

Intervention parlementaire

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: du
Direction: Direction des finances
Classification: –
Proposition du
Conseil-exécutif:



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.

Destinataire

- Grand Conseil