Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS,

Secrétariat général DDPS
Droit DDPS

16 octobre 2014

Projet de loi fédérale sur la sécurité de l'information (LSI)

Rapport sur le résultat de la procédure de consultation

Projet de loi fédérale sur la sécurité de l'information (LSI). Rapport sur le résultat de la procédure de consultation

Table des matières

1 Contexte

En raison de l'évolution vers une société de l'information, les risques et les dangers concernant les informations sont devenues plus complexes et dynamiques. Plusieurs attaques contre des systèmes d'information de la Confédération ont démontré que la protection des informations au sein de la Confédération présente des lacunes. Or, ces lacunes, – en particulier sur le plan organisationnel – sont dues à des bases légales obsolètes ou incohérentes.

Le DDPS a élaboré le projet d'une nouvelle loi fédérale sur la sécurité de l'information en collaboration avec les départements fédéraux, la Chancellerie fédérale et d'autres autorités fédérales. La loi fédérale sur la sécurité de l'information vise à regrouper en une seule réglementation homogène tous les éléments clés de la sécurité de l'information. Cette loi régit en particulier la gestion du risque, la classification des informations et les principes de la sécurité lors de la mise en œuvre de la technologie en matière d'information et de communication. Le principe de la transparence dans l'administration doit continuer d'être maintenu de manière illimitée, ce qui explique pourquoi la LSI prévoit explicitement la réserve de la loi fédérale sur la transparence LTrans. La présente loi fédérale doit définir une nouvelle manière de réglementer les contrôles de sécurité relatifs aux personnes (CSP) et établir une procédure uniforme de sécurité concernant les entreprises (PSE). Elle doit par ailleurs régler le soutien aux infrastructures critiques (IC) pour la gestion des risques dans le domaine de la sécurité de l'information. Enfin, cette loi prévoit de conférer au Conseil fédéral une base légale pour la conclusion de conventions internationales dans le domaine de la sécurité de l'information.

En raison de la mise en réseau toujours plus vaste des systèmes et de l'échange électronique des informations, cette loi ne doit pas seulement déployer ses effets pour l'administration fédérale et l'armée, mais également pour le Parlement, les tribunaux fédéraux, le Ministère public de la Confédération et ses autorités de surveillance ainsi que pour la Banque nationale. Les cantons, les particuliers et les milieux économiques ne doivent être concernés par ces dispositions légales que lorsqu'ils mènent des activités sensibles en matière de sécurité sur mandat de la Confédération.

Le Conseil fédéral a chargé le DDPS, le 26 mars 2014, de lancer une procédure de consultation relative au projet de loi fédérale sur la sécurité de l'information auprès des cantons, des partis politiques, des associations faîtières des communes, des villes et des régions de montagne, des associations faîtières économiques ainsi qu'auprès des milieux intéressés. La procédure de consultation était ouverte jusqu'au 4 juillet 2014.

2 Participants à la consultation[1]

62 organisations ont été invitées à se prononcer, à savoir:

- les 26 cantons et la Conférence des gouvernements cantonaux;
- les 13 partis politiques représentés au sein de l'Assemblée fédérale;
- 3 associations faîtières suisses représentant les communes, les villes et les régions de montagne;
- 9 associations faîtières suisses représentant les milieux économiques;
- 10 autres associations intéressées.

L'ouverture de la procédure de consultation a été annoncée officiellement dans la Feuille fédérale du 8 avril 2014.

Ont pris position:

- tous les 26 cantons;

[1] Dans la suite du document, les participants à la consultation (à l'exception des cantons) de même que leurs prises de position apparaissent dans l'ordre (alphabétique) de la version **originale allemande**.

- 4 des partis politiques représentés au sein de l'Assemblée fédérale;
- 1 association faîtière des communes, des villes et des régions de montagne;
- 4 associations faîtières suisses représentant les milieux économiques;
- 9 autres organisations intéressées;
- 11 autres participants non invités à titre individuel;

Soit au total cinquante-cinq prises de position.

Les participants à la consultation qui se sont prononcés par écrit sont mentionnés nommément ci-dessous. Les abréviations entre parenthèses sont reprises dans la suite du texte.

2.1 Cantons

Ont présenté une prise de position:

- canton de Zurich (ZH)
- canton de Berne (BE)
- canton de Lucerne (LU)
- canton d'Uri (UR)
- canton de Schwyz (SZ)
- canton d'Obwald (OW)
- canton de Nidwald (NW)
- canton de Glaris (GL)
- canton de Zoug (ZG)
- canton de Fribourg (FR)
- canton de Soleure (SO)
- canton de Bâle-Ville (BS)
- canton de Bâle-Campagne (BL)
- canton de Schaffhouse (SH)
- canton d'Appenzell-Rhodes-Intérieures (AI)
- canton d'Appenzell-Rhodes-Extérieures (AR)
- canton de Saint-Gall (SG)
- canton des Grisons (GR)
- canton d'Argovie (AG)
- canton de Thurgovie (TG)
- canton du Tessin (TI)
- canton de Vaud (VD)
- canton du Valais (VS)
- canton de Neuchâtel (NE)
- canton de Genève (GE)
- canton du Jura (JU)

2.2 Partis politiques représentés au sein de l'Assemblée fédérale

Ont présenté une prise de position:

- Parti démocrate-chrétien (PDC)
- Parti libéral-radical (PLR)
- Union démocratique du centre (UDC)
- Parti socialiste (PSS)

2.3 Associations faîtières suisses des communes, villes et régions de montagne

En dépit de l'incontestable importance du présent projet de loi, l'Union des villes suisses (UVS) a expressément renoncé à répondre à la consultation faute de capacités suffisantes, mais elle renvoie à l'avis exprimé par la Conférence suisse sur l'informatique (CSI).

2.4 Associations faîtières suisses représentant les milieux économiques

Ont présenté une prise de position:

- economiesuisse
- Union suisse des arts et métiers (USAM)

L'Union patronale suisse (UPS) a renoncé expressément à se prononcer étant donné que le projet de loi ne concernait pas directement l'économie en tant qu'employeur. La Société suisse des employés de commerce (SEC), en raison de ressources limitées, a expressément renoncé à se prononcer au sujet d'un projet de loi qui ne comporte aucun point concernant spécifiquement les employés de commerce.

2.5 Autres organisations intéressées

Ont présenté une prise de position:

- Autorité de surveillance du Ministère public de la Confédération (AS MPC)
- Ministère public de la Confédération (MPC)
- Privatim, l'association des commissaires suisses à la protection des données (privatim)
- Conférence suisse sur l'informatique (CSI)
- Banque nationale suisse (BNS)
- Tribunal fédéral suisse (TF)
- Swico – L'association économique pour une Suisse digitale (swico)

Ont renoncé expressément à se prononcer:

- Tribunal fédéral des brevets (TFB)
- Tribunal administratif fédéral (TAF)

2.6 Participants non invités à titre individuel

Ont présenté une prise de position:

- Association suisse de la sécurité de l'information (Clusis)
- Centre Patronal, Equipes Patronales (CP)
- Centre Patronal, Chambre vaudoise des arts et métiers (CVAM)
- Fédération des Entreprises Romandes (FER)
- Insecor Sàrl (insecor)
- IT-Riskmanagement Sàrl (it-rm)
- Lehmann Beat (LB)
- Service de renseignement de la Confédération (SRC)
- Conseil des Ecoles polytechniques fédérales (Conseil des EPF)
- Conférence des recteurs des universités suisses (crus.ch)
- Fédération des médecins suisses (FMH)

3 Appréciation générale

Les tableaux figurant ci-dessous donnent un aperçu de l'appréciation générale des participants quant au projet de loi mis en consultation.

Synthèse des résultats de la procédure de consultation

Qui	Oui	Oui, mais	Non, mais	Non	Aucun commentaire	Total
Cantons	7	18	1			*26*
Partis	1	2		1		*4*
Association faîtière des communes, villes et régions de montagne					1	*1*
Associations faîtières économiques		1	1		2	*4*
Autres	1	6			*2*	*9*
Non invités	2	8	1			*11*
Total	**11**	**35**	**3**	**1**	**5**	**55**

Légende:

Oui:	approbation sans réserves
Oui, mais:	approbation quant au fond, avec des propositions d'amendements
Non, mais:	rejet quant au fond, avec des propositions d'amendements
Non:	rejet en bloc
Aucun commentaire:	participant ayant expressément renoncé à se prononcer

Résumé synthétique des résultats, avec indication de la provenance

Appréciation générale	Nombre	Participants
Oui: approbation sans réserves	**11**	7 cantons (SZ, OW, BL, SH, AR, VS, JU) 1 parti politique représenté au sein de l'Assemblée fédérale (PLR) 1 autre organisation intéressée (TF) 2 participants non invités individuellement (CP, CVAM)
Oui, mais: approbation quant au fond, avec des propositions d'amendements	**35**	17 cantons (ZH, LU, UR, NW, GL, ZG, FR, SO, BS, AI, SG, GR, AG, TG, TI, VD, NE, GE) 2 partis politiques représentés au sein de l'Assemblée fédérale (PDC, PSS) 1 association faîtière des milieux économiques (economiesuisse) 6 autres organisations intéressées (AS-MPC, MPC, CSI, BNS, swico)

		8 participants non invités individuellement (Clusis, FER, insecor, it-rm, NDB, ETH-Rat, crus.ch, FMH)
Non, mais: rejet quant au fond, avec des propositions d'amendements	**3**	1 canton (BE) 1 association faîtière des milieux économiques (USAM) 1 participant non invité individuellement (LB)
Non: rejet en bloc	**1**	1 parti politique représenté au sein de l'Assemblée fédérale (UDC)
Aucun commentaire: participants ayant expressément renoncé à se prononcer	**5**	1 association faîtière des communes, villes et régions de montagne (USV) 2 associations faîtières des milieux économiques (UPS, SEC) 2 autres organisations intéressées (TFB, TAF)
Total	**55**	

Eléments essentiels des avis exprimés en procédure de consultation

- Une majorité prépondérante des milieux consultés salue la création d'une loi fédérale sur la sécurité de l'information.
- De nombreux cantons demandent que soient précisées les modalités de l'application de cette loi aux cantons ainsi que la collaboration entre la Confédération et les cantons.
- Quelques cantons souhaitent qu'ils n'aient pas à créer d'organismes parallèles, mais puissent avoir accès à ceux de la Confédération.
- Quelques cantons demandent à être impliqués dans l'élaboration des dispositions d'exécution.
- D'aucuns font valoir que les notions utilisées dans la loi sont trop ouvertes ou trop vagues, ce qui aurait pour conséquence de donner un pouvoir d'appréciation considérable aux autorités. Ils demandent par conséquent que les dispositions d'exécution soient claires et concises.
- D'aucuns font également valoir que les interfaces entre la sécurité de l'information, la protection des données et le principe de la transparence de l'administration devraient être encore mieux clarifiées.

3.1 Cantons

ZH salue le fait que l'on édicte des dispositions uniformes pour le traitement sécurisé d'informations par les autorités fédérales et d'autres organisations. A son avis, le projet de loi lui semble globalement bien élaboré et sa conception bien pensée. Toutefois, les répercussions sur les cantons sont encore floues et devront être clarifiées au plus tard lors de la mise en œuvre de cette loi et lorsqu'on édictera les dispositions d'exécution y relatives.

BE ne peut adhérer à ce projet de loi qu'à condition que les autorités cantonales et communales – dans la mesure où elles appliquent la LSI (soit directement en tant qu'autorité contraignante, soit dans le cadre de la reprise des dispositions de la LSI dans le droit cantonal) – puissent également mandater les organismes spécialisés centraux de la Confédération afin qu'il ne faille pas mettre en place à nouveau des services spécialisés. Ce canton demande également que les dispositions légales prévoient des délais transitoires raisonnables.

LU salue sur le principe l'intention du projet de loi et son orientation. Ce canton estime que, grâce à son orientation sur une sécurité intégrale de l'information, ce projet de loi tient

compte de manière adéquate des récentes mutations sociétales et techniques en matière de traitement de l'information. Au chapitre 3 (contrôles de sécurité relatifs aux personnes), LU constate que ce projet de loi prévoit une certaine sur-réglementation qui risque de créer une charge excessive de travail pour les cantons. Par ailleurs, les coûts incombant aux cantons ne sont pas clairement définis. L'exécution de cette loi devra donc être aménagée de telle manière que les cantons ne soient pas exposés à une lourde charge administrative.

UR salue sur le principe le projet de LSI et, partant, la sécurité du droit à créer dans le domaine de la sécurité de l'information. Concernant les frais dans le cadre du management de risques ainsi que pour les mesures de sécurité et de protection nécessaires, il s'agira de faire preuve de discernement. Par ailleurs, il conviendra de tenir compte – au moyen de dispositions complémentaires juridiquement contraignantes – du traitement des données et systèmes classifiés et des conséquences qui en résulteront pour les cantons. UR reconnaît l'importance des contrôles de sécurité relatifs aux personnes.

SZ plébiscite la création d'une base légale homogène quant à la forme pour la gestion de la sécurité de l'information dans le domaine de compétences de la Confédération. Ce canton soutient la LSI. SZ part de l'idée que les cantons, dans la mesure où ils seraient concernés, devraient également être invités à se prononcer en procédure de consultation concernant les dispositions d'exécution.

OW salue l'orientation du présent projet de loi qui prévoit de réglementer de manière globale la sécurité de l'information avec la profondeur qu'exigent les divers domaines. La charge excédentaire que devraient supporter les cantons devrait se situer dans un cadre étroit, défini en fonction de la quote-part plutôt modeste des tâches fédérales par rapport aux tâches globales.

Pour NW, le projet de loi sur la sécurité de l'information est au premier chef une bonne et vaste mise en œuvre du système de gestion d'informations (ISMS) selon les normes ISO 2700x. NW estime que les cantons ne sont concernés que dans la mesure où ils exercent des activités sensibles du point de vue de la sécurité à la demande directe de la Confédération et sous sa surveillance. Ce canton est également d'avis qu'il sera probablement difficile d'élaborer des critères uniformes pouvant aussi répondre aux conditions prédominantes prévalant dans les différents cantons. Si ce projet de loi devait aboutir et entrer en vigueur avec la teneur présentée en procédure de consultation, les ordonnances d'exécution de la LSI pourraient générer une énorme charge opérationnelle pour NW. Dès lors, NW part de l'idée que les cantons seront également invités à se prononcer lorsqu'il s'agira de déterminer les dispositions d'exécution en la matière.

Pour GL, la loi sur la sécurité de l'information apporte davantage de clarté pour les autorités fédérales. Pour les cantons, une récapitulation de leurs tâches essentielles, de leurs compétences et de leurs responsabilités serait utile. Quant à certains termes utilisés dans le projet de loi, il conviendrait encore de les concrétiser. Sous quelle forme et sous quelles conditions les cantons sont-ils concernés? Quelles sont les formations nécessaires? Ces éléments manquent de clarté.

ZG soutient les efforts de la Confédération en vue d'améliorer la sécurité de l'information et ainsi répondre aux exigences d'une société civile d'informations mise en réseau. Ce canton salue aussi le fait que la Confédération joue un rôle de précurseur dans la législation en matière de sécurité de l'information. Le but recherché est d'atteindre un niveau de sécurité aussi homogène que possible et une doctrine cohérente. Certes, le projet de loi semble approprié quant au fond pour atteindre cet objectif, mais ZG se demande si la réglementation de la clause d'exemption (opting out) proposée peut y mener. En effet, cette réglementation implique que chaque autorité soit autonome dans son domaine en matière d'exécution et édicte un droit respectif par voie d'ordonnance. Voilà pourquoi la loi devrait définir davantage que des normes minimales si l'on veut que la sécurité de l'information puisse être garantie dans toutes les autorités affiliées. Des standards et des normes qui se chevauchent seraient alors nécessaires et importantes. Il serait donc aussi judicieux d'impliquer de manière générale les cantons dans ces réflexions. En effet, tant dans le projet de loi que dans le rapport explicatif, il semble que l'on ait trop peu réfléchi aux incidences sur les cantons.

FR salue la volonté du Conseil fédéral d'uniformiser les standards applicables en matière de sécurité de l'information au niveau fédéral. Il relève toutefois que les règles applicables à la vérification de la mise en œuvre des mesures fondées sur la LSI ainsi qu'à l'exécution des contrôles de sécurité relatifs aux personnes pour les organes cantonaux doivent encore être fixées par le Conseil fédéral. Il souhaite avoir la possibilité de se déterminer sur les dispositions d'exécution qui seront élaborées par le Conseil fédéral.

SO salue le fait que la Confédération règle les principes de la sécurité de l'information dans une loi. De l'avis de SO, on ne peut répondre de la sécurité de l'information que si l'on dispose d'instruments modernes pour en assurer la protection et que les lacunes existant dans le droit actuellement en vigueur sont comblées. SO estime qu'il est aussi important d'élaborer des règles très claires à l'échelon de la loi pour les contrôles de sécurité relatifs aux personnes, car les mesures ad hoc constituent une ingérence importante quant aux droits de la personnalité des individus concernés. SO a par ailleurs des propositions d'amendements portant sur quelques points.

BS salue de manière générale la réglementation prévue. Sur divers points toutefois, ce canton souhaite proposer des amendements ou apporter des remarques complémentaires.

BL adhère à ce projet de loi et dit que l'on reconnaît de manière générale la nécessité d'agir dans le domaine de la sécurité de l'information. Comme les mesures législatives prévues contribueront à augmenter la sécurité de l'information, BL les appuie. Etant donné que le rapport explicatif ne dit rien des frais qui pourraient être à la charge des cantons, il ne faudrait toutefois pas que la subordination des cantons à cette nouvelle loi entraîne des frais à leur charge.

SH se déclare d'accord avec ce projet de loi.

AI est d'accord avec cette nouvelle loi sous réserve de trois points, à savoir l'indemnisation intégrale par la Confédération des frais encourus par les cantons, l'accès gratuit des cantons aux services spécialisés de la Confédération et la soumission préalable des ordonnances du Conseil fédéral aux cantons pour qu'ils puissent se prononcer.

AR salue ce projet de loi même si les cantons, respectivement quelques offices cantonaux ne sont que marginalement touchés par cette loi fédérale. Dans ces conditions, AR n'estime pas nécessaire de se prononcer plus en détail.

SG limite sa prise de position au chapitre des contrôles de sécurité relatifs aux personnes, car, de fait, seules ces dispositions concernent directement le canton. Au demeurant, de manière générale, SG n'a pas d'opposition à formuler à l'encontre de ces nouvelles dispositions.

GR salue de manière générale l'élaboration d'une loi fédérale sur la sécurité de l'information. Mais à son avis, les interfaces entre la Confédération et les cantons ne sont pas énoncées de manière suffisamment claire. Par ailleurs, il convient de concéder aux cantons la possibilité de mandater les services centraux spécialisés de la Confédération qui, selon la LSI, devront encore être créés. En outre, pour la mise en œuvre de cette loi, il convient de prévoir des délais de transition appropriés d'au moins cinq à dix ans adaptés à la durée de vie des systèmes TIC.

AG adhère de manière générale à l'acte législatif de la LSI, mais demande que l'on clarifie dans le cadre de la procédure législative, les questions en suspens concernant le contrôle de sécurité relatif aux employés cantonaux, la procédure de surveillance par la Confédération ainsi que la question des interfaces du droit en matière de sécurité de l'information avec la surveillance des cantons en matière de protection des données. Il convient ensuite que ces points soient commentés dans le message.

TG estime que ce projet de loi sur la sécurité de l'information peut constituer un acte législatif de grande importance au niveau du droit en matière de protection des données. Mais si une telle loi comportait un libellé trop strict, elle pourrait aussi présenter divers risques pour les droits de la personnalité des individus concernés.

TI salue l'intention et l'orientation de la révision de loi. TI rappelle que ce projet de loi a pour but principal la consolidation et la coordination des dispositions existantes en la matière. Une telle loi permettrait d'anticiper correctement en fonction des menaces éventuelles liées à l'augmentation continue du nombre de systèmes TIC, à l'externalisation de données et à leur mise en réseau croissante. C'est pourquoi des bases légales très claires assorties d'une densité réglementaire élevée à l'échelon de la loi dans chaque domaine se justifieraient là où se produisent des ingérences souvent graves dans les droits fondamentaux qui protègent la liberté individuelle, la personnalité et la sphère privée des citoyens.

VD n'a pas d'objection de principe contre le projet considéré, qui vise à uniformiser les bases légales régissant la gestion et l'organisation de la sécurité de l'information au sein de la Confédération, dans un contexte de risques qui vont en se diversifiant et en augmentant, ceci dans le respect des exigences légales de la protection des données. VD a pris note de l'analyse selon laquelle les conséquences pour les cantons seraient minimes, ces derniers n'étant concernés que dans la mesure où ils exercent des activités sensibles sur mandat de la Confédération et sous la surveillance de celle-ci. Néanmoins, VD ne peut exclure que l'impact en terme de ressources humaines et sous l'angle financier soit plus important que prévu: ce point devra évidemment être dûment analysé lorsque seront élaborées les dispositions d'applications. VD souhaite en particulier que dans ce cadre, les services cantonaux de police et de renseignements, actuellement chargés d'exécuter les contrôles de sécurité relatifs aux personnes et autorisés ä accéder aux données nécessaires ä cette tâche, conservent dans le futur cette compétence et les moyens qui l'accompagnent.

VS salue ce projet de loi dont le but est de créer des bases légales uniformes pour la gestion et l'organisation de la sécurité de l'information au sein de la Confédération. VS comprend aussi que le Conseil fédéral devra régler, dans ses dispositions d'exécution, le contrôle de l'application des mesures ainsi que les contrôles de sécurité relatifs au personnel cantonal. A cet égard, VS souhaite que les services compétents du canton du Valais puissent être intégrés ä ces travaux dès leurs débuts afin d'y pouvoir participer de manière active.

NE soutient la volonté du Conseil fédéral de placer un cadre transversal à sa politique de gestion de la sécurité de l'information. La loi proposée va dans le bon sens et répond certainement déjà aux préoccupations du Conseil fédéral, sans avoir une prolongation forte au sein des cantons. Néanmoins, la sécurité de l'information doit aussi être vue avec ses partenaires cantonaux et communaux comme pour tous les problèmes de sécurité. NE souhaite donc que puisse être intégré dans cette nouvelle loi, un organe de coordination entre la Confédération et les cantons afin de pouvoir défendre une politique commune en matière de sécurisation de nos infrastructures de communication et surtout de lutte contre la cybercriminalité.

D'une manière générale, GE salue l'initiative visant à sécuriser la gestion et l'organisation de la sécurité de l'information au sein de la Confédération. Cette loi est complète et prend en compte tous les paramètres nécessaires. GE est donc favorable à ce projet de loi qui ne devrait guère avoir d'impact pour l'administration cantonale.

JU salue ce projet de loi, conscient de la nécessité d'adapter le cadre légal face aux évolutions des technologies numériques et des risques associés. L'ensemble du texte apporte les éléments fondateurs d'une politique de sécurité permettant à la Suisse de limiter grandement les risques liés au domaine du numérique, et rien n'est à signaler tant sur la forme que sur le fond. Ces bases légales mettent en avant la gestion des risques comme moyen d'amélioration de la sécurité, et vont clairement dans le sens d'un progrès global du niveau de sécurité requis à l'échelle nationale. JU adhère pleinement à ce projet.

