Intervention parlementaire

Réponse du Conseil-exécutif

N° de l'intervention :	166-2023
Type d'intervention :	Interpellation
Motion ayant valeur de directive :	☐
N° d'affaire :	2023.RRGR.232
Déposée le :	22.08.2023
Motion de groupe :	Non
Motion de commission :	Non
Déposée par :	Reinhard (Thun, PLR) (porte-parole)
Cosignataires :	0
Urgence demandée :	Oui
Urgence accordée :	Non 12.09.2023
N° d'ACE :	167/2024 du 21 février 2024
Direction :	Direction des finances
Classification	Non classifié

Sécurité des données et sauvegarde des données

Dans notre monde de plus en plus connecté, la sécurité des données et la stratégie de sauvegarde des données sont des thèmes capitaux qui concernent à la fois l'administration publique et les milieux économiques.

Les annonces quotidiennes dans les médias de piratages ou de fuites de données incitent à penser que tous les problèmes pourraient être résolus si toutes les données étaient stockées sur un serveur propre. Le choix entre la sauvegarde des données sur un serveur propre ou dans un nuage informatique est bien plus qu'un choix d'ordre technique : en effet, il a des répercussions importantes sur la sécurité, la conformité et l'efficience de notre infrastructure numérique. Le canton de Berne fait face au défi de développer une stratégie qui réponde aussi bien aux exigences de notre temps qu'aux évolutions à venir. La sauvegarde actuelle des données auprès de la BEDAG et la transmission sécurisée entre les utilisatrices et utilisateurs et le serveur ne constituent qu'une partie du tableau. Le choix entre un serveur propre et une solution infonuagique requiert une pesée des intérêts minutieuse entre responsabilités, risques et opportunités. Les principaux risques se situent au niveau de la transmission des données entre l'utilisateur ou le terminal et leur sauvegarde, d'où la nécessité d'un cryptage efficient. Un autre risque non négligeable est l'être humain lui-même. Si l'on croit, par exemple, que les données figurant dans un nuage Microsoft peuvent être lues par une personne non autorisée, il faut savoir que c'est également le cas avec la solution actuelle. La technologie infonuagique offre flexibilité et extensibilité, mais elle requiert aussi une stratégie claire en matière de cryptage, de conformité et de gestion des risques. Le choix d'un prestataire de nuage informatique, qu'il se trouve en Suisse ou à l'étranger, doit donc se fonder sur une analyse détaillée des besoins et des exigences réglementaires.

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

1. Est-il judicieux que chaque canton évalue de façon individuelle si le recours à des prestataires infonuagiques est possible et dans quelles conditions ? Un échange a-t-il déjà eu lieu à ce sujet avec d'autres cantons ou avec la Confédération ? Pourrions-nous tirer parti des expériences faites par d'autres cantons ou la Confédération ?

2. Comment s'articulent la coopération et la communication avec l'Administration numérique suisse (ANS) en lien avec ce sujet ?

3. Qui, au sein du canton de Berne, est compétent pour l'évaluation des risques liés à l'utilisation de services infonuagiques par l'administration cantonale ?

4. Sur quels critères cette évaluation des risques repose-t-elle ?

5. Quels sont les résultats de l'évaluation des risques ? Quels sont les résultats de l'évaluation des risques de la chaîne logistique lors de l'utilisation de services infonuagiques (prestataire actuel inclus) ?

6. Qui, en fin de compte, est responsable de la sécurité des données et de la protection des données au sein du canton lors de l'utilisation de services infonuagiques ? Comment le respect des règles fixées est-il contrôlé ?

7. À quels indicateurs-clés de performance recourt-on pour vérifier que l'utilisation de services infonuagiques est sécurisée et efficiente ?

8. Que pense le canton de l'applicabilité aux affaires cantonales de la nouvelle loi fédérale sur la protection des données ?

Motivation de l'urgence : actuellement, de nombreux projets informatiques sont en cours ou recommandés en vue de leur acquisition. Ces questions aident à créer une évaluation en vue de la prise de décision en lien avec des projets à venir. Finalement, la transparence contribue aussi au sentiment de sécurité de la population.

