Le Grand Conseil du canton de Berne **Der Grosse Rat des Kantons Bern**

Mercredi (après-midi) 11 juin 2014

Interpellations de la Direction des finances

124 2013.1491 Interpellation 297-2013 Sancar (Berne, Les Verts)
Où sont stockées les données sensibles du canton de Berne?

N° de l'intervention:	297-2013
Type d'intervention:	Interpellation
Déposée le:	14.11.2013
Déposée par:	Sancar (Berne, Les Verts) (porte-parole)
Cosignataires:	0
N° d'ACE:	600/2014 du 7 mai 2014
Direction:	Direction des finances

Où sont stockées les données sensibles du canton de Berne?

Avec la numérisation et l'accumulation d'énormes quantités de données enregistrées surgissent de nouveaux problèmes relatifs à la protection des données. Un grand nombre d'entreprises privées et d'administrations stockent leurs données ultra-confidentielles et ultra-sensibles sur l'aide sociale, les procédures de justice, les impôts, les profils des clients et clientes, etc. dans des solutions dites « de nuage ». Cela signifie que les données et les programmes sont enregistrés sur des serveurs, qui généralement ne se trouvent pas en Suisse mais sont accessibles en permanence depuis Internet. Les données ultra-confidentielles et ultra-sensibles ne peuvent être déposées dans un nuage qu'à condition que la confidentialité soit garantie, c'est-à-dire que le cryptage du fournisseur de nuage empêche l'accès à ces données. Plus les données sont sensibles, plus les exigences organisationnelles, techniques et juridiques du service doivent être vastes.
Comme on le sait, les services secrets américains (NSA) interceptent des flux de données à grande échelle. D'autres services secrets le font certainement aussi. C'est pourquoi nous aimerions savoir où sont stockées les données cantonales et avec quelles mesures de sécurité, comment la confidentialité est assurée et comment les exigences bernoises de protection sont remplies.
Le Conseil-exécutif est donc prié de répondre aux questions suivantes :
1. Où les données ultra-sensibles et ultra-confidentielles du canton de Berne sont-elles stoc-kées?
2. Sait-on où sont traitées ces données et les changements de lieu sont-ils annoncés et autorisés ?
3. Qui a accès à quelles données ? Comment l'accès est-il réglementé afin que les données sensibles ne puissent pas être piratées (double contrôle, organes de contrôle, etc.) ?
4. Le niveau de protection des données appliqué à l'étranger lors du traitement des données satisfait-il aux exigences suisses ou a-t-on convenu de mesures supplémentaires ? Si oui, quelles sont-elles ?
5. Est-ce que le droit applicable est compatible avec le droit suisse ?
6. Où se trouve le for ? Qu'adviendrait-il si le for se trouvait à l'étranger et quels seraient les coûts d'un tel transfert ?
7. Combien coûte le stockage des données garantissant la confidentialité et combien coûte le stockage en nuage?
8. Le délégué à la protection des données est-il associé au stockage en ligne ?
9. A combien le Conseil-exécutif évalue-t-il le risque associé au stockage en ligne et que pense-t-il faire, le cas échéant, pour empêcher qu'il ne soit autorisé pour les données ultra-sensibles ?

Réponse du Conseil-exécutif

Question 1 :
Les technologies de l'information et de la communication (TIC) de l'Administration cantonale sont actuellement gérées de manière décentralisée. Tandis que l'Office d'informatique et d'organisation

(OIO) fournit certaines prestations transversales, les Directions et la Chancellerie d'Etat (ou une partie de leurs offices) ainsi que la Justice et les entreprises et établissements cantonaux sont seuls responsables de leur approvisionnement de base en TIC et de l'exploitation de leurs applications techniques, y compris en ce qui concerne la sécurité de l'information. Dresser une liste de tous les endroits où les données du canton sont traitées impliquerait donc un énorme investissement, en particulier lorsqu'il s'agit de tâches cantonales confiées à des institutions externes, comme par exemple des hôpitaux, des EMS ou des centres de consultation. La publication d'une telle liste poserait en outre des problèmes de sécurité. Pour résumer, on peut néanmoins constater 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. L'un des défis auxquels nous sommes confrontés aujourd'hui est l'extension croissante des instruments TIC mobiles, comme les smartphones et les tablettes, qui sont souvent reliés par défaut à des solutions en nuage étrangères telles que iCloud, OneDrive ou Google Drive. Il incombe à toutes les autorités de veiller à ce que leur personnel ne traite aucune donnée cantonale digne de protection avec ce type de solutions, qui ne répondent souvent pas aux exigences légales exposées ci-après.
La question des serveurs de l'administration sera soumise à un examen approfondi dans le cadre de l'actuel projet d'audit indépendant de l'informatique dans l'Administration cantonale (UPI). Pour de plus amples renseignements, il convient donc de se référer aux résultats de l'audit présentés aux commissions de surveillance du Grand Conseil.