3.2 Les partis politiques représentés au sein de l'Assemblée fédérale

Le PDC adhère de manière générale à l'élaboration d'une loi fédérale sur la sécurité de l'information. Ce parti estime que dans notre société civile toujours davantage mise en réseau, la protection des informations prend de plus en plus d'importance. De fait, l'évolution vers une société de l'information n'offre pas uniquement des chances mais comporte aussi des risques. Voilà pourquoi le PDC se prononce en faveur d'une base légale uniforme pour

la gestion et l'organisation de la sécurité de l'information pour les autorités qui doivent effectuer cette tâche. Le PDC demande toutefois au Conseil fédéral qu'il indique, dans son message, où il y a des interfaces, d'une part avec des systèmes déjà existants, d'autre part entre les institutions et les particuliers en dehors de l'administration fédérale.

Le PLR soutient cette loi dans son principe de fond qui vise à améliorer la sécurité de notre pays. Il est en faveur de son principe général qui définit comme objectif une mise à niveau de la sécurité de l'information en adéquation avec l'utilisation croissante des TIC (technologies de l'information et de la communication), dont dépendent de plus en plus les autorités de la Confédération. La gestion des risques liés à l'utilisation des TIC dans tous les secteurs de la Confédération est donc devenue une nécessité inhérente au développement de la société de l'information. Cette loi est en effet nécessaire pour combler les lacunes techniques de notre système de protection des informations, mais également les lacunes organisationnelles. C'est pourquoi, le PLR se prononce en faveur du rassemblement des mesures en matière de protection d'informations en une seule réglementation homogène concernant toutes les autorités fédérales ainsi que leurs subordonnées. Pour le PLR il est important qu'un équilibre soit trouvé entre le niveau de sécurité et les coûts nécessaires pour l'obtenir, afin d'éviter une explosion des dépenses.

Du point de vue de l'UDC, il y a lieu de rejeter ce projet de loi, car une loi fédérale sur la sécurité de l'information ne générerait pas de valeurs ajoutées déterminantes. Au contraire, une telle loi ne ferait qu'engendrer beaucoup trop de bureaucratie supplémentaire et ne pourrait que modestement contribuer à une mise en œuvre uniforme des dispositions. Ce projet laisse aux autorités fédérales concernées, pour ce qui est de leur indépendance et de leur autonomie organisationnelle, un grand pouvoir d'appréciation dans la mise en œuvre de cette loi. L'UDC est ainsi d'avis qu'il y a plus d'avantages à maintenir le système actuellement en vigueur en y apportant au besoin des améliorations ciblées dans le cadre des structures existantes.

Le PSS salue l'intention et l'orientation du projet de loi. A son avis, le présent projet de loi sur la sécurité de l'information (LSI), de par son orientation sur une sécurité intégrale de l'information, tient compte de manière appropriée – en matière de gestion de l'information – des changements sociétaux et techniques de ces dernières années. Dans l'ensemble, la nouvelle LSI constitue une bonne base pour instituer une organisation globale, moderne et professionnelle de la protection de l'information. Quant à savoir si l'objectif sera atteint au bout du compte, tout dépendra de manière déterminante des ressources financières et en personnel à disposition. Pour le PSS, il est crucial que la LSI ne soit pas en conflit avec les principes de la transparence de l'administration, de la protection des données ainsi qu'avec les exigences qu'impliquent un bon service public et d'autres principes tout aussi importants. Le PSS attend de cette loi que la classification des informations – tel que l'art. 12 en indique le principe – se limite effectivement «au minimum requis» et que les catégories de sécurité des moyens TIC soient mises en œuvre de manière à ce que les «fonctionnaires» concernés puissent continuer à accomplir leurs tâches de manière simple grâce à des instruments conviviaux pour l'utilisateur. Le PSS demande en outre que le législateur renforce la protection des données de divers éléments de la loi et qu'il s'assure que l'obligation d'archivage soit respectée.

3.3 Associations faîtières suisses des communes, villes et régions de montagne

L'Union des villes suisses (UVS) renonce expressément à se prononcer, mais elle renvoie toutefois à l'avis exprimé par la Conférence suisse sur l'informatique (CSI).

3.4 Associations faîtières suisses représentant les milieux économiques

Economiesuisse salue l'intention exprimée dans le projet de loi, à savoir, adapter la gestion de l'information des autorités fédérales aux exigences de la société de l'information moderne et mise en réseau. Economiesuisse adhère de manière générale à la loi proposée visant à créer une base légale formelle uniforme en vue de la protection des informations et de la sécurité dans la mise en œuvre des moyens TIC. Il est important pour les entreprises que la

confidentialité des informations sensibles traitées par les autorités fédérales soit garantie. Toutefois, de l'avis d'economiesuisse, le présent projet de loi comporte nombre de définitions trop floues et trop globales. C'est pourquoi cette association faîtière demande que le pouvoir d'appréciation des autorités concernées soit limité par le biais de dispositions plus précises et de critères d'appréciation clairs figurant dans la future ordonnance d'exécution.

L'Union suisse des arts et métiers (USAM) rejette le présent projet du fait que la loi porte un titre qui induit en erreur et que la qualité des éléments explicatifs est lacunaire. Toutefois, si le rapport explicatif était significativement amélioré et l'intitulé de la loi davantage précisé, l'USAM serait d'accord sur le fond du projet de loi. En même temps, dans sa prise de position, l'USAM joint l'avis exprimé par la Chambre vaudoise des arts et métiers (Fédération patronale vaudoise, FPV) qui, quant à elle, soutient expressément ce projet de loi.

L'Union patronale suisse (UPS) et la Société suisse des employés de commerce (SEC), ont renoncé expressément à se prononcer, étant donné que le projet de loi ne les concerne pas directement.

3.5 Autres organisations intéressées

AS-MPC prend acte que la haute autorité de surveillance, concernée par les dispositions de l'art. 2, let. d, en tant qu'autorité devant appliquer cette loi pourrait, aux termes de l'art. 87, al. 1, édicter ses propres dispositions d'exécution. De ce fait, certaines réserves que cette autorité avait émises dans le cadre de la consultation des offices, du 2 avril 2013 n'ont plus cours. Deux points, cependant, sont encore flous concernant l'autorité de surveillance, respectivement le Ministère public de la Confédération: premièrement, auprès de quelle autorité une décision rendue par l'organe de contrôle peut-elle être contestée? Deuxièmement, comment devraient s'effectuer après coup les contrôles de sécurité relatifs aux personnes qui n'ont jusqu'ici pas été soumises à un tel contrôle de sécurité, mais devraient l'être selon les nouvelles dispositions de cette loi?

Dans le traitement et la protection d'informations dans le contexte d'une procédure pénale, le MPC estime devoir appliquer les consignes découlant du Code de procédure pénale (CCP). Or, ces dispositions-là règlent déjà, en particulier, l'accès aux informations provenant d'une procédure pénale, ceci de manière détaillée et pertinente. Le MPC prend déjà en considération les consignes de la LSI dans le contexte de la mise en œuvre du projet relatif à la sécurité intégrale. Par ailleurs, il renvoie à sa prise de position du 12 avril 2013 (classification de dossiers / d'informations provenant d'une procédure pénale, classification de sécurité de moyens TIC).

Privatim peut se déclarer d'accord de manière générale avec l'élaboration d'une loi fédérale sur la sécurité de l'information et ce pour deux raisons: le législateur accorde enfin à la sécurité de l'information le rôle qu'elle aurait dû jouer depuis longtemps dans les tâches quotidiennes de l'administration et dans la société civile. Par ailleurs, l'exécution des contrôles de sécurité relatifs aux personnes (CSP) serait réglementée dans une base légale indispensable à cette tâche. Toutefois, le projet de loi sur la LSI ainsi que le rapport explicatif soulèvent encore diverses questions de droit concernant la protection des données et de l'information, questions qu'il convient impérativement de discuter, clarifier et améliorer.

La Conférence suisse sur l'informatique (CSI) apprécie toute amélioration et collaboration dans le domaine de l'information à l'échelon national entre la Confédération, les cantons et les communes. Au vu des modestes ressources du service spécialisé de la CSI, cet organisme se limite, dans sa prise de position, aux sujets qui sont pertinents pour les cantons. Ainsi, la CSI ne peut-elle adhérer au projet de loi qu'à deux conditions. La première est que les autorités cantonales et communales – pour autant qu'elles appliquent cette loi, puissent également mandater les services centraux spécialisés de la Confédération, et notamment les services spécialisés, pour effectuer des contrôles de sécurités relatifs aux personnes (CSP) ou demander la mise en œuvre de la procédure de sécurité pour les entreprises, ceci afin que les cantons ou les communes n'aient pas besoin de mettre en place à nouveau de tels services en propre. La deuxième condition est que le législateur doit prévoir une période transitoire raisonnable. A défaut de ces deux conditions, il conviendrait d'exclure les cantons

du champ d'application de la LSI. La CSI s'attend aussi à ce que les cantons, respectivement leurs services spécialisés, soient invités à collaborer étroitement lors de l'élaboration des dispositions d'exécution de cette loi fédérale, en particulier dans la mesure où les dispositions d'exécution concernent également les cantons.

La BNS salue également de manière générale l'orientation de ce projet de loi visant à protéger les intérêts du pays et en particulier les intérêts de l'économie, de la finance et de la politique monétaire de la Suisse. La BNS estime que ce projet de loi se propose de relever le défi de créer une base commune pour la sécurité de l'information des autorités d'une part et d'organisations d'autre part. Dans ce contexte, l'obligation des autorités aux termes de l'art. 2, al. 1, du projet de loi s'avère exigeante, étant donné que lesdites autorités ne sont, par principe, nullement subordonnées à un pouvoir d'instruction directe de la part d'une autre autorité. La BNS relève que le projet de loi ne respecte pas le principe selon lequel l'autonomie conférée aux autorités concernées par la Constitution fédérale ne doit pas être remise en cause. La BNS attache une grande importance à ce que les consignes édictées par le projet de loi soient conciliables avec l'autonomie de la Banque nationale suisse garantie par la Constitution fédérale (art. 99, al. 2, Cst).

Le TF déclare que quelques-uns des articles ont une grande importance pour le Tribunal fédéral et qu'ils ne devraient par conséquent pas être modifiés à son détriment. Pour le reste, le TF renonce à se prononcer de manière plus détaillée.

Le TFB, après avoir étudié la documentation qui lui a été remise, renonce à se prononcer.

Le TAF renonce expressément à se prononcer mais tient à préciser que son abstention ne doit pas être considérée comme une approbation du projet de loi.

Swico approuve l'adaptation des bases légales prévue dans le présent projet de loi à une société d'information moderne largement mise en réseau. Cet organisme constate toutefois que le projet de loi est en majeure partie très flou dans ses définitions et qu'il est rédigé lato sensu, ce qui donne évidemment beaucoup trop de pouvoir d'appréciation aux autorités concernées. Swico demande dès lors que la mise en œuvre de l'ordonnance d'exécution en la matière soit concrète et comporte des notions et définitions claires.

3.6 Participants non invités à titre individuel

Clusis se prononce sur quelques articles spécifiques sans donner d'appréciation générale sur le projet de loi.

CP et CVAM peuvent soutenir le projet de loi fédérale sur la sécurité de l'information (LSI). Au mieux, cette loi d'organisation permettra à la Confédération de poser des bases juridiques claires et homogènes en la matière, même si, concrètement, elle ne devrait renforcer que de peu le niveau de sécurité. En outre, la procédure relative aux entreprises est de nature à améliorer leur compétitivité dans un domaine sensible.

La FER ne se prononce que sur quatre articles et une section, sans donner d'appréciation générale sur le projet de loi.

Insecor salue la réglementation uniforme de la sécurité de l'information, ainsi que celle énoncée à l'échelon de la loi. Insecor déclare que la nouvelle loi sur la sécurité de l'information comblerait une lacune, ce qui devient urgent dans le contexte légal de la sécurité de l'information et non seulement aura sans nul doute une portée considérable pour l'administration fédérale ou les autorités cantonales, mais donnera aussi des points de repère importants pour l'économie privée. Insecor approuve donc de manière générale ce projet de loi mais y ajoute quelques réflexions et suggestions.

It-rm salue le fait que l'on présente au Parlement un projet de loi qui règle la protection des informations au sein de l'administration fédérale et d'autorités qui leur sont proches. Toutefois, de l'avis d'it-rm, ce projet de loi accorde une importance trop élevée à la confidentialité des informations (comme par exemple lors de la classification selon l'at. 14) et édulcore ainsi la protection d'autres informations confidentielles. Pour assurer le fonctionnement d'une société civile et d'une administration modernes dotées de moyens TIC ainsi que pour garantir

les intérêts économiques et financiers d'un état, il convient de ne pas disposer d'une protection concernant exclusivement des informations confidentielles, mais surtout aussi des informations auxquelles tous les citoyens et fonctionnaires doivent pouvoir se fier – telles que des informations issues d'un registre ou d'archives.

LB a l'impression que l'approche globale prévue par la LSI pour garantir la sécurité de l'information dans tous les champs d'application dévolus aux autorités concernées de la Confédération et des cantons ainsi qu'aux organisations privées chargées d'exécuter des tâches administratives ne répond pas au but que la LSI s'est assigné. Il conviendrait plutôt de viser une voie qui permettrait de limiter l'application de la LSI à des domaines décisifs en vue de la protection des intérêts de notre pays, de sa société civile et de son économie. A cet égard, la LSI, de par ses 94 articles et ses plus de 30 pages, s'apparente à un monstre législatif qui n'est comparable à aucune réglementation étrangère connue, qui comporte nombre de notions juridiques floues et qui laisse bien des questions sans réponse. Sa mise en œuvre dans des domaines qui ne devraient pas être décisifs pour l'intérêt global de notre pays se traduira sans nul doute par des charges très élevées. Il conviendrait dès lors d'axer le champ d'application de la LSI sur des menaces existentielles concernant les domaines essentiels – décrits à l'art. 1, al. 2, LSI – pour la gestion d'informations vitales et les moyens TIC mis en œuvre dans ce contexte. On obtiendrait ainsi un rapport optimal entre les coûts et les avantages en matière de sécurité de l'information. Par ailleurs, il conviendrait aussi de se demander s'il ne vaut pas mieux épurer la LSI de nombre de dispositions détaillées, dont beaucoup vont de soi dans le domaine de la sécurité de l'information. Lesdites dispositions relèvent en effet d'autres échelons, à savoir notamment ceux de l'ordonnance d'exécution, des recommandations, des directives ou des listes de contrôle.

Le SRC évoque quelques articles dont le contenu devrait être adapté. En dehors de ce point, le SRC ne s'exprime pas sur ce projet de loi.

Le Conseil des EPF soutient de manière générale le présent projet de loi et salue surtout l'uniformisation des consignes pour toute l'administration fédérale. Cependant, le Conseil des EPF relève que la recherche occupe une position particulière au sein du domaine de la Confédération, étant donné qu'elle est tributaire d'un échange aussi ouvert que possible et d'une collaboration nationale et internationale sans accrocs. C'est pourquoi le Conseil des EPF saluerait le fait que les dispositions de l'ordonnance d'exécution de la LSI tiennent compte aussi largement que possible de ces éléments, en prévoyant éventuellement des dispositions d'exception pour le domaine de la recherche. Si ce n'était pas le cas, le pôle de recherche que constitue la Suisse pourrait être en danger dans sa forme actuelle. Le Conseil des EPF constate en résumé que ce projet de loi n'est encore pas assez cohérent, ni assez pensé. Il estime que ce projet de loi comporte encore de nombreuses incertitudes sur le plan juridique et, partant, laisse une trop large marge d'interprétation.

La CRUS est consciente de l'importance de la sécurité des informations. Le projet de Loi sur la sécurité de l'information s'applique toutefois uniquement aux instances mentionnées explicitement à l'art. 2. Les universités ne devraient être concernées que dans la mesure où elles se voient confiés des mandats par une de ces instances. Les mesures relatives à la sécurité des informations qui découleraient de tels mandats dépendront ainsi des dispositions de l'autorité donnant le mandat. Pour la CRUS, il importe que l'autorité en question veille à couvrir les coûts qui découleront de l'application de ces dispositions par les universités. Il convient par ailleurs de veiller à ce que lesdites mesures n'empêchent la publication de résultats scientifiques résultant de mandats de recherche.

La FMH salue l'orientation de ce projet de loi visant à élaborer des bases légales uniformes en matière de sécurité de l'information pour l'ensemble des autorités fédérales. La FMH se réjouit que ce projet comporte des exigences et des mesures permettant de faire face à toutes les éventualités en matière de protection de la confidentialité, de la disponibilité, de l'intégrité et la reproductibilité/la traçabilité de l'information, ceci indépendamment du fait que les informations soient fournies par voie électronique, oralement ou sous forme de papier. De l'avis de la FMH, il importe toutefois de protéger en particulier les données personnelles au sens large de la sécurité de l'information, telle qu'elle est décrite dans le rapport explicatif.

4 Prises de position au sujet de la partie générale du rapport explicatif

Figurent ci-après les prises de position à propos des différents sujets que contient la partie générale du rapport explicatif. Nous ne ferons toutefois figurer que les sujets de la partie générale du rapport explicatif ayant fait l'objet d'un avis explicite ou implicite.

4.1 Risques de la société de l'information

Le PSS est d'accord avec l'analyse, figurant dans le rapport, des chances et des risques que représente la société de l'information, et notamment avec la déclaration selon laquelle la lutte contre les risques ne doit pas amener à une diminution des chances qu'offre la société de l'information. Il serait inacceptable pour le PSS que la Suisse s'engage dans la course aux instruments numériques orchestrée par quelques grandes puissances. Ce que l'on demande aujourd'hui, ce sont plutôt des mesures génératrices de confiance, en instaurant la plus grande transparence possible et une collaboration internationale. Par conséquent, le PSS soutient la déclaration figurant dans le rapport explicatif, selon laquelle il ne faudrait pas identifier les risques seulement dans le domaine cybernétique, mais les analyser dans un contexte beaucoup plus large. Cependant, le PSS constate en même temps que le Conseil fédéral a certes fait du bon travail jusqu'ici dans le domaine de l'analyse et de la formulation d'une «Stratégie nationale pour une société de l'information Suisse 2011-2015», d'une Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) et d'une «Stratégie nationale de protection des infrastructures critiques (stratégie PIC)».Pourtant, selon le PSS, la mise en œuvre de ces stratégies comporte de grandes lacunes.

4.2 Organisation actuelle de la sécurité de l'information dans l'administration fédérale

SO relève qu'au chiffre 1.3.1.2 à la p. 28 du rapport explicatif, l'organisation de la protection des données est commentée sans que les compétences des préposés cantonaux à la protection des données soient mentionnées. Pourtant ces préposés sont compétents pour la haute surveillance de la protection des données d'autorités cantonales, et cela même si les autorités cantonales exécutent des tâches relevant de la compétence de la Confédération. SO estime qu'il convient par conséquent de spécifier que la loi proposée ne modifierait en rien les compétences en matière de haute surveillance de la protection des données et que les autorités cantonales qui effectuent, sur mandat de la Confédération, des activités sensibles sur le plan de la sécurité resteraient sous la haute surveillance des préposés cantonaux à la protection des données.

Privatim demande aussi de préciser dans le message, au chiffre 1.3.1.2, que les préposés cantonaux à la protection des données resteraient compétents concernant la haute surveillance, en matière de protection des données, des autorités cantonales accomplissant sur mandat de la Confédération des tâches sensibles sur le plan de la sécurité. En effet, les organes publics des cantons qui effectuent des tâches de la Confédération ne peuvent être considérés comme des organes de la Confédération et doivent dès lors continuer à être subordonnés aux lois cantonales relatives à l'information et à la protection des données, et donc être assujettis à la haute surveillance cantonale en matière de protection de données.

5 Prises de position à l'égard des projets de loi et leurs commentaires

Figurent ci-après les prises de position concernant spécifiquement des articles individuels des projets de loi ou des commentaires desdits projets. Ne figureront donc ici que les articles ayant fait l'objet d'une prise de position explicite ou implicite.

5.1 Loi fédérale sur la sécurité de l'information

Généralités

NW relève que l'on utilise dans cette loi fédérale la notion de sécurité de l'information. Or, ce n'est pas encore le cas de la législation du canton de NW. Il sera donc quelque peu difficile d'élaborer des critères uniformes qui satisferont aux conditions prépondérantes existant dans les différents cantons. NW donne comme exemple, d'une part, la définition des «activités sensibles» donnée à l'art. 2, al. 3, LSI et, d'autre part, les niveaux de classification des données et des informations (par ex. «interne», «confidentiel», «secret»).

SO relève que ni le projet de loi de la LSI ni le rapport explicatif n'abordent le cycle de vie des documents, respectivement des informations. Pourtant, il serait important de régler quelles sont les relations des différentes dispositions de la LSI avec la création de documents, leur utilisation, leur sauvegarde, leur archivage et leur destruction.

L'USAM déplore les aspects lacunaires du rapport explicatif relatifs à la loi sur la sécurité de l'information. Des phrases telles que «L'information est la monnaie d'échange de la société de l'information» (p. 1) ou encore «Depuis quelques décennies, le monde connaît une mutation sociétale fondamentale provoquée par le développement des technologies de l'information et de la communication (TIC)» (p. 9) ne sont que des mots creux qui n'ont pas la moindre teneur explicative. Même si ces déclarations étaient substantielles, elles seraient encore et toujours objectivement fausses et sont intégrées au rapport explicatif de matière décousue ou irréfléchie. L'USAM estime que ce défaut de qualité se retrouve aussi dans les modèles conceptuels utilisés dans le rapport explicatif. Un exemple particulièrement flagrant d'idée simpliste figure à la p. 78 du rapport: «La société est concernée de deux points de vue. D'une part, elle aura davantage confiance dans le traitement des informations par les autorités fédérales.» L'USAM trouve surprenant de constater le rapport de cause à effet «à bon marché» utilisé dans cette déclaration. Même la vérification empirique de cette déclaration semble si manifestement invraisemblable que l'on ne peut s'expliquer comment elle a pu être conçue et encore moins comment elle a pu être publiée.

Selon la swico, le présent projet de loi comporte un certain nombre de définitions et de dispositions floues et prêtant à interprétation (par ex. activités sensibles, domaines sensibles, etc.). La swico demande donc que l'on délimite avec précision la marge d'appréciation et que l'on élabore des définitions ainsi que des critères clairs dans la future ordonnance d'exécution, ceci afin de prévenir le risque d'inégalité de traitement et de distorsions en matière de concurrence.

Insecor relève que certains contenus essentiels figurent dans le rapport explicatif mais pas dans le projet de loi. Cette observation concerne notamment une série de notions. Il conviendra de vérifier systématiquement, pour une meilleure compréhension du projet, quels contenus figurant dans le rapport explicatif devraient être intégrés dans le texte de loi et lesquels ne devraient pas l'être.

