canton de vaud
LIBERTÉ ET PATRIE

CONSEIL D'ÉTAT

Château cantonal
1014 Lausanne

Madame la Conseillère fédérale
Viola Amherd
Cheffe du Département fédéral de la défense, de la protection de la population et des sports
Palais fédéral est
3003 Berne

Par courriel (en Word et PDF) :
sicherheit.vbs@gs-vbs.admin.ch

Réf. : 22_COU_6293

Lausanne, le 23 novembre 2022

Législation d'exécution de la loi sur la sécurité de l'information : procédure de consultation

Madame la Conseillère fédérale,

Le Conseil d'Etat du Canton de Vaud vous remercie d'avoir sollicité son avis dans le cadre de la procédure de consultation relative à la législation d'exécution de la loi sur la sécurité de l'information.

La sécurité de l'information est un élément fondamental, en particulier dans le cadre de la transformation numérique des organisations et de la société en général. Le Conseil d'Etat a rappelé dans sa Stratégie numérique, adoptée en 2018, l'importance du principe de sécurité dans ce contexte. Il a pris connaissance des quatre projets d'ordonnances d'application qui visent à la mise en œuvre de la loi sur la sécurité de l'information. En juillet 2014, il s'était prononcé favorablement sur ce projet de loi tout en rappelant la nécessité de prévoir des dispositions d'application en collaboration avec les cantons, étant donné les conséquences financières et humaines non négligeables qui pourraient survenir. Il regrette que les projets mis en consultation ne permettent toujours pas aux cantons d'évaluer avec précision ces conséquences.

Le Conseil d'Etat vous prie de trouver ci-après les réponses aux questions posées dans le cadre de cette consultation :

1. La mise en œuvre des ordonnances est-elle compréhensible pour les cantons ?

Le Conseil d'Etat constate l'important travail réalisé par les services de la Confédération et relève la clarté du texte des ordonnances. Toutefois, leur mise en œuvre dans les cantons nécessitera très probablement de faire évoluer la législation cantonale, des ressources humaines et financières additionnelles, et une adaptation des systèmes d'information. Le Conseil d'Etat n'est pas en mesure aujourd'hui d'évaluer ces éléments, les projets mis en consultation n'étant pas suffisamment précis à cet égard.

2. Comment les cantons envisagent-ils la mise en œuvre des ordonnances ?

Le Conseil d'Etat prévoit que la mise en œuvre des ordonnances se déroule de manière coordonnée entre les différents services de son administration, afin de créer des synergies mais également dans un souci d'efficacité, de maîtrise des coûts et d'uniformisation. La mise en œuvre devra s'appuyer sur le système de management de la sécurité de l'information (SMSI) déjà formellement en place au sein de l'administration cantonale, par la Direction générale du numérique et des systèmes d'information (DGNSI). Ce système est en préparation pour une certification à la norme ISO 27001, prévue en décembre 2022.

Le Conseil d'Etat relève également que l'adoption des ordonnances par le Conseil fédéral nécessitera vraisemblablement l'élaboration de bases légales et réglementaires cantonales complémentaires, par exemple pour procéder à des contrôles conformément à l'art. 35 de l'ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP).

Au vu de la complexité de la mise en œuvre sur les plans technique et juridique, le Conseil d'Etat demande que l'entrée en vigueur des ordonnances se fasse de manière échelonnée, avec une période transitoire suffisante.

3. À quelles conséquences financières s'attendent les cantons ?

Le Conseil d'Etat n'est pas en mesure à ce stade d'estimer les conséquences financières pour le Canton de Vaud : les informations nécessaires à cet égard, de même que celles portant sur les conséquences organisationnelles, ne sont en effet pas suffisamment détaillées dans le projet mis en consultation. Toutefois, le Conseil d'Etat constate que cette législation aura principalement un impact sur les systèmes d'informations qui communiquent avec les systèmes fédéraux. Le Conseil d'Etat demande que le Conseil fédéral apporte rapidement les précisions sur les systèmes et les données concernées, qui lui permettront de procéder à l'évaluation de ces conséquences.

Le Conseil d'Etat a par ailleurs pris note que des prescriptions techniques d'exécution restent à venir. Ceci induit des incertitudes sur les conséquences pour les cantons. Des questions subsistent encore également quant aux modalités d'application et aux dispositions transitoires de cette législation d'exécution, dans les cas où elle s'appliquera aux autorités cantonales.

Dans ce contexte, le Conseil d'Etat demande que les services de la Confédération communiquent les prescriptions techniques ainsi que toutes les précisions utiles dans les meilleurs délais et que le Conseil fédéral définisse qui aura la charge de vérifier le respect de la mise en œuvre.