Réponse du Conseil-exécutif

Comme l'auteur de l'interpellation, le Conseil-exécutif pense en effet que la numérisation croissante de la société, de l'économie et de l'administration complique la sécurité de l'information, qu'il est nécessaire de s'attaquer au problème sous l'angle des risques et que la solution la plus efficace pour s'en emparer est de s'associer à d'autres autorités. Face à ce défi, le Conseil-exécutif a soumis un projet de loi sur la sécurité de l'information et la cybersécurité (LSIC) au Grand Conseil en août 2023. Étant donné que la documentation relative à ce texte (cf. www.be.ch/lsic) fournit des explications approfondies, le Conseil-exécutif se bornera ici à des réponses succinctes.

1. *Est-il judicieux que chaque canton évalue de façon individuelle si le recours à des prestataires infonuagiques est possible et dans quelles conditions ?*

   Bien que cette question et d'autres ne portent que les prestataires de services en nuage, le Conseil-exécutif estime que le souci de sécurité de l'information que soulève l'interpellation se pose de la même manière pour tout traitement de données que les autorités confient à des tiers, que ceux-ci fournissent leur service en nuage ou dans des centres de calcul conventionnels. À ces yeux, la véritable question à se poser est donc la suivante : dans quelles conditions de sécurité et de protection des données les autorités externalisent-elles le traitement de données, que ce soit en nuage ou non ?

Dans une perspective sécuritaire, il y a effectivement peu d'intérêt à ce que les cantons et la Confédération les définissent chacun de leur côté, d'autant moins que les risques et les conditions générales sont les mêmes partout. Une uniformisation nationale de la réglementation légale de la sécurité de l'information et de la protection des données (SIPD) simplifierait nettement la formation du personnel ainsi que l'application et le contrôle des règles. Malheureusement, aucune disposition de la Constitution fédérale ne fonde une harmonisation en la matière. En conséquence, le Conseil-exécutif se mobilise pour que les cantons et la Confédération légifèrent dans ce domaine en se concertant et en se fondant sur les normes nationales et internationales.

Un échange a-t-il déjà eu lieu à ce sujet avec d'autres cantons ou avec la Confédération ? Pourrions-nous tirer parti des expériences faites par d'autres cantons ou la Confédération ?

Les autorités bernoises responsables de la sécurité et de la protection des données échangent en permanence avec leurs homologues de la Confédération et des autres cantons, afin de tirer parti de leurs expériences.

2. *Comment s'articulent la coopération et la communication avec l'Administration numérique suisse (ANS) en lien avec ce sujet ?*

   L'ANS est en cours de création. Elle dispose cependant déjà d'un groupe de travail sur la sécurité de l'information et sur la cybersécurité, qui est chargé de définir des règles de bonnes pratique, d'évaluer les aspects sécuritaires des nouvelles technologies et tendances et de formuler des recommandations de minimisation des risques.

3. *Qui, au sein du canton de Berne, est compétent pour l'évaluation des risques liés à l'utilisation de services infonuagiques par l'administration cantonale ?*

   La SIPD, et avec elle l'évaluation des risques, relèvent de la responsabilité des autorités qui traitent des données ou en externalisent le traitement. Ce sont notamment l'Office d'informatique et d'organisation (OIO), dans le cadre de la fourniture des services TIC de base (p. ex. réseau cantonal, poste de travail cantonal), les offices de l'administration cantonale, pour les applications spécialisées et les applications de groupe dont ils sont responsables, et les autres autorités dans le canton (comme les communes, les hautes écoles, les établissements), pour les outils TIC qu'elles utilisent.