Titre

Selon l'USAM, le titre de cet acte législatif est quelque peu déroutant. En effet, selon l'article qui définit le but de cette loi et le rapport explicatif, il est clair que la LSI s'adresse à des autorités et institutions similaires et que l'on n'a ainsi en particulier pas créé une réglementation sociétale globale en matière d'information et de sécurité de l'information. Mais cette intention devrait figurer directement dans le titre, par exemple en le complétant comme suit: «Loi fédérale sur la sécurité de l'information au sein des autorités fédérales et organisations similaires».

Chapitre 1 Dispositions générales

Généralités

BS propose, dans l'intention d'une compréhension des notions de la sécurité de l'information et de ses trois domaines – la protection de l'information, la protection des données et la sécurité informatique – de les définir dans une disposition liminaire.

Pour privatim, ni la LSI ni le rapport explicatif n'abordent le sujet du cycle de vie des documents ou des informations qu'il convient de protéger. Comment se déroule la classification dans les divers stades du cycle de vie d'un document ou d'une information que constituent sa création, son utilisation, sa sauvegarde jusqu'à sa destruction? Ce sujet doit impérativement être réglé et s'il ne l'est pas dans la loi elle-même, il devrait au moins être abordé dans le message.

Insecor suggère de libeller les articles introductifs de la LSI comme suit (pour en connaître les motifs, voir aussi ci-après les observations relatives aux art. 2 et 3 LSI) et définir les notions les plus importantes de la sécurité et de la classification de l'information dans la présente loi déjà: art. 1 But (ou objet); art. 2 Champ d'application; art. 3 Définitions. En pratique, ce sont précisément les définitions légales faisant défaut dans le domaine de la sécurité de l'information qui ont généré de grandes ambiguïtés et des discussions à ce sujet. S'agissant de bases légales concernant des thèmes complexes, il est très important de clarifier les définitions déjà au niveau de la loi fédérale.

Le Conseil des EPF regrette la suppression totale de l'ancien art. 5 LSI dans sa version de 2013, qui comportait une définition de ces notions. Du fait que la définition des notions importantes dans la version actuelle du projet de LSI a été supprimée, on ne sait plus d'emblée ce qu'il faut par exemple entendre globalement par moyens TIC. Le Conseil des EPF propose donc que l'on intègre à nouveau à un endroit approprié le catalogue des définitions desdites notions, que ce soit dans la LSI elle-même ou, si c'est plus simple pour apporter un complément ou une correction aux définitions, dans l'ordonnance d'exécution de la LSI.

Art. 1 But

Vu la réglementation prévue de la clause d'exemption (opting out) figurant à l'art. 87, al. 3, LSI – qui précise que toute autorité concernée peut édicter des dispositions d'exécution et que les exigences standard et les mesures fixées par le Conseil fédéral n'ont que le caractère d'une recommandation, ZH estime qu'il existe un risque que les définitions parfois très larges figurant dans la loi puissent être interprétées différemment d'une autorité à l'autre. Cela aurait pour conséquence que les diverses autorités concernées pourraient édicter des dispositions d'exécution elles aussi différentes d'une autorité à l'autre. Par conséquent, ZH est d'avis que, dans cette loi en soi très détaillée, il conviendrait de définir à l'art. 1, al. 2, LSI les intérêts publics devant être protégés, tout comme il y aurait également lieu de spécifier plus en détail les échelons de classification.

TI tient à signaler qu'à son avis, la liste des objectifs de ces dispositions légales est trop restrictive du fait qu'elle ne se référerait qu'à la protection des intérêts publics (en particulier ceux de la Confédération) et qu'elle ne concernerait qu'indirectement les intérêts privés. L'exigence de protéger les droits de la personnalité et de la sphère privée (et ainsi également les données personnelles) ainsi que le secret professionnel, commercial et de fabrication ne devrait pas être limité implicitement à la disposition figurant à la let. e. Car finalement on renforcerait la confiance dans les entités qui traiteraient ce type d'informations sur la base du droit spécial. Pour TI, il convient donc d'indiquer expressément ces éléments même seulement à titre d'exemples, en adaptant en conséquence les lettres respectives de la réglementation. Vu ce qui précède, TI est donc d'avis qu'il convient d'ajouter dans la phrase introductive de l'al. 2 la protection des intérêts privés (et non pas seulement des intérêts publics).

Le PSS soutient le but défini à l'art. 1, al. 1, de la LSI, à savoir la garantie de la sécurité du traitement des informations et de l'engagement de moyens technologiques en matière d'information et de communication. Ce parti approuve également la renonciation à une définition légale de ce qu'il faut comprendre par «information». En effet, selon ce parti, il va de

soi que cette notion englobe implicitement aussi les données (électroniques) en tous genres. La tentative exprimée à l'al. 2 de mentionner la protection des «intérêts publics» est également compréhensible. Certes, les termes choisis sont parfois abstraits au point qu'ils permettent une marge d'interprétation extrêmement large. De ce fait, il existe le risque d'interprétations excessives, risque d'autant plus grand que, plus loin dans la loi, l'art. 1, al. 2, let. a à d, sert de base pour déterminer les échelons de classification (art. 14 LSI) et les catégories de sécurité des moyens TIC (art. 21 LSI). Il y a lieu de se réjouir que le rapport explicatif comporte des définitions limitatives des «intérêts publics» à protéger. Cette limitation ne découle toutefois pas de la teneur de l'art. 1, al. 2, let. d, LSI. Voilà pourquoi le PSS suggère de préciser le but figurant à l'art. 1, c'est-à-dire d'utiliser des termes et un libellé plus explicites.

Privatim regrette que l'art. 1 LSI proposé ne se réfère qu'à la garantie des intérêts propres de la Confédération et que cette disposition ne vise qu'indirectement à garantir les intérêts de la population. La garantie de la protection des droits de la personnalité figurant dans la Constitution fédérale (art. 10, al. 2, et art. 13, al. 2, Cst) ou celle des secrets professionnels, commerciaux et de fabrication ne sont pas inclus dans le but de cette loi, en ce sens que d'éventuels défauts de sécurité de l'information engendreraient une perte de confiance en la Confédération (cf. rapport explicatif relatif à l'art. 1, al. 2, let. d, LSI). De l'avis de privatim, la sécurité de l'information doit également protéger les intérêts des personnes directement concernées dont les autorités traitent des données. Privatim propose donc d'adapter l'art. 1, al. 2, P-LSI comme suit:

[2] Elle vise ce faisant à protéger les intérêts publics et privés suivants:

a) la capacité de décision et d'action des autorités fédérales;
b) la sécurité intérieure et extérieure de la Suisse;
c) les intérêts de politique extérieure de la Suisse;
d) les intérêts économiques, financiers et monétaires de la Suisse;
e) les droits fondamentaux des personnes concernées, garantis par la Constitution
f) les secrets professionnels, commerciaux et de fabrication;
g) l'exécution des obligations légales et contractuelles des autorités fédérales quant à la protection des informations.

Vu l'importance accordée par la Suisse à la protection des données et le respect de la sphère privée, il semble opportun pour la FER d'indiquer ou d'ajouter un point supplémentaire à cet article, al. 2 «La classification des informations concernant les individus et/ou les profils de la personnalité éventuellement déterminés/collectés dans le cadre de la protection des intérêts ci-dessus décrits». L'objectif étant de signifier que les informations détenues par la confédération sont traitées comme étant classifiées dans la catégorie «protection très élevée» que ce soit sur les donnes issues de la collecte (dans le cadre du contrôle relatif aux personnes) ou pour tout autre processus ciblant spécifiquement les individus ou leur personnalité.

LB estime que la let. e mériterait d'être clarifiée et complétée de la manière suivante: «l'exécution des obligations légales et contractuelles des autorités fédérales quant à la protection des informations et des données». Il y aurait par ailleurs lieu d'examiner s'il convient de faire figurer les infrastructures critiques nécessaires au fonctionnement de la société civile, de l'économie et de l'Etat dans le catalogue de l'art. 1, al. 2, LSI en tant qu'intérêts particulièrement dignes d'être protégés.

Le Conseil des EPF demande que l'art. 1, al. 2, let. d, soit complété et propose le libellé suivant: «d. les intérêts économiques, financiers et monétaires de la Suisse, de ses autorités et organisations ainsi que ceux de tiers concernés». En effet, au vu de l'ensemble des dispositions de la LSI, il ne s'agit pas seulement des intérêts du pays mais aussi, en particulier, d'intérêts spécifiques des autorités et organisations concernées dont les activités comportent également leurs propres secrets professionnels, commerciaux et de fabrication, ainsi que les intérêts de tiers dignes d'être protégés. En adoptant le libellé proposé ci-dessus, il serait possible que la classification «INTERNE», «CONFIDENTIEL» et «SECRET» couvre égale-

ment les intérêts économiques du domaine des EPF, sans pour autant porter atteinte à la compatibilité avec le principe de transparence.

Par ailleurs, le législateur ne mentionne à l'art. 1, al. 2, let. e, que les autorités fédérales, ce qui est déroutant pour le Conseil des EPF, vu que ces termes n'apparaissent pas ailleurs dans le texte et qu'il n'y est finalement question que d'autorités et d'organisations concernées. On ne sait ainsi pas si, par «autorités fédérales», on n'entend que les autorités concernées définies à l'art. 2 ou aussi les organisations concernées. En outre, l'EMPA considère qu'il est choquant que seules les autorités – et pas les organisations – puissent bénéficier d'une telle protection de l'information.

La FMH demande de mentionner explicitement les données personnelles à l'art. 1, al. 2, let. e. A son avis, la protection du citoyen doit figurer clairement dans cet acte législatif. En cas d'utilisation abusive de données, les droits de la personnalité des personnes dont les données sont traitées peuvent être gravement violés. Certaines données personnelles sont tout aussi recherchées que les informations technologiques de l'industrie et leur valeur financière ne doit pas être sous-estimée.

Art. 2 Autorités et organisations concernées

En dépit de certains doutes, ZH pense que, par essence, il est fondamentalement judicieux de placer dans le champ d'application de cette loi, aux termes des dispositions de l'art. 2, al. 2, let. f, LSI, les autorités et services cantonaux qui exercent des activités sensibles sur mandat de la Confédération et sous sa surveillance. Il n'y a qu'ainsi que l'on peut garantir en permanence la sécurité des informations dans tout le domaine de responsabilité de la Confédération. Cette réglementation empiète certes sur l'autonomie organisationnelle des cantons, mais il ne serait pas réalisable d'appliquer, au sein d'une administration, deux voire davantage de régimes de sécurité différents.

ZG demande de modifier le libellé de l'art. 2, al. 2, let. f, de la manière suivante: «^{2} Elle s'applique également aux organisations (organisations concernées) suivantes: f. les autorités et services cantonaux qui exercent des activités sensibles ~~sur mandat de la Confédération et sous sa surveillance~~ en collaboration avec la Confédération.» De fait, la sécurité de l'information concerne les cantons, mais pas uniquement en tant qu'autorités d'exécution de tâches dévolues par la Confédération ainsi qu'en allègue le projet de loi. En effet, dans le domaine de la sécurité, les cantons n'opèrent pas en tant qu'organes d'exécution classiques «sur mandat de la Confédération et sous sa surveillance». Dans le domaine de la sécurité intérieure du pays, les cantons disposent de pouvoirs de souveraineté. Les organes de la Confédération sont des participants au Réseau national de sécurité et occasionnellement, ils sont même les mandataires des cantons. Mais alors, les cantons ne seraient pas intégrés dans le champ d'application de cet acte législatif s'ils n'agissent pas «sur mandat de la Confédération». Cela n'a aucun sens, puisque précisément dans le domaine de la sécurité intérieure du pays aussi, on est en présence d'informations et de données sensibles et classifiées qui sont échangées et qui méritent une protection particulière.

BS ne distingue clairement ni dans le libellé proposé de la loi (art. 2, al. 2, let. f, LSI), ni dans le rapport explicatif quelles sont les activités des autorités cantonales qui tombent dans le champ d'application de cette loi. BS suggère donc de compléter l'art. 87 LSI par une disposition prévoyant que le Conseil fédéral détermine, dans l'ordonnance d'exécution, les activités que vise l'art. 2, al. 2, let. f. Et pour que l'on puisse évaluer l'impact de ces mesures sur le canton, il conviendrait de répertorier la liste de ces activités – dans l'optique actuelle –, déjà dans le message. En outre, le message devrait aussi définir clairement ce qu'il y a lieu de comprendre par «sous sa surveillance».

Pour GE, il conviendra de préciser exactement les autorités et services cantonaux prévus à l'art. 2, let. f, notamment ce que vous entendez par «des activités sensibles sur mandat de la Confédération et sous sa surveillance». Ces informations permettent de mesurer précisément les éventuelles conséquences techniques et financières sur les infrastructures.

Le PSS est d'avis que dans le libellé de l'art. 2, le champ d'application de la LSI, est très large. De l'avis du PSS, il y a de bonnes raisons de l'avoir prévu ainsi, puisque la LSI se

meut dans un domaine si fortement interconnecté qu'une procédure législative fortement sectorielle ou fédéraliste atteindrait rapidement ses limites.

Privatim estime en principe pertinent que les autorités et services cantonaux exerçant des activités sensibles sur mandat de la Confédération et sous sa surveillance tombent dans le champ d'application de la LSI en vertu des dispositions de l'art. 2, al. 2, let. f, LSI. Il n'y a qu'ainsi que l'on peut garantir de manière constante la sécurité de l'information dans l'ensemble du domaine de responsabilité de la Confédération. Mais il en découlerait alors pour les cantons la nécessité pratique d'adapter leurs propres règles en matière de sécurité de l'information aux dispositions de la LSI. Il ne serait en effet pas réalisable d'appliquer, dans une administration, deux, voire davantage de régimes de sécurité différents. Cela étant, on déclenche à l'échelon cantonal (et éventuellement à l'échelon communal) une nécessité d'agir, parce que la LSI prévoit des mesures (notamment des contrôles de sécurité relatifs aux personnes et des procédures de sécurité relative aux entreprises) qui, au niveau cantonal (et éventuellement au niveau communal) sont probablement encore loin d'être réglementées ou ne le sont pas suffisamment. C'est pourquoi les cantons devraient pouvoir bénéficier des prestations des services spécialisés de la Confédération en la matière. Dans la mesure où la LSI astreint directement les services cantonaux, les prestations (par ex. exécution de CSP) devraient être financées par la Confédération. C'est pourquoi privatim demande que l'art. 89 LSI soit pourvu d'une réglementation complémentaire prévoyant que les autorités et services cantonaux puissent solliciter les prestations des services spécialisés de la Confédération prévues dans les dispositions de la LSI. Au cas où d'autres services prévus à l'art. 2, al. 2, let. f, LSI sollicitaient ce genre de prestations (donc lorsque le canton introduit une CSP pour d'autres membres du personnel du canton encore), la Confédération devrait percevoir un émolument couvrant ses frais. Si cette proposition n'était pas mise en œuvre, il faudrait préférer la loi fédérale sur la protection des données (LPD) à la réglementation proposée par l'art. 2, al. 2, let. f, LSI (propre responsabilité des cantons, pour autant qu'ils assurent un traitement de données personnelles à un niveau de protection adéquat art. 37, al. 1, LPD).

La CSI demande de rayer la let. f, au cas où sa proposition relative à l'art. 89 ne peut être mise en œuvre (voir remarques de la CSI à propos de l'art. 89).

Insecor suggère d'intituler cet article «champ d'application». Définir les autorités fédérales concernées dans un article évoquant aussi des «activités sensibles» engendre davantage de confusion que de clarté. Insecor recommande donc de scinder ces deux thèmes différents (cf. les remarques faites à propos des «définitions»). Insecor suggère donc instamment de préciser le passage consacré au champ d'application concret dans le rapport explicatif (chapitre 1.2.2.1) ainsi que dans l'acte législatif proprement dit, de manière à ce que la considération globale des risques (sécurité intégrale) prenne de l'importance. Bien qu'il soit difficile de distinguer la thématique de la «sécurité des TIC» de celle de la «cybersécurité», il convient tout de même de procéder à cette séparation.

Pour it-rm, il n'est pas suffisant, pour des réflexions en matière de sécurité, que seules des autorités cantonales exerçant des activités sensibles du point de vue de la sécurité sur mandat de la Confédération et sous sa surveillance soient assujetties à cette loi. Devraient y être assujetties toutes les autorités cantonales qui, dans leur fonction, ont accès à des informations sensibles du point de vue de la sécurité de la Confédération, en transmettent à cette dernière ou doivent en traiter. Si ce n'était pas le cas, les services cantonaux appliqueraient moins de mesures de sécurité ou des mesures plus efficientes, ce qui aboutirait à ce que l'information soit davantage ou moins protégée. La notion de mandat suggère un rapport de subordination. Or, il se pourrait aussi que des informations sensibles, nécessaires à des tâches qui relèvent clairement de la souveraineté des cantons, soient transférées de la Confédération aux cantons (et vice-versa). Il conviendrait également de compléter cette disposition dans le sens que les organisations et les institutions qui exploitent des infrastructures critiques (art. 81 ss) tombent dans le champ d'application de la loi. De l'avis d'it-rm, la liste figurant à l'al. 3 n'est pas exhaustive. Il convient dès lors d'y ajouter «notamment» ou «entre autres».

Les «organisations de droit privé» accomplissant des activités sensibles du point de vue de la sécurité devraient également être assujetties à la LSI. Le Conseil fédéral déterminera

dans une ordonnance quelles organisations de droit privé seront entièrement ou partiellement assujetties à la LSI aux termes de l'art. 87, al. 4, LSI. LB recommande que les cercles intéressés de l'économie, y compris les associations professionnelles – TIC Switzerland et ses membres inclus – ainsi que les organisations spécialisées dans le domaine de la sécurité de l'information, telles qu'ISSS, Clusis, swissecurity.org et leurs organisations membres soient invités à se prononcer lorsqu'il s'agira d'élaborer l'ordonnance d'exécution de cette loi.

Art. 3 Rapport avec la législation spéciale

Bien que l'art. 3, al. 1, LSI précise que l'application de la loi fédérale sur la transparence (Ltrans) est réservée, ZH se demande si une classification effectuée d'avance selon les dispositions de l'art. 14 LSI peut encore laisser à une autorité compétente – en vertu de l'art. 10, al. 1 Ltrans – une liberté de décision et d'appréciation pleine et entière. ZH en doute et estime qu'une coordination législative est ici souhaitable.

TI salue le principe selon lequel les dispositions de la loi sur le principe de transparence dans l'administration (Ltrans) relatives à l'accès à des documents administratifs doivent s'appliquer sur la base de la LSI (interne, confidentiel et secret), et ce tant pour des informations classifiées que non classifiées. Le résultat de la mise en balance habituelle des intérêts en jeu sur la base des dispositions de la Ltrans (art. 7) justifierait alors les restrictions éventuelles du droit d'accès à ces informations. Quant au rapport de la LSI avec d'autres législations, l'al. 2 mentionne à juste titre que lorsque les informations doivent être protégées, en particulier en vertu d'autres lois fédérales, les dispositions de la LSI doivent être considérées comme un acte législatif complémentaire. Cela signifie que les données personnelles qui se situent dans le champ d'activités des autorités fédérales doivent continuer à être traitées en fonction de la loi sur la protection des données LPD. En ce qui concerne les mesures de protection (protection organisationnelle, technique, physique ou personnelle), ce sont alors les dispositions ponctuelles de la LSI qui sont déterminantes. Mais en même temps, cela signifie que les données personnelles importantes pour garantir la sécurité publique devraient pouvoir être classifiées selon les consignes de la LSI sans que le caractère général, respectivement pluridisciplinaire de la LPD ne soit touché ou tout au moins relativisé.

Pour le PSS, il est crucial que la nouvelle LSI ne mène pas à davantage de classification que jusqu'ici. Dans le cas contraire, on courrait le risque d'une limitation du principe de transparence de l'administration puisque la pratique selon la LPD démontre que des documents classifiés une fois sont clairement plus rarement rendus accessibles en vertu dudit principe de transparence de l'administration. Bien que l'art. 3, al. 1, LSI indique expressément que la loi sur la transparence de l'administration (Ltrans, RS152.3) est réservée, les interactions entre la LSI et le principe de la transparence de l'administration ancré dans la Ltrans ne sont pas vraiment expliquées. Le PSS attend donc que les dispositions relatives à la classification soient aménagées quant à leur contenu de telle manière qu'en aucun cas elles ne dépassent le cadre du catalogue d'exceptions visé à l'art. 7 Ltrans et que leur contenu ne le contredise pas. Il convient par ailleurs de s'assurer qu'à l'avenir, les dispositions de la LSI ne génèrent pas encore davantage de litiges entre les utilisateurs de la Ltrans et l'administration.

Le PSS estime que le principe de la transparence dans l'administration est étroitement lié au concept de l'Open Government Data (OGD). L'OGD est un des éléments de la stratégie e-gouvernement de la Confédération. La ratification de la convention d'Aarhus (portant sur l'accès à l'information, la participation du public au processus décisionnel et l'accès à la justice en matière d'environnement) a pour effet que la Suisse respecte le principe de transparence concernant des données relatives à l'environnement. Le projet-pilote «point unique d'accès» (Single Point of Orientation) qui est un pôle d'informations centralisé des Archives fédérales illustre comment pourrait être réalisé un aperçu des documents de l'administration fédérale, proche du citoyen. Le PSS attend de la nouvelle LSI qu'elle ne fasse pas obstacle aux projets du Conseil fédéral et, de manière générale, à la stratégie OGD réaffirmée par le Conseil fédéral dans son rapport du 13 septembre 2013. C'est pourquoi il convient d'examiner s'il y a lieu d'ancrer expressément une réserve dans la LSI.

Clusis regrette l'absence de référence à la loi fédérale sur la protection des données personnelles. L'al. 2 qui précise «lorsque les informations doivent être protégées en vertu d'autre loi

fédérale, les dispositions de la présente loi s'appliquent à titre complémentaire.», devrait être complété: «Les dispositions de la LPD s'appliquent pour le surplus.»

Pour Insecor, il n'est pas compréhensible que l'al. 2 ne se réfère qu'aux «informations». Selon insecor, la phrase devrait être formulée comme suit: «Lorsque les informations ainsi que les technologies d'information et de communication doivent être protégées en vertu d'autres lois fédérales, les dispositions de la présente loi s'appliquent à titre complémentaire.»

La notion – mise entre parenthèses à l'al. 3 – d'«infrastructures critiques» et la référence générale à la «législation spéciale» nécessitent, selon LB, une description plus concrète et plus précise parce que la loi devrait être aussi applicable aux infrastructures critiques des exploitants de droit privé.

Le projet de loi fédérale sur le renseignement (LRens) prévoit, à son art. 66, des exceptions au principe de transparence dans l'administration, concernant des documents relevant de la recherche d'informations en matière de renseignement. Le SRC part de l'idée que le principe énoncé par l'art. 3 LSI ne devrait en rien modifier la disposition de la LRens en la matière. Par ailleurs, le SRC ne comprend pas totalement pourquoi notamment les documents classifiés SECRET et dont la divulgation à des personnes non autorisées pourrait gravement nuire aux intérêts publics aux termes des dispositions de l'art. 1, al. 1, LSI devraient rester assujettis au principe de transparence dans l'administration.

