Kommission für Staatspolitik und Aussenbeziehungen
Commission des institutions politiques et des relations extérieures

Loi sur la sécurité de l'information et la cybersécurité

Explications pour la 2e lecture

Table des matières

1. Contexte

Le 5 décembre 2024, le Grand Conseil a examiné le projet de loi sur la sécurité de l'information et la cybersécurité (LSIC, affaire 2020.KAIO.134) en première lecture. À cette occasion, il a renvoyé les dispositions suivantes à la Commission des institutions politiques et des relations extérieures (CIRE) pour qu'elle les amende :

- Article 5 : « Renvoi à la commission assorti du mandat d'examiner la pertinence d'introduire une obligation pour l'autorité d'effectuer un contrôle régulier des mesures prises, par analogie avec l'article 7, alinéa 1 de la loi fédérale sur la sécurité de l'information (LSI). »

- Article 21 : « Renvoi à la commission assorti de la charge d'étudier et de proposer une réglementation qui définit les fonctions à contrôler et les autorités chargées des contrôles, ainsi que la périodicité des contrôles de sécurité des personnes. Elle doit en outre examiner la validité des dispositions en ce qui concerne les juges. »

- Article 30 : « Renvoi à la commission assorti du mandat d'examiner la pertinence d'introduire une évaluation périodique de l'exécution, de l'adéquation, de l'efficacité et de l'économicité de la loi, par analogie avec l'article 88 de la loi fédérale sur la sécurité de l'information (LSI). »

Sur mandat de la CIRE, la Direction des finances propose les amendements suivants pour mettre en œuvre ces décisions.

2. Article 5 (Obligations des autorités)

2.1 Proposition

Ajout de la lettre *d* à l'article 5, alinéa 1 :

Art. 5 Obligations des autorités
[1] Chaque autorité veille à ce que
a les besoins de protection des informations relevant de son domaine de responsabilité soient évalués ;
b la confidentialité, la disponibilité, l'intégrité et la traçabilité des informations au sens de la lettre a soient garanties en fonction de leur besoin de protection ;
c ses outils TIC soient protégés contre les utilisations abusives et les perturbations ;
d la sécurité de l'information soit régulièrement contrôlée.

2.2 Commentaire

L'obligation de contrôler régulièrement la sécurité est déjà inscrite de manière implicite à l'article 5, alinéa 2, qui dispose que les risques pour la sécurité de l'information doivent être constamment évalués et que les mesures nécessaires doivent être prises. Rien ne s'oppose néanmoins à ce que cette obligation au sens où l'entend la décision de renvoi soit expressément inscrite dans la loi.

Comme le prévoit la décision de renvoi, cette nouvelle disposition est formulée sur le modèle de l'article 7, alinéa 1 LSI, dont voici les termes : « Les autorités soumises à la présente loi veillent, chacune dans son domaine de compétence, à ce que la sécurité de l'information soit organisée, mise en œuvre et contrôlée conformément à l'état des connaissances scientifiques et techniques. »

Bien que le renvoi porte sur l'article 5, alinéa 2 (gestion des risques), nous proposons d'introduire cette nouvelle obligation à l'article 5, alinéa 1, car elle ne concerne pas véritablement la gestion des risques.

3. Articles 20 et suivants (Contrôle de sécurité relatif aux personnes)

3.1 Proposition

Les dispositions régissant le contrôle de sécurité relatif aux personnes sont reformulées de la manière suivante (les modifications de fond sont soulignées mais pas les déplacements). L'ajout de nouveaux articles change la numérotation des articles concernés et des suivants.

Art. 20 But
[1] Le contrôle de sécurité des personnes sert à évaluer si l'accès d'une personne à des informations ou à des installations sensibles dans l'exercice de ses fonctions ou dans le cadre de l'exécution d'un mandat pourrait présenter un risque pour la sécurité de l'information ou des installations.
[2] Il consiste à recueillir les données relatives à la loyauté de la personne contrôlée, notamment à ses éventuelles activités pénalement répréhensibles et à sa situation financière, qui sont nécessaires à l'évaluation au sens de l'alinéa 1.

