**DÉCEMBRE 2015** **15_INT_421**

**RÉPONSE DU CONSEIL D'ETAT**
**à l'interpellation Lena Lio - Des logiciels informatiques de plus en plus intrusifs : le Canton a-t-il les moyens de se prémunir ?**

***Rappel de l'interpellation***

*La question de la sécurité des données traitées par ordinateur n'est pas nouvelle et a déjà conduit à de nombreux développements. Il apparaît toutefois qu'elle donne lieu à une évolution insidieuse débouchant sur une problématique nouvelle.*

*En effet, jusqu'à présent, les conseils donnés aux utilisateurs portaient surtout sur les moyens à mettre en œuvre pour se protéger contre les démarches de personnes extérieures au système, celles-ci cherchant à utiliser les réseaux pour s'infiltrer dans les ordinateurs et dans les serveurs, pour y récupérer des informations personnelles ou confidentielles. Afin de contrer ce type d'attaque, des logiciels d'antivirus, des mises à jour régulières et des règles à respecter en matière de mots de passe ou de stockage des sauvegardes semblaient devoir prémunir contre ces attaques malveillantes.*

*Or, il s'avère qu'aujourd'hui une source importante d'intrusion vient non plus de l'extérieur, mais des applications et des logiciels eux-mêmes qui sont conçus pour obtenir de l'information sur les utilisateurs. La mise en circulation récente du système d'exploitation Windows 10 a joué un rôle de détonateur à cet égard, du fait que les conditions générales d'utilisation (que tout un chacun est censé lire attentivement…) ne fait même plus mystère de ce genre de procédé :*

*" Nous accédons, divulguons et conservons les données personnelles, dont votre contenu tel que le contenu de vos courriels, d'autres communications privées ou des fichiers dans des dossiers privés. "*

*Cette " découverte " a provoqué diverses réactions : de la part du préposé fédéral à la protection des données (qui parle déjà d'actions contre Microsoft jusqu'au Tribunal fédéral) ou encore du préposé valaisan à la protection des données (qui va jusqu'à préconiser l'interdiction de vente de Windows 10 sur tout le territoire cantonal !). Les spécialistes font toutefois remarquer que Microsoft n'est pas le seul développeur qui s'intéresse aux données des utilisateurs, comme on peut bien le penser du fait des enjeux commerciaux que permettent ces pratiques : les antivirus qui scannent tous les fichiers présents en mémoire (prétendument pour y déceler des virus) ne sont pas en reste, ni les moteurs de recherches qui stockent les mots-clés utilisés, ni, mieux encore, les mots de passe que requièrent certains sites protégés (et cela prétendument pour épargner à l'utilisateur le souci d'introduire son mot de passe à chaque fois). Or, généralement, les conditions d'utilisation n'indiquent pas explicitement l'existence de ces procédés. À cet égard, Windows 10 est plus transparent, en précisant que les données personnelles ne sont pas seulement conservées, mais bien divulguées !*

*Pour utiliser une métaphore du domaine militaire (d'où provient, d'ailleurs, le principe des mots de passe) : ce n'est plus seulement l'ennemi qui cherche à découvrir notre mot de passe, c'est la*

*sentinelle qui l'enregistre pour aller le vendre au plus offrant !*

*Dans ces conditions, je pose les questions suivantes :*

- *Les systèmes d'exploitation et les logiciels utilisés par l'administration cantonale sont-ils évalués par rapport aux informations qu'ils peuvent obtenir sur les données traitées par l'utilisateur ?*
- *Les conditions d'utilisation rédigées par le fournisseur font-elles l'objet d'analyses techniques, voire de négociations, en vue de s'assurer que les intrusions dans les données de l'utilisateur se réduisent au minimum que nécessite le bon fonctionnement du système ?*
- *Le Conseil d'État a-t-il défini les critères de ce qui est acceptable en la matière ? Ces critères sont-ils coordonnés avec ceux admis dans d'autres cantons ?*

*Je remercie d'avance le Conseil d'État pour ses réponses.*

*Ne souhaite pas développer.*

**Réponse du Conseil d'Etat à l'interpellation Lena Lio - Des logiciels informatiques de plus en plus intrusifs : le Canton a-t-il les moyens de se prémunir ?**

**Préambule**

Dans son programme de législature 2012 – 2017, le Conseil d'Etat a confirmé sa volonté d'offrir à la population des prestations efficientes, grâce à des processus administratifs simplifiés et des services informatiques adaptés, performants et sûrs (mesure 5.1).