Chapitre 2 Mesures générales de la sécurité de l'information

Généralités

LB recommande que la LSI soit systématiquement examinée pour déceler si une exigence, prescription ou règle déterminée ne s'applique qu'aux «autorités concernées» ou se réfère aussi aux «organisations» (de droit privé), lorsqu'elles sont assujetties au champ d'application de la LSI en vertu de son art. 2, al. 2, let. e.

La FMH remet en question la distinction entre la classification d'informations et les échelons de classification de moyens TIC, d'un côté, et leurs champs d'application distincts, de l'autre: de fait, la protection des systèmes doit servir à la protection des informations au sein même des systèmes.

Art. 4 Sécurité de l'information

TG déplore l'absence du principe de la proportionnalité. Ainsi, il convient de compléter cette disposition dans le sens qu'une mesure est légitime jusqu'au moment où son but a été atteint ou qu'il soit constaté qu'il ne peut être atteint. En outre, une telle mesure ne doit pas être manifestement disproportionnée ni appliquée au détriment du but à atteindre. Il est vrai que, quelques articles plus loin (à l'art. 12 du projet LSI) il est dit que la classification doit «se limiter au minimum requis». Cependant, ce principe-là devrait s'appliquer à l'ensemble des dispositions relatives à la sécurité de l'information, d'où l'importance majeure d'intégrer clairement ce principe dans les dispositions générales. Selon TG, il conviendrait, en matière de sécurité de l'information, de s'assurer aussi que les documents proviennent du service idoine, c'est-à-dire que l'on puisse d'emblée en identifier la source. Mais à l'art. 4, al. 4, du projet LSI, on ne mentionne à cet égard que la «traçabilité» et il convient d'y ajouter le terme «authenticité». Cela permettrait de garantir que les informations sont bel et bien authentiques, ce qui, en matière de sécurité de l'information, constitue un aspect important.

Du point de vue du PSS, il manque à l'art. 4, al. 3, LSI la mention du principe de proportionnalité. Le PSS suggère dès lors d'apporter le complément suivant: «[3bis] Elles veillent à assurer la proportionnalité des mesures de protection prises. Ces mesures sont légitimes jusqu'au moment où leur but a été atteint ou qu'il soit constaté qu'il ne peut être atteint. En outre, une telle mesure ne pourra être manifestement disproportionnée et prononcée au détriment du but à atteindre.

Pour la FER il semble opportun de focaliser sur la classification des informations, et non pas sur «… une responsabilité évaluée en fonction d'une atteinte éventuelle aux intérêts au sens

de l'art. 1, al. 2». L'objectif étant de définir une stratégie préventive et non pas réagir ou surréagir sur évènement nécessitant d'adapter les processus existants, à postériori.

Insecor constate qu'à l'al. 3, figure soudain l'abréviation «moyens TIC» pour la notion de «technologies d'information et de communication». Etant donné que cette définition a déjà été utilisée à plusieurs reprises dans les articles précédents, il convient d'utiliser cette abréviation beaucoup plus tôt, au début du projet de loi et donc dès l'art. 1, al. 1 (cette remarque ne concerne toutefois que la version en allemand).

Pour it-rm, l'al. 2 de cet article devrait être complété par une lettre supplémentaire, à savoir la let. e «doivent être fiables».Cette fiabilité implique aussi l'exactitude du contenu, c'est-à-dire la saisie correcte et intégrale de l'information ainsi que son traitement. Pour it-rm, la fiabilité des informations est cruciale. Le citoyen doit pouvoir être sûr de l'exactitude des indications figurant dans les registres (protection de la bonne foi). Si les informations figurant dans les registres étaient erronées, il y aurait des réclamations en masse qui pourraient aboutir à des procédures litigieuses. Pour it-rm, il y aurait encore lieu d'ajouter une autre lettre à l'al. 2, à savoir une let. f avec le libellé suivant: «f. doivent être authentiques ou anonymes». Les données et les informations sont authentiques lorsqu'elles peuvent être attribuées à une personne ou à une machine. Si tel n'était pas le cas, on serait confronté à un problème de sécurité, du fait que l'on ne saurait pas qui a eu accès à ces informations et les a envoyées. Pour établir la légitimité d'une demande en ligne de données et d'informations confidentielles, il faut d'abord avoir la preuve de qui assume la responsabilité d'une telle demande. Cela implique une vérification de l'authenticité de la demande. Quant à l'anonymat, il engendre le contraire de l'authenticité, à savoir que l'information ne peut être attribuée à quelqu'un de précis. Par exemple, la protection de l'anonymat est exigée pour le secret d'un scrutin. En l'occurrence, c'est le vote qui doit être protégé, de sorte qu'il ne pourra être attribué à aucune personne physique.

Art. 5 Responsabilité de conduite des autorités

Insecor ne voit pas pourquoi à l'al. 1, seules les «autorités concernées» devraient avoir la responsabilité «suprême» et que cette responsabilité-là ne pourrait pas aussi incomber aux «organisations concernées» (c'est-à-dire, par exemple, «l'administration fédérale»). Déjà rien qu'en se fondant sur les responsabilités mentionnées dans la loi sur l'organisation du gouvernement et de l'administration (LOGA; SR 172.010), il ne pouvait pas être question que l'administration fédérale ne considère pas non plus la sécurité comme étant «l'affaire de chef» (cf. à ce propos le rapport explicatif concernant l'art. 5, p. 40). Et en p. 41 au sujet de l'al. 4: «Les autorités concernées doivent veiller à *informer* régulièrement, et en fonction des niveaux de responsabilité, les cadres et le personnel à propos des affaires en lien avec la sécurité de l'information. […] Les cadres et le personnel doivent donc aussi être instruits en conséquence.» Autrement dit, une simple information concernant la sécurité de l'information n'a jamais encore amené au but.

It-rm estime que d'après l'état d'avancement des connaissances et de la technologie dans le domaine de la technologie de l'information, le contrôle de la technologie de l'information exigé par l'al. 1, let. a, n'est pas réalisable, car il serait alors sans fin. Il importerait bien plus pour ce contrôle que le service de coordination assume la responsabilité de l'élaboration et de la mise à jour d'une norme minimale en la matière. Les autorités pourraient ainsi faire le contrôle requis en fonction de ces consignes. Sinon, on risque que l'ampleur de ce contrôle soit définie individuellement d'une autorité à l'autre, ce qui ne manquerait pas de se traduire par un total manque d'homogénéité dans les mesures de sécurité et de leur mise en œuvre. It-rm propose donc d'ajouter un renvoi à l'art. 88 LSI et là de compléter cette disposition en ajoutant l'aspect du contrôle et d'autoriser le service de coordination d'édicter des directives précisant quelles étapes de contrôle doivent être effectuées en fonction du besoin de protection.

LB propose que l'art. 5, tout comme l'art. 6, se réfèrent aux autorités et organisations concernées. En effet, c'est précisément dans l'économie privée qu'il serait souhaitable de pouvoir se fonder sur un principe du contenu aux termes duquel la garantie de la sécurité de l'information appartient sans conteste à la responsabilité de l'organe de conduite suprême.

Même au vu des commentaires relatifs à l'art. 6, le Conseil des EPF ne voit pas très bien si les dispositions de l'art. 5 doivent effectivement aussi s'appliquer aux unités décentralisées de la Confédération. D'autant plus que de propres dispositions relatives à la gestion des risques s'appliqueraient au domaine des EPF.

Art. 6 Gestion des risques

TG et le PSS demandent de biffer l'adjectif «identifiés» à la dernière phrase de l'al. 2. Pour TG, selon la doctrine de la gestion des risques, les risques – tels qu'ils sont mentionnés dans le projet de loi – sont identifiés, évalués, appréciés et vérifiés. Mais, justement, l'al. 2 de l'article mentionné s'emmêle beaucoup trop fortement dans cette systématique de définitions. Autrement dit, il conviendrait à juste titre de ne pas seulement éviter les risques «identifiés» mais bel et bien tous les risques. Pour le PSS, les autorités et organisations responsables devraient veiller d'une manière générale à éviter les risques ou alors à faire en sorte que ces risques se réduisent «dans une proportion supportable» et ce bien sûr, tant en ce qui concerne les risques identifiés que tous les autres que l'on n'aura pas encore identifiés.

Du point de vue d'it-rm, l'expression «dans une proportion supportable», utilisée à l'al. 2 manque grandement de concrétisation et, de plus, contient une grande portion d'appréciation individuelle dans la mise en œuvre. Par ailleurs cette ambiguïté se situant dans un cadre technique suscite une insécurité du droit, pis, encore amener un manque d'homogénéité dans le dispositif de sécurité. It-rm propose dès lors d'ajouter par analogie le complément suivant: «Le service de coordination détermine des normes minimales pour les échelons respectifs de classification pour lesquels l'ampleur du dommage pourrait être considérée comme supportable en cas de violation ou de détournement de la sécurité de l'information.»

Art. 7 Exigences et mesures de sécurité

TG considère que l'al. 2 pourrait également être biffé, étant donné que le législateur dit à l'art. 88 du projet de LSI que le Conseil fédéral détermine les exigences et les mesures standard (lors de l'exécution) en fonction de l'état d'avancement de connaissances et de la technologie. Il en découle donc déjà des dispositions d'exécution mentionnées à la fin du projet d'acte législatif que les mesures de sécurités citées devront correspondre à l'état (reconnu) de l'avancement des connaissances et de la technologie.

Insecor trouve inhabituel de renvoyer d'abord à un article de loi qui ne se trouve qu'à la fin de l'acte législatif en question. Aussi l'organisation Insecor recommande-t-elle de prévoir une observation au sujet des exigences et mesures standard tout au début de la LSI déjà et d'y faire référence à l'art. 88.

Etant donné qu'aux termes du rapport explicatif, les autorités et les organisations qui ne sont pas subordonnées au Conseil fédéral n'ont pas d'obligation de se soumettre aux exigences standard en vertu de l'art. 88, le Conseil des EPF suggère de préciser éventuellement les dispositions de l'art. 7, al. 1, dans ce sens.

Art. 8 Collaboration avec les tiers

Privatim déplore ici l'absence du principe selon lequel c'est bel et bien l'autorité ou l'organisation qui doit répondre de la garantie de la sécurité de l'information lorsque qu'elle a recours à un tiers pour accomplir sa mission. Pour donner d'autant plus de poids à ce principe, l'art. 8 LSI devrait dès lors contenir un passage au sujet de la responsabilité que doit assumer l'autorité ou l'organisation concernée qui mandate un tiers.

D'après it-rm, un contrat passé avec un tiers ne justifie par principe pas de laisser accéder un tiers de l'extérieur à un secret professionnel ou de fonction. Or, la clause prévue ici permettrait justement, de par ces dispositions légales, de laisser la porte ouverte à des tiers pour accéder à des données sensibles du point de vue pénal. Il conviendra d'expliciter clairement ce point dans les commentaires afin que le Parlement puisse en prendre conscience. Si l'autorité concernée n'était pas propriétaire du secret mais qu'elle en était seulement la détentrice, il faudrait alors émettre de sérieux doute lorsque cette autorité aurait recours aux services de tiers. Pour pouvoir identifier précocement, le cas échéant, un conflit d'intérêt, il serait souhaitable de pouvoir informer le propriétaire du secret. It-rm estime d'ailleurs qu'en

vertu de la sécurité du droit et de la transparence à l'égard du tiers mandaté, il y aurait également lieu de régler la question de la responsabilité lorsque le tiers auquel l'autorité aura eu recours cause un dommage à un particulier. It-rm ajoute qu'il y également lieu de compléter cette disposition en ce sens que le service de coordination sera tenu d'édicter des dispositions d'exécution relatives au mode de sélection de tiers et d'établir une liste de critères que ces tiers devront remplir en particulier.

Le Conseil des EPF est d'avis que cet article devrait clarifier de quel genre de collaboration il s'agit ici. Un assujettissement du domaine des EPF à l'art. 8, al. 2, serait disproportionné et engendrerait des coûts. Cette disposition pourrait considérablement alourdir la procédure de recherche de tiers, en particulier en ce qui concerne le déroulement opérationnel de l'évaluation des offres (retards). Le Conseil des EPF est d'avis qu'une telle disposition allant aussi loin et selon laquelle tout accord et tout contrat conclu avec un tiers devrait tenir compte des exigences et des mesures au sens de la LSI ne peut tout simplement pas être mise en œuvre en pratique: il est difficile de concevoir les effets en largeur et en profondeur qu'auront lesdites vastes exigences et mesures commandées par la LSI et, par conséquent, aucune autorité ni aucune organisation ne pourra se permettre d'intégrer dans ses contrats de telles clauses ainsi que l'exige l'art. 8. L'EMPA, de son côté, considère qu'une ingérence aussi vaste que celle-ci n'est pas conciliable avec l'autonomie accordée à un établissement de droit public et que ces prescriptions le sont encore moins avec le principe de liberté en matière de contrats, de recherche et d'enseignement. Le Conseil des EPF propose donc de formuler un nouveau texte qui aurait le libellé suivant: «Les autorités et organisations concernées collaborant contractuellement avec des tiers sont tenues de leur indiquer sommairement l'application et le respect des dispositions de la loi sur la sécurité de l'information.»

Art. 9 Procédure en cas de violation de la sécurité de l'information

Pour TG, il manque ici une disposition selon laquelle en cas de violation identifiée, il y aura lieu de mettre en œuvre des contre-mesures en réponse à ces violations. L'article de loi se contente de mentionner qu'en cas de violation de la sécurité de l'information, leurs éventuelles conséquences doivent être limitées à leur strict minimum. Cet article devrait donc être complété dans le sens proposé par TG afin d'en faire un tout.

La FER se demande, quid d'une définition explicite des éventuelles suites judiciaires et/ou pénales découlant d'une violation de la sécurité de l'information?

Art. 10 Plans préventifs

LB propose que l'art. 10 se réfère aux «autorités et organisations concernées». En effet, c'est surtout dans le domaine de l'économie privée qu'il serait souhaitable de pouvoir se référer au principe du contenu pour s'assurer que des plans préventifs sont élaborés et dûment exercés en vue de garantir la sécurité de l'information.

Art. 11 Contrôles

TG est d'avis que la confidentialité doit être imposées aux services indépendants par la loi et ce à plus forte raison que lors de leur contrôle ils prendront forcément connaissance de documents ultra confidentiels.

Pour VD les commentaires sont peu précis à propos des modalités et des coûts des contrôles dans les cas où la loi s'appliquera aux autorités cantonales. Un organe tel que le Contrôle cantonal des finances est au demeurant légalement et professionnellement apte à remplir les missions d'audits visés à l'al. 2.

Le PSS propose d'ajouter un alinéa supplémentaire qui aurait le libellé suivant: «[3] Les résultats des contrôles effectués en vertu des al. 1 et 2 sont portés périodiquement à la connaissance des Commissions de gestion des Chambres fédérales». L'art. 11 prescrit aux autorités de faire vérifier périodiquement le respect des dispositions de la LSI et l'efficacité des mesures prises. Ce sont des informations que la haute surveillance parlementaire intéresse.

Art. 12-18 Classification des informations

Vu l'absence de définition en la matière, insecor pose la question de savoir, à propos de cette section, si les dispositions mentionnées s'appliquent aussi au «matériel classifié». De l'avis d'insecor, ceci est insatisfaisant et il convient absolument de le préciser.

Art. 12-14 Classification

Le PDC donne son aval à la création d'une réglementation uniforme quant aux échelons de classification et aux motifs de classification pour toutes les autorités.

Le MPC s'oppose à une obligation de classification des pièces de dossiers issus d'une procédure pénale. A l'époque déjà, l'ordonnance concernant la protection des informations (OPrI) n'avait pas ancré d'obligation de classification pour les dossiers liés à une procédure pénale. Le traitement de ces dossiers et leur accès se fondent exclusivement sur les règles du Code de procédure pénale (CCP). Le MPC est d'avis qu'une obligation de classification en vertu de la LSI est non seulement superflue (puisque le secret d'instruction est de mise en procédure pénale), mais également impraticable dans les procédures pénales lourdes et complexes telles que le MPC les mènent. Ordonner une classification en vertu des dispositions de la LSI conduirait à ce que les dossiers issus d'une seule et même procédure pénale fassent l'objet de différents échelons de classification et doivent dès lors être traités différemment. Or, une telle dissociation de pièces du dossier ne permettrait pas de gérer correctement les dossiers comme le demande la loi et la jurisprudence, mais irait au contraire à l'encontre des principes d'unité et d'intégralité des pièces de procédure. Et pour éviter cela, il y aurait alors lieu d'attribuer l'ensemble des pièces d'un dossier – comme cela se fait jusqu'ici dans le contexte du Code de procédure pénale en vigueur sous la garantie du secret d'instruction – à un seul échelon de classification, c'est-à-dire celui des informations les plus sensibles. Pourtant, cette manière de procéder ne devrait pas aller dans le sens du présent projet de loi, à plus forte raison qu'en vertu des commentaires donnés dans le rapport explicatif et pour que la charge de l'exécution reste supportable, la quantité des informations doit se limiter au strict minimum requis. C'est reconnaître du même coup qu'un effectif global de dossiers ne doit pas être attribué uniformément à un seul et unique échelon de classification. Cet assujettissement causerait du reste encore d'autres problèmes au MPC, à savoir dans la relation avec des autorités cantonales de poursuite pénale. Le MPC fait observer que les autorités cantonales ne sont par principe pas assujettis aux règles de la LSI.

Art. 12 Principes de classification

It-rm est d'avis qu'il convient d'apporter encore un complément à cet article, à savoir que le service de coordination soit tenu d'élaborer des directives indiquant comment les informations sensibles doivent être classifiées.

Le SRC pense qu'au niveau des dispositions d'exécution de l'al. 4 il y aura encore lieu d'édicter des prescriptions simplifiées, destinées au SRC (semblables aux règles actuellement applicables au traitement simplifié d'informations classifiées dans le domaine des services de renseignement et de la police, du 18 janvier 2008).

Art. 13 Compétences

Pour TG, en cas de délégation de la compétence de classification à un autre service respectivement à une personne, l'autorité concernée (ici, seulement le service et les supérieurs hiérarchiques opérant la classification) devrait le cas échéant elle-même avoir la faculté de modifier la classification.

De l'avis du PSS, suivant la situation qui se présente, l'autorité concernée devrait elle aussi avoir la possibilité de modifier ou de supprimer la classification et non pas seulement le service de classification ou le service hiérarchique supérieur auquel il est subordonné.

Le SRC pense qu'au niveau des dispositions d'exécution de l'al. 2 il y aura encore lieu d'édicter des prescriptions simplifiées, destinées au SRC (semblables aux règles actuellement applicables au traitement simplifié d'informations classifiées dans le domaine des services de renseignement et de la police, du 18 janvier 2008).

Art. 14 Echelon de classification

UR salue le fait que le législateur n'ait fixé que trois seuls échelons de classification. Mais comment faire face à des données et des systèmes classifiés? Comment faire face aux conséquences qui en résulteront pour les cantons? UR n'a pas trouvé un mot à ce sujet dans le projet. Il s'agira donc d'en tenir compte en prévoyant des dispositions complémentaires juridiquement contraignantes.

TG ne comprend pas pourquoi à tous les échelons de classification le législateur ne fait qu'un renvoi aux let. a à d de l'art. 1 du projet de LSI mais ignore totalement la let. e. S'agit-il ici, à l'art. 1 du projet, d'un complément qui aurait été fait après coup et que l'on aurait malencontreusement oublié de reporter ce renvoi à cette let. e? On peut manifestement le supposer.

Par souci d'exhaustivité, privatim est d'avis que l'on devrait tout au moins indiquer dans le message ce que signifie une non-classification: mais alors ce type d'informations est-il malgré tout soumis au secret de fonction? Et qu'en est-il alors ici de l'accessibilité en vertu du principe de transparence de l'administration?

Clusis comprend bien les trois échelons INTERNE, CONFIDENTIEL, SECRET. Mais comment se fait-il qu'il n'y ait pas l'échelon PUBLIC? Il est impossible qu'il n'y ait pas de documents publics par défaut, d'autant plus que la loi sur la transparence est réservée.

It-rm trouve le schéma de classification proposé beaucoup trop peu différencié pour que le déroulement ordinaire correct des autorités fédérale puisse être protégé par la loi tel qu'elle en a l'intention. Mais ce n'est pas tout, car il y a d'autres obstacles encore dans le domaine du traitement des informations que la divulgation d'informations confidentielles pour nuire massivement à l'Etat et à son administration. It-rm propose dès lors de modifier les échelons de classification en «à usage interne», «mérite d'être protégé ou protection élevée» et «mérite extrêmement d'être protégé ou protection très élevée». Pour qu'une société civile et une administration équipées de moyens TIC modernes puissent fonctionner et pour que les intérêts économiques et financiers d'un Etat soient défendus, il n'y a pas seulement besoin de protéger particulièrement les informations confidentielles, mais également celles auxquelles doivent pouvoir se fier tous les citoyens et les fonctionnaires, comme les informations provenant d'un registre ou d'archives.

LB mentionne pour la bonne forme que les critères de l'attribution d'un échelon de classification des informations sont très généraux et que le service chargé de la classification dispose d'une marge de manœuvre considérable dans son appréciation. On pourrait éventuellement compléter le présent acte législatif par un principe, à savoir que les informations qui se réfèrent à des informations classifiées ou en contiennent doivent présenter au moins le même échelon de classification. Cela constituerait une indication utile aux organisations privées pour savoir comment procéder lorsqu'elles reçoivent, traitent, échangent, etc. des informations classifiées provenant des autorités concernées.

Le Conseil des EPF relève que les institutions du domaine des EPF, à l'instar de toutes les organisations, disposent évidemment elles aussi de données internes confidentielles qui devraient être protégées par le biais de mesures organisationnelles ou – en ce qui concerne les systèmes, au moyen d'une gestion pertinente des droits d'accès. Dans les activités centrales que constituent la recherche, l'enseignement et le conseil, la plupart des informations sont généralement en libre accès. Le Conseil des EPF précise qu'il n'existe que quelques rares projets qui ne sont pas librement accessibles parce qu'il en a été convenu ainsi contractuellement avec les bailleurs de fonds.

La FMH se demande pourquoi on a explicitement exclu les données personnelles du citoyen des échelons de classification d'informations (art. 14), ce qui est en contradiction avec les commentaires figurant dans le rapport explicatif: «La Confédération traite également un volume important de données personnelles qui, en vertu de la législation sur la protection des données, doivent être traitées de façon conforme au droit et au but recherché de même que dans le respect du principe de proportionnalité. Elles doivent être protégées par des mesures tant organisationnelles que techniques. En cas d'utilisation abusive, les personnes dont les

données sont traitées peuvent être gravement lésées dans leurs droits individuels. Certaines données personnelles sont aussi recherchées que les informations technologiques de l'industrie. Leur valeur financière ne doit pas être sous-estimée: il existe un marché florissant pour l'acquisition et la diffusion de données personnelles.» De l'avis de la FMH, l'échange électronique croissant d'informations met aussi toujours plus en danger les données personnelles. En particulier, le recoupement d'informations sur une personne permet que cette dernière soit de plus en plus facilement «réidentifiable».