Art. 21 Degrés de contrôle
[1] Le contrôle de sécurité relatif aux personnes prend la forme d'un contrôle de base ou d'un contrôle élargi.
[2] Lors du contrôle de sécurité de base, l'autorité de contrôle peut
a recueillir des données du casier judiciaire ou des registres des offices des poursuites et faillites ;
b tenir compte d'informations extraites de sources publiques ou de ses propres dossiers ;
c interroger la personne concernée ou des tiers si la personne concernée y consent.
[3] Lors du contrôle de sécurité élargi, l'autorité de contrôle peut en outre demander à la Police cantonale de recueillir des données
a des systèmes de traitement de données de la Police cantonale au sens de l'article 143 de la loi du 10 février 2019 sur la police (LPol),
b des systèmes de traitement de données de la Confédération ou des cantons, dans la mesure où la Police cantonale s'est vu conférer un accès direct conformément à l'article 147 LPol.
[4] La Police cantonale ne communique à l'autorité de contrôle que les données visées à l'alinéa 3 qui sont nécessaires au contrôle. Si les données s'y prêtent, elle les anonymise et les résume.

Art. 22 Conditions
[1] Le contrôle de sécurité de base peut être réalisé lorsque la personne à contrôler est dans l'une ou l'autre des situations suivantes :
a elle a accès soit fréquemment, soit en grand nombre à
1. des informations classifiées « confidentiel » ;
2. des données personnelles particulièrement dignes de protection, dont la publication pourrait porter gravement atteinte aux droits de la personnalité des personnes concernées ;
b elle a accès à d'importantes affaires politiques ou sensibles ;
c elle a accès à des installations ou à des zones de sécurité au sens de l'article 18 ;
d elle exerce une activité présentant des risques similaires.
2 Le contrôle de sécurité élargi peut être réalisé lorsque la personne à contrôler est dans l'une ou l'autre des situations suivantes :
a elle a accès soit régulièrement, soit à un grand nombre
1. d'informations classifiées « secret » ;

2. de données personnelles, dont la publication pourrait porter gravement atteinte à l'intégrité physique des personnes concernées ;

b elle a accès à des installations ou à des zones de sécurité au sens de l'article 18 soit régulièrement, soit sans accompagnement ;
c elle exerce une activité présentant des risques similaires.

Art. 23 Personnes à contrôler
[1] Les autorités suivantes règlent, chacune pour leur domaine, le degré de contrôle valant pour chaque fonction :
a le Grand Conseil :
1. pour les personnes qu'il a élues : par décret ;
2. pour les personnes employées par les Services parlementaires et les personnes mandatées par le Grand Conseil ou les Services parlementaires : par voie d'instruction du Bureau ;
b le Conseil-exécutif : pour les personnes qu'il a nommées ainsi que pour les personnes employées ou mandatées par les Directions et la Chancellerie d'État : par voie d'ordonnance ;

c la Direction de la magistrature : pour les personnes employées ou mandatées par les autorités judiciaires ou le Ministère public : par voie d'instruction.
[2] Le Conseil-exécutif peut décider, par voie d'ordonnance, que la réglementation prévue à l'alinéa 1, lettre *b* relative aux personnes employées ou mandatées soit fixée par instruction des Directions, de la Chancellerie d'État ou d'organes spécialisés de l'administration.
[3] [variante :] Les juges [variante 1 : sont soumis à un contrôle de sécurité de base] [variante 2 : sont soumis à un contrôle de sécurité élargi] [variante 3 : ne sont pas soumis au contrôle de sécurité relatif aux personnes].

Art. 24 Autorité de contrôle
[1] Les personnes employées par une autorité sont contrôlées par leur autorité d'engagement.
[2] Les personnes mandatées par une autorité sont contrôlées par l'autorité qui a établi le mandat.
[3] Les personnes candidates à l'élection au sein d'une autorité sont contrôlées
a par l'autorité qui propose leur candidature ;
b par l'autorité de nomination lorsque leur candidature n'est pas proposée par une autorité.

