Intervention parlementaire. Réponse du Conseil-exécutif

N° de l'intervention:	115-2016
Type d'intervention:	Interpellation
Motion ayant valeur de directive:	☐
N° d'affaire:	2016.RRGR.593
Déposée le:	05.06.2016
Motion de groupe:	Non
Motion de commission:	Non
Déposée par:	Graber (La Neuveville, UDC) (porte-parole)
Cosignataires:	0
Urgence demandée:	Non
Urgence accordée:	
N° d'ACE:	1378/2016 du 7 décembre 2016
Direction:	Direction des finances
Classification:	–

Sécurité des données numériques

Le 12 mai 2016, les médias ont révélé que des données très confidentielles de la Confédération stockées chez RUAG avaient sans doute été interceptées par des hackers dans le cadre d'une cyber-attaque. Cet incident hautement regrettable a pu se produire parce que l'Office fédéral de l'informatique et des télécommunications (OFIT) a transféré l'an dernier l'ensemble des données du personnel de la Confédération chez RUAG, société privée dont la Confédération est l'actionnaire unique. Des noms d'agents du renseignement pourraient être en mains étrangères.

Cet évènement pose, une fois de plus, le problème de la sécurité des données informatiques détenues et traitées par des corporations de droit public.

Il est essentiel que les personnes dont les données sont enregistrées, traitées et conservées par l'administration cantonale puissent avoir l'assurance que ces données soient entièrement sécurisées et qu'elles ne puissent pas faire l'objet d'une malencontreuse interception par des individus ou des groupements animés par des desseins délictueux et inavouables.

L'épisode des données de la Confédération qui ont pu être portées à la connaissance d'individus non autorisés à y avoir accès nous incite à poser les questions suivantes au Conseil-exécutif :

1. Où sont stockées les données numériques des habitants du canton de Berne, celles des agents de la fonction publique et encore celles qui concernent d'autres catégories de la population que les autorités cantonales possèdent légitimement et légalement ?

2. Quelles mesures le Conseil-exécutif a-t-il prises pour assurer la non-transmission de ces données à des individus ou à des groupements non habilités à y avoir accès ?

3. L'incident survenu au détriment de la Confédération a-t-il engagé le Conseil-exécutif à prévoir des mesures supplémentaires pour assurer la sécurité des données numériques en sa possession ?

Remarque complémentaire : Il est évident que nous ne souhaitons pas obtenir du Conseil exécutif des informations qu'il ne peut pas nous donner pour des raisons de sécurité.

Réponse du Conseil-exécutif

Question 1 :

Un grand nombre d'applications de l'administration utilisent des données personnelles. Ces applications se répartissent en trois catégories :

- Les applications spécialisées sont utilisées pour assister des processus administratifs spécialisés ou pour répondre à des exigences particulières.
- Les applications de groupe assistent des processus administratifs essentiels et répondent à des exigences générales. Elles sont à la disposition de toute l'administration.
- Les services de base TIC (technologies de l'information et de la télécommunication) servent à l'ensemble de l'administration. Ils comprennent les systèmes et les prestations TIC dans les domaines des postes de travail, des réseaux et des communications, y compris les serveurs requis pour l'exploitation de toutes les applications.

La responsabilité des applications spécialisées et des applications de groupe incombe à la Direction ou à l'office spécialisé qui les utilise, tandis que la responsabilité des systèmes TIC centraux et des services TIC de base incombe à l'Office d'informatique et d'organisation (OIO).

Le Conseil-exécutif a déjà indiqué, dans sa réponse à l'interpellation 297-2013, Sancar (Berne, Les Verts) intitulée « Où sont stockées les données sensibles du canton de Berne ? », qu'une grande partie des données sensibles de l'administration, à savoir les données relatives au personnel, aux finances et aux impôts ainsi que les données harmonisées des registres des habitants et des électeurs, sont traitées et stockées dans les centres de calcul suisses de la société Bedag Informatique SA, qui appartient au canton. Un registre central des fichiers accessible au public fournit des indications sur les fichiers du canton.