La FMH demande de compléter les 3 alinéas de l'art. 14 par «intérêts au sens de l'art. 1, al. 2, let. a à e». En effet, les informations qui concernent le citoyen – par exemple les données au sujet de sa santé – méritent également d'être protégées par le biais des échelons de classification en vertu de l'art. 14. Les classifications ne doivent pas uniquement être limitées à la capacité de décision et d'action des autorités fédérales, à la sécurité intérieure ou extérieure et aux intérêts économiques, financiers ou de politique monétaire de la Suisse.

Art. 15 Accès aux informations classifiées

La FMH est d'avis que, lors de la mise en œuvre de l'art. 15, il conviendra de veiller à ce que la preuve soit vraiment fournie qu'il n'est pas possible d'accomplir la tâche légale concernée sans pouvoir accéder aux informations classifiées requises.

Art. 17 Communication d'informations classifiées dans le cadre de procédure spéciale

TG, estimant que les procédures judiciaires doivent être loyales, est d'avis qu'il convient de biffer l'al. 2 de l'art. 17 du projet de LSI, sinon cet alinéa pourrait donner ici l'impression que des tribunaux pourraient se fonder sur des moyens de preuves secrets, ce qui ne devrait en aucun cas être admissible. TG relève que l'art. 17 du projet de LSI mentionne certes que c'est le droit de procédure applicable au cas d'espèce qui régit la communications d'informations classifiées au sein de […] et auprès des tribunaux et des ministères publics. Cette disposition vise à garantir que l'instrument que constitue la classification des informations n'alourdisse pas les démarches de mise au jour de la vérité lors des procédures judiciaires. Toutefois, le législateur introduit un complément à l'al. 2 selon lequel le tribunal compétent a le droit d'entendre le service qui a procédé à la classification. Cela pourrait signifier que des procédures judiciaires pourraient éventuellement être restreintes de par la classification d'informations. Pour que les tribunaux puissent continuer à accomplir leurs propres tâches, il ne devrait y avoir aucune classification d'informations en procédure judiciaire. La classification implique qu'il s'agit de données secrètes. Or, il s'agit d'éviter absolument l'existence de tribunaux secrets, car sinon on pourrait ouvrir la porte à un arbitraire étatique.

Le TF déclare que cet article est crucial pour le Tribunal fédéral et qu'il ne faut rien y changer à son détriment.

Art. 18 Mesures provisoires de protection

Le Conseil des EPF demande de biffer le terme «organisations concernées» à l'art. 18 ou d'exclure explicitement de cette réglementation les unités décentralisées de l'administration fédérale, respectivement le domaine des EPF. En effet, aux termes des dispositions de l'art. 13, seules les autorités concernées seraient tenues de désigner les personnes ou les services compétents pour classifier les informations.

Art. 19 à 27 Sécurité lors de l'utilisation des moyens TIC

Dans l'art. 19 LSI, la «procédure de sécurité» mentionnée recouvre de toute évidence les mesures décrites aux art. 20 à 23 LSI. Dans ce contexte, LB est d'avis qu'il convient de spécifier que les autorités fédérales, cantonales et communales concernées assujetties à la LSI en vertu des dispositions de l'art. 2, al. 2, let. f, et qui, naturellement recourent à de vastes moyens TIC pour accomplir leurs tâches, devront probablement faire face à des dépenses considérables – qui seront finalement à la charge du contribuable ! – pour remplir les exigences en la matière énoncées aux art. 19 ss LSI. Il conviendrait dès lors, tout au moins dans le domaine de la «protection de base», de prévoir un système de mesures pouvant être mis en œuvre de manière simple, rapide et peu coûteuse. Voilà qui correspond à la conception actuelle de la sécurité de l'informatique, à savoir 1. hautement protéger les informations-

clés nécessaires à la poursuite des affaires; 2. ne protéger les données et processus mis en œuvre dans le travail quotidien que pour garantir qu'ils ne puissent être sans autre modifiés, effacés, utilisés abusivement ou «écrasés».

Art. 19 Procédure de sécurité

TG déplore ici l'absence du principe de la proportionnalité, d'où la nécessité de l'intégrer absolument – comme il a été dit précédemment – dans le cadre de l'art. 4 du projet de LSI.

Pour VD, la notion de procédure de sécurité devrait être plus explicite.

Insecor ne voit pas clairement ce que recouvre exactement le terme «Procédure de sécurité» ni pourquoi cette procédure ne devrait concerner que les «autorités» (et pas les «organisations»). Il convient dès lors de préciser que la procédure de sécurité doit inclure les dispositions des articles suivants (20 à 26).

It-rm est d'avis que chacun a une perception différente de la protection nécessaire et pertinente pour tel ou tel échelon de sécurité ou de classification. C'est pourquoi il est nécessaire de désigner un service centralisé, le service de coordination, qui soit autorisé à déterminer quelles mesures de sécurité au minimum il conviendra de mettre en œuvre dans le contexte du besoin de protection ou de la classification des informations. L'autorité pourra alors définir une procédure en vertu des dispositions de l'al. 1.

Aux termes des commentaires figurant dans le rapport explicatif à propos de l'art. 19, al. 1, seules les autorités concernées – mais pas les organisations concernées – déterminent une procédure de sécurité pour les moyens TIC. Pourtant, on ne saurait nier que les prescriptions figurant dans les art. 19 à 27 se réfèrent à plusieurs reprises aussi aux organisations concernées. Le Conseil des EPF se demande dès lors à quoi les organisations concernées sont concrètement tenues.

Art. 20 Analyse du besoin de protection et évaluation des risques

Privatim est d'avis qu'il convient de compléter à ce sujet les dispositions de l'art. 20, dans le sens où il y aura lieu de ne pas seulement analyser le besoin de protection et d'évaluer les risques en vue de l'engagement de nouvelles technologies mais de le faire également concernant ceux qui pourraient se produire lors de la mise en œuvre. En effet, de nouveaux système TI peuvent générer de nouveaux risques et vulnérabilités, les lacunes de systèmes existants pourront être comblées et il sera éventuellement possible d'institutionnaliser de nouvelles mesures et mécanismes de contrôle.

Selon l'art. 20, al. 2, en cas d'engagement de nouvelles technologies, ce ne sont pas seulement les organisations mais également les autorités concernées qui devront communiquer les résultats de leurs propres évaluations au service spécialisé de la Confédération en matière de sécurité de l'information. La BNS soutient expressément l'échange volontaire de connaissances issues des évaluations de risques. En revanche, elle rejette l'obligation d'informer instituée par l'al. 2 de l'art. 20, étant donné que, sur la base de la technologie engagée (par exemple des logiciels), on pourrait tout à fait arriver par déduction à connaître les activités spécifique que la BNS déploie pour mettre en œuvre des mesures de politique monétaire. Dans ces domaines, le but visé par cette obligation d'informer, à savoir l'échange de connaissances, ne peut pas non plus être atteint parce qu'aucune autre autorité ou organisation ne se situe dans le même champ d'activités et d'affaires que la BNS. En reformulant le libellé actuel de l'art. 20, al. 2, en disposition facultative, on pourrait tenir compte du souhait de la BNS.

Pour LB, l'engagement de «nouvelles technologies» (ce terme donne d'ailleurs quelque peu matière à interprétation: en effet, une nouvelle génération de moyens TIC proposée sur le marché, mais pas encore mise en œuvre par le service concerné, constitue-t-elle une nouvelle technologie?) dans le domaine de l'application est quasi quotidien du fait de l'évolution technique rapide des outils TIC. Pour des organisations privées, l'obligation d'informer le service spécialisé de la Confédération en matière de sécurité de l'information quant aux résultats de leurs évaluations est délicate à mettre en pratique, car les informations à fournir pourraient comporter des secrets d'affaires qui pourraient ainsi être dévoilés. Par principe, le

secret professionnel devrait être explicitement garanti pour toutes les informations provenant d'organisations privées et qui ne sont de manière générale pas accessibles, mais qui devraient être communiquées aux autorités concernées ou au service spécialisé de la Confédération en matière de sécurité de l'information. LB suggère de modifier la LSI dans ce sens.

Art. 21 Catégories de sécurité des moyens TIC

De l'avis d'it-rm, il convient de compléter l'al. 2, let. a, en y ajoutant les notions de fiabilité, d'authenticité et d'anonymat (voir observations au sujet de l'art. 4, al. 2).

Pour le Conseil des EPF, le classement de moyens TIC par lesquels des données personnelles méritant d'être particulièrement protégées sont traitées reste flou. Les commentaires figurant en p. 44, 48 et 49 du rapport explicatif sont difficilement compréhensibles et ne fournissent pas d'indications claires. La déclaration figurant en p. 44 du rapport explicatif – selon laquelle «le traitement de données personnelles sensibles dans un système d'information implique la classification du concept de sécurité de l'information y relatif» – est surprenante. Concrètement, il conviendrait ainsi de protéger le concept, mais pas les données elles-mêmes, ce qui n'a pas de sens.

Selon l'appréciation du Conseil des EPF, cette disposition est très floue (que signifie exactement le terme «protection de base»?) et génère des incertitudes qui ne devraient pas simplement être réglée au niveau des dispositions d'exécution. Quelques institutions du domaine des EPF sont parties de l'idée qu'elles ne disposent ou ne disposeront pratiquement d'aucune information qui devrait être classifiée en tant que document interne, confidentiel ou secret au sens de la présente loi (selon l'art. 14 échelons de classification). Le rapport explicatif corrobore d'ailleurs cette appréciation et, par conséquent, ces institutions n'exploitent pas de moyen TIC des échelons de sécurité «protection élevée» ou «protection très élevée».

Art. 22 Exigences de sécurité pour la catégorie de sécurité «protection de base»

Insecor se demande qui détermine les exigences minimales. L'al. 1 est en contradiction avec le mandat légal de la LSI, qui doit fixer les exigences minimales applicables aux moyens TIC pour l'administration fédérale (cf. par ex. l'art. 17, al. 1, let. d, OIAF). Par ailleurs, il est dit à l'al. 2: «Tous les moyens TIC doivent répondre à ces exigences minimales». Qui contrôle que ces normes soient respectées et sur quelle base, respectivement quelles exigences? Tous ces points devraient encore être précisés.

Selon it-rm, l'al. 1 devrait être complété par la phrase suivante: «Il convient de respecter les normes minimales fixées par le service de coordination.» Des normes minimales relatives aux besoins de protection devront également être déterminées par le service de coordination.

Indépendamment de ses préoccupations au sujet des ingérences dans la souveraineté des cantons (art. 3 Cst) et de la subsidiarité (art. 5a et art. 43a Cst), LB propose, pour ce qui est du domaine de l'infrastructure TIC, que l'on confère au service spécialisé de la Confédération la compétence de définir des exigences uniformes pour toute la Suisse concernant les trois échelons de sécurité des moyens TIC, au moins par l'élaboration de normes, de directives, de recommandations, de listes de contrôle ou d'exigences minimales. L'art. 88 LSI en constituerait la base légale.

Art. 23 Concept de sécurité de l'information

SO est d'avis que les contenus minimaux des concepts de sécurité de l'information devraient être inscrits dans la loi ou tout au moins concrétisés dans les dispositions d'exécution de l'ordonnance.

Pour privatim, le texte de cet acte législatif laisse planer le flou sur ce que signifie concrètement un concept de sécurité de l'information, sur son contenu minimal et sur les effets d'un tel concept. Privatim suggère donc d'examiner si c'est dans la loi, dans l'ordonnance d'exécution de la LSI ou dans le message y relatif qu'il convient de spécifier ce qui doit comporter un concept de sécurité de l'information. Si l'on ne le fait pas, on ne pourra garantir une uniformité à l'échelon fédéral et le libellé de l'art. 23 LSI ne constituera alors que des mots creux.

Clusis se demande, pourquoi l'analyse du risque et le concept de sécurité ne sont établis que pour les moyens des catégories de sécurité «protection élevée et protection très élevée»? L'analyse de risque devrait précéder les mesures de sûreté que l'on prendra, alors, selon les catégories.

Comme aucune notion n'a été préalablement définie, insecor ne comprend pas clairement ce qu'il faut entendre par «concept de sécurité de l'information». S'agit-il de ne prendre en considération que la sécurité de l'information? Qu'est-ce que cela signifie exactement? La protection des données n'est-elle plus concernée par cette obligation comme le prévoit HERMES, la méthode de gestion de projet pour les systèmes d'information, respectivement les «concepts ISDS»?

Le Conseil des EPP rappelle que quelques institutions disposent d'ores et déjà actuellement d'un concept de sécurité de l'information.

Art. 24 Contrôles de conformité et d'efficacité

Privatim propose que les contrôles de conformité et d'efficience prévus par l'art. 24 LSI soient assortis de conséquences. Privatim est d'avis qu'il convient de régler ou tout au moins d'expliquer dans le message si, outre l'efficience, on ne devrait pas aussi examiner l'effectivité des mesures décidées et mises en œuvre (cf. à ce sujet l'art. 4, al. 4, LSI). Privatim estime ainsi qu'il s'agit de déterminer ce qu'il advient si les résultats de ces contrôles sont ignorés.

De l'avis de LB, les exigences posées quant à la sécurité des moyens TIC devraient également être remplies lorsqu'on met en œuvre des produits certifiés. Pour de tels produits certifiés d'après des normes de sécurité reconnues sur le plan international comme les «Common Criteria» et en vertu d'un procédé défini, on ne devrait pas imposer un contrôle de conformité et d'efficacité supplémentaire. En revanche, l'obligation de dresser un inventaire des moyens d'information et de communication engagés devrait avoir des conséquences considérables sur les charges organisationnelles et administratives, étant donné le constant changement des moyens engagés et la proportion croissante de terminaux privés utilisés professionnellement.

Art. 25 Autorisation relative à la sécurité

TG ne comprend pas pourquoi, en délivrant l'autorisation relative à la sécurité, l'autorité ou l'organisation accepte les risques résiduels. Pour que l'on ne contourne pas de manière inconsidérée les autorisations relatives à la sécurité, TG préconise dès lors de renoncer totalement à l'al. 2. Si le législateur mentionne, à l'art. 23 du projet de LSI, qu'il y a lieu d'actualiser au fur et à mesure le concept de sécurité, il n'est pas adéquat d'annoncer, deux articles plus loin et par analogie, que dans les autorisations relatives à la sécurité, il n'est plus nécessaire de penser aux risques résiduels et qu'il faut simplement les accepter. TG plaide donc pour que soit purement et simplement supprimée la disposition selon laquelle les risques résiduels peuvent être acceptés. En effet, si cette disposition est maintenue, on court le risque que d'aucuns recourent aux technologies d'information et de communication à la légère et de manière inconsidérée si, aux termes de cette disposition de LSI, on peut se fonder sur l'autorisation et ainsi ne pas devoir davantage penser aux risques.

Art. 27 Sécurité durant l'exploitation

Pour VD Il serait utile de préciser que la sécurité traite des quatre critères de confidentialité, d'intégrité, de disponibilité et de traçabilité.

La notion de stockage et sauvegarde, en regard de l'accès octroyés aux techniciens semble tacite, à l'avis de la FER. En vue des actes de vol constatés, ces deux points pourraient être abordés.

Art. 28 et 29 Mesures relatives aux personnes

Quid d'une différentiation quant aux mesures préventives et celles curatives ? La section 4, contenant les articles 28 et 29 pourrait être intitulées «Mesures préventives relatives aux personnes».

Selon le Conseil des EPF, cet article va trop loin en ce qui concerne les mandataires devant traiter des informations ou utiliser des moyens TIC des EPF, respectivement de la Confédération dans le cadre de leurs tâches ou d'un mandat. Dans la pratique, cela signifierait que lorsqu'elle confierait un mandat à un tiers (une entreprise), l'EPF devrait veiller à la formation et à la formation continue des mandataires dans le domaine de la sécurité de l'information. Une mise en œuvre de cette réglementation aurait un impact financier dans la pratique.

Art. 29 Délivrance restrictive d'autorisations

TG salue le fait qu'il n'y ait pas ici diverses catégories de contrôles de sécurité généraux, mais que les autorités s'assurent de ne délivrer que les autorisations dont les personnes concernées ont besoin pour l'accomplissement de leurs tâches. Il pourrait éventuellement s'avérer judicieux d'instaurer ici une période pour le contrôle de sécurité par analogie à la répétition du contrôle de sécurité relatif aux personnes figurant à l'art. 50 du projet de LSI A l'al. 2, il est dit que les autorisations peuvent être bloquées ou retirées sans préavis lorsque des indices concrets donnent lieu de penser que la sécurité de l'information est menacée. Pour les personnes concernées, cela pourrait constituer une mesure très sévère, étant donné qu'éventuellement, dans le cas concret et en y regardant de plus près, on pourrait conclure ultérieurement que, malgré la présence d'indices, la sécurité de l'information n'aurait nullement été menacée. Lorsque, par exemple, une personne ayant fait l'objet d'un contrôle de sécurité épouse un conjoint provenant d'une région en crise, ce fait peut de prime abord constituer un indice concret donnant lieu de penser que la sécurité de l'information est menacée. Mais, ultérieurement, cette personne devrait avoir la possibilité d'apporter la preuve concrète qu'en dépit de l'existence d'indices, il n'existe aucun danger concret. En se fondant sur le principe juridique «audiatur et altera pars» («que l'autre partie soit aussi entendue»), la possibilité devrait exister, dans le contexte des mesures personnelles, que la personne concernée soit en droit, après que l'autorisation lui a été provisoirement retirée, d'exposer dans une procédure d'envergure qu'en dépit d'indices présumés, elle continuait précisément à ne constituer aucune menace pour la sécurité de l'information.

Le PDC est favorable à ce que les autorités délivrent de manière restrictive des autorisations pour traiter des informations et utiliser des moyens TIC et que la validité de ces autorisations soit régulièrement vérifiée.

Clusis salue le contenu de cet article, mais se demande pourquoi le retrait des autorisations n'est pas expressément mentionné comme automatique? Si cela va de soi, cela va encore mieux en le disant.

Art. 31 Zones de sécurité

Concernant les méthodes de vérifications biométriques, SO estime, au vu de réflexions relatives à la protection des données, qu'il conviendrait de mentionner clairement (dans le texte de loi ou tout au moins dans les commentaires) que les données brutes elles-mêmes ne devront pas être sauvegardées.

TG est d'avis que la mise en œuvre des méthodes de vérifications biométriques devrait faire l'objet d'une réglementation précise. Ainsi, il conviendrait, par exemple en particulier de déterminer la durée de conservation des profils en la matière. En ce qui concerne l'autorisation de contrôler les sacs et les personnes, on pourrait aussi de fait violer par ce biais des secrets de fonctions ou des secrets professionnels. Par ailleurs, cette disposition présente un grand danger pour la sécurité, en ce sens que, lors d'un contrôle des effets de détenteurs des plus hauts secrets, du personnel de contrôle qui n'est pas assez qualifié concernant les échelons hiérarchiques prenne inévitablement connaissance de secrets pour lesquels l'échelon de sécurité auquel est soumis ledit personnel de contrôle est insuffisant. Voilà pourquoi il convient absolument, pour que le but de la loi ne devienne pas obsolète, de définir avec plus de précision l'autorisation de procéder à des fouilles corporelles et à des contrôles de sacs, contrôles qui concerneront certainement aussi à l'avenir les ordinateurs portables (avec le risque d'une manipulation effective). Les contrôles spontanés de pièces/bureaux du personnel devraient également être définis avec davantage de précision, d'autant plus qu'ils peuvent éventuellement concerner des pièces d'habitation privées, ce qui, en cas d'autorisation d'un contrôle général, pourrait se traduire par un conflit face au principe énoncé à l'art. 8 de la

Convention de sauvegarde des droits de l'homme et des libertés fondamentales, selon lequel toute personne a droit notamment au respect de sa vie privée et familiale.

TI estime que les consignes édictées à l'al. 3, let. a, sont restrictives, étant donné qu'elles ne tiennent compte que de la technique actuellement utilisée. Pour TI il conviendrait de modifier la formulation de manière à prendre en compte les futures évolutions technologiques. Cela aurait pour avantage que l'on n'aurait plus besoin de modifier la loi ultérieurement.

Pour VD, les besoins que les autorités concernées peuvent invoquer pour une exploitation selon l'al. 4 devraient être précisés à la lumière du principe de proportionnalité.

Lorsqu'il est question de recourir à des méthodes de vérification biométriques, le PSS souhaite que l'on règle de manière plus précise les dispositions de l'al. 3, let. a. On devrait en particulier fixer la durée pendant laquelle les profils concernés doivent être sauvegardés. Concernant l'autorisation de pratiquer des fouilles corporelles et des contrôles de sacs/mallettes en vertu des dispositions de l'al. 3, let. d, il se pourrait que, dans les faits, on viole ainsi des secrets de fonctions et des secrets professionnels. Il y aurait donc lieu de définir avec plus de précision l'autorisation de pratiquer des fouilles corporelles et le contrôle de sacs/mallettes afin que le but de cette loi ne devienne pas obsolète. Quant à la manière de procéder inopinément à des contrôles dans les locaux, même en l'absence des employés, en vertu des dispositions de l'al. 3, let. e, il conviendrait également de la décrire plus en détail du fait que des locaux privés pourraient être concernés, ce qui pourrait – en admettant que l'autorisation de décréter un tel contrôle soit générale – être en conflit avec le principe énoncé à l'art. 8 de la Convention européenne des droits de l'homme, en vertu duquel, notamment, toute personne a droit au respect de sa vie privée et familiale.

Privatim demande que l'on complète – au moins dans le message concernant l'art. 31, al. 3, let. a, LSI – que, pour les méthodes de vérification biométriques, seules les valeurs de hachage des données respectives soient sauvegardées et non pas les données brutes elles-mêmes.

Clusis salue cet article qui constitue une base légale suffisante au traitement de données personnelles, notamment sensibles.

Chapitre 3 Contrôle de sécurité relatif aux personnes

Généralités

LU constate que le chapitre 3 consacré aux contrôles de sécurité relatifs aux personnes comporte une certaine sur-réglementation qui obligera sans nul doute les cantons à introduire divers nouveaux processus, qui seront surtout onéreux. LU demande par conséquent que ce chapitre 3 fasse l'objet d'un remaniement général avec le but de réduire les charges administratives pour les cantons.

UR reconnaît l'importance des contrôles de sécurité relatifs aux personnes étant donné que lorsque des personnes qui ont accès à des informations classifiées à l'échelon le plus élevé se rendent coupables d'une trahison ou d'un sabotage, cela peut constituer l'une des menaces les plus graves en matière de sécurité. Les fonctions sensibles devraient dès lors être exclusivement confiées à des personnes offrant un aussi haut degré de fiabilité que possible de sorte que l'on ait la certitude qu'elles n'abuseront pas de la confiance qu'on leur accorde.

Pour SG, la réduction des degrés de contrôle n'a aucune incidence sur la collaboration de la Police cantonale dans la procédure des contrôles de sécurité relatifs aux personnes. SG rappelle que la collaboration en la matière de la part de la Police cantonale est régie par les dispositions de l'art. 39 LSI et que ces dernières ne se distinguent guère des dispositions actuellement en vigueur de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI; RS 120). Vu que les dispositions actuellement en vigueur ont fait leurs preuves, SG n'a dès lors aucune objection de principe à l'encontre des nouvelles dispositions proposées par la LSI au sujet des contrôles de sécurité relatifs aux personnes.