Art. 25 Contrôle par le service spécialisé chargé des contrôles de sécurité relatifs aux personnes de la Confédération
[1] À la demande des autorités de contrôle au sens de l'article 24, les responsables de la sécurité du Grand Conseil, des Directions, de la Chancellerie d'État ainsi que des autorités judiciaires et du Ministère public peuvent exceptionnellement, dans l'un ou l'autre des cas suivants, confier le contrôle de sécurité élargi relatif aux personnes au service spécialisé compétent de la Confédération :
a l'activité exercée présente un risque particulièrement élevé ;
b la personne contrôlée a un lien avec l'étranger qui pourrait présenter des risques ;
c il semble opportun que la personne contrôlée soit interrogée par des spécialistes.
[2] Dans ce cas, la portée et la procédure du contrôle de sécurité élargi sont régis par les articles 34 à 39 de la loi fédérale du 18 décembre 2020 sur la sécurité de l'information (LSI) ainsi que par les dispositions d'exécution correspondantes de la législation fédérale. Une audition au sens de l'article 34, alinéa 2, lettre *d* LSI est possible.
[3] L'autorité de contrôle peut renoncer à soumettre une personne au contrôle de sécurité lorsque celle-ci produit une déclaration de sécurité établie par le service spécialisé de la Confédération (art. 40 LSI) et que le délai de renouvellement (art. 30) n'est pas encore échu.

Art. 26 Consentement et collaboration
[1] Aucun contrôle de sécurité ne peut être réalisé sans le consentement de la personne à contrôler.
[2] La personne soumise au contrôle est tenue de collaborer à l'établissement des faits.

Art. 27 Législation fédérale réservée
[1] Pour les personnes traitant des informations fédérales classifiées ou ayant accès à des outils TIC de la Confédération, les dispositions de la législation fédérale régissant la sécurité de l'information sont réservées.

Art. 28 Résultat
[1] L'autorité de contrôle communique les résultats du contrôle de sécurité à la personne contrôlée.
[2] La personne contrôlée peut consulter le dossier correspondant dans les dix jours et demander la rectification de données inexactes. Ce délai peut être prolongé dans des cas motivés.
[3] L'autorité de contrôle détruit le dossier du contrôle
a dans les trois mois après que la personne contrôlée
1. a refusé l'engagement ou le mandat ;
2. n'a pas été retenue pour le poste ou le mandat ;
3. a cessé d'exercer la fonction pour laquelle elle a été contrôlée ;
b mais au plus tard au bout de dix ans.

Art. 29 Conséquences
[1] Si la personne devant être contrôlée ne consent pas à subir ce contrôle (art. 26) ou si le contrôle aboutit à des conclusions qui s'opposent à un rapport de travail, à une élection ou à l'attribution d'un mandat, il est possible
a de renoncer à la conclusion d'un contrat de travail, à l'élection ou à l'attribution d'un mandat ;
b de se départir d'une promesse d'engagement orale ou écrite ;
c de prendre des mesures relevant du droit du personnel, si les rapports de travail sont déjà établis.

Art. 30 Renouvellement
[1] Le contrôle de sécurité relatif aux personnes employées ou mandatées est renouvelé comme suit :
a contrôle de base : au plus tôt après cinq ans, mais au plus tard après dix ans,
b contrôle élargi : au plus tôt après trois ans, mais au plus tard après cinq ans.
[2] L'autorité de contrôle peut renouveler le contrôle plus tôt si elle a des raisons de penser que de nouveaux risques sont apparus depuis le dernier contrôle.
[3] Le premier contrôle de sécurité relatif aux personnes déjà employées ou mandatées à l'entrée en vigueur de la présente loi est réalisé dans les délais prévus à l'alinéa 1.
[4] Le contrôle de sécurité relatif aux personnes membres d'une autorité est renouvelé à l'occasion de leur réélection.

3.2 Commentaire

Les dispositions proposées répondent à la demande du Grand Conseil, qui souhaite que le contrôle de sécurité relatif aux personnes (CSP) soit réglementé plus précisément, et à celle du Conseil-exécutif, qui entend réglementer le CSP comme il l'est dans la loi sur la police, le plus simplement possible et de manière moins bureaucratique qu'en droit fédéral.

Ces dispositions ont été élaborées en concertation avec la Direction de la sécurité, la Police cantonale et le service spécialisé chargé des CSP de la Confédération, qui est rattaché au Secrétariat d'État à la politique

de sécurité (SEPOS). La Direction des finances avait préalablement discuté de ses propositions clés avec le président et les porte-parole de la CIRE le 13 janvier 2025.

3.2.1 Article 20 (But)

L'accès à des installations sensibles, condition d'un CSP déjà prévue dans le projet du Conseil-exécutif (à l'art. 22, lit. *c* selon numérotation d'alors), est aussi ajouté à l'article définissant le but du CSP, afin d'établir clairement qu'un CSP sert non seulement à prévenir les risques menaçant les informations, mais aussi d'autres risques pour l'ordre public et la sécurité (art. 1, al. 2, lit. *c* projet LSIC).