4. *Sur quels critères cette évaluation des risques repose-t-elle ?*

   Les risques sont mesurés en fonction de leur probabilité d'occurrence et de l'ampleur des dommages pouvant être causés au bien protégé, à savoir les intérêts publics à défendre ou les droits fondamentaux des personnes concernées. Cette ampleur varie en fonction des objectifs de protection de la sécurité de l'information (confidentialité, disponibilité, intégrité) et de la protection des données (confidentialité, exactitude, conformité légale, proportionnalité) ainsi que des autres dommages potentiels, comme les préjudices financiers ainsi que les atteintes aux personnes, aux droits de la personnalité, aux biens ou à la réputation. La mesure des risques consiste également à évaluer la possibilité de contrôler les dispositifs définis pour écarter les risques (dits bruts) ou les réduire à un niveau acceptable (risques résiduels).

5. *Quels sont les résultats de l'évaluation des risques ?*

   L'autorité responsable (cf. réponse à la question 3) doit mesurer les risques de tout projet de traitement de données ou d'outil TIC, quels qu'en soient les objectifs et les conditions générales. La mesure des risques n'est donc pas une démarche générale dont on peut présenter les résultats ici. Les risques résiduels liés à l'installation de M365 dans toute l'administration cantonale ont été présentés dans un rapport au Conseil-exécutif, qui les a acceptés le 30 juin 2023[1].

   Quels sont les résultats de l'évaluation des risques de la chaîne logistique lors de l'utilisation de services infonuagiques (prestataire actuel inclus) ?

   Comme les autres, les risques liés à la chaîne logistique (c'est-à-dire le risque d'interruption de de services en raison de perturbations dans les chaînes d'approvisionnement) doivent être évalués au cas par cas. De par leur taille, leur implantation géographique globale et leur capacité de mise à l'échelle des performances, les grands fournisseurs internationaux de services en nuage (dits « géants du cloud ») sont en principe moins exposés à ces risques que les autres.

6. *Qui, en fin de compte, est responsable de la sécurité des données et de la protection des données au sein du canton lors de l'utilisation de services infonuagiques ?*

   Cf. réponse à la question 3 ci-dessus. La responsabilité de la protection des données incombe à l'autorité qui, pour accomplir les tâches que lui assigne la loi, traite ou fait traiter des données personnelles (art. 8 LCPD). L'OIO, qui est chargé de fournir les services TIC de base à l'administration cantonale, doit garantir qu'ils sont propres à une utilisation sécurisée et conforme au droit, mais c'est aux Directions et offices qui utilisent ces services de veiller à ce que la sécurité et la protection des données soient effectivement respectées.

   Comment le respect des règles fixées est-il contrôlé ?

   Les autorités responsables vérifient que les prestataires de services respectent les normes de SIPD en définissant, par contrat, des instruments de contrôle adaptés, comme
   - l'obligation, pour le prestataire, de rendre régulièrement compte des mesures de sécurité mises en place et des incidents de sécurité rencontrés ;
   - la publication, par le prestataire, de rapports d'audit et d'autres documents relatifs à la sécurité ;
   - la réalisation d'audits de sécurité auprès du prestataire.

7. *À quels indicateurs-clés de performance recourt-on pour vérifier que l'utilisation de services infonuagiques est sécurisée et efficiente ?*

   Les indicateurs de performance (*indicateurs clés de performance*, ICP) sont définis au cas par cas en fonction des besoins. Parmi eux figurent la disponibilité, plus exactement le taux de défaillance maximum, et le temps de réaction et de réparation en cas de panne. Toutefois, la fourniture de services en nuage est par nature très standardisée et non pas adaptée aux besoins spécifiques du client, de sorte que celui-ci n'a souvent que peu de marge de manœuvre pour fixer des ICP.

[1] Communiqué de presse et rapport (en allemand), cf. L'administration cantonale bernoise adopte Microsoft 365

8. *Que pense le canton de l'applicabilité aux affaires cantonales de la nouvelle loi fédérale sur la protection des données ?*

   Même dans sa dernière version du 25 septembre 2020, la loi fédérale sur la protection des données (LPD) ne s'applique pas au traitement de données par les autorités cantonales ou communales : elle régit le traitement de données par des personnes privées et par des organes fédéraux (art. 2, al. 1 LPD). La protection des données traitées par des autorités cantonales ou communales relève donc de la loi cantonale sur la protection des données (LCPD).

Destinataire
– Grand Conseil