Le PSS suggère de reprendre dans la LSI le libellé de l'art. 20, al. 1, LMSI, mais dans une forme modifiée, à savoir: «Art. 32bis Teneur du contrôle de sécurité: Le contrôle consiste à

recueillir des données pertinentes pour la sécurité touchant au mode de vie de la personne concernée, notamment à ses liaisons personnelles étroites et à ses relations familiales, à sa situation financière, à ses rapports avec l'étranger et à des activités illégales menaçant la sûreté intérieure et extérieure. Aucune donnée n'est recueillie sur l'exercice de la liberté d'opinion et d'information garanti par la Constitution fédérale.» Vu qu'il s'agit de données extrêmement sensibles du point de vue de la protection des données et de la personnalité, le PSS est d'avis qu'une densité régulatrice suffisamment élevée s'impose en la matière. Il s'agira aussi d'exclure explicitement, comme c'est le cas jusqu'ici, que des fiches relatives aux activités politiques des particuliers soient établies.

Pour le CP et la CVAM, le chapitre 3 de la LSI (art. 32 à 55) qui réglemente les conditions et modalités du contrôle de sécurité relatif aux personnes constitue un notable gain sur le plan de la garantie des droits individuels et de la sécurité juridique pour les personnes physiques dans le domaine sensible de la sécurité de l'information où l'intérêt public est d'importance, voire prépondérant.

Privatim salue le fait que le projet de loi instaure une règle claire au sujet des contrôles de sécurité relatifs aux personnes (CSP) ainsi que concernant les systèmes d'information. Toutefois, privatim estime qu'il est nécessaire de clarifier d'urgence deux points (cf. observations au sujet des art. 47 et 53).

Insecor salue le fait que les contrôles de sécurité relatifs aux personnes répondent à des règles claires et uniformes.

LB relève que, dans le domaine des contrôles de sécurité relatifs aux personnes, il y aurait lieu de tenir compte des exigences formulées en matière de protection des données et de la personnalité étant donné que ces contrôles constituent une atteinte à la protection de la sphère privée des personnes concernées, protection garantie par la Constitution fédérale (art. 13 Cst).

Le Conseil des EPF estime qu'il règne un certain flou dans le chapitre 3 et se demande si les dispositions de ce chapitre ne s'appliquent qu'aux autorités concernées (il est d'avis qu'on pourrait le comprendre ainsi en interprétant les dispositions au pied de la lettre) et que dès lors les organisations concernées, elles, n'entreraient pas dans le champ d'application de ce chapitre-là. Ainsi, aux termes de l'art. 34, al. 1, let. b, on pourrait se trouver devant la situation suivante: lors d'un mandat très sensible au niveau de la sécurité, les employés de l'entreprise à mandater pourraient être soumis au contrôle CSP alors que les employés d'une institution du domaine des EPF ne le seraient pas. Etant donné qu'aux termes des dispositions des art. 38, al. 3, et 46, al. 2, il convient d'attendre les résultats du contrôle CSP avant d'attribuer un mandat, cela peut engendrer, pour l'institution concernée du domaine des EPF, des retards considérables dans l'attribution de mandats. Il conviendrait dès lors de fixer une durée maximale (brève) pour le contrôle CSP afin de ne pas retarder des attributions de mandats de manière disproportionnée.

Art. 33 Liste des fonctions liées à des activités sensibles

Le TF relève que cet article est essentiel pour le Tribunal fédéral et qu'il ne faut pas le modifier à son détriment.

Art. 34 Personnes assujetties au contrôle

Si, à l'échelon fédéral, les membres du Conseil fédéral et le chancelier de la Confédération étaient exemptés du contrôle de sécurité relatif aux personnes, il ne fait aucun sens pour TG qu'à l'échelon des cantons, seuls les membres du gouvernement soient exclus de ces contrôles. TG estime que, dans cette disposition, on oublie que les chanceliers d'Etat des cantons ont également une fonction de magistrat et qu'il convient donc également qu'ils ne soient pas assujettis au contrôle. Dans le cas contraire, il serait impossible d'accomplir les affaires que commande le gouvernement.

Le TF fait observer que cet article est essentiel pour le Tribunal fédéral et qu'il ne faut pas le modifier à son détriment.

Art. 33 en corrélation avec l'art. 34

Le Conseil des EPF relève que, alors que l'art. 34, al. 1, let. b intègre aussi – dans le contrôle de sécurité relatif à des personnes – des personnes au service des autorités ou des organisations concernées, l'art. 33, lui, ne prescrit aux autorités concernées que d'édicter pour leur domaine de compétence, une liste des fonctions dont les tâches exigent d'effectuer une activité sensible. Cela pourrait conduire à des situations singulières en ce sens que, dans le cas d'une mission comportant une haute sensibilité en matière de sécurité, des employés de l'entreprise à mandater devraient être assujettis au contrôle de sécurité relatif aux personnes mais que les collaborateurs de l'EPF confiant ce mandat à l'entreprise ne le seraient point. Le Conseil des EPF est d'avis qu'il convient de repenser complètement cet art. 33. Il est possible que l'ordonnance sur les contrôles de sécurité relatifs aux personnes. (OCSP) (RS 120.4) ne fasse qu'ordonner l'exécution de cette liste des fonctions dont les tâches exigent l'exercice d'une activité sensible et la liste demandée par l'art. 33 devrait être si possible identique à la celle mentionnée dans l'OCSP. Dès lors, si la liste des fonctions dont les tâches exigent l'exercice d'une activité sensible était identique à celle mentionnée dans l'OCSP, le Conseil des EPF propose de l'expliciter en conséquence dans la LSI et l'OCSP devrait, elle aussi, renvoyer à l'art. 33 LSI.

Art. 35 Degré de contrôle

De l'avis du SRC, un interrogatoire personnel standard mené par du personnel formé serait de mise, sans exception, pour chaque contrôle CSP concernant les personnes ayant accès à des informations classifiées SECRET. Le rapport explicatif de la LSI affirme à juste titre que l'une des menaces les plus critiques et les plus graves se présente lorsque des personnes qui ont accès à des informations classifiées aux échelons supérieurs, ou qui gèrent ou exploitent des moyens TIC particulièrement critiques se rendent coupables de trahison ou de sabotage (rapport explicatif, p. 21) En règle générale, il est quasi impossible de pouvoir dépister en amont déjà de telles menaces uniquement en consultant des registres, mais il convient procéder à une analyse approfondie de la personne. Or, renoncer à cette mesure est en contradiction avec l'analyse susmentionnée et implique une limitation significative de la possibilité de dépister précocement des risques en matière de sécurité. Voilà pourquoi le SRC demande que le législateur exige qu'il soit procédé à des interrogatoires personnels standard lors de contrôles de sécurité élargis tels que le prescrit l'art. 35, let. b.

Art. 37 Consentement

BE demande de compléter l'art. 37 par un nouvel al. 3 ayant la teneur suivante: «[3] Les cantons peuvent prévoir, par un acte législatif, que les contrôles de sécurité relatifs aux personnes puissent être réalisés pour d'autres fonctions sans le consentement des personnes concernées.» BE estime que les cantons devraient avoir la possibilité de prévoir un contrôle de sécurité de personnes également dans d'autres domaines sensibles des administrations cantonales ou communales – par exemple dans la police – sans devoir obtenir le consentement de la personne concernée (par ex. pour que ladite personne puisse avoir accès aux infrastructures importantes ou aux données classifiées).

TI ne souhaite pas remettre en question le principe de la réglementation qu'elle approuve, mais se demande néanmoins quelles seront les conséquences dans le cas où la personne concernée refuse justement de donner son consentement à un tel contrôle de sécurité.

Pour Clusis il est certain que le contrôle de sécurité ne peut être réalisé sans le consentement de la personne concernée. Mais il faudrait préciser que l'engagement d'une telle personne pour des mandats sensibles présuppose que ledit contrôle de sécurité ait été effectué. Une formulation du type «un contrôle de sécurité peut être réalisé préalablement à tout octroi de mandat sensible, ce dont les candidats sont préalablement dûment informés» conviendrait mieux.

LB fait relève que, selon les principes de la protection de la personne et des données (art. 4 et 5 LPD), la collecte de données définie à l'art. 39 LSI requiert le consentement et l'information préalable suffisante de la personne concernée au sujet du contrôle de sécurité relatif aux personnes. Vu que les données collectées comprennent également des données

qui méritent particulièrement d'être protégées au sens de l'art. 3, let. e, LPD, la personne concernée devrait donner son consentement.

Art. 38 Moment du contrôle de sécurité

Le Conseil des EPF trouve qu'il manque, dans l'actuel projet mis en consultation, une réglementation exposant clairement comment procéder lorsque qu'un contrôle de sécurité relatif aux personnes (CSP) n'a pas été préalablement effectué, respectivement lorsqu'il ne l'a pas été avant l'attribution d'une fonction à une personne. De fait, c'est précisément dans le domaine de la recherche qu'il se peut que, dans le cadre d'un projet de recherche, on ne confie des tâches – dont l'aspect sécuritaire n'est pas d'emblée évident et qui n'a pas non plus été identifié par les partenaires concernés du projet – à des personnes qu'ultérieurement ou seulement pour une courte durée et que, de ce fait, on n'a pas eu la possibilité d'effectuer de contrôle préalable. L'absence d'une réglementation claire concernant la réalisation après coup d'un CSP et en particulier les conséquences qui en résultent conduiront inévitablement, dans la pratique, à un conflit entre les exigences de la personne concernée quant à ses droits personnels et les intentions en matière de politique de sécurité exprimées par la LSI, conflit qui s'accompagne d'une perte de temps contrariante. Le conseil des EPF propose que, dans ce type de situation, le CSP puisse être effectué après coup avec le consentement de la personne concernée. Au cas où cette dernière refuse de donner son accord pour ce contrôle de sécurité, les autorités compétentes devraient être autorisées à retirer une fonction ou à interdire l'exercice d'une activité à la personne, ceci sans être tenue d'assumer de quelconques conséquences, qu'elles soient financières ou liées aux droits en matière de personnel.

Art. 39 Collecte des données

Pour VD, les services cantonaux de police et de renseignements, devront comme aujourd'hui être chargés d'exécuter les contrôles de sécurité relatifs aux personnes; ils devront être autorisés à accéder à l'ensemble des données mentionnées à l'art. 39.

NE constate qu'en tant qu'autorité fiscale, il peut être amené à transmettre des informations relevant du secret fiscal dans le cadre d'un contrôle de sécurité relatif aux personnes (CSP). Conformément à l'art. 176, al. 2, LCdir, des renseignements peuvent être communiqués dans la mesure où une base légale fédérale ou cantonale le prévoit expressément. A ce titre, l'art. 39, al. 2, let. a, de la nouvelle loi constitue une base légale suffisante. De telles données ne seront demandées que dans le cadre d'un CSP élargi. Il s'agit ainsi d'identifier et d'évaluer le risque d'une menace des intérêts visés à l'art. 1, al. 2, de la loi par une personne dans l'exercice d'une activité sensible.

Le PSS suggère de maintenir la restriction codifiée jusqu'à présent dans la LMSI, selon laquelle l'on n'est en droit d'interroger des tiers que lorsque la personne concernée a donné son consentement. Le PSS rejette le démantèlement complet du secret bancaire proposé par l'art. 39, al. 2, let. c. Le secret bancaire devrait être levé sous une forme appropriée à l'égard des autorités fiscales. Les organes compétents en matière de contrôles de sécurité relatifs aux personnes pourront alors avoir accès, auprès des autorités fiscales, à toutes les données importantes sur la situation financière des personnes concernées et ne devront pas s'adresser à des établissements financiers ou des banques.

Clusis salue cet article qui constitue une base légale suffisante pour le traitement de données personnelles, notamment les données sensibles.

Le SRC demande que l'on précise, à l'échelon des dispositions d'exécution, que l'échange d'informations doit se faire par le truchement du SRC lorsque le service étranger fait partie d'un organisme de renseignement.

Art. 40 Prise en charge des coûts

AI demande de doter l'art. 40 d'une réserve en vertu de laquelle la Confédération prendra intégralement à sa charge les frais des contrôles de sécurité relatifs aux personnes effectués à sa demande. Les charges financières des cantons découlant des activités qu'ils exercent

sur mandat de la Confédération devraient en effet être pleinement indemnisées. AI est d'avis que ce principe devrait être ancré clairement et sans ambiguïté dans la loi.

Selon TG, il y aura lieu de mentionner le principe que les frais d'un contrôle de sécurité ne devront pas être à la charge du particulier qui doit se soumettre à un tel contrôle, sinon on risque que ces contrôles de sécurité soient réalisés le plus rarement possible par égard financier pour les personnes que l'on connaît éventuellement.

TI relève que les services compétents pour réaliser des contrôles de sécurité relatifs aux personnes peuvent, dans le cas d'un contrôle de sécurité de base, collecter des données pour évaluer le risque que constitue la personne concernée, du fait qu'ils ont aussi accès à divers registres (voir let. d et e). Pour la police en particulier, qui dispose de nombreuses banques de données comportant une grande quantité d'informations (par ex., journal cantonal), il convient de donner une définition exacte de cette notion afin d'éviter l'utilisation de données qui n'ont rien à voir avec le but recherché.

Art. 41 Suspension de la procédure

TG déplore l'absence d'une réglementation qui spécifie ce qu'il doit advenir des données collectées lorsqu'un contrôle de sécurité a été effectué avec succès. Ainsi, par exemple, le projet de loi ne dit rien à propos de la durée de conservation de telles données. Ce point devrait être réglé par la loi. Il conviendrait également de mentionner le droit à une suppression pleine et entière de données anciennes afin que les personnes qui n'ont pas subi le contrôle avec succès puissent ultérieurement à nouveau avoir l'occasion de faire l'objet d'une nouvelle appréciation.

Art. 42 Risque pour la sécurité

Le PDC souhaite que l'on définisse ce qu'il faut comprendre par risque pour la sécurité.

Pour LB, un point n'est pas clair: comment le risque pour la sécurité peut-il être évalué lorsque la personne concernée ne donne pas son consentement au premier contrôle – ou à sa répétition selon l'art. 50 LSI –, le refuse, revient sur son consentement ou ne coopère pas lors du contrôle (art. 41, al. 1, LSI). La personne concernée est alors réputée non contrôlée (art. 41, al. 2, 2^{e} phrase, LSI). La personne concernée ne peut-elle dès lors pas du tout être engagée pour exercer une activité réputée sensible au sens des dispositions de l'art. 33 LSI ou, au cas où elle est revenue sur son consentement lors de la répétition du contrôle, ladite activité devrait-elle lui être retirée? Selon les art. 46 et 47 LSI, la décision quant à l'engagement de la personne concernée incombe apparemment à l'instance de décision.

Art. 43 Résultat de l'évaluation

TI estime que le libellé de l'art. 43, al. 1, let. d, est insatisfaisant. En effet, le commentaire au sujet de cet article dans le rapport explicatif ne précise pas si, à la suite d'une telle déclaration de constatation, il y a lieu de réexaminer le résultat de l'évaluation après une période déterminée.

Art. 44 Communication de l'évaluation

ZG souhaite que l'on transforme la norme facultative de l'art. 44, al. 4, en une disposition impérative. Dans le cas de personnes potentiellement violentes, l'instance chargée de statuer sur la remise ou le retrait de l'arme militaire doit absolument être informée. L'information concernant de telles personnes ne doit pas être laissée à la libre appréciation des services spécialisés CSP, car les risques qui pourraient en découler seraient beaucoup trop importants.

SG relève que l'art. 14 de la loi fédérale sur l'armée (LAAM; RS 510.10), auquel le rapport explicatif renvoie en p. 59 dans ses commentaires au sujet de l'art. 44, al. 3, LSI, n'existe plus et a été abrogé au 1er janvier 2004.

Art. 47 Devoir de communication

Les déclarations des services spécialisés (CSP) ont valeur de recommandation (art. 46 LSI). Et pourtant l'instance de décision informe le service spécialisé CSP lorsqu'elle confie ou non

une activité sensible à une personne ou encore si elle (l'instance) déroge aux conditions recommandées par le service spécialisé CSP en confiant l'activité sensible. Selon le rapport explicatif, le but du devoir de communication prévu à l'art. 47 est que le service CSP ait toujours un aperçu de la pratique des instances de décision et qu'il puisse en tirer les enseignements nécessaires. Pour BS cette argumentation n'est pas convaincante: pourquoi les services spécialisés CSP qui procèdent à leur évaluation selon des critères objectifs devraient-ils adapter leur pratique lorsqu'ils constatent que l'instance de décision ne suit pas ou seulement partiellement leurs recommandations? On court alors le risque que les services spécialisés CSP n'effectuent plus leur évaluation avec l'objectivité requise. On peut même imaginer que cette pratique conduise à ce que les services spécialisés CSP s'axent sur les souhaits et les besoins de l'instance de décision. Voilà qui conduirait à de nouveaux risques en matière de sécurité.

Privatim ne comprend pas pourquoi les services spécialisés CSP qui procèdent à leur évaluation selon des critères objectifs devraient adapter leur pratique, lorsqu'ils constatent que les instances de décision ne suivent pas ou seulement partiellement leurs recommandations. Privatim se demande si cette consigne n'inciterait pas les services spécialisés CSP à satisfaire les souhaits et les besoins des instances de décision et à ne plus accomplir leur tâche essentielle – l'évaluation d'un éventuel risque en matière de sécurité présenté par une personne – avec toute l'objectivité nécessaire. Ne devrait-on pas plutôt attribuer aux services spécialisés CSP des moyens plus contraignants pour qu'ils puissent agir en cas d'éventuels risques en matière de sécurité et qu'ils ne soient pas limités à émettre des recommandations? Ces questions devraient figurer dans les commentaires du rapport explicatif au sujet des art. 46 et suivants.

La Banque nationale est très critique à l'égard du libellé de l'art. 47 prescrivant un devoir de communication par écrit lorsque l'instance de décision confie une activité sensible à une personne en passant outre aux déclarations de risques ou aux constatations du service spécialisé CSP, ou en dérogeant aux conditions recommandées par ce service. La Banque nationale estime que ce devoir de communication est également en contradiction avec les dispositions de l'art. 46 selon lesquelles les déclarations du service effectuant le contrôle a (seulement) un caractère de recommandation et que la décision relative à la délégation de tâches sensibles est exclusivement dans les mains de l'instance qui délègue cette mission.

Art. 50 Répétition du contrôle

TI estime que les délais mentionnés pour la répétition des contrôles de sécurité sont trop longs. TI propose donc de préciser que les contrôles de sécurité de base devront être effectués dans un délai de 5 ans et les contrôles de sécurité élargis dans un délai de 3 ans.

Art. 51 Voies de droit

De l'avis de TG, la réglementation selon laquelle la personne contrôlée peut exiger du service spécialisé CSP compétent, qu'il rende une décision sur le résultat de son contrôle, dans un délai de 30 jours à compter de la remise de la déclaration (cf. al. 3) est contradictoire, puisqu'il est dit à l'al. 1 que la personne concernée peut consulter les documents de contrôle dans un délai de dix jours à compter de la remise d'une déclaration. Lorsque les voies de recours sont utilisées, il convient de pouvoir consulter les pièces du dossier pendant toute la période des délais de recours. Il convient donc d'étendre le délai de recours de 10 jours, mentionné à l'al. 1, à 30 jours. En effet, cela ne fait aucun sens que, par exemple, une personne consulte un avocat après deux semaines et que cet avocat ne puisse pas avoir accès aux pièces du dossier car le droit de les consulter aurait déjà expiré et qu'il interjette recours sans avoir étudié le dossier au préalable.

Se référant à l'autorité de surveillance, respectivement au Ministère public de la Confédération, AS-BA relève que le texte légal ne dit rien concernant l'autorité auprès de laquelle le recourant peut interjeter recours contre une décision du service spécialisé CSP.

Le TAF peut assurer qu'il n'a rien à objecter à la nouvelle conception des voies de recours en vertu des dispositions de l'art. 51, al. 3, LSI.

Art. 52 Système d'information sur le contrôle de sécurité relatif aux personnes

Clusis salue cet article qui constitue une base légale suffisante pour le traitement de données personnelles, notamment les données sensibles.

Pour LB, le libellé de l'art. 52, al. 1, LSI n'est pas clair: les services spécialisé CSP mettent-ils en œuvre un système d'information en vertu d'une structure élaborée selon les consignes de la Confédération – ce qui faciliterait l'accès aux services concernés selon l'art. 53 LSI – ou, au contraire, la LSI laisse-t-elle aux services spécialisés CSP le soin d'installer et d'exploiter un système d'information de leur choix?

Pour des motifs relevant de la protection des données, LB fait part de ses préoccupations quant au fait que le système d'information doive comporter le numéro d'assuré des personnes concernées, puisqu'en vertu des dispositions de l'art. 52, al. 4, let. a, LSI, le système dispose d'ores et déjà des données d'identité des personnes devant être contrôlées ou qui ont été contrôlées. Par ailleurs, aux termes des dispositions de l'art. 36, al. 4, let. c, LPD et de l'art. 50e LAVS, l'enregistrement du numéro AVS dans un autre contexte que celui des assurances sociales fédérales est soumis à des conditions et des restrictions très strictes du fait qu'il faciliterait la collecte d'informations sur des personnes concernées et le «profiling». De l'avis de LB, rien ne justifie que l'on enregistre le numéro d'assuré AVS dans les systèmes d'information sur le contrôle de sécurité relatif aux personnes: le fait que l'on facilite ainsi l'accès à des informations sur des personnes, en vertu des dispositions de l'art. 53 LSI, ne constitue pas une justification suffisante pour l'utilisation supplémentaire du numéro d'assuré AVS, d'ailleurs sujet à caution du point de vue de la loi sur la protection des données, en dehors des assurances sociales fédérales. Au demeurant, LB recommande que, par analogie avec les dispositions de l'art. 77, al. 4, LSI, l'art. 52, al. 2, LSI soit doté d'un complément précisant que le service spécialisé CSP est responsable de la sécurité du système d'information. En effet, comparées aux données concernant les résultats du contrôle de sécurité, les données personnelles enregistrées dans le système d'information impliquent des exigences beaucoup plus élevées en matière de sécurité.

Art. 53 Communication des données

TG estime que la disposition de l'art. 53, al. 3, let. c, ch. 1, du projet de loi LSI en vertu de laquelle l'Etat-major de conduite de l'armée peut accéder – par l'intermédiaire d'une interface – au système d'information, en vue du contrôle de l'accès aux zones de sécurité, va beaucoup trop loin. Ainsi en vertu de l'art. 3 de l'ordonnance sur la protection des ouvrages militaires (SR 510.518.1), la zone protégée 1 consiste en des ouvrages, parties d'ouvrages et aires attenantes qui sont en règle générale visibles de l'extérieur et même en partie librement accessibles. Par conséquent, l'Etat-major de conduite de l'armée ne devrait être autorisé à avoir accès aux données découlant du contrôle de sécurité relatif aux personnes qu'en ce qui concerne les zones protégées 2 et suivantes. TG propose donc d'adapter cette règle en conséquence. Par ailleurs TG estime qu'on peut se demander dans quelle mesure l'Etat-major de conduite de l'armée devrait avoir accès – en vertu de cette même let. c, mais ch. 3 – aux contrôles de sécurité relatifs aux personnes dans le cadre du recrutement des conscrits, d'autant qu'il s'agit essentiellement de jeunes personnes qui n'ont vraisemblablement jamais, pour la plupart, été soumises à un contrôle de sécurité relatif aux personnes.