Cette précision répond au besoin exprimé par la Police cantonale lors de la préparation de la proposition de réglementation. Elle souhaitait pouvoir soumettre à un CSP élargi les artisanes et artisans et autres mandataires qui travaillent parfois sans surveillance dans des locaux sensibles de la police, comme le local de stockage de scellés. Ce contrôle correspond à la pratique actuelle : avec le consentement des personnes concernées, les banques de données de la police sont interrogées à leur sujet. Cela réduit le risque que le crime organisé tente par ce biais de manipuler des pièces à conviction ou le travail de la police ou introduise par exemple un appareil d'écoute.

Cette proposition s'inspire de la disposition analogue de l'article 18 du projet de loi sur la sécurité de l'information du canton d'Argovie (projet InfoSIG), à la différence qu'elle ne porte pas seulement sur les zones de sécurité, mais sur toute installation sensible, terme qui peut désigner des immeubles, des bâtiments ou des locaux. Il peut s'agir d'installations de la police, mais aussi de structures, comme celles de l'exécution judiciaire ou de la protection de la population contre les dangers naturels, ou encore d'infrastructures vulnérables dont l'accès est restreint, comme les infrastructures routières, de télécommunication ou d'approvisionnement en énergie.

La différence par rapport à l'article 18 du projet InfoSIG se justifie du fait que les institutions à protéger ne sont pas nécessairement des zones de sécurité au sens de l'article 18 LSIC, c'est-à-dire des zones réservées à des informations classifiées SECRET et à des ressources TIC exigeant ce même niveau de protection. Cette disposition permet donc de mettre en place, pour les installations sensibles du canton, une protection similaire à celle que prévoit la législation fédérale pour les installations militaires, afin d'éviter que des personnes à risque puissent y accéder. En effet, l'article 27, alinéa 1 LSI prévoit un CSP pour les « activités sensibles » qui, selon l'article 5, lettre *b* LSI, recouvrent non seulement les cas déjà cités à l'article 20 du projet de LSIC, mais aussi l'accès à des ouvrages militaires nécessitant un haut niveau de protection.

3.2.2 Article 21 (Degrés de contrôle)

Comme la législation fédérale (art. 30 LSI), le projet de LSIC prévoit désormais deux degrés de contrôle de sécurité relatif aux personnes : le contrôle de base (ci-après CSPb) et le contrôle élargi (ci-après CSPe). Cette nouveauté répond à un double objectif : pouvoir adapter plus facilement le plan de contrôle aux risques et ainsi mieux satisfaire au principe de proportionnalité en l'ancrant dans la loi.

Le CSPb porte sur des extraits du casier judiciaire et du registre des poursuites ainsi que (ce qui est maintenant expressément mentionné, comme à l'art. 34 LSI) sur des sources d'information publiques, comme les médias (en langage technique, « renseignements d'origine sources ouvertes », ROSO [OSINT en anglais]) et sur d'autres pièces et informations dont dispose l'autorité de contrôle (comme le dossier personnel des RH). L'évaluation du risque peut ainsi mettre au jour des risques qui ne ressortent pas des extraits

de registres. L'autorité de contrôle peut ainsi notamment tenir compte de conflits familiaux ou d'une addiction (p. ex. aux jeux, à l'alcool ou à d'autres drogues) susceptibles de mettre à mal la probité et la fiabilité de la personne contrôlée.

Si elle a des craintes, elle peut aussi auditionner la personne contrôlée pour lui permettre de s'exprimer sur ces points. Pour pouvoir auditionner des tiers (p. ex. ses précédents responsables hiérarchiques), l'autorité de contrôle doit préalablement s'assurer du consentement de la personne contrôlée.

Quant au CSPe, il porte en supplément sur des fichiers de la police. Son étendue ne change pas par rapport à ce que prévoyait le projet du Conseil-exécutif.

L'alinéa 3 définit comment les données sont transmises dans le cadre du CSPe : la Police cantonale ne doit pas transmettre les « données brutes » figurant dans ses fichiers, car cela risquerait souvent de violer l'intimité d'autres personnes ou de compromettre la confidentialité de procédures en cours. Elle doit donc les résumer et les anonymiser, de sorte à protéger ces intérêts tout en permettant à l'autorité de contrôle d'évaluer les risques.

