Intervention parlementaire

Réponse du Conseil-exécutif

N° de l'intervention :	274-2022
Type d'intervention :	Interpellation
Motion ayant valeur de directive :	☐
N° d'affaire :	2022.RRGR.414
Déposée le :	06.12.2022
Motion de groupe :	Non
Motion de commission :	Non
Déposée par :	Gerber (Hinterkappelen, Les Verts) (porte-parole) Riesen (La Neuveville, ES)
Cosignataires :	0
Urgence demandée :	Non
Urgence accordée :	
N° d'ACE :	569/2023 du 17 mai 2023
Direction :	Direction des finances
Classification :	Non classifié

Que se passe-t-il avec nos données qui se trouvent sur des supports obsolètes ?

Comme l'a rappelé une fois de plus une affaire zurichoise, où des données sensibles des autorités judiciaires se seraient retrouvées aux mains de personnes mal intentionnées après l'élimination de supports de données, la question de la gestion correcte des données se pose avec une acuité particulière dans le contexte numérique. Même si la plupart des données étaient cryptées, celles-ci ont pu être récupérées sur des ordinateurs mis au rebut.

Le Conseil-exécutif est prié de répondre aux questions suivantes :

1. Que se passe-t-il avec les données stockées sur un ordinateur ou un serveur dont on se débarrasse ?
2. Le canton stocke des données chez des prestataires de services du secteur privé. Comment le Conseil-exécutif s'assure-t-il que les données stockées sur des serveurs qui ont fait leur temps ne tombent pas ensuite dans des mains inconnues ou mal intentionnées ?
3. Qui est responsable de la sécurité des données, de leur élimination ou de leur destruction ?
4. Que sait le Conseil-exécutif du commerce de données sur des serveurs hors d'usage en rapport avec leur utilisation à des fins criminelles ?
5. Quelles sont les mesures concrètes prises par le canton de Berne pour éviter qu'un cas comme celui qui s'est produit à Zurich ne puisse également se produire dans les administrations bernoises ?
6. Comment se passait la mise au rebut d'ordinateurs et de serveurs hors d'usage il y a dix ans ?

12|00|F|v03

Réponse du Conseil-exécutif

L'affaire zurichoise à laquelle l'interpellation fait allusion témoigne du risque croissant que la numérisation d'un nombre toujours plus grand de domaines de la vie et de l'administration fait peser sur la sécurité de l'information et sur la cybersécurité. Le Conseil-exécutif est conscient de ces dangers, et le projet IS@BE en cours vise à actualiser et à améliorer les bases juridiques, techniques et organisationnelles de la sécurité de l'information dans l'administration cantonale. Le projet va déboucher sur la loi sur la sécurité de l'information et la cybersécurité (LSIC) – qui était récemment en procédure de consultation – et sur un système de gestion de la sécurité de l'information (SGSI) pour l'administration cantonale obéissant à la norme internationale ISO-27001.

C'est dans ce contexte que le Conseil-exécutif répond comme suit aux questions posées :

1. *Que se passe-t-il avec les données stockées sur un ordinateur ou un serveur dont on se débarrasse ?*

   Ces données doivent être effacées de manière irrémédiable. Les autorités responsables vérifient pour chaque projet si des données personnelles ou autres informations dignes de protection sont concernées. Le cas échéant, elles passent avec des prestataires externes des contrats fixant les mesures nécessaires à la suppression sûre des données des autorités qui ne sont plus nécessaires ou à la destruction des supports de données devenus inutiles.

2. *Le canton stocke des données chez des prestataires de services du secteur privé. Comment le Conseil-exécutif s'assure-t-il que les données stockées sur des serveurs qui ont fait leur temps ne tombent pas ensuite dans des mains inconnues ou mal intentionnées ?*

   Les entreprises privées mandatées par des autorités cantonales pour traiter des données pour le compte du canton de Berne doivent s'engager par contrat à effacer ces données de manière irrémédiable lorsqu'elles ne sont plus nécessaires ou à détruire leurs supports (voir réponse à la question 1).

   Des contrats de ce type ont ainsi été conclus avec les sous-traitants fournissant des services TIC de base de l'administration cantonale, comme la SA Bedag Informatique, qui exploite le centre de calcul, le prestataire de services d'imprimerie Ricoh et le fournisseur de terminaux Business IT. Comme les plans de sécurité de l'information et de protection des données, les contrats prévoient que les données doivent être supprimées ou détruites selon des normes reconnues, que cette opération doit être consignée par écrit et qu'elle peut être contrôlée par le mandant et/ou par des autorités de surveillance.

   Les supports de données actuels sont cependant nettement mieux protégés au plan technique que ceux qui ont manifestement été perdus à Zurich il y a 10 ans. Aujourd'hui par exemple, le disque dur des ordinateurs portables est crypté par défaut et, sur les serveurs, les données sont réparties sur plusieurs disques durs de sorte qu'il est impossible de les reconstruire à partir d'un seul. Cela réduit donc nettement le risque de fuite d'informations en cas de perte de supports de données.

3. *Qui est responsable de la sécurité des données, de leur élimination ou de leur destruction ?*

   La responsabilité incombe aux Directions et aux offices qui traitent les données ou qui externalisent leur traitement.

4. *Que sait le Conseil-exécutif du commerce de données sur des serveurs hors d'usage en rapport avec leur utilisation à des fins criminelles ?*

   Le Conseil-exécutif ne sait rien à ce sujet.

5. *Quelles sont les mesures concrètes prises par le canton de Berne pour éviter qu'un cas comme celui qui s'est produit à Zurich ne puisse également se produire dans les administrations bernoises ?*

   Comme mentionné plus haut, il mène à bien le projet IS@BE, qui consiste notamment à vérifier les règles régissant la protection de base en matière de sécurité de l'information, à les impulser ou à les mettre à jour, cela incluant les normes de suppression sûre des données et les exigences à remplir par les prestataires de services de stockage en nuage.

   Les agentes et agents cantonaux sont régulièrement sensibilisés aux risques pesant sur la sécurité de l'information et aux méthodes à appliquer pour l'améliorer, par le biais par exemple de l'Instruction régissant l'emploi des TIC par les utilisateurs et utilisatrices finals dans l'administration cantonale bernoise, de la formation BE-Secure et d'une campagne annuelle de sensibilisation à l'hameçonnage consistant à tester les agentes et agents sur leur capacité à repérer les courriels pouvant être à l'origine de cyberattaques et à y réagir correctement.

   Dans le cadre du contrôle préalable prévu par la loi sur la protection des données, le Bureau cantonal pour la surveillance de la protection des données (BPD) prend position, avant leur mise en service, sur les plans de sécurité de l'information et de protection des données concernant des systèmes informatiques cantonaux qui présentent des risques particuliers. Il procède également à des audits de certains systèmes déjà en service. Le contrôle préalable du BPD consiste notamment à vérifier les plans (objectif). Des contrôles sont ensuite nécessaires pour s'assurer que ces plans sont correctement appliqués (réalité).

6. *Comment se passait la mise au rebut d'ordinateurs et de serveurs hors d'usage il y a dix ans ?*

   À l'époque, l'informatique était largement décentralisée dans l'administration cantonale. Chaque office et chaque Direction définissait sa propre approche en la matière. Il est donc impossible de répondre à cette question de manière générale pour l'ensemble de l'administration cantonale.

Destinataire
– Grand Conseil