Réponse du Conseil d'Etat au Grand Conseil
à l'interpellation David Raedler et consorts au nom Les Vert.e.s vaudois.e.s –
Quelle stratégie est mise en place pour éviter les applications de « messagerie boiteuses » ?
(21_INT_11)

Rappel de l'intervention parlementaire

Les outils de communication sont aujourd'hui toujours plus variés et prennent des formes diverses, allant des applications spécifiques aux réseaux sociaux en passant – encore – par le SMS ou l'appel « traditionnels ». Les utilisateurs et utilisatrices se retrouvent ainsi confronté.es à un large éventail de possibilités quant au moyen de communication utilisé. Un choix qui s'avère central dans la mesure où les spécificités et modalités de chaque outil divergent et peuvent avoir des incidences importantes sur la sphère privée des personnes concernées ainsi que sur la sécurité des communications. La collecte et les traitements de données personnelles issues de ces outils varient fortement d'un cas à l'autre : protocoles de sécurité et de confidentialité appliqués, chiffrement, mise en commun des données récoltées, hébergement, transparence et caractère open source ne sont ainsi que quelques-uns des sujets qui doivent être examinés et considérés lors du choix. Des sujets qui ont très récemment encore été discutés suite à l'annonce par Facebook Inc. de la modification des conditions générales applicables à l'un de ses services de messagerie extrêmement populaire (Whatsapp) impliquant un transfert et une mise en commun encore plus important et large de données personnelles des utilisateurs et utilisatrices.

Ces questions trouvent une assise particulière pour les autorités publiques, ceci principalement à trois égards :

- *soumis aux exigences de la Loi cantonale sur la protection des données personnelles (LPrD) ainsi qu'aux limites issues du secret de fonction, le Canton doit s'assurer de limiter au maximum les transferts et traitements de données personnelles effectuées par lui ou ses agent.es et employé.es, notamment à l'étranger ;*
- *traitant des sujets parfois hautement stratégiques et confidentiels, le Canton doit s'assurer de la sécurité et de la confidentialité de ses échanges ;*
- *en tant qu'employeur, le Canton doit offrir à ses employé.es les outils permettant de protéger leur propre sphère privée.*

Ce sont ces motifs qui ont notamment mené la Confédération à introduire la solution Threema Work pour les échanges professionnels de ses employés ou la Commission européenne à privilégier l'application open source Signal, chaque fois à l'exclusion de Whatsapp.

Par ses démarches entreprises ces dernières années sur le thème de l'évolution technologique et de la stratégie numérique, le Canton a montré qu'il prenait sérieusement le sujet de la sécurité informatique ainsi que le respect des exigences issues de la LPrD.

Cela étant, l'identification de la stratégie adoptée spécifiquement pour les outils de communication utilisés par le Canton appelle les interpellateurs et interpellatrices sous-signé.es à poser les questions suivantes :

1. *Quels outils de messagerie et de communication sont utilisés au sein de l'administration cantonale ?*

2. *Quelles directives s'appliquent à l'utilisation d'applications de messagerie par les employé.es et agent.es du Canton dans le cadre de leurs activités professionnelles ?*

3. *Quelle stratégie est appliquée par le Canton pour les outils de communication utilisés au sein de l'administration, notamment vis-à-vis d'un outil particulier qui serait privilégié (à l'image de la Confédération avec Threema ou de la Commission européenne avec Signal) ou, à l'inverse, interdit (Whatsapp dans les deux cas précités) ?*

4. *Le Canton examine-t-il la possibilité d'intégrer un outil spécifique à son environnement ou la création d'un outil in-house ?*

5. *Cas échéant (selon l'outil utilisé), quelles garanties et mesures sont mises en place pour limiter les traitements de données personnelles ainsi que garantir le respect de la LPrD, et du secret de fonction, notamment dans le cas d'échanges transfrontaliers de données personnelles ?*

Réponse du Conseil d'Etat

Préambule

Par sa Stratégie numérique de novembre 2018 et son Plan directeur cantonal des SI 2018-2023, le Conseil d'État s'est résolument engagé depuis de nombreuses années dans des initiatives visant à renforcer la sécurité des données et des systèmes d'information de l'Administration, notamment pour protéger la population et les entreprises de toute utilisation abusive de leurs données détenues par l'Etat.