3.2.3 Article 22 (Conditions)

Les conditions déterminant le degré de contrôle dont relève telle ou telle fonction correspondent à celles que prévoit le droit fédéral, qui, en substance, fait également une distinction en fonction du besoin de protection des informations classifiées CONFIDENTEL ou SECRET (cf. art. 30 LSI). Repris du projet du Conseil-exécutif, ces critères sont néanmoins formulés plus concrètement que dans la LSI, afin d'en simplifier l'application. Comme dans la LSI, la liste n'est pas exhaustive, ce qui permet de tenir aussi compte d'éventuels autres risques pour les objectifs de protection de la LSI.

Pour comparer les risques, se référer à l'illustration 8 figurant en page 16 du rapport relatif au projet de LSIC (également ci-dessous avec le titre actuel de l'ordonnance) :

Loi sur la sécurité de l'information et la cybersécurité (LSIC)		**Ordonnance sur la sécurité de l'information et des données OSID**	**Loi sur la protection des données (LCPD)**
protection des intérêts publics		*Mesures de sécurité de l'information et des données*	*Protection des intérêts des personnes physiques*
Outils TIC	Informations	Mesures de protection à la pointe de la technique	Données personnelles
Protection très élevée	SECRET	Niveau de protection 3	Données personnelles représentant une grave menace pour la sécurité de l'intéressée ou de l'intéressé (intégrité physique, vie, liberté)
Protection élevée	CONFIDENTIEL	Niveau de protection 2	Données personnelles particulièrement dignes de protection ou sous le sceau du secret (secret professionnel, fiscal, etc.)
Protection de base	INTERNE	Niveau de protection 1	Données personnelles générales
	Non classifié	Niveau de protection 0	Données non personnelles (hors du champ de protection de la LCPD)

Les données personnelles relevant du niveau de protection 3 sont celles dont la divulgation pourrait mettre en danger l'intégrité physique des personnes intéressées, p. ex. le lieu de séjour de personnes particulièrement menacées ou l'adresse de personnes placées par la police dans un programme de protection de témoins.

Parmi les fonctions pouvant donner lieu à un CSPe figurent notamment (sous réserve de l'évaluation du risque par l'autorité compétente) celles des membres du corps de police, des artisanes et artisans qui interviennent dans des installations sensibles (cf. art. 20 plus haut) et des spécialistes informatiques (comme les gestionnaires de services, les administratrices et administrateurs système et le personnel du support) qui ont accès à des fichiers relevant du niveau de protection 3.

3.2.4 Article 23 (Personnes à contrôler)

Sur le modèle du droit fédéral (art. 28 LSI), la décision de contrôler une personne et la méthode à utiliser n'est plus du ressort individuel de l'autorité responsable sur la base de son évaluation du risque, comme le prévoyait le projet du Conseil-exécutif, mais se fonde sur une liste des fonctions devant donner lieu à un contrôle. Par analogie à l'article 28 LSI, chaque autorité soumise à la loi doit édicter cette liste pour son propre domaine de responsabilité, et ce, par ordonnance ou décret pour les personnes nommées membres d'une autorité ou par instruction pour les personnes employées ou mandatées.

L'alinéa 2 autorise le Conseil-exécutif, pour certaines fonctions définies uniformément dans toute l'administration cantonale, à déléguer cette compétence à l'organe spécialisé de l'administration cantonale. Concernant les fonctions TIC dans l'administration (comme celles des techniciennes et techniciens du support ou les administratrices et administrateurs système), il est prévu de confier cette tâche à la Conférence pour l'administration numérique et les TIC (CNT), qui doit également être l'organe de pilotage de la sécurité de l'information dans l'administration cantonale.

Étant donné que les tribunaux constituent le troisième pouvoir étatique (pouvoir judiciaire), la commission peut, si elle le souhaite, choisir la variante présentée à l'alinéa 3 et ainsi ancrer le CSP pour les juges dans la loi, plutôt que de le régler par décret comme en dispose l'alinéa 1. La Direction des finances s'abstient de déterminer si et comment les juges doivent être soumis à un CSP, car c'est au parlement, en sa qualité d'autorité de nomination, que ressortit cette décision fondée sur les risques. En droit fédéral, les juges ne font pas l'objet d'un CSP (art. 29, al. 4 LSI), alors que dans le canton de Berne, la Commission de justice du Grand Conseil demande des extraits de casier judiciaire et du registre des poursuites pour les candidates et candidats à la magistrature, ce qui revient à réaliser un CSP.

