banques de données de l'Etat ?
- Y a-t-il en pratique réellement de tels contrôles ?
- Que risque la personne ayant utilisé sans y avoir droit le mot de passe du médecin imprudent pour s'introduire dans la banque de données ?
- De combien de banques de données en tout dispose l'Etat ?
- Quelles mesures seront prises pour éviter de tels incidents à l'avenir ?

Le représentant des Verts ajoute qu'à son avis les données de l'Etat sont insuffisamment protégées et il aimerait enfin savoir si la personne en question s'est rendue ou a été découverte.

M. le Ministre signale dans sa réponse qu'au Luxembourg le Ministre des Communications est également en charge de la protection des données, alors que normalement il s'agit du Ministre de la Justice.

Il ajoute qu'une directive européenne de 1995 règle les questions concernant la protection des données, directive qui a été transposée avec un certain retard au Luxembourg parce que les responsables étaient un peu réticents pour introduire une sorte d'Etat « big brother », mais finalement on s'est rendu compte qu''une certaine culture de la protection des données était nécessaire, de sorte qu'en 1999 une loi afférente a été élaborée par le Ministre en charge de la protection des données.

Les Commissions sont encore informées de l'existence d'un nouveau texte européen y relatif, à savoir une proposition de directive européenne, qui trouve en principe l'accord du Gouvernement luxembourgeois, tout comme de la Commission chargée de la protection des données.

Pour ce qui est de la loi de 2002 sur la protection des données, elle prévoit que le contenu des banques de données est défini par la Commission chargée de la protection des données.

Par la suite des discussions en matière de « cyber security » ont eu lieu et le Gouvernement envisage de créer un organe spécifique en charge de cette question. Les sujets à traiter par cet organe seront les suivants : <u>anticiper, prévenir, rétablir, réparer</u>.

<u>Anticiper</u>

Il est précisé que l'affaire du Centre médico-sportif n'a pas été l'œuvre d'un « hacker », mais qu'elle est due à une erreur humaine, difficile à anticiper.

Prévenir

Cette phase est censée permettre d'éviter qu'un tel fait se reproduise.

Rétablir

Si par impossible une attaque à une base de données a eu lieu, il s'agira de rétablir par la suite le standard normal.

Réparer

Ici il s'agit de prendre des mesures permettant d'éviter à l'avenir des incidents, mais la procédure pénale est elle aussi engagée pendant cette phase.

M. le Ministre rappelle que dans l'incident au Centre médico-sportif un médecin avait laissé un « post-it » avec son mot de passe sur son ordinateur et qu'une personne en a profité pour s'introduire dans la base de données. C'est le Ministre des Sports qui a donné la procuration au Directeur du CTIE pour porter plainte contre cette personne, la sanction pénale qui en découlera le cas échéant étant du ressort de la Justice, qui est en train de mener son enquête.

De l'avis de M. Biltgen, l'affaire précitée soulève quelques questions, à savoir :

- Il n'était pas possible d'anticiper l'attaque, vu que celle-ci a été rendue possible suite à une erreur humaine.
- En matière de prévention, l'Etat s'est engagé à faire suivre à son personnel des formations afférentes, au cours desquelles ce dernier apprendra p.ex. à choisir des mots de passe faciles à retenir, mais diificiles à décoder (au Ministère des Affaires étrangères p.ex.).

Pour ce qui est du matériel utilisé, le personnel aimerait toujours pouvoir disposer d'équipements faciles à utiliser, mais il faut leur faire comprendre que ces derniers ne sont pas forcément les plus sûrs.

En ce qui concerne le nouveau Cyber Security Board, celui-ci a décidé de faire établir une liste des bases de données de l'Etat par ordre d'importance, ainsi que d'introduire dans tous les services l'utilisation de « Luxtrust », l'incident ayant ainsi réussi à surmonter les hésitations du Gouvernement liées à son coût.

Une question reste encore à trancher, à savoir si ou bien un délégué chargé de la protection des données sera prévu dans chaque administration ou bien si le personnel de la Commission chargée de la protection des données sera renforcé.

Pour conclure M. le Ministre signale que si un fonctionnaire commet une faute, il s'en suivra une affaire disciplinaire, alors que pour une personne relevant du droit privé, une procédure pénale sera engagée.