Si la sécurisation des SI est fondamentale à cet égard, il est également indispensable que celles et ceux qui travaillent pour l'Etat soient sensibilisés et formés aux bonnes pratiques en la matière.

C'est ainsi que la Direction générale du numérique et des systèmes d'information (DGNSI) formule depuis quelques années de fréquentes recommandations et mène des actions de sensibilisation en matière de sécurité numérique à l'intention du personnel de l'ACV, par l'intermédiaire de l'intranet et de la Gazette de l'État, portant sur des thèmes tels que « comment gérer des e-mails suspects, comment choisir son mot de passe, comment organiser son poste pour le télétravail, …). Ces actions dont certaines s'inscrivent dans le cadre de la semaine nationale d'actions pour la sécurité numérique, sont complétées par la mise à disposition de formations en ligne, figurant au catalogue du Centre d'éducation permanente (CEP) ou publiques, comme celle sur « la sécurité de l'information », réalisée en partenariat avec d'autres cantons romands. L'efficacité de ces mesures est vérifiée périodiquement par la DGNSI grâce à des exercices d'hameçonnage adressés à l'ensemble des collaboratrices et collaborateurs de l'État. La récente actualité avec plusieurs piratages qu'ont connu des entités publiques ces derniers mois a montré l'importance de ces mesures pour la sécurité des données détenues par les collectivités publiques.

Il faut par ailleurs préciser que deux directives internes à l'Etat, soit la directive LPers 50.1 sur « l'utilisation d'internet, de la messagerie électronique, de la téléphonie et du poste de travail » et la directive LPers 48.8 sur le « Télétravail » précisent les droits et devoirs des collaboratrices et collaborateurs sur ces thématiques.

L'Etat se mobilise par ailleurs pour soutenir les PME grâce à son application www.vd.ch/cybersecurite. Dans les prochains mois, ces mesures de sensibilisation s'étendront aux communes et à l'ensemble de la population vaudoise, dans le cadre de la mise en œuvre de la stratégie numérique et de son initiative d'accompagnement des personnes et des entreprises. Ces actions porteront sur des éléments d'hygiène numérique de base sur internet (mots de passe, protection des données, phishing, ransomwares).

À l'interne, un ensemble d'outils de communication sont aujourd'hui proposés aux collaboratrices et collaborateurs de l'État. Ces solutions sont toutes déployées en recherchant un niveau de sécurité élevé et sont en principe hébergées sur site.

À l'instar de la Confédération, la DGNSI recommande l'usage de solutions de messagerie instantanée pour téléphone mobile de type Threema ou Signal.

Réponse aux questions

1. *Quels outils de messagerie et de communication sont utilisés au sein de l'administration cantonale ?*

   L'État met à disposition de ses collaboratrices et collaborateurs un ensemble de solutions sécurisées répondant aux principaux besoins en termes de communication et de collaboration.

   Les solutions standards sont :
   - Messagerie électronique et agenda : Microsoft Outlook
   - Messagerie instantanée interne et téléphonie : Cisco Jabber
   - Vidéoconférence : Cisco Webex
   - Partage de fichiers : Partage.vd.ch
   - Messagerie instantanée privée, recommandations : Threema ou Signal

2. *Quelles directives s'appliquent à l'utilisation d'applications de messagerie par les employés.es et agents.es du Canton dans le cadre de leurs activités professionnelles ?*

   La directive Lpers 50.1 sur « l'utilisation d'internet, de la messagerie électronique, de la téléphonie et du poste de travail » définit les droits et les devoirs des utilisatrices et utilisateurs concernant les moyens de communication (Internet, messagerie électronique, téléphonie) et les postes de travail informatiques mis à leur disposition dans le cadre professionnel.