3.2.5 Article 24 (Autorités de contrôle)

L'article 24 correspond sur le fond au projet du Conseil-exécutif. La participation de la Police cantonale au CSPe est réglée à l'article 21, et la délégation du CSPe à la Confédération, à l'article 25.

3.2.6 Article 25 (Contrôle par le service spécialisé chargé du contrôle de sécurité relatif aux personnes de la Confédération)

Dans de rares cas, il peut exceptionnellement être justifié de confier le CSPe au service spécialisé chargé des CSP de la Confédération, qui est rattaché au Secrétariat d'État à la politique de sécurité (SEPOS ; al. 1).

- Cela peut s'avérer opportun lorsque l'activité exercée présente un risque particulièrement élevé (lit. *a)*, par exemple parce que la personne concernée a de larges pouvoirs ou de hautes responsabilités. Cela

pourrait être le cas par exemple pour l'élection du procureur général ou de la commandante de la Police cantonale (sachant que la Direction des finances n'entend en aucune façon empiéter sur les prérogatives de l'autorité de nomination en citant ces exemples).
- Il peut également être judicieux de confier le contrôle à la Confédération lorsque la personne à contrôler a un lien avec l'étranger (lit. *b*), parce qu'elle y a vécu plusieurs années ou qu'elle y entretient des relations familiales ou professionnelles significatives. Les sources d'information auxquelles ont accès les autorités cantonales ne permettent la plupart du temps pas d'établir les risques liés à ce genre de liens, alors que le service spécialisé chargé des CSP de la Confédération peut, le cas échéant, les obtenir en consultant les sources du Service du renseignement auxquelles il a accès (art. 34, al. 1, lit. *c* LSI).
- Et si l'audition réalisée par l'autorité de contrôle ne fait pas suffisamment la lumière sur les risques, il peut s'avérer utile de confier l'audition aux spécialistes formés de la Confédération (lit. *c*).

En droit fédéral, l'article 35 de l'ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP) autorise les cantons à recourir, moyennant émolument, aux prestations du Service spécialisé CSP DDPS pour leur propre sécurité de l'information. Voici le montant de l'émolument par contrôle que prévoit le tarif 2024 du SEPOS :

Type de contrôle	*Données suisses uniquement (en CHF)*	*Données étrangères aussi (en CHF)*
CSPb	500	650
CSPe	1 700	2 000
CSPe avec audition	3 000	4 500

Aux termes de l'article 35 OCSP, ces mandats de contrôle supposent que les cantons disposent d'une base légale suffisante pour les CSP, entendent effectuer des évaluations à l'instar de la Confédération pour garantir la sécurité de l'information et ont conclu une convention de prestations avec le DDPS. La LSIC satisfait aux deux premières conditions. La dernière devra être réglée par voie d'ordonnance.

Concernant l'étendue et la procédure de ces contrôles, l'alinéa 2 renvoie à la législation fédérale applicable, unique droit qu'applique le service spécialisé CSP. La possibilité de recourir à une audition au sens de l'article 34, alinéa 2, lettre *d* LSI est mentionnée ici pour établir clairement que cette audition n'est pas contraire à l'article 19 OCSP. Celui-ci définit notamment qui, à la Confédération, peut être auditionné, et ne mentionne naturellement que des membres du personnel fédéral (la réglementation cantonale correspondante se trouve désormais à l'art. 25, al. 1 LSIC).

La possibilité, pour les personnes ainsi contrôlées, de contester devant le Tribunal administratif fédéral la déclaration de sécurité délivrée à l'issue du contrôle, comme le prévoit l'article 44, alinéa 3 LSI, ne peut pas être réglée ici. La LSI ne permet pas d'établir clairement si cette possibilité vaut aussi dans le cas d'un CSP cantonal délégué à la Confédération. Le législateur cantonal n'ayant aucune influence en la matière, il incombera au Tribunal administratif fédéral de statuer sur sa compétence lorsqu'il sera saisi d'un tel recours.

Pour décharger l'autorité de contrôle et les personnes à contrôler, l'alinéa 3 autorise à se fonder sur une déclaration de sécurité de la Confédération encore valable plutôt que de réaliser un CSP cantonal. Il est en effet relativement fréquent que les personnes employées ou mandatées par le canton disposent déjà d'une déclaration de sécurité délivrée par la Confédération, soit parce qu'elles ont exercé une activité pour son compte, soit parce qu'elles sont militaires.