4. *Les cantons devront désigner un service faisant office d'interlocuteur pour les questions de sécurité de l'information. Quel est cet interlocuteur dans votre canton ?*

Le Conseil d'Etat a désigné la Direction générale du numérique et des systèmes d'information (DGNSI), et en particulier son directeur de la sécurité numérique pour être l'interlocuteur pour les questions de sécurité de l'information dans le cadre de la mise en œuvre des ordonnances.

Pour le surplus, le Conseil d'Etat vous adresse en annexe de ce courrier différentes remarques et observations sur les quatre ordonnances.

En conclusion, le Conseil d'Etat peut soutenir les projets mis en consultation mais demande que le Conseil fédéral apporte dans les meilleurs délais toutes les précisions nécessaires pour diminuer les risques liés à leur mise en œuvre.

En vous souhaitant bonne réception de la présente, nous vous prions de croire, Madame la Conseillère fédérale, à l'assurance de notre considération distinguée.

AU NOM DU CONSEIL D'ETAT

LA PRESIDENTE	LE CHANCELIER
Christelle Luisier Brodard	Aurélien Buffat

Annexe

- Remarques sur les ordonnances

Copies

- Direction générale du numérique et des systèmes d'information
- Office des affaires extérieures

Annexe : remarques sur les ordonnances

Ordonnance sur la sécurité de l'information au sein de l'administration fédérale et de l'armée (OSI)

Article 18 al. 1 let. c : L'OSI prévoit que les informations susceptibles de nuire aux intérêts définis à l'art. 1, al. 2, let. a à d LSI, si elles sont portées à la connaissance d'une personne non autorisée, sont classifiées « interne » notamment si « c. des personnes subissent des lésions corporelles ». Or, la limitation à des lésions corporelles, sans spécifier s'il s'agit de lésions corporelles simples, graves ou de voies de fait, ne prend pas en compte le fait qu'une atteinte psychologique peut également entraîner de très lourdes conséquences (dépression, suicide, automutilation, perte de confiance, inefficacité au travail, etc). Ainsi, les conséquences d'une atteinte psychologique pouvant être parfois plus lourdes que celles d'une atteinte physique, la disposition légale devrait prévoir ce cas.

Articles 18 à 20 : Il n'est pas clair comment serait classifiée une fuite de données qui exposerait des données personnelles de citoyens et citoyennes à des tentatives ou des cas d'arnaques, d'escroqueries, de chantages, d'atteintes à la sécurité informatique d'entreprises ou d'individus, etc. A la lecture de ces articles, il apparait que ce sont les intérêts de la Confédération qui sont essentiellement pris en compte et non pas ceux des entreprises et des particuliers, à la protection de leur personnalité et de leurs biens juridiquement protégés en raison d'atteintes à la sécurité informatique des systèmes de la Confédération. Il conviendrait donc d'adapter ces dispositions.

Ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP)

Remarque générale : Cette ordonnance aura un impact sur les entités en charge des contrôles de sécurité relatifs aux personnes dans le cadre cantonal. Il s'agit là de rappeler que la récolte importante de données prévue et les traitements de données personnelles éventuellement sensibles nécessitent un encadrement rigoureux qui soit conforme à la législation sur la protection des données.

Ordonnance sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération (OIAM)

Remarque générale : La révision de cette ordonnance concerne principalement des aspects d'ordre technique pour les systèmes de gestion des données d'identification. Ces derniers pourraient avoir un impact sur la gestion des identités du portail IAM du canton (Identity and Access Management), ou autres bases de données, en particulier en ce qui concerne l'obligation de gestion des accréditations et des accès aux systèmes d'information de la Confédération. Il s'agit là de prendre également en compte l'impact sur les systèmes d'information sous mandat d'exploitants « tiers », qui utilisent aussi ces systèmes d'identification.

Ordonnance sur la procédure de sécurité relative aux entreprises (OPSE)

Articles 2 et al. : Il conviendrait de préciser les relations entre l'art. 2 al. 1, fixant le champ d'application de l'ordonnance, qui énonce « La présente ordonnance s'applique aux entreprises dont le siège est en Suisse », l'art. 2 al. 2 qui stipule « La procédure s'appliquant aux entreprises dont le siège est à l'étranger est régie par un traité international conformément à l'art. 87 LSI », et l'art. 6 précisant une partie de la procédure en cas de présence d'une entreprise étrangère.

Article 14 : Cet article prévoit un plan de sécurité et un examen lors de la procédure d'adjudication, mais il n'est pas prévu que ce plan soit vérifié en cours de mandat alors que la technologie et les risques évoluent rapidement. Il conviendrait d'adapter la disposition pour prendre en compte les évolutions techniques.