Conseil communal de Lausanne

Initiative : Interpellation (ordinaire)

Titre : **Risques cybers et protection des données personnelles**

Initiant-e(-s) : Angélique Chatton et consorts

Dans les lignes directrices relatives à la transformation numérique de la Ville de Lausanne, figure le principe de « responsabilité et transparence en matière de captation des données personnelles en application de la LPrD ». Cette interpellation questionne la Municipalité sur la manière dont cela est mis en œuvre en pratique.

Le nombre de cyberattaques ne cesse d'augmenter et touche tous les secteurs. En Suisse, leur nombre a augmenté de 65% entre 2020 et 2021[1]. Les institutions publiques n'y font pas exception comme le montre les récents vols de données dans les communes de Rolle et Montreux ou encore à l'Université de Neuchâtel.
Les cyberattaques exposent les organisations qui en sont victimes à différents types de risques :

- Risque d'image ;
- Risque réglementaire en cas de défaillance grave de l'encadrement des risques cybers étant en dernière instance de la responsabilité du conseil d'administration qui est chargé d'exercer la haute direction de la société et d'établir une organisation appropriée selon le Code suisse des obligations ;
- Risque de chantage par les pirates informatiques ;
- Risque de paralysie des systèmes d'information et ses potentiels effets en cascade.

Dès lors, disposer d'une connaissance complète et précise des données personnelles traitées et de leurs flux (de la création à la destruction) est essentielle :

- afin de les protéger de manières adéquates vis-à-vis des cyberattaques ;
- en cas de cyberattaque, de pouvoir rapidement identifier les données volées ou corrompues et de prendre les mesures appropriées dans les meilleurs délais.

L'administration communale et ses prestataires sont soumis à la loi cantonale sur la protection des données (LPrD) pour l'encadrement des données personnelles. Les entreprises privées, quant à elles, seront soumises à la nouvelle loi fédérale sur la protection des données (nLPD) dès son entrée en vigueur d'ici début 2023. Ces deux lois visent à prévenir le traitement abusif des données relatives aux personnes et à protéger leur personnalité ainsi que leur sphère privée.

Le récent audit de l'Administration cantonale vaudoise par la Cour des comptes du canton a mis en évidence des lacunes dans la mise en application de la LPrD[2] :

- peu d'entités de l'Administration ont procédé à une identification exhaustive des données personnelles traitées
- aucune analyse complète en regard des exigences de la LPrD n'a été réalisée
- les entités de l'Administration n'ont pas ou peu entamé de réflexion sur la conservation des données personnelles qu'elles gèrent, les stockant le plus souvent indéfiniment sans les avoir anonymisées.

[1] https://www.ictjournal.ch/etudes/2022-01-11/en-suisse-les-cyberattaques-augmentent-davantage-que-dans-le-monde

[2] https://www.vd.ch/toutes-les-autorites/cour-des-comptes/recherche-dans-les-publications-de-la-cour-des-comptes/news/15376i-rapport-n-74-la-protection-des-donnees-personnelles-dans-ladministration-cantonale-vaudoise/

Conseil communal de Lausanne

Nous posons les questions suivantes à la Municipalité :

Dans sa vision et principes de la transformation numérique, la Ville de Lausanne se fixe un principe de « responsabilité et transparence en termes de captation des données personnelles en application de la LPrD » . Dans la pratique, comment ces principes sont-ils cadrés et mis en œuvre ? Plus spécifiquement :

- Une analyse complète en regard des exigences de la LPrD (notamment, en lien avec le registre des fichiers) a-t-elle été réalisée ?
- Une identification exhaustive des données personnelles traitées par l'administration de la ville a-t-elle été réalisée ?
- Une politique de conservation claire des données personnelles a-t-elle été définie ? Est-elle mise en œuvre ?

Plus largement, comment la gouvernance des données s'inscrit-elle dans la gouvernance documentaire énoncée dans le préavis 2016/6 ?

Quelles ressources (audit, certifications, tests d'intrusion,...) sont mises en œuvre pour prévenir les risques cybers?

Par ailleurs, comment la Municipalité s'assure-t-elle que les dispositifs nécessaires à la mise en conformité de la nLPD soient mis en place au sein des entreprises dont elle est actionnaire majoritaire ? Quelles ressources (audit, certifications, tests d'intrusion,...) sont mises en œuvre par ces dernières pour prévenir les risques cybers?

Lausanne, le 9 septembre 2022

Mme Angélique CHATTON

Signataire(s) :

M. Eric BETTENS

Mme Karine ROCH