M

Intervention parlementaire. Réponse du Conseil-exécutif

N° de l'intervention:	277-2018
Type d'intervention:	Motion
Motion ayant valeur de directive:	☐
N° d'affaire:	2018.RRGR.737
Déposée le:	28.11.2018
Motion de groupe:	Non
Motion de commission:	Non
Déposée par:	Gerber (Hinterkappelen, Les Verts) (porte-parole) Ammann (Bern, LG) Egger (Hünibach, PS) Müller (Orvin, UDC)
Cosignataires:	14
Urgence demandée:	Non
Urgence accordée:	
N° d'ACE:	451/2019 du 8 mai 2019
Direction:	Direction des finances
Classification:	–
Proposition du Conseil-exécutif:	**Vote point par point** 1. Adoption et classement 2. Adoption en tant que postulat 3. Rejet 4. Adoption et classement

Sécurité de la communication et échange des données

Le Conseil-exécutif est chargé de faire en sorte ou plus exactement de garantir :

1. qu'à tous les niveaux de l'administration et au sein de la police de Berne, ce soient toujours les logiciels et les applications les plus sûrs qui sont utilisés pour la communication électronique ;

2. que dans les écoles aussi, des logiciels et des applications sûrs soient utilisés pour la communication ;

3. que les données soient enregistrées et conservées sur des serveurs suisses ;

4. qu'en ce qui concerne également la communication avec des externes, lorsqu'il s'agit de données et de documents dignes de protection, des logiciels et des applications sûrs soient utilisés pour la communication.

Développement :

Nous sommes confrontés sans cesse à des fuites de données : celles de Whatsapp sont comparées à celles de Facebook et les utilisatrices et utilisateurs sont ciblés individuellement, ou ces données sont revendues à des tiers.

Gratuit n'est pas synonyme de gratuit. Les messageries conventionnelles ne sont certes pas payantes, mais leur utilisation est payée avec des données. L'attitude des grosses entreprises qui consiste à réaliser d'immenses profits avec la vente et l'analyse de données qu'ils ne possèdent pas et qui n'ont pas été achetées, est irresponsable. Cela se produit toujours dans des proportions plus importantes lorsque les utilisatrices et utilisateurs n'ont pas encore la majorité.

Il est plus agréable de séparer vie professionnelle et vie privée. Et cela n'a pas de sens d'avoir dans la même application des photographies de ma famille et un projet de contrat de mon supérieur hiérarchique. En outre l'application doit être cryptée de A à Z.

Il existe des applications qui peuvent être adaptées en fonction des besoins. Ainsi, des écoles ou des départements de l'administration peuvent par exemple empêcher que des tiers entrent en contact avec une écolière ou une collaboratrice.

Le nombre des cyberattaques ne cesse de progresser. Cela ne signifie pas qu'un attaquant cible directement le téléphone mobile d'une autre personne. Il suffit qu'il achète les données d'utilisation d'un certain groupe de personnes et y reconnaisse des habitudes de comportement grâce auxquelles il pourra plus facilement et plus efficacement attaquer l'infrastructure visée (p. ex. reconnaissance des périodes en dehors des heures de travail habituelles ou de classes d'âge qui se prêtent mieux à une attaque). Autrement dit, la prévention va au-delà de la simple protection de l'appareil. Il importe donc de réduire au strict minimum les informations qui pourraient servir à la planification d'attaques. Ces métadonnées peuvent être achetées soit légalement soit sur le marché noir.

Cinq cantons utilisent déjà des applications sûres dans l'ensemble de leurs administrations et de leurs écoles. A titre d'exemple, Threema Work, ou Wire est également utilisé dans le monde politique, non seulement à la Confédération mais aussi en Allemagne. Ainsi que dans de nombreux ministères nationaux de pays membres de l'UE, et par des forces de police en Suisse et à l'étranger.

Réponse du Conseil-exécutif

1. Comme les auteurs de la motion, le Conseil-exécutif pense que la numérisation croissante de l'administration et de tous les autres domaines de la vie pose des défis de plus en plus nombreux en matière de sûreté de l'information et de protection des données (SIPD). C'est la raison pour laquelle les prescriptions en matière de SIPD de l'administration cantonale prévoient que chaque application fasse l'objet d'une analyse SIPD et que si un risque élevé est décelé en la matière, il soit évalué plus en détail dans un concept SIPD. Le concept décrit les mesures visant à réduire les risques ou à les éviter. Mais il n'existe pas de sécurité absolue. Le moyen le plus sûr de communiquer est de se parler en tête à tête. Toute forme de communication par voie électronique présente des risques déterminés, qui sont considé-

rés comme encore acceptables et dont on s'accommode pour des raisons par exemple de durée, de coûts, de convivialité ou d'organisation. L'important, c'est que cela soit fait en toute conscience.

Dans l'administration cantonale, la communication passe par l'application Skype Entreprise, qui garantit un cryptage. Les courriels échangés au sein de l'administration sont également automatiquement cryptés. Pour améliorer la sécurité de la communication mobile, l'administration va mettre en place dès la fin de l'année 2019 une solution de gestion de la mobilité en entreprise (Enterprise Mobility Management, EMM) : cette technologie crée, sur un smartphone ou une tablette, un domaine protégé et crypté où les applications et les données professionnelles et privées sont traitées séparément les unes des autres.

La Police cantonale emploie déjà la technologie EMM. Pour la communication entre ses collaborateurs et collaboratrices, elle utilise aussi l'appli IMP (Instant Messenger Police) qui garantit un cryptage de bout en bout de la communication et la suppression automatique des données. Plusieurs corps de police utilisent cette solution, qui leur permet aussi de communiquer en toute sécurité entre eux.