M. Lommel aborde ensuite la loi de 2002, en formulant d'abord quelques remarques liminaires, à savoir :

- L'incident sous objet a permis de se rendre compte d'un problème fondamental, à savoir celui de la culture de la protection des données. Il précise que l'accès aux

données du Centre médico-sportif était en cours de modification lors de l'incident et qu'il ne sera désormais possible que par le biais de « Luxtrust ».
- L'incident a été analysé par la Commission, mais il faut savoir que depuis la modification de la loi sur la protection des données en 2007, la base de données du Centre n'est en fait plus soumise à une autorisation de la Commission.
- Il est ainsi rappelé qu'en 1997 l'accent était mis sur l'élaboration d'un cadastre des banques de données, ainsi que sur des contrôles a priori, alors que depuis 2007 est plutôt visée une responsabilisation des administrations concernées et les contrôles réalisés par la Commission ont lieu a posteriori.
- Pour ce qui est de l'analyse de l'incident au Centre, elle a révélé quelques insuffisances, mais rien de grave.
- La question de la sécurité évolue constamment et les campagnes de sensibilisation et de formation entamées par le Gouvernement sont à saluer dans ce contexte.
- Il ne faut d'ailleurs pas croire que la négligence au Centre constitue un cas isolé, vu que des pratiques analogues avec le mot de passe sur un post-it ont ainsi déjà été rencontrées dans des cliniques p.ex.
- Il faut enfin encore savoir qu'un registre des banques de données de l'Etat existe bel et bien, mais qu'en fait il n'est pas forcément à jour vu que depuis 2007 certaines d'entre elles ne nécessitent plus l'autorisation de la Commission.
- C'est également la raison pour laquelle il n'est pas possible de répondre avec la dernière précision à la question de savoir de combien de banques de données dispose l'Etat, mais il devrait s'agir de plusieurs centaines.

M. le Ministre précise que c'est dans un souci de simplification administrative qu'a été opéré le changement d'approche fondamentale en 2007, vu qu'avant l'on évoquait parfois certaines lourdeurs de procédure.

Mme Sax signale que les examens réalisés au Centre médico-sportif respectent les derniers standards internationaux et que les données personnelles recueillies sont l'âge, le sexe et dans certains cas, l'origine des sportifs. Il faut en effet savoir que les Africains p.ex. présentent lors de l'examen ECG une anomalie, mais qui est sans conséquences du point de vue de la santé. Cette information est ainsi recueillie pour des raisons strictement médicales, afin d'éviter une hospitalisation inutile de certaines personnes, et il ne s'agit en aucun cas d'un acte raciste.

Débat

Un certain nombre de sujets sont abordés lors du débat, qui pourront être résumés succinctement comme suit :

- Les contrôles de la Commission se font ou bien suite à un incident, une demande ou une plainte, ou bien il s'agit de contrôles réalisés périodiquement suivant le degré de sensibilité des banques de données, un tel contrôle concernant l'Union des Caisses de Maladie p.ex. étant encore en cours.
- Des engagements de collaborateurs supplémentaires seraient les bienvenus, surtout si l'on veut augmenter le nombre de contrôles ; un spécialiste des questions informatiques sera toutefois engagé prochainement.

M. le Ministre ajoute que l'engagement de personnel dépendra également de la décision concernant ou bien la création d'un poste de chargé de la protection des données spécifique dans les administrations concernées – ces personnes ne devraient toutefois pas faire partie du cadre de personnel de celle-ci – sa préférence personnelle s'orientant plutôt vers un renforcement de la Commission ad hoc. Le Gouvernement n'a pas encore fait son choix à ce sujet et la question sera également examinée par la commission parlementaire compétente.

- en réponse à une remarque du représentant des Verts concernant une certaine responsabilité du Ministre qui n'a pas été en mesure d'assurer efficacement la protection des données des citoyens, en ajoutant qu'il faudrait peut-être aussi se demander si la faute n'incombe pas au système de protection, M. Biltgen réfute cette dernière remarque, vu que l'on ne pourra pas critiquer le système dans un cas où ses règles n'ont pas été respectées. De toute façon, M. Biltgen aimerait attendre la décision pénale avant de discuter de toutes les questions en détail. Il ajoute que la Justice examinera si un fait pénal a été commis et si oui, par qui.

- il est précisé que le système informatique de conservation des données a été mis en place au Centre médico-sportif en 2005 et que celles-ci sont conservées pendant 10 ans suivant l'autorisation de la Commission chargée de la protection des données. Après cette échéance, les données sont supprimées.