Dans un contexte caractérisé par la dépendance croissante aux systèmes d'information – ni la société ni l'Etat ne pourraient à l'heure actuelle fonctionner sans informatique - il est en effet indispensable de sécuriser les systèmes d'information (SI), pour protéger l'intégrité des données des citoyens et préserver la souveraineté de l'Etat. Ainsi, le Conseil d'Etat a adopté en 2011 une politique générale de sécurité des systèmes d'information (PGSSI-VD) dont les 5 axes sont :

1. Un système de management de la sécurité conforme aux meilleures pratiques ;
2. Une gestion des risques régulière, efficace et proportionnelle ;
3. Des mesures de sécurité conformes aux meilleures pratiques ;
4. Une exploitation et une évolution des SI conformes aux politiques de sécurité ;
5. Une mise en œuvre progressive et pragmatique.

En 2013, le Grand Conseil, sur proposition du Conseil d'Etat, a octroyé un crédit d'investissement de 8,6 millions de francs pour financer la mise en place de mesures de diminution du risque et de pilotage de la sécurité des SI au sein de la Direction des systèmes d'information (DSI).

Ainsi, grâce à ce financement, une analyse des risques la plus complète possible a été lancée en vue d'une part d'estimer les risques qui n'ont pas encore été pris en compte et, d'autre part, de s'assurer de la complétude du périmètre.

Sur la base des analyses et évaluations d'ores et déjà effectuées, la DSI s'est attelée à diminuer les risques les plus critiques, en parallèle au déploiement d'un système de management de la sécurité des systèmes d'information (SMSI) qui définit les processus de sécurité applicables selon les normes internationales. Fin 2014, un Centre de Sécurité Opérationnelle (SOC) a été mis en place, ce qui permet d'avoir une vision exhaustive des flux de données entrant et sortant du système d'information de l'Administration.

Dans ce contexte, la DSI a identifié le risque soulevé par l'interpellatrice, à savoir le risque de détournement ou vol de données à des fins de renseignement économique, mais après analyse, ce risque n'a pas été classifié comme élevé, au regard de sa probabilité et de son impact sur les activités de l'Etat.

*Réponses aux questions*

*Question 1. Les systèmes d'exploitation et les logiciels utilisés par l'administration cantonale sont-ils évalués par rapport aux informations qu'ils peuvent obtenir sur les données traitées par l'utilisateur ?*

Dans le cadre de ses activités opérationnelles, la DSI recourt à l'observation attentive (veille technologique, centre de sécurité opérationnelle) et à l'utilisation d'outils spécifiques d'audit des mécanismes logiques d'une application ou d'un système. Concrètement, les processus d'industrialisation de la distribution et de l'installation des logiciels et des systèmes d'exploitation sont menés par les ingénieurs de la DSI de manière rigoureuse, conformément aux bonnes pratiques dans le domaine.

Par ailleurs, en raison de la taille importante du parc informatique de l'Etat, les changements de versions et les évolutions technologiques sont introduits sur les postes de travail dans un laps de temps permettant la mise en lumière des fonctionnalités controversées de logiciels et systèmes d'exploitation, soit qu'elles sont explicitées par l'entreprise mettant le logiciel ou le système d'exploitation sur le marché elle-même, soit qu'elles sont découvertes par les milieux informatiques, comme c'est le cas pour la dernière version du système d'exploitation Windows 10 de Microsoft évoquée par l'interpellatrice.

Le Conseil d'Etat rappelle dans ce contexte que la migration technique des postes de travail en cours à l'ACV, pour laquelle le Grand Conseil a accordé un crédit d'investissement de 7.94 millions de francs en 2014 vise non seulement à la modernisation des postes de travail mais également à leur sécurisation. En effet, le financement octroyé permet l'acquisition de nouveaux logiciels et licences, et de développer des prestations de service qui y sont liées, et notamment le support et le soutien aux utilisateurs.

Dans le cadre de son activité, la DSI diffuse en effet des directives de sécuritédétaillant précisément les usages admis et ceux qui sont proscrits, en parallèle à la promotion des solutions techniques évitant les problèmes de confidentialité et d'intégrité des données. Les utilisateurs finaux bénéficient également de sensibilisations et formations, généralement facultatives, dédiées à la sécurité de l'information et à l'utilisation sûre des outils informatiques.