Privatim relève que les commentaires figurant dans le rapport explicatif ne disent pas pourquoi l'autorité de contrôle doit pouvoir par principe avoir accès à des données personnelles «ultrasensibles» pour accomplir ses tâches. Le contrôle portant sur l'exécution du contrôle CSP ne peut-il donc pas être effectué à l'aide de données anonymisées? Ne pourrait-on pas éventuellement envisager la possibilité de ne recourir à des données «ultrasensibles» que dans des situations exceptionnelles et, dans les cas ordinaires, effectuer les contrôles avec des ensembles de données (blocs de données) ne comportant pas d'autres références à des personnes? Pour privatim, il convient d'éclaircir cette question.

Clusis salue cet article qui constitue une base légale suffisante pour le traitement de données personnelles, notamment les données sensibles. La communication électronique de données doit se faire de manière sécurisée. Là encore, il faut le préciser.

Art. 54 Conservation et destruction des données

SG estime que le système d'information concernant le contrôle de sécurité relatif aux personnes a largement fait ses preuves. Mais, s'agissant des délais en matière de destruction des données au sens de l'art. 54, al. 2, LSI, il convient de tenir compte du fait que ceux qui ont été définis auparavant se prolongeraient de facto. SG est également d'avis qu'il importe également, pour des raisons de protection des données, que le législateur soit conscient qu'il prolonge de fait lesdits délais de destruction. Voilà pourquoi SG suggère d'évoquer expressément cette problématique dans le rapport relatif aux résultats de la procédure de consultation, respectivement dans le futur message et d'en évaluer la portée.

TG est d'avis que la teneur de l'al. 6 devrait figurer immédiatement après l'al. 2 afin que l'on puisse garantir que les données qui doivent être détruites ne tombent pas sous le coup de la réserve de remise aux Archives fédérales.

Le PSS estime que la teneur du texte concernant la réserve d'archivage, définie à l'al. 6 selon les dispositions de la législation fédérale relative à l'archivage, est quelque peu spécieuse. En effet, en ne faisant pas figurer ce libellé immédiatement après l'al. 2 et en ne mentionnant pas l'existence de l'obligation d'archivage dans le titre, on peut donner l'impression que la destruction de certains dossiers ne tombe pas sous le coup de l'obligation d'archivage. Mais cette interprétation contreviendrait alors clairement aux dispositions de la législation fédérale relative à l'archivage actuellement en vigueur, qui énonce l'obligation d'archivage. Voilà pourquoi il convient impérativement de mentionner la réserve d'archivage juste après l'énoncé de l'al. 2 ainsi que dans le titre. Le PSS est par ailleurs d'avis qu'il convient d'instituer une norme selon laquelle l'obligation d'archivage, en vertu de la législation fédérale actuellement en vigueur en matière d'archivage, ne peut être contournée par la destruction arbitraire de dossiers. Il convient aussi de conférer aux Archives fédérales le droit explicite de vérifier que l'obligation d'archivage est respectée. C'est pourquoi le PSS propose un nouveau titre pour l'art. 54 et les deux nouveaux al. 2^{bis} et 2^{ter} ainsi que le déplacement de l'al. 6 qui deviendrait l'al. 2^{quater}

> Art. 54 Nouveau titre: «Obligation d'archivage, conservation et destruction des données»
>
> al. 2^{bis} (nouveau) Les services spécialisés CSP proposent tous les documents dont ils n'ont plus besoin et les données et dossiers destinés à être détruits aux Archives fédérales en vue de leur archivage. Les données et dossiers jugés sans valeur archivistique par les Archives fédérales sont détruits.
>
> al. 2^{ter} (nouveau) En vue de la sécurité à long terme des documents, les services spécialisés CSP autorisent les Archivages fédérales à consulter l'index du système d'information mentionné à l'art. 52.
>
> al. 2^{quater} Sont réservées l'archivage des données selon les dispositions de la loi fédérale sur l'archivage (LAr; RS 152.1) et de la loi fédérale sur le renseignement civil (LFRC; RS 121; art. 7*a*)

Clusis salue cet article qui constitue une base légale suffisante pour le traitement de données personnelles, notamment les données sensibles.

Art. 55 Dispositions complémentaires édictées par le Conseil fédéral

TG estime que, pour des motifs sécuritaires et en raison du risque de chantage, il pourrait être judicieux d'édicter des dispositions sur des restrictions en matière de voyages pour les personnes accomplissant des activités sensibles en matière de sécurité. Certes, cette disposition pourrait limiter les déplacements de ces personnes, mais si l'on considère un cadre plus ample, elle pourrait tout autant constituer une protection à la fois de ces personnes et des données.

Chapitre 4 Procédure de sécurité relative aux entreprises PSE

Généralités

S'agissant de la procédure de sécurité relative aux entreprises, Economiesuisse salue le fait qu'on ait préféré, dans la version allemande du projet, la notion de «Betrieb» («Betriebssicherheitsverfahren») à celle de «Unternehmen»[2]. Ainsi, selon Economisuisse, le fait de parler de « Betrieb », permet de délimiter avec précision le domaine à contrôler, ce qui facilite les mesures de sécurité à engager et cela à un moindre coût. Economiesuisse estime que l'on peut aussi qualifier de positif le fait que le législateur ait étendu le champ d'application de la procédure, actuellement limité à la protection du secret des mandats classifiés du domaine militaire. Le fait que la LSI institue une PSE uniforme pour le domaine militaire et civil et que, dès lors, l'instance puisse établir des attestations de PSE pour des situations internationales renforcera certainement la capacité concurrentielle des entreprises helvétiques dans la procédure d'adjudication à l'étranger.

Le CP et la CVAM constatent que le chapitre 4 du projet LSI (art. 56 à 79) concernant la procédure de sécurité relative aux entreprises ne constitue aucun obstacle majeur pour les acteurs économiques, mais tend au contraire à renforcer les principes d'objectivité et d'équité, de transparence et de sécurité juridique, ainsi qu'à affermir le droit d'être entendu ainsi que les voies de droit des entreprises suisses lorsqu'elles souhaitent se voir adjuger un mandat sensible lié à un marché public fédéral. Enfin, la possibilité offerte à l'avenir par l'art. 57, al. 1, let. b, LSI aux autorités fédérales compétentes d'émettre, à l'intention d'entreprises dont le siège est en Suisse, un certificat de sécurité officiel pour que ces entreprises puissent soumissionner pour des mandats sensibles d'une autorité étrangère ou d'une organisation internationale, renforce la compétitivité des entreprises helvétiques.

Insecor salue la règle uniforme et claire édictée en matière de procédure de sécurité relative aux entreprises.

Pour le Conseil des EPF, le nouveau projet de LSI n'est pas du tout clair. Quand faut-il qualifier un mandat de sensible en matière de sécurité et quand ne le faut-il pas? Alors que les art. 62 et suivants LSI indiquent clairement que le service spécialisé PSE doit apprécier la qualification d'une entreprise, le projet ne dit pas clairement quelle instance doit évaluer si le mandat doit être classifié ou non en tant que sensible pour la sécurité. L'absence d'une telle attribution claire et nette en la matière laisse beaucoup trop de liberté de manœuvre avec le risque de décisions arbitraires. En particulier, la teneur actuelle de l'art. 59 LSI laisse supposer qu'une autorité ou une organisation concernée peut décider elle-même si un mandat doit être considéré ou non comme sensible du point de vue de la sécurité. Si on laisse à l'autorité ou à l'organisation la compétence d'en juger elle-même sans qu'elle ait la possibilité d'être aidée, en matière de vérification, par les autorités de sécurité fédérale, il convient alors de garantir qu'elle ne subisse pas de préjudices dans le cas d'une situation problématique ultérieure. Le Conseil des EPF propose donc de fixer dans la loi quelle instance doit procéder à cette appréciation, respectivement à qui une organisation peut s'adresser en vue de faire vérifier si un mandat doit être ou non qualifié de sensible en matière de sécurité. La décision doit également pouvoir être contestée dans le cas où ce n'est pas l'organisation concernée qui prend cette décision et qu'elle n'est pas d'accord avec la décision prise. Le Conseil des EPF estime qu'il convient de définir très exactement les critères obligeant à réaliser une telle procédure de sécurité relative aux entreprises.

Art. 62 ss Qualification des entreprises concernant la sécurité de l'information

Le Conseil des EPF estime qu'idéalement, l'évaluation de la qualification en vertu des art. 62 et suivants devrait avoir lieu avant l'appel d'offre d'un mandat; quant à la déclaration de sécurité pour les entreprises selon les dispositions de l'art. 69 LSI, elle devrait elle aussi se faire avant l'appel d'offres en vertu de la législation sur les marchés publics. Le Conseil des

[2] NdT : dans la version française du projet, il est ici question d'*entreprise* (= *Unternehmen* en allemand). Il n'aurait en effet guère été envisageable d'opter pour le terme *exploitation,* qui est une autre traduction possible de *Betrieb,* mais dans un contexte précis, par ex. dans le domaine agricole (*exploitation agricole* pour *landwirtschaftlicher Betrieb)*

EPF estime que, lorsqu'un contrôle de sécurité ou de qualification n'a lieu qu'après coup pour des entreprises candidates à l'appel d'offres, l'entreprise à laquelle on a adjugé le mandat dans la procédure d'adjudication court le risque de ne pouvoir l'exécuter si le résultat du contrôle de sécurité est négatif. Aussi le Conseil des EPF propose-t-il de prévoir dans la LSI une disposition relevant du droit spécial et selon laquelle, en cas de résultat négatif du contrôle de sécurité, une entreprise qui serait empêchée d'exécuter son mandat ou dont le contrat serait résilié n'a pas droit à une indemnité, que le contrôle de sécurité ait été effectué avant ou après une procédure d'adjudication. Le Conseil des EPF est aussi d'avis qu'il devrait en être de même en cas de contrôle de sécurité relatif aux personnes lorsqu'un contrat a dû être résilié ou n'a pas pu être conclu en raison d'un résultat négatif du contrôle de sécurité.

Art. 62 Evaluation de la qualification

En raison des conditions délicates de l'adjudication – selon la procédure des marchés publics – de mandats relatifs à l'ordre national et international et sensibles du point de vue de la sécurité (voir à ce sujet l'observation générale), LB est surpris que l'adjudicateur ait le droit, voire l'obligation aux termes des dispositions de l'art. 62, al. 1 P-LSI, de désigner au service spécialisé PSE, avant ou hors de l'appel d'offres, les entreprises entrant en considération pour l'exécution du mandat sensible. En effet, cela exclut automatiquement toutes les autres entreprises de la procédure d'adjudication. Le législateur confère alors aux adjudicateurs une très large compétence, puisqu'ils pourraient ainsi – dans les domaines sensibles du point de vue de la sécurité – apprécier et décider librement quelles entreprises ils souhaitent inviter à se mettre sur les rangs en vue d'exécuter un mandat sensible.

Art. 63 Collecte des données

Le SRC demande que l'on précise, dans les dispositions d'exécution, que l'échange d'informations doit intervenir par le biais du SRC lorsqu'un service étranger fait partie d'une organisation relevant du renseignement.

Art. 64 Risque pour la sécurité

Economiesuisse demande que la marge d'appréciation, en particulier à l'art. 64 LSI, soit limitée, dans les dispositions d'exécution de l'ordonnance qui devra encore être édictée, au moyen de définitions précises des notions abordées et de critères d'évaluation clairs. Selon economiesuisse, le présent projet de loi comporte de nombreuses notions imprécises ou trop larges. Ainsi, à l'art. 64 LSI (risque pour la sécurité), surtout à l'al. 2, let. b (entreprise contrôlée par un Etat étranger ou organisations étrangères de droit public ou privé ou se trouvant sous leur influence), l'autorité dispose d'un trop large pouvoir d'appréciation dans l'examen du risque pour la sécurité découlant de l'exécution d'un mandat par une entreprise. La disposition permet en effet à l'autorité d'exclure des prestataires indésirables de la procédure d'adjudication sans devoir leur donner de motif concret. Il y a là un potentiel d'inégalités de traitement (motivé par des intérêts protectionnistes) et de distorsions en matière de concurrence. Economiesuisse relève que toute réduction artificielle du nombre de prestataires se traduit par des prix plus élevés, ce qui affaiblit la Suisse en tant que place économique.

L'association swico, se référant à un arrêt intermédiaire du Tribunal fédéral administratif du 21 mai 2014 (no de dossier B-998/2014), qualifie de discutable, dans le domaine de la concurrence et des marchés publics, la disposition spécifiant que la probabilité d'une exécution inadéquate ou contraire aux prescriptions du mandat sensible peut être élevée lorsque l'entreprise est contrôlées par des Etats étrangers ou des organisations étrangères de droit public ou privé ou se trouvant sous leur influence En effet, une telle disposition pourrait aggraver encore la problématique des acquisitions. Toute réduction artificielle du nombre de prestataires se traduit par des prix plus élevés. De l'avis de swico, cette pratique affaiblit l'économie helvétique et la Suisse en tant que place économique. La présente disposition légale ouvre la porte à une interprétation arbitraire, voire même abusive de la part des autorités. Ainsi, la marge d'appréciation et d'interprétation beaucoup trop large risque d'écarter des prestataires indésirables. swico demande dès lors que, dans la future ordonnance, on limite clairement la marge d'appréciation et qu'on détermine des critères et des définitions des notions clairs.

On sait en général que les sociétés-mères de nombreuses entreprises travaillant dans le domaine du traitement et de la transmission de l'information sont domiciliées à l'étranger et qu'elles sont contrôlées par des actionnaires. On pourrait déduire des dispositions de l'art. 64, al. 2, let. b, LSI que de telles entreprises présentent d'emblée une probabilité élevée qu'elles exécuteront un mandat sensible de manière contraire aux prescriptions. Dans ce contexte, et en vertu des dispositions de l'art. 65, al. 2, LSI, ces entreprises devraient être exclues de la procédure d'adjudication. LB est dès lors d'avis que l'hypothèse ci-dessus pourrait être interprétée, selon la législation internationale en matière de marchés publics, comme une discrimination non justifiée objectivement parlant à l'encontre de prestataires étrangers dans le domaine du traitement et de la transmission d'informations. Dans tous les cas, il conviendrait, selon LB, de faire examiner par une instance compétente, dans la procédure législative, si et dans quelle mesure l'art. 64, al. 2, let. b, LSI est compatible avec les normes de la législation internationale en matière de marchés publics. Par ailleurs, la stricte application de la règle prescrite par l'art. 64, al. 2, let. b, LSI pourrait conduire à ce que le cercle des entreprises qualifiées pour exécuter de tels mandats sensibles se resserre de manière disproportionnée et qu'ainsi, il y ait encore moins – sinon plus du tout – d'entreprises qualifiées qui soumettent une offre. On pourrait dès lors en arriver à un conflit entre l'intérêt d'assurer une sécurité optimale et l'intérêt de sélectionner le prestataire le mieux qualifié pour exécuter telle ou telle tâche.

Art. 66 Concept de sécurité

LB estime que la prescription selon laquelle le service spécialisé PSE établit un concept de sécurité pour l'entreprise est non seulement inappropriée mais constitue également une ingérence inutile dans l'autonomie de l'entreprise ayant obtenu l'adjudication et donc chargée du mandat sensible. Il serait beaucoup plus adéquat d'édicter une réglementation selon laquelle l'entreprise sélectionnée pour exécuter un mandat sensible doit élaborer un concept de sécurité qu'elle soumet au service spécialisé PSE pour approbation. .

Art. 68 Déclaration de sécurité pour les entreprises / **Art. 69** Exécution d'un mandat sensible

Selon privatim, il faudrait absolument préciser pourquoi cette déclaration de sécurité pour les entreprises doit être établie sous la forme d'une décision alors que pour les contrôles de sécurité relatifs aux personnes, il s'agit seulement d'une recommandation. Privatim est d'avis qu'il y a lieu d'expliquer les raisons de cette différence.

Art. 69 ss Conséquences de la déclaration de sécurité pour les entreprises

De l'avis de Clusis, on ne traite nulle part la problématique de la sous-traitance. Or, vu le caractère sensible des mandats, la sous-traitance est à exclure. A défaut, des conditions strictes doivent être mentionnées dans la loi.

Art 69 Exécution d'un mandat sensible

Le Conseil des EPF considère que cette disposition permet une trop grande ingérence dans l'autonomie des institutions du domaine des EPF. Par ailleurs, cette disposition conduit, spécialement pour les institutions du domaine des EPF qui ne sont pas soumis à l'ordonnance sur l'organisation des marchés publics de l'administration fédérale (Org-OMP), à un surcroît de travail administratif considérable et à des retards disproportionnés surtout si l'on considère que, parallèlement aux dispositions de la LSI, il convient aussi de tenir compte des consignes en matière d'achats publics.

Art. 76 Voies de droit

TG a déjà expliqué, au sujet de l'art. 51 P-LSI, pourquoi il n'est pas judicieux d'imposer que le délai soit différent pour consulter les pièces de dossiers et pour interjeter recours. En vertu de l'art. 50 de la loi fédérale sur la procédure administrative (PA; RS 171.021), les recours contre les décisions de la Confédération peuvent être déposés par principe dans les 30 jours qui suivent la notification de la décision auprès du Tribunal administratif. Voilà pourquoi il convient de prolonger à 30 jours le délai de 10 jours prévu dans cette disposition.

Art. 79 Conservation et destruction des données

TG est d'avis qu'il convient d'intervertir les al. 2 et 3 (et de procéder à l'adaptation grammaticale nécessaire) afin que l'on puisse garantir que les données qui doivent être détruites ne tombent pas sous le coup de la réserve de remise aux Archives fédérales.

Le PSS est d'avis qu'il convient d'émettre pour l'art. 79 les mêmes considérations que celles qu'il a exprimées à propos de l'art. 54, où il s'agit de la conservation et de la destruction de données que le service spécialisé PSE compétent collecte pour exécuter la procédure de sécurité relative aux entreprises.

> Art. 79 Nouveau titre: «Obligation d'archivage, conservation et destruction des données»
>
> al. 2bis (nouveau) Le service spécialisé PSE propose tous les documents dont il n'a plus besoin et les données et dossiers destinés à être détruits aux Archives fédérales en vue de leur archivage. Les données et dossiers jugés sans valeur archivistique par les Archives fédérales sont détruits.
>
> al. 2ter (nouveau) En vue de la sécurité à long terme des documents, le service spécialisé PSE autorise les Archives fédérales à consulter son propre système d'archivage.
>
> al. 2^{quater} Sont réservées les dispositions de la loi fédérale sur l'archivage (LAr; RS 152.1 et de la loi fédérale sur le renseignement civil (LFRC; RS 121; art. 7*a*)

Chapitre 5 Sécurité de l'information dans les infrastructures critiques (art. 81 à 83)

De l'avis du PSS, tout le chapitre 5 consacré à la sécurité de l'information dans les infrastructures critiques (LSI art. 81 à 83) doit être fondamentalement remanié. En effet, ce chapitre du projet comporte des habilitations forfaitaires inacceptables à propos d'activités de renseignement. De plus, on n'y clarifie pas suffisamment les interfaces entre la garantie de la protection des informations dans le cadre des infrastructures critiques d'une part, et la protection des infrastructures critiques en soi d'autre part. Le PSS estime que la protection d'infrastructures critiques est une tâche beaucoup trop importante du point de vue de la politique de sécurité pour être traitée de manière aussi globale et peu méticuleuse que le projet de LSI le prévoit.

Art. 81 Tâches de la Confédération

Le PSS s'étonne que l'al. 3 de cette disposition soit si vague à propos de l'échange des informations; elle ne précise pas de quels types d'informations il s'agit, pas plus qu'elle ne définit ni le cercle des exploitants d'infrastructures critiques ni les services compétents de la Confédération. Le PSS demande d'apporter davantage de clarté à ce sujet et d'augmenter significativement la densité de la réglementation. Le PSS estime dès lors qu'il convient pour le moins d'ajouter un nouvel al. 4 avec la teneur suivante: «[4] Sont réservées les dispositions de la loi sur la protection des données.»

It-rm considère que l'expression «prêter son concours» ne suffit de loin pas, car le sabotage d'infrastructures critiques pourrait de fait porter bien davantage atteinte au bien-être de notre Etat que la divulgation d'informations confidentielles. Par conséquent, de l'avis d'it-rm il convient d'édicter des dispositions minimales et, selon les circonstances, de prévoir le soutien financier de la Confédération pour la mise en œuvre de ces directives. It-rm propose donc d'inscrire une légitimation ad hoc dans la loi.

Art. 82 Traitement des données personnelles

SO considère que cette disposition permet aux services compétents de traiter des données personnelles à l'insu des personnes concernées. Cela constituerait une ingérence considérable dans les droits de la personne. Au plus tard dès la disparition du risque présumé, la personne doit être informée à ce propos. SO estime donc qu'il faut en l'occurrence fixer une réglementation semblable à celle visée aux art. 283, 298 et 298 d du Code de procédure pénale (CPP) pour l'observation et les recherches secrètes.

TG demande la radiation de la disposition de l'art. 82 du projet de LSI selon laquelle, afin de prévenir des dangers pour les infrastructures critiques, les services compétents sont habilités à traiter des données personnelles – notamment des ressources d'adressage dans le domaine des télécommunications – et à les communiquer sans que les personnes concernées s'en aperçoivent. Sous prétexte de sécurité de l'information, on crée ici un instrument autorisant à traiter des données personnelles particulièrement dignes d'être protégées appartenant à de nombreuses personnes. Par ailleurs, TG estime qu'il n'y a pas le moindre élément de contrôle ou la possibilité d'intervenir judiciairement en cas d'abus. Dans la loi fédérale sur la sécurité de l'information, il s'agit de garantir la sécurité dans le traitement d'informations. Cette loi ne doit pas être utilisée comme porte de service discrète pour se livrer à des activités de renseignement.

TI propose de compléter les dispositions de l'art. 82 LSI par un al. 4 prévoyant qu'en cas d'une identification de l'utilisateur, ce dernier en soit informé et que les données respectives puissent être communiquées aux autorités compétentes. En effet, au cas où une personne est identifiée sur la base de données personnelle en vertu de l'art. 82, elle doit en être informée, pour le moins lorsqu'il n'y a plus de raison de craindre qu'elle représente un danger (règle analogue à celle des art. 283, 298 et 298d du CPP) concernant l'observation des personnes ainsi que les recherches et investigations secrètes). TI pense donc à cet égard que le libellé de l'al. 1 est trop faible et que même la description ponctuelle qu'apporte le rapport explicatif n'est pas suffisante.