Le premier point de la motion est une préoccupation constante (« toujours ») qui est en permanence mise en œuvre en vertu des prescriptions mentionnées. Le Conseil-exécutif considère dans ce sens que le chiffre 1 de la motion est réalisé et propose par conséquent de l'adopter et de le classer.

2. Le canton ne peut édicter des prescriptions d'utilisation de logiciels de communication que pour le degré secondaire II. Les consignes se réfèrent à la Stratégie TIC pour les écoles du degré secondaire II[1] et sont régulièrement vérifiées dans un comité d'experts TIC, où les écoles sont représentées. En ce qui concerne l'école obligatoire, les communes sont compétentes pour édicter des consignes en la matière, et le canton peut seulement émettre des recommandations.

   En collaboration avec la Haute école pédagogique germanophone, la Direction de l'instruction publique assiste les écoles pour une approche des données numériques qui soit plus sûre et conforme à la loi, à l'aide d'un système de feux tricolores (http://kibs.ch/datenschutz). La mise en place et le développement des compétences médiatiques à l'école obligatoire et au degré secondaire II sont en outre garantis par les dispositions des plans d'études. En particulier l'échange d'informations sensibles (p. ex. qui concernent la santé ou les performances scolaires) obéit à des consignes strictes. Les écoles en sont informées et les écoles cantonales qui se procurent des services informatiques auprès de la Direction de l'instruction publique sont équipées techniquement pour pouvoir échanger des données particulièrement dignes de protection.

   Certains services de messagerie utilisés présentent une contradiction entre leur acceptation dans la société et les consignes en matière de protection des données. L'agence spécialisée TIC et éducation (educa.ch) de la Confédération et des cantons est actuellement en train de négocier, avec un fournisseur suisse, une solution attrayante pour remplacer l'offre gratuite largement répandue. Lorsque cette offre sera disponible, la Direction de l'instruction publique envisagera, au sujet de l'utilisation de services de messagerie en milieu scolaire,

[1] Stratégie TIC pour les écoles secondaires II 2017-2021

d'édicter une consigne obligatoire à l'intention du degré secondaire II ainsi qu'une recommandation à l'intention de l'école obligatoire.

Le Conseil-exécutif propose par conséquent d'adopter le chiffre 2 de la motion sous forme de postulat.

3. Le lieu physique où se trouve un serveur ne garantit en rien la sécurité des données qui y sont traitées. Il est aussi possible d'accéder à des serveurs suisses depuis l'étranger et des entreprises dont le siège est en Suisse peuvent être contrôlées par des personnes se trouvant à l'étranger. Sous cet aspect de la sûreté de l'information aussi, il faut évaluer au cas par cas dans le cadre d'une analyse des risques les mesures à prendre pour protéger les données en fonction des risques. Le fait que les données soient conservées dans un pays membre de l'UE peut même, selon les circonstances, accroître la sûreté de l'information : le Règlement européen sur la protection des données (RGPD)[2] contraint les entreprises TIC à faire preuve de davantage de diligence et de prendre davantage de mesures pour protéger les données que la législation suisse en la matière qui est toujours en vigueur. Le Préposé fédéral à la protection des données et à la transparence tient une liste des Etats offrant une protection adéquate des données des personnes physiques.

   Concernant les données les plus importantes pour l'accomplissement des tâches publiques, le Conseil-exécutif a décidé, dans le cadre de la stratégie de propriétaire de Bedag Informatique SA, qu'elles devaient être conservées en Suisse par cette entreprise qui appartient au canton.[3] Mais de plus en plus d'applications ne sont plus développées que sous forme de « logiciel en tant que service » : autrement dit, elles ne peuvent plus être installées sur un serveur propre, mais sont disponibles uniquement via internet dans un nuage (« cloud ») qui est souvent exploité à l'étranger. L'administration cantonale ne peut pas se fermer à cette évolution technique, sous peine d'avoir, le cas échéant, à utiliser des solutions bien plus onéreuses ou d'un niveau technique insuffisant qui ne permettraient pas d'atteindre les objectifs de numérisation de l'administration. Il doit donc rester possible d'utiliser aussi des solutions de « cloud » étrangères dans certains cas, après une analyse des risques et en adoptant des mesures de sécurité appropriées. La loi sur la protection des données (LCPD) ne l'exclut pas.

   Le Conseil-exécutif propose par conséquent de rejeter le chiffre 3 de la motion.

4. Pour la sûreté de la communication électronique avec des tiers, l'administration cantonale applique différentes méthodes qui garantissent une transmission cryptée ou un cryptage des contenus confidentiels. En voici quelques-unes :

   - une solution de messagerie électronique exploitée par Bedag qui permet aux destinataires d'aller chercher les messages via un portail internet sécurisé ;
   - des interfaces avec le réseau HIN (Health Info Net) et avec l'administration fédérale pour des échanges de courriels cryptés de bout en bout avec d'autres cantons, des autorités fédérales et des organisations du domaine de la santé ;

[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE

[3] Voir le communiqué de presse du Conseil-exécutif du 21 septembre 2018.

- une solution de cryptage de supports de données externes intégrée au poste de travail cantonal (PTC).

Aussi le Conseil-exécutif juge-t-il la demande du chiffre 4 de la motion comme étant réalisée. Il propose donc de l'adopter et de la classer.

Destinataire
- Grand Conseil