Question 2 :

Les dispositions de l'Administration cantonale concernant la sécurité de l'information et la protection des données (SIPD) dans les TIC figurent dans la législation relative à la protection des données, dans l'ordonnance de direction concernant la sûreté de l'information et la protection des données (OD SIPD, RSB 152.040.2) et dans les instructions d'exécution édictées à ce sujet par l'OIO.
Selon les conditions générales (CG) SIPD de l'Administration cantonale qui, en vertu des dispositions susmentionnées sont intégrées à tous les contrats relatifs aux TIC, tout prestataire de services est tenu d'indiquer les méthodes et les processus qu'il utilise pour réaliser ses prestations contractuelles, y compris le lieu où les prestations sont fournies. Le mandant est habilité à consulter les documents correspondants sur place et à se faire expliquer les processus opérationnels. Le prestataire de services doit en outre communiquer immédiatement au mandant tout incident inhabituel concernant les données, les systèmes et les processus liés au mandat, et notamment toute violation de la SIPD.
Le lieu du traitement des données fait aussi partie des éléments pris en compte dans l'analyse SIPD à respecter et le concept SIPD à définir pour les projets TIC. Le traitement des données à l'étranger n'est admis que lorsqu'un niveau de SIPD suffisamment élevé est garanti (voir réponse aux questions 4 et 5 ci-dessous).

Question 3 :

Les règles de protection de base SIPD édictées par l'OIO prescrivent avant tout, en matière de traitement des données, la réglementation des éléments suivants : zones de sécurité, règlementation des droits d'accès, plan de fermeture, système de fermeture et d'accès, mesures de sécurisation de l'espace, octroi, blocage et suppression de comptes d'utilisateurs, consultation des outils périphériques, authentification, protocoles à suivre et système de blocage en cas de tentatives infructueuses, concept d'autorisation pour les utilisateurs, instructions relatives au transfert de données, utilisation de services de réseau et limitation des accès pour les partenaires externes. Si ces mesures de protection de base ne suffisent pas, un concept SIPD doit être établi pour montrer quelles mesures permettraient de réduire les risques SIPD. La réponse à la question posée varie ainsi en fonction de l'application concernée.
Contrairement à ce qui se passe dans l'Administration fédérale, l'Administration cantonale ne dispose pas encore de procédure de vérification de la sûreté du personnel du canton ou des tiers assumant des fonctions sensibles. Il conviendrait pour ce faire de créer les bases légales nécessaires et de mettre à disposition les moyens financiers et le personnel correspondants. Cela étant, ni une vérification de la sûreté ni la mise en place de mécanismes de contrôle ne pourront jamais empêcher le comportement déviant de certains.

Questions 4 et 5 :

Le traitement des données à l'étranger comporte des risques particuliers. Aussi l'article 14a de la loi sur la protection des données[1] prévoit-il, en accord avec les dispositions du droit fédéral, qu'aucune donnée personnelle ne peut être communiquée à l'étranger, et cela inclut le traitement de données sur des systèmes TIC à l'étranger, en l'absence d'une législation assurant un niveau de protection adéquat, à moins que des garanties suffisantes, notamment contractuelles, permettent d'assurer un niveau de protection adéquat à l'étranger. Selon la pratique des autorités fédérales et les instructions du préposé fédéral à la protection des données et à la transparence (PFPDT), le niveau de protection de données à l'étranger est considéré comme suffisant lorsqu'il est conforme à la législation et à la pratique de la Convention pour la protection des données du Conseil de l'Europe. Le PFPDT tient une liste des Etats qui satisfont à ces exigences. Les Etats de l'UE en font partie. En vertu de la directive du PFPDT, le traitement des données aux Etats-Unis est en outre admis lorsque l'entreprise américaine concernée est signataire du *U.S.-Switzerland Safe Harbor Framework* (http://export.gov/safeharbor) et figure sur la liste correspondante du *U.S. Department of Commerce*. S'agissant des Etats ou des prestataires qui ne répondent pas à ces exigences, les clauses contractuelles établies sur la base des modèles publiés par le PFPDT peuvent aussi constituer une protection adéquate. Les autorités cantonales chargées de l'adjudication de mandats TIC sont tenues de tenir compte de ces conditions et de prendre les mesures requises pour garantir que le prestataire respecte les dispositions SIPD (art. 3, al. 3 de l'ordonnance sur la protection des données)[2].
Il est toutefois souvent extrêmement difficile d'imposer des dispositions suisses particulières en matière de sécurité à de grandes entreprises internationales dont les prestations sont fortement standardisées. En outre, les dispositions et recommandations susmentionnées datent d'une époque où l'on ne connaissait pas encore l'étendue de l'acquisition des informations par les services de renseignements étrangers dans le domaine des systèmes TIC. En février 2014, le Conseil fédéral a déclaré que, se fondant sur les connaissances actuelles en matière de risques, il entendait confier la fourniture des prestations destinées aux infrastructures centrales d'importance vitale de l'administration uniquement à des entreprises soumises exclusivement au droit suisse, détenues en majorité par des propriétaires suisses et fournissant toutes leurs prestations sur le territoire suisse. Le Conseil-exécutif et l'Administration cantonale adhèrent eux aussi à ces principes.