La migration en cours permet ainsi d'assurer une maîtrise suffisante des postes de travail garantissant des niveaux de sécurité adéquats pour les évolutions à venir des systèmes d'information.

*Question 2. Les conditions d'utilisation rédigées par le fournisseur font-elles l'objet d'analyses techniques, voire de négociations, en vue de s'assurer que les intrusions dans les données de l'utilisateur se réduisent au minimum que nécessite le bon fonctionnement du système ?*

Les négociations qui sont menées avec les éditeurs/fournisseurs de logiciels portent en priorité sur les prix d'acquisition et de maintenance. Si nécessaire, notamment au regard de la protection des données, des discussions peuvent également porter sur les conditions générales, mais avec les grandes entreprises fournissant les logiciels de bureautique, de gestion de bases de données ou encore les microprogrammes gérant les composants matériel, la marge de négociation est très limitée voire inexistante. Dans le domaine, en effet, s'il s'avère que les conditions générales contiennent des clauses défavorables au client, ce dernier n'a en pratique que peu de choix possibles. Il s'agit avant tout de mesurer le risque encouru et de décider, ensuite, de l'option à retenir : utiliser tout de même le logiciel car le coût d'utilisation peut être avantageux ou mettre en place un plan de remplacement, cette option pouvant coûter extrêmement cher en termes d'adaptation du patrimoine applicatif d'une part et d'exploitation et de compatibilité d'autre part.

*Question 3.Le Conseil d'État a-t-il défini les critères de ce qui est acceptable en la matière ? Ces critères sont-ils coordonnés avec ceux admis dans d'autres cantons ?*

La politique générale de sécurité des systèmes d'information de l'Etat de Vaud, approuvée par le

Conseil d'Etat, ainsi que les politiques, directives et décisions de sécurité qui en découlent fixent les règles et critères de sécurité applicables. L'Administration cantonale vaudoise applique le plus strictement possible les standards et bonnes pratiques internationaux en termes de sécurité de l'information.

Comme indiqué ci-dessus, une gestion des risques informatiques est en phase de mise en œuvre au sein de la DSI ; elle implique une analyse permanente des menaces, impacts et probabilités de survenance. Cette gestion des risques continue comprend aussi la mise en place de mesures proportionnées visant à réduire les risques (mesures de mitigation), tenant compte des moyens disponibles (compétences et ressources internes et externes).

Sur le plan fédéral, la Confédération et les cantons ont développé des critères communs en cas de cyber-incidents de sécurité, liés par exemple à la cybercriminalité ou au cyberespionnage afin de permettre la qualification et la transmission d'informations à des tierces parties pour la résolution de la problématique. Cette approche de maîtrise du risque comprend là encore une partie importante de mesures de sensibilisation et de formation à la fois des informaticiens et de l'ensemble des usagers des administrations en termes de sécurité de l'information.

Dans ce contexte, la CSI/SIK (Conférence suisse de l'informatique, groupe " CSI/SIK latin ", qui inclut les cantons de Vaud, Genève, Tessin, Jura, Neuchâtel, Fribourg et Valais) a inscrit dans ses objectifs annuels 2015 et 2016 des collaborations sur ce thème, matérialisées par un cours commun (e-learning) de sensibilisation à la sécurité de l'information et à l'e-réputation, à destination de l'ensemble des 80'000 utilisateurs des administrations cantonales latines. De même, les membres de la CSI/SIK procèdent régulièrement à des partages d'informations, de modes opératoires et de problématiques notamment sécuritaires.

En conclusion, le Conseil d'Etat rappelle que dans le cadre de sa mission de base, la DSI veille en permanence à assurer les conditions nécessaires permettant de garantir que les informations des services métiers soient protégées contre l'intrusion logique et physique, la perte, la soustraction, l'accès non autorisé, la divulgation, la panne et l'erreur. La montée en puissance de la gestion des risques informatiques s'inscrit dans cette volonté d'amélioration continue de la maîtrise de la qualité des prestations, du bon fonctionnement et de l'évolution du patrimoine informatique, conformément aux bonnes pratiques en la matière.

Ainsi adopté, en séance du Conseil d'Etat, à Lausanne, le 16 décembre 2015.

| Le président : | Le chancelier : |
| --- | --- |
| *P.-Y. Maillard* | *V. Grandjean* |