   La directive Lpers 48.8 sur le « Télétravail » précise les conditions d'exercice d'un télétravail et définit les exigences relatives à l'utilisation des ressources informatiques depuis la Suisse ou depuis l'étranger.

   Plusieurs guides pratiques sont mis à disposition des collaboratrices et collaborateurs. Ils couvrent notamment les questions d'utilisation d'outils de messagerie instantanée ou de vidéoconférence, hors infrastructures de l'État. Ces guides sont accessibles depuis vd.ch : « Messagerie instantanée », « Vidéoconférence », « Organiser son poste pour le télétravail ».

3. *Quelle stratégie est appliquée par le Canton pour les outils de communication utilisés au sein de l'administration, notamment vis-à-vis d'un outil particulier qui serait privilégié (à l'image de la Confédération avec Threema ou de la Commission européenne avec Signal) ou, à l'inverse, interdit (Whatsapp dans les deux cas précités) ?*

   L'État privilégie les communications réalisées avec les outils standards (listés ci-dessus) via des PC professionnels sur son réseau interne. Les accès à distance sont réalisés au travers d'un réseau virtuel privé (VPN) et permettent aux PC fixes ou portables professionnels d'accéder aux outils de communication interne avec un niveau de sécurité équivalent. L'accès aux messageries privées (gmail, hotmail, whatsapp, …) est bloqué par défaut sur les postes de travail de l'Administration cantonale.

   Le téléphone mobile reste un moyen de communication tant professionnel que privé. Les téléphones mobiles mis à disposition par l'État sont configurés afin de permettre ce double usage, en isolant les données et applications professionnelles dans un container logique sécurisé. Pour l'usage privé, des recommandations sont formulées sans pour autant interdire l'utilisation de certaines applications.

   L'État recommande ainsi l'utilisation des produits de type *Threema* ou *Signal* qui répondent aux plus hautes exigences de sécurité. Ils sont disponibles sur les téléphones professionnels en self-service pour l'application gratuite *Signal* ou à la demande pour l'application *Threema*.

4. *Le Canton examine-t-il la possibilité d'intégrer un outil spécifique à son environnement ou la création d'un outil in-house ?*

   Les outils actuels répondent aux besoins en matière d'usage et de sécurité. Le Canton n'envisage pour l'instant pas d'intégrer de nouveaux outils en matière de messagerie instantanée sur téléphone mobile.

5. *Cas échéant (selon l'outil utilisé), quelles garanties et mesures sont mises en place pour limiter les traitements de données personnelles ainsi que garantir le respect de la LPrD, et du secret de fonction, notamment dans le cas d'échanges transfrontaliers de données personnelles ?*

   Conformément à la directive Lpers 48.8 « *Les collaborateur-trice-s peuvent, sous réserve de dispositions légales excluant un traitement de données depuis l'étranger, effectuer du télétravail depuis les pays frontaliers de la Suisse… Hors des pays frontaliers, et sous réserve d'une exception temporaire formellement accordée par l'autorité d'engagement et à la condition que le pays concerné offre une sécurité suffisante de protection des données au sens de la liste des pays reconnus sûrs par la Confédération, seules les données professionnelles de la messagerie (e-mail, contacts, agenda) peuvent être accédées et synchronisées sur un outil professionnel ou privé* ».

   Un accès sécurisé aux courriels professionnels reste possible en déplacement, y compris depuis un téléphone mobile professionnel ou privé.

   Une surveillance technique des connexions à distance sur le système d'information de l'ACV est réalisée par la DGNSI en termes d'origine géographique des connexions et de mode d'échanges de données.

Ainsi adopté, en séance du Conseil d'Etat, à Lausanne, le 22 septembre 2021.

La présidente :	Le chancelier :
N. Gorrite	*V. Grandjean*