- Est ensuite discutée la question d'une diffusion par la presse de données sensibles concernant les sportifs, à savoir la prise de substances illicites p.ex., mais la Commission constate qu'une sécurité à 100% est sans doute illusoire et que le Centre médico-sportif ne réalise pas de recherches concernant l'évolution des sportifs. M. Biltgen ajoute qu'il est clair que si certaines données sensibles se retrouvent sur la place publique, cela aura des conséquences, une personne se sentant lésée pouvant toutefois intenter un recours au civil, le cas échéant contre l'Etat.

- Le représentant du DP remarque qu'à son avis l'Etat devrait quand même garantir à ses citoyens un minimum de protection de leurs données. Il se demande ainsi si les fonctionnaires luxembourgeois sont vraiment suffisamment outillés à cet effet. Il croit également savoir que des systèmes de protection plus efficaces que celui avec les mots de passe existent à l'étranger. M. le Ministre considère que l'efficacité du système de protection n'est pas en cause dans l'incident, vu qu'il s'agissait d'une simple erreur humaine, presqu' inexplicable, vu que le personnel du Centre médico-sportif avait déjà reçu une formation avant l'incident. Il est cependant d'accord pour dire qu'en matière d'accès à des données par internet, des améliorations sont sans doute encore possibles.

- M. Zimmer intervient ensuite pour préciser les mesures prises par le CTIE en vue d'une meilleure sécurité des données de l'Etat. Il signale ainsi que l'on distingue entre les « bons » et les « mauvais » hackers, le CTIE s'efforçant dans un souci de transparence d'avoir des contacts avec cette première catégorie d' »experts », qui en sont arrivés à la conclusion qu'aucun problème grave de sécurité se pose actuellement au sujet des bases de données de l'Etat, ce qui n'exclut bien entendu pas l'élément humain qui joue toujours. Il faut ainsi savoir que dans le cas au Centre médico-sportif, il ne s'agissait pas d'une attaque par un ou plusieurs « hackers », qui ont cependant tenté de telles atteintes par après, mais sans succès. Il cite encore les quelques mesures supplémentaires ci-après :

- Création d'un service audit sécurité au sein du CTIE

- Création de l'identification forte en collaboration avec Luxtrust

- Existence d'audits externes relatifs au CTIE

- Les bases de données ne sont pas mises sur internet avant d'avoir consulté les « bons hackers ».

- Toutes les bases de données sont désormais uniquement accessibles en utilisant Luxtrust.

- L'utilisation de plusieurs mots de passe n'apporte aucun surplus en matière de sécurité, d'où l'importance de l'introduction de Luxtrust.

- Des « hackers » ont également essayé de s'introduire dans d'autres bases de données, mais une fois de plus sans succès.

M. le Ministre ajoute que l'Université de Luxembourg offre même à des hackers une formation en tant qu'expert en sécurité informatique qui mène jusqu'au doctorat. Il signale encore qu'une circulaire a été adressée aux fonctionnaires afin de les rendre attentifs aux règles élémentaires de sécurité.

M. Zimmer précise en réponse à la remarque du représentant du DP concernant la prétendue supériorité de systèmes de protection étrangers que la collaboration entre l'Etat et le secteur privé dans le cadre de Luxtrust est toujours citée en tant qu'exemple à l'étranger. Ce dernier voudrait précisément revenir à la question de la saisie de l'origine des sportifs africains, vu qu'à son avis il s'agit quand même d'une information sensible qui devrait le cas échéant nécessiter une autorisation spécifique. Mme Sax lui répond que les médecins du Centre médico-sportif ne considèrent pas cette donnée comme étant sensible, ce qui est en principe confirmé par M. Lommel, suivant lequel la loi afférente ne qualifie en effet pas une telle donnée comme étant sensible. Il admet cependant que vu qu'un critère de race est impliqué, il n'est pas illogique d'y voir un caractère sensible et il est ainsi plutôt d'accord avec le représentant du DP pour dire qu'il faudrait au moins informer la personne concernée que cette donnée est saisie.

Il s'avère encore qu'à sa demande tout sportif peut être informé de la nature des données saisies qui le concernent, M. le Ministre tenant finalement à souligner qu'en aucun cas un but de discrimination a été visé par la saisie de l'origine.

Luxembourg, le 29 février 2012

Le Secrétaire,
Nicolas Bock

Le Président de la Commission de l'Education nationale, de la Formation professionnelle et des Sports,
Ben Fayot

Le Président de la Commission de l'Enseignement supérieur, de la Recherche, des Media, des Communications et de l'Espace,
Marcel Oberweis

Le Président de la Commission de la Fonction publique et de la Simplification administrative,
Norbert Haupert