Question 6 :

Conformément aux conditions générales de la Conférence suisse sur l'informatique (CG de la CSI ; www.sik.ch), qui s'appliquent à tous les contrats TIC de l'administration, le for est en Suisse. Dans certains cas exceptionnels, notamment lorsque les prestataires occupent une position dominante sur le marché, il n'est pas possible d'imposer l'application des CG de la CSI. Le cas échéant, il appartient aux autorités responsables d'évaluer les risques liés à un for situé à l'étranger. Si, de manière générale, ce type de situation implique une plus grande insécurité juridique, elle peut aussi se traduire, en particulier en cas de litige aux Etats-Unis, par des frais judiciaires beaucoup plus élevés.

Question 7 :

« Cloud » (en français « nuage ») désigne une forme de fourniture globale de prestations informatiques sur Internet, dans laquelle le prestataire ne crée pas une infrastructure propre à chaque client (p. ex. un serveur qui lui est propre), mais où tous les clients se partagent la même infrastructure, au sein de laquelle leurs données sont naturellement séparées les unes des autres et visibles uniquement par eux-mêmes. Cette méthode de fourniture de services est avantageuse à la fois pour les clients, qui peuvent accéder à leurs données en « self-service », souvent sans aucun délai d'attente, et pour les prestataires, qui, grâce à l'important effet d'échelle, peuvent proposer des prix plus intéressants. Aussi, mais également en raison de l'intensification de la concurrence internationale, les solutions en nuage sont-elles généralement meilleur marché que les solutions offrant une infrastructure dédiée. Dans certains domaines, les différences sont très marquées : les offres de grands fournisseurs étrangers de solutions en nuage, comme Google, Amazon ou Microsoft, peuvent être cent fois moins onéreuses, pour des services de masse comme la gestion d'un espace de stockage ou le courrier électronique, que les offres proposées par les exploitants de centres de calcul conventionnels. A noter qu'il existe de nombreux modèles de services en nuage différents, dont les niveaux de sécurité et les coûts peuvent considérablement varier. Mentionnons à cet égard le système « infrastructure as a service » (IaaS), qui ne propose aux clients qu'une infrastructure matérielle, la « platform as a service » (PaaS), qui propose des serveurs virtuels sur

[1] Loi du 19 février 1986 sur la protection des données (LCPD ; RSB 152.04)
[2] Ordonnance du 22 octobre 2008 sur la protection des données (OPD ; RSB 152.040.1)

lesquels les clients peuvent exploiter leurs propres logiciels ou le « software / business process as a service » (SaaS / BPaaS), qui met à la disposition des clients des applications spécifiques ou des processus opérationnels entiers. Toute déclaration généralisée concernant les aspects sécuritaires et financiers des solutions en nuage doit donc faire l'objet d'une grande prudence.

Question 8 :

Selon l'article 17a LPD, si une autorité prévoit de traiter des données à l'aide de moyens techniques présentant des risques particuliers, elle soumet auparavant le traitement des données envisagé à l'autorité de surveillance en vue de sa prise de position. Bien que le recours à un modèle de services en nuage ne comporte pas de risques particuliers en soi, les solutions en nuage impliquent plus souvent des risques accrus, notamment parce que de nombreux fournisseurs dominants sur le marché se trouvent à l'étranger. Ces cas sont alors soumis à l'autorité de surveillance de la protection des données, afin qu'elle puisse prendre position sur la solution proposée et les mesures de sécurité prévues.

Question 9 :

Comme nous l'avons indiqué ci-dessus, ce n'est pas tellement le modèle de services en nuage en soi qui comporte des risques SIPD, mais plutôt d'autres aspects, comme le lieu de traitement des données. Ceux-ci doivent impérativement être pris en considération dans tous les mandats d'externalisation des TIC, quel que soit le modèle de services concerné. Nous renvoyons à ce sujet aux réponses données aux questions précédentes.

Le recours, aujourd'hui inévitable, à des systèmes matériels et logiciels développés à l'étranger comporte néanmoins déjà le risque que des services de renseignements étrangers y introduisent sciemment des points faibles et les exploitent. Or, l'utilisation de logiciels en Open Source, plus transparents en termes de sécurité, ou de technologies de cryptage, ne permet de réduire ce risque que dans une certaine mesure. Par ailleurs, le fait de renoncer à employer des solutions de masse en nuage situées à l'étranger, potentiellement plus risquées en terme de SIPD, peut aussi impliquer de renoncer à la réalisation d'économies parfois substantielles. Dans ce contexte de conflit d'objectifs entre la réduction des risques SIPD et l'investissement économique des fonds publics, le Conseil-exécutif estime qu'il est indispensable de continuer activement à développer le domaine de la sécurité informatique et, au cas par cas, de trouver des solutions permettant de tenir compte à la fois du risque rencontré et des critères économiques. A cet égard, l'OIO a décidé, dans le cadre d'une redéfinition de ses priorités financières, d'étendre ses capacités dans le domaine des conseils en SIPD à partir de 2014.