3.2.7 Article 28 (Résultat)

Le nouvel alinéa 3 correspond à la disposition de l'article 47 LSI. Il met en œuvre le principe légal de protection des données, selon lequel les données personnelles (souvent particulièrement dignes de protection, comme ici) ne doivent pas être conservées plus longtemps que nécessaire.

3.2.8 Article 29 (Conséquences)

L'article 29 ne change pas par rapport au projet du Conseil-exécutif. Pour compléter les travaux préparatoires, il est précisé ici, sur la base des discussions menées avec les membres de la commission, que les éventuelles mesures relevant du droit du personnel (lit. *c*) doivent être proportionnées. L'autorité d'engagement devra étudier si des conditions (sur le modèle de l'art. 39, al. 1, lit. *b* LSI) sont susceptibles de réduire les risques éventuels à un niveau acceptable, par exemple en confiant à un spécialiste informatique à risque des tâches sur une application ou un fichier contenant des informations nécessitant un moindre niveau de protection.

3.2.9 Article 30 (Renouvellement)

L'article 30 règle désormais le renouvellement du CSP pour les personnes employées ou mandatées, ce que le projet du Conseil-exécutif laissait à la discrétion de l'autorité de contrôle. Cette disposition correspond à la réglementation légale fédérale (art. 43 LSI).

Elle tient compte du fait que des risques de sécurité peuvent apparaître au cours d'un engagement ou d'un mandat. Il convient donc de réitérer le CSP dès l'apparition de signes de nouveaux risques (al. 2) et en tout cas tous les trois à dix ans, en fonction du risque (al. 1).

L'alinéa 3 est en soi une disposition transitoire, qui est placée ici en raison du lien de connexité matériel. Il permet de réaliser le premier contrôle des personnes déjà engagées ou mandatées dans les délais de renouvellement prévus, de sorte que leur réalisation soit gérable. Il est ainsi possible, par exemple, de ne pas contrôler les personnes qui sont proches de la retraite.

Il n'est pas nécessaire de réitérer le contrôle des membres d'une autorité durant leur mandat, mais seulement si elles sont réélues (al. 4).

4. Article 33, jusqu'à présent article 30 (Dispositions d'exécution du Conseil-exécutif)

4.1 Proposition

La Direction des finances conseille à la CIRE de renoncer à la disposition d'évaluation qui est demandée en complément dans la décision de renvoi.

Mais si la CIRE souhaite tout de même ancrer ce point dans la loi, elle pourrait, par exemple, ajouter le nouvel alinéa 4 ci-dessous à l'article 33 (jusqu'à présent art. 30) :

> [4] Il [le Conseil-exécutif] règle le contrôle périodique de l'exécution et de l'efficacité de la présente loi dans le cadre de l'application de l'article 88, alinéas 1 et 2 LSI.

4.2 Commentaire

Le renvoi s'appuie sur l'article 88 LSI, dont voici la teneur : « Le Conseil fédéral veille à ce que l'exécution, l'adéquation, l'efficacité et l'économicité de la présente loi soient contrôlées périodiquement par un service indépendant, en particulier par le Contrôle fédéral des finances. Il en rend compte régulièrement aux commissions compétentes de l'Assemblée fédérale. »

La Direction des finances estime qu'il n'est pas nécessaire d'introduire une disposition analogue dans la LSIC, car l'évaluation qu'elle règlerait est déjà prescrite par le droit fédéral, à savoir à l'article 86, alinéas 1 et 2 : « Les cantons veillent au contrôle périodique de la mise en œuvre et de l'efficacité de la sécurité de l'information visée à l'article 3. Ils informent le service spécialisé de la Confédération pour la sécurité de l'information des résultats de ces contrôles. »

En application de cette disposition, le canton sera donc tenu de contrôler régulièrement l'exécution et l'efficacité de la LSIC. La procédure devra en être réglée par voie d'ordonnance après concertation avec les autorités fédérales compétentes.

En outre, si un manque d'adéquation ou d'économicité de la LSIC se fait jour dans la pratique, les autorités de surveillance – le Contrôle des finances, le Bureau cantonal pour la surveillance de la protection des données ou les organes de surveillance parlementaires – ont toute latitude de s'en saisir à tout moment.

* * *