La Stratégie TIC 2016 – 2020 du canton de Berne prévoit l'exploitation centralisée de toutes les applications de l'administration. Cette prestation est fournie par l'OIO dans le cadre des services de base TIC, au moyen de plateformes d'applications qui sont actuellement exploitées par la société cantonale Bedag Informatique SA sur différents sites en Suisse. C'est seulement avec

l'achèvement du programme IT@BE, prévu en 2021, que le canton pourra mettre en œuvre la Stratégie TIC, donc migrer toutes les applications vers les plateformes centralisées et créer un portefeuille d'applications offrant une vue d'ensemble de toutes les applications. Et c'est seulement à ce moment-là qu'il sera possible d'indiquer le lieu où sont traitées toutes les données de l'administration. Mais comme la Stratégie TIC exempte la Police cantonale et les écoles relevant du domaine de compétences de la Direction de la santé publique et de la prévoyance sociale de l'obligation d'utiliser les services de base, il sera impossible même à l'avenir de fournir des informations centralisées sur le traitement des données de ces organisations.

Question 2 :

L'autorité responsable qui traite des données personnelles ou qui met à disposition un réseau télématique assure par des mesures techniques et organisationnelles la confidentialité, la disponibilité et l'exactitude des données. Les exigences techniques et organisationnelles sont énoncées aux articles 4 et 5 de l'ordonnance du 22 octobre 2008 sur la protection des données (OPD, RSB 152.040.1). Garantir la sûreté de l'information et la protection des données (SIPD) incombe à l'autorité responsable qui, pour accomplir les tâches que lui assigne la loi, traite des données personnelles ou en confie le traitement à des tiers.

La législation sur la protection des données et les prescriptions SIPD de l'administration prévoient que le service responsable réalise une analyse SIPD pour déterminer s'il existe un besoin de protection poussée. Si tel est le cas, il élabore un concept SIPD dans lequel il définit qui peut accéder à quelles données et de quelle manière, et quelles mesures de protection de l'information il faut adopter. Dans les cas prévus par la législation où il existe un risque SIPD particulièrement élevé, le Bureau cantonal pour la surveillance de la protection des données (organe indépendant) vérifie de plus dans le cadre d'une procédure de contrôle préalable, avant que ne débute le traitement des données, si la législation sur la protection des données et les prescriptions SIPD sont respectées.

En plus de cette vérification du respect des prescriptions SIPD et de la législation sur la protection des données, les prestataires TIC externes auxquels est confiée l'exécution de mesures techniques et organisationnelles doivent en règle générale garantir, dans le cadre de conventions contractuelles standard passées avec le canton, le respect de clauses de confidentialité et d'autres obligations visant à empêcher toute utilisation frauduleuse de données et dont la violation entraînerait des peines conventionnelles.

Question 3 :

L'incident évoqué n'a pas entraîné l'adoption de mesures supplémentaires car, même auparavant, l'OIO surveillait déjà, avec les Directions, continuellement la situation en matière de sûreté de l'information. Avec le concours de ses fournisseurs, en particulier Bedag Informatique SA (centre de calcul), SPIE ICS (réseaux) et Swisscom (téléphonie), il a déjà mis en œuvre – ou est en train de réaliser – différentes mesures techniques et organisationnelles pour améliorer la sécurité. Il s'agit notamment des mesures suivantes :

- Une importance croissante est accordée à la sensibilisation des agents et agentes et à leur formation aux exigences en matière de sécurité et de protection des données.

- Le contrôle permanent ainsi que l'amélioration et le développement continus des systèmes de sécurité est une tâche permanente de l'organisation TIC du canton.

- Bedag Informatique SA, société qui exploite les plateformes d'applications du canton, est certifiée selon la norme internationale ISO/CEI 27001. Cette norme règlemente les exigences relatives aux systèmes de gestion de la sécurité de l'information (SGSI). Avec la certification ISO/CEI 27001, une organisation apporte la preuve qu'elle met en œuvre des mesures adéquates, aux plans technique et organisationnel, pour garantir un niveau de sécurité approprié dans l'exploitation des TIC.

- En sa qualité de prestataire de services de base TIC, l'OIO devrait obtenir lui aussi la certification selon cette norme dès 2017. Tous les aspects concernant la sécurité des services de base TIC du canton seront dès lors gérés par un SGSI garantissant le recensement et le traitement systématiques des risques en matière de sécurité.

- S'il est impossible d'exclure intégralement tout risque résiduel et tout accès illicite aux données, ils sont toutefois réduits à un minimum acceptable dans le canton de Berne grâce aux mesures organisationnelles et techniques appliquées.

Destinataire
- Grand Conseil