Le PSS demande la radiation de l'art. 82 du projet de LSI. Aux termes de cette disposition, les services compétents sont habilités à traiter des données personnelles – notamment des ressources d'adressage dans le domaine des télécommunications – et à les communiquer afin de prévenir des dangers pour les infrastructures critiques. La loi dit même que ces données peuvent être traitées à l'insu des personnes concernées. Sous le prétexte d'œuvrer en faveur de la sécurité de l'information, on crée ici un instrument permettant de traiter des données personnelles particulièrement dignes d'être protégées appartenant à un grand nombre de personnes. Par ailleurs, le PSS considère qu'il n'y a ici ni élément de contrôle ni possibilité d'intervenir judiciairement en cas d'abus. Dans la loi fédérale sur la sécurité de l'information, il s'agit de garantir la sécurité dans le traitement d'informations. Cette loi ne doit pas être utilisée comme porte de service discrète pour des activités de renseignement.

Pour privatim, vu le principe de la bonne foi ancré dans la Constitution fédérale et l'impératif de transparence qui en découle en matière de protection des données, le traitement de données personnelles à l'insu de la personne afin de prévenir des dangers pour les infrastructures critiques ne se justifie qu'à condition que la personne concernée soit informée lorsqu'il n'y a plus de raison de craindre qu'elle représente un danger (réglementation semblable à celle visée aux art. 283, 298 et 298d du CPP pour l'observation et les recherches et investigations secrètes).

Pour LB, il est hors de question que la protection d'infrastructures qui, en vertu de l'art. 3, al. 3, est indispensable au fonctionnement de la société, de l'économie et de l'Etat, doive bénéficier d'une valeur élevée. Ce nonobstant, il convient, dans ce domaine aussi, de tenir compte du principe de la proportionnalité dans l'activité qu'exerce l'Etat (en vertu de l'art. 5, al. 2, Cst) en matière d'ingérence dans les droits fondamentaux garantis par la Constitution fédérale. Dès lors, il est difficilement compréhensible que, dans le projet de LSI – et surtout à une époque où les citoyens sont de plus en plus méfiants à l'égard des mesures étatiques de surveillance – le législateur puisse conférer des compétences aux exploitants d'infrastructures critiques, qui les autorisent:

- d'office et sans éléments particuliers tels que présomptions d'un crime,
- sans avoir l'autorisation d'une instance judiciaire ou tout au moins d'une autorité compétente et responsable à l'échelon politique,
- à traiter des données personnelles, en particulier des ressources d'adressage, mais aussi des données sensibles au sens de la définition donnée par l'art. 3, let. c, LPD dans tout le domaine des télécommunications,

- et ce, sans aucune limitation temporelle ni matérielle ;
- traiter les données (cf. art. 3, let. e/f, LPD) signifiant collecter, conserver, exploiter, modifier et archiver les données pour une durée indéterminée;
- à communiquer les données saisies aux autorités et organisations concernées, aux services compétents des cantons et même à des tiers (naturellement toujours lorsque c'est nécessaire à l'exécution de leurs tâches);
- à ne pas informer les personnes concernées après l'exécution de la surveillance, contrairement aux normes édictées par l'art. 279 CPP;
- et, qu'en la matière, les exploitants d'infrastructures ne doivent pas être soumis à un contrôle par une instance indépendante pour ces activités de surveillance.

LB admet que la protection des infrastructures critiques a certes une importance fondamentale pour l'Etat, l'économie et la société civile. Toutefois, il ne convient pas de sacrifier les principes élémentaires de l'activité de l'Etat ni la garantie des droits fondamentaux de la personne sur l'autel de la protection de ces infrastructures critiques. Il devrait y avoir un rapport équilibré entre la sécurité et la protection des droits fondamentaux.

Art. 83 Dispositions complémentaires édictées par le Conseil fédéral

TG demande, par analogie à ses remarques à propos de l'art. 82 du projet de LSI, de renoncer aux activités en matière de renseignement.

Le PSS rejette la délégation de compétences au Conseil fédéral prévue à l'art. 83 LSI. Une loi fédérale sur la sécurité de l'information n'a pas pour mission d'autoriser, par la «petite porte» des services privés anonymes et des autorités à exercer des activités de renseignement. Le PSS estime que la répartition des tâches et la collaboration entre des services effectuant des tâches selon l'art. 81 et le Service de renseignement de la Confédération doivent être réglementées à l'échelon de la loi. Le PSS est d'avis que les services qui doivent obtenir la compétence d'échanger des informations relevant du renseignement doivent être mentionnés expressément et individuellement, ceci pour des raisons relevant du droit en matière de protection des données. Il convient également de spécifier quelles informations ces services sont habilités à échanger avec le Service de renseignement de la Confédération. Et parce qu'il s'agit souvent de données particulièrement sensibles, il convient de respecter la densité normative élevée habituelle. Si cet objectif ne peut être atteint, il convient d'exclure explicitement toute activité de renseignement à l'art. 83 LSI.

Chapitre 6 Organisation et exécution

Art. 84 Préposé à la sécurité de l'information / **Art. 85** Conférence des préposés à la sécurité de l'information

GL demande qu'un représentant de la Conférence suisse sur l'informatique CSI soit désigné comme préposé à la sécurité de l'information des cantons. Ce représentant pourrait également être intégré au sein de la Conférence des préposés à la sécurité de l'information aux termes des dispositions de l'art. 85 LSI.

ZG demande de compléter l'art. 84, al. 1, par la let. «g. les cantons.» L'organisation floue que propose la LSI avec des «antennes cantonales» ne permet de mettre en œuvre ni une coordination fonctionnelle ni une harmonisation entre la Confédération et les cantons. Il est nécessaire d'instaurer une liaison beaucoup plus étroite et institutionnalisée avec les cantons, ce qui permettra aussi de mieux atteindre les objectifs fixés. Cela pourrait se faire par l'occupation d'un siège permanent d'une représentation cantonale au sein de la Conférence des préposés à la sécurité de l'information prévue par le législateur à l'art. 85, comme c'est par exemple le cas dans la politique européenne (représentation constante des cantons dans la Direction des affaires européennes (DAE). Les cantons devraient nommer de con-

cert un préposé à la sécurité de l'information, comme pour les différents organes de la Confédération (art. 84).

Pour éviter des doublons lors de demandes concernant des problèmes sécuritaires, TG demande d'étendre la portée de l'art. 85 du projet de LSI en ce sens que la Conférence des préposés à la sécurité de l'information n'assume pas seulement la coordination avec le préposé fédéral à la protection des données et à la transparence (PFPDT) mais aussi la coordination avec les préposés cantonaux à la protection des données.

Dans la mesure où la loi sera applicable aux autorités cantonales mandatées par la Confédération, VD pose la question de la représentation de ces dernières dans la Conférence des préposés à la sécurité de l'information.

De l'avis du PSS, la Conférence des préposés à la sécurité de l'information ne devrait pas uniquement assumer la coordination avec le préposé fédéral à la protection des données et à la transparence (PFPDT), mais aussi avec les préposés cantonaux à la protection des données concernés.

Clusis salue la nouvelle fonction du préposé à la sécurité de l'information. Mais pourquoi ne pas mettre celle-ci en lien avec la fonction de conseiller en protection des données prévue par la LPD, notamment en mentionnant que «le préposé à la sécurité de l'information collabore étroitement avec le conseiller en protection des données personnelles de l'entreprise, cas échéant»? En outre, les tâches des uns et des autres devraient être mieux coordonnées.

Le Service de renseignement de la Confédération demande que les systèmes opérationnels et les informations collectées par le renseignement soient exclus de l'examen effectué par le préposé à la sécurité de l'information du DDPS, étant donné que le SRC applique des mesures particulières de protection pour des raisons de protection des sources lors de la collecte opérationnelle d'informations. Ces mesures-là font par ailleurs régulièrement l'objet d'une vérification par une instance de surveillance interne du DDPS (haute surveillance du SRC).

Art. 86 Service spécialisé de la Confédération en matière de sécurité de l'information

TI estime qu'en vue de l'élaboration d'une seule et unique structure centralisée prévue par cette disposition, l'art. 86 ne définit pas clairement les différents rôles entre les différents services pluridisciplinaires. D'ailleurs, selon TI ces dispositions sont contradictoires à plusieurs égards ou – pis encore – redondantes.

Art. 87 Dispositions d'exécution

Vu la réglementation relative à la clause d'exemption (opting out) (art. 87, al. 3, LSI) – selon laquelle chaque autorité concernée peut édicter ses propres règles d'exécution – et le fait que les exigences standard fixées par le Conseil fédéral ainsi que les mesures qu'il propose d'appliquer n'ont qu'un caractère de recommandations, ZH voit un risque que les définitions, qui sont somme toute très floues, soient interprétées différemment d'une autorité à l'autre. ZH pense qu'on court ainsi le risque que les dispositions d'exécution des diverses autorités soient réglées différemment. Aussi ce canton est-il d'avis que ce projet de loi – en soi très détaillé – devrait apporter des précisions, tout au moins en ce qui concerne les intérêts publics dignes de protection définis à l'art. 1, al. 2, LSI et les échelons de classification prévus méritant, eux aussi, d'être spécifiés.

BE demande de compléter l'art. 87 par un nouvel al. 5 avec la teneur suivante: «[5] Le Conseil fédéral détermine, par voie d'ordonnance, les activités exercées en vertu de l'art. 2, al. 2, let. f.» BE demande par ailleurs que le message du Conseil fédéral relatif à la LSI établisse la liste de ces activités dans une perspective actuelle. Aux termes de l'art. 2, let. f, la LSI s'applique également aux autorités et services cantonaux qui exercent des activités sensibles sur mandat de la Confédération et sous sa surveillance. Mais le rapport explicatif ne mentionne pas en quoi consistent ces activités. Afin que les cantons et les communes sachent exactement à quoi s'en tenir et dans quelle mesure ils sont soumis aux normes de la LSI, il importe donc, selon BE, de le préciser par voie d'ordonnance. Pour que les cantons et les communes puissent d'emblée évaluer quelles incidences la LSI aura sur leurs tâches, il

serait judicieux de publier, dans le message du Conseil fédéral concernant la LSI déjà, une liste de ces activités dans une perspective actuelle. Ce message devrait aussi clarifier ce qu'il convient d'entendre par «sous sa surveillance».

ZG se demande si la réglementation relative à la clause d'exemption prévue par le projet de loi – à savoir que chaque autorité pourrait fixer des dispositions d'exécution de manière autonome et édicter ainsi une ordonnance – permettra réellement d'atteindre le but recherché. ZG estime par ailleurs que la loi devrait fixer des dispositions allant bien au-delà de simples normes minimales s'il s'agit de garantir la sécurité de l'information au sein de toutes les autorités assujetties à la LSI. Il serait nécessaire d'établir des standards et des normes applicables aux divers services. Selon ZG, il serait dès lors judicieux que les cantons soient impliqués.

BS considère que ni le libellé actuel proposé par le projet de loi (art. 2, al. 2, let. f, LSI) ni encore le rapport explicatif ne mentionnent clairement les activités des autorités cantonales qui tombent dans le champ d'application de cette loi. BS suggère donc de compléter l'art. 87 LSI par une disposition supplémentaire selon laquelle le Conseil fédéral doit déterminer, par voie d'ordonnance, les activités qui tombent sous le coup de l'art. 2, al. 2, let. f. Pour qu'il soit possible d'évaluer les incidences de la LSI sur les tâches du canton, il serait judicieux de publier, dans le message du Conseil fédéral concernant la LSI déjà, une liste de ces activités dans une perspective actuelle. Par ailleurs, de l'avis de BS, le message du Conseil fédéral concernant la LSI doit expliquer clairement ce qu'il convient d'entendre par «sous sa surveillance».

Quant à la clause d'exemption, TI constate que le fait que les autorités puissent édicter de manière autonome des dispositions d'exécution – norme qui d'ailleurs devrait s'appliquer par analogie à toutes les autres autorités fédérales – offre justement la base «idéale» pour générer des inégalités de traitement dans l'exécution de cette loi. TI estime que ce n'est de loin pas une solution idéale dans le contexte de la sécurité de l'information.

Le PDC salue le fait que le présent projet de LSI ne limite pas l'autonomie des autorités et trouve dès lors judicieux que les autorités concernées puissent édicter leurs propres dispositions d'exécution. Le PDC soutient également la règle selon laquelle les dispositions d'exécution du Conseil fédéral s'appliquent par analogie aux autorités concernées qui n'édicteraient pas leurs propres dispositions d'exécution.

AS-MPC prend acte que l'autorité de surveillance – mentionnée en tant qu'autorité concernée à l'art. 2, let. d – peut édicter ses propres dispositions d'exécution conformément à l'art. 87, al. 1. De ce fait, quelques-unes des réserves que cette autorité a émises lors de la consultation des offices du 2 avril 2013 ne sont plus de mise.

Privatim considère que ni la teneur proposée à l'art. 2, al. 2, let. f, LSI, ni le rapport explicatif ne permettent de savoir quelles activités des autorités cantonales tombent dans le champ d'application de cette loi. Privatim demande dès lors de compléter l'art. 87 LSI par une disposition selon laquelle le Conseil fédéral doit déterminer, par voie d'ordonnance, les activités qui tombent sous le coup des dispositions de l'art. 2, al. 2, let. f. Pour pouvoir évaluer les incidences de la LSI sur les tâches des cantons, privatim estime qu'il serait judicieux que le Conseil fédéral publie, dans son message déjà, une liste de ces activités dans une perspective actuelle. Par ailleurs, selon Privatim, le message du Conseil fédéral concernant la LSI devrait préciser clairement ce qu'il convient d'entendre par «sous sa surveillance».

La Conférence suisse sur l'informatique (CSI) demande de compléter l'art. 87 par un nouvel al. 5 avec la teneur suivante: «[5] Le Conseil fédéral détermine, par voie d'ordonnance, les activités exercées en vertu de l'art. 2, al. 2, let. f.» La CSI demande en outre que le Conseil fédéral publie, dans son message déjà, une liste de ces activités dans une perspective actuelle. La CSI estime en effet que le rapport explicatif ne mentionne pas quelles activités sensibles confiées aux autorités et services cantonaux et placées sous la surveillance de la Confédération, tombent dans le champ d'application de cette loi au sens de l'art. 2, al. f. Pour que les cantons et les communes puissent évaluer clairement quelles incidences la LSI aura sur leurs tâches, la CSI estime qu'il serait judicieux que le Conseil fédéral publie, dans son message déjà, une liste de ces activités dans une perspective actuelle.

La BNS salue expressément le fait que les autorités soient libres d'édicter leurs propres dispositions d'exécution aux termes de l'art. 87 du projet de LSI. Toutefois, le rapport explicatif (en p. 17) mentionne que «l'exécution en toute autonomie présente un inconvénient: toutes les exigences minimales de la sécurité de l'information devant être satisfaites par toutes les autorités de la Confédération doivent nécessairement figurer dans la loi: dès lors, le projet comporte de nombreuses dispositions qui, si l'on se tenait à la hiérarchie normative, relèveraient davantage du niveau de l'ordonnance». La BNS comprend tout à fait les efforts que déploie le législateur dans le projet de loi en vue de régler également certaines exigences sur le plan de l'organisation des autorités concernées qui sont indépendantes au niveau constitutionnel. Mais, précisément, le fait de tenir compte du fait que les dispositions d'exécution du Conseil fédéral s'appliquent par analogie aux autorités concernées – dans la mesure où ces dernières n'édictent pas de dispositions au sens de l'art. 87 – et qu'il entraîne ainsi un retrait d'autonomie de ces autorités mérite d'émettre une certaine réserve. En effet, sur le plan pratique, le projet ancre sur le plan de la loi des éléments devant se situer à l'échelon de l'ordonnance, ce qui porte atteinte à l'autonomie en matière d'exécution.

Le TF fait observer que cet article a une portée considérable pour le TF et qu'il ne doit pas être modifié à son détriment.

Insecor estime que le fait que chaque autorité fédérale puisse édicter ses propres dispositions d'exécution n'est pas vraiment pertinent quant à l'objectif visé. En effet, c'est justement dans les ordonnances que l'on trouve des précisions importantes au sujet du texte légal, précisions qui, dans le domaine de la sécurité de l'information, ne doivent pas à nouveau être dispersées dans divers actes législatifs. En fin de compte, il existe encore et toujours la possibilité d'édicter des ordonnances départementales ou des directives prenant en compte les besoins spécifiques d'une unité administrative.

Pour le Conseil des EPF, il s'agira d'examiner de quelles parties de la loi les institutions du domaine des EPF et le Conseil des EPF pourraient être exclus; le Conseil des EPF demande que, tout au moins, le chapitre concernant le contrôle de sécurité relatif aux entreprises ne soit applicable ni aux institutions du domaine des EPF ni au Conseil des EPF (voir à ce sujet en particulier la prise de position relative aux art. 65 et suivants).

Art. 88 Exigences et mesures standard

BE demande de compléter l'art. 88 par un nouvel al. 4 avec la teneur suivante: «[4] Le Conseil fédéral règle, par voie d'ordonnance, quelles autorités concernées sont compétentes, individuellement ou collectivement, pour établir des déclarations obligatoires au sujet des exigences et mesures standard ayant trait à des activités ou à des systèmes exécutés ou utilisés en commun par plusieurs autorités. Dans la mesure où des autorités cantonales concernées sont touchées par cette disposition, il est nécessaire de demander leur consentement.» Dans divers domaines, les autorités fédérales et cantonales collaborent étroitement ou les autorités cantonales exécutent des mandats qui leur sont conférés par la Confédération, par exemple, dans le domaine de la police. Par ailleurs, des fichiers ou des systèmes TIC (par exemple des réseaux) de diverses autorités doivent fréquemment être reliés pour que les autorités puissent accomplir les tâches qui leur sont dévolues. Dans ces cas-là, BE estime qu'il n'est pas judicieux que les autorités partenaires adoptent des niveaux de sécurité différents. De ce fait, une autorité compétente unique désignée par le Conseil fédéral devrait déterminer le niveau de sécurité de l'information pour l'ensemble de l'activité à accomplir. Toutefois, pour éviter qu'une autorité fédérale détermine de manière unilatérale des mesures qui se traduiraient par un surcroît élevé de frais pour les cantons, il conviendra de toujours s'assurer du consentement des autorités cantonales éventuellement concernées.

De l'avis du PDC, il importe que le Conseil fédéral définisse des exigences de sécurité standardisées ainsi que des mesures en matière d'organisation, de personnel, de techniques et de construction également standardisées en matière de sécurité de l'information. Ces exigences et mesures devraient tenir compte des acquis de l'enseignement et de la technique et constituer des recommandations pour les autorités concernées.

Privatim recommande d'examiner d'urgence dans quelle mesure les exigences et mesures standard doivent être déclarées obligatoires pour toutes les autorités et organisations sou-

mises aux règles de la LSI. Si l'on se limite au caractère de recommandation ou de déclaration facultative, il est impossible, selon privatim – d'atteindre un niveau de protection uniforme.

La CSI déclare qu'étant donné que, d'une part, des autorités fédérales et cantonales collaborent très étroitement dans divers domaines ou que des autorités cantonales et communales accomplissent des mandats de la Confédération et que, d'autre part, des fichiers ou systèmes TIC de différentes autorités doivent souvent être reliés pour que ces autorités puissent accomplir leurs tâches, il n'est pas judicieux que les différentes autorités partenaires appliquent des niveaux de sécurité distincts. Voilà pourquoi c'est une autorité compétente unique désignée par le Conseil fédéral qui devrait déterminer le niveau de sécurité de l'information pour l'ensemble de l'activité à accomplir. Pour éviter qu'une autorité fédérale détermine unilatéralement des mesures qui engendreraient davantage de frais supplémentaires pour les cantons, il conviendrait d'avoir l'accord des autorités cantonales éventuellement concernées. La CSI demande dès lors de compléter l'art. 88 par un nouvel al. 4 ayant la teneur suivante:

> «[4] Le Conseil fédéral règle, par voie d'ordonnance, quelles autorités concernées sont compétentes, individuellement ou collectivement, pour établir des déclarations obligatoires au sujet des exigences et mesures standard ayant trait à des activités ou à des systèmes exécutés ou utilisés en commun par plusieurs autorités concernées. Lorsque des autorités cantonales concernées sont impliquées, leur consentement est nécessaire.»

Le TF déclare que cet article est crucial pour le Tribunal fédéral et qu'il ne faut rien y changer à son détriment.

Pour it-rm, il y a impérativement lieu de désigner une institution (service de coordination) chargée d'édicter les dispositions d'exécution qui seront contraignantes pour toutes les autorités concernées par la présente loi et qui, par conséquent devront être respectées (contradiction avec l'art. 88, al. 3, LSI). Sinon cela conduirait à un manque d'homogénéité dans le dispositif de sécurité et contribuerait en outre à ce que l'on tienne trop peu compte de l'évolution de la technique et donc des modifications en matière de besoins de sécurité qui en découlent. Par ailleurs, it-rm estime qu'il est improductif pour l'échange d'informations que les autorités prennent des mesures distinctes pour protéger un même bien juridique. En effet, l'autorité qui a mis en œuvre les mesures de sécurité les plus efficientes – et donc les plus onéreuses –considérera que le manque d'homogénéité n'est pas rentable. On sait pertinemment que l'on évalue la sécurité de l'information en se fondant sur le maillon le plus faible du dispositif. Il ne faudrait donc pouvoir s'écarter de cette règle que dans des cas exceptionnels et par le biais d'une demande écrite motivée.

Selon le SRC, le fait de déléguer l'élaboration et le traitement de standards de sécurité au SRC (par analogie à fedpol, voir à ce sujet les commentaires au sujet de l'art. 88, al. 2, LSI, p. 71-72 du rapport explicatif) se justifie tout à fait. A l'instar de fedpol, le SRC a des besoins particuliers quant au traitement et à l'archivage des données. Notamment, l'échange de données entre différents services étatiques en Suisse et à l'étranger revêt une importance particulière pour le SRC. On ne saurait donc comparer ces besoins-là avec ceux des autres services fédéraux. Et même à l'égard de la protection des sources, les standards de sécurité spécifiques au SRC sont incontournables.

Art. 89 Cantons

Aux termes des dispositions de l'art. 89 LSI, les autorités et les services cantonaux ne sont soumis à cette loi que s'ils exercent des activités sensibles sur mandat et sous la surveillance directe de la Confédération. «La présente loi ne s'applique pas aux autorités et services cantonaux qui appliquent la législation fédérale de manière autonome» dit le rapport explicatif en p. 37. Mais pour ZH, cette réglementation cruciale concernant le champ d'application de la loi soulève davantage de questions qu'elle n'en résout. Quelles activités des cantons entend-on ici? Dans quels domaines les cantons exercent-ils des mandats et sous quelle surveillance directe? Comme le rapport explicatif ne mentionne pas un seul exemple concret, on peut donc partir du principe que, pour la Confédération aussi, ce point n'est pas clair. Pourtant, il est nécessaire que les cantons puissent évaluer si cette loi est

applicable à leurs activités cantonales et, le cas échéant, dans quelle ampleur. S'ils sont soumis à cette loi, les cantons doivent savoir quelles en seront les conséquences – en particulier au niveau financier. C'est au plus tard dans son message aux Chambres fédérales que le Conseil fédéral devra clarifier ce point.

ZH et BE demandent de compléter l'art. 89 LSI par une règle disposant que les autorités et services cantonaux peuvent solliciter les prestations des services spécialisés de la Confédération prévus à cet effet dans la LSI. ZH motive sa demande par le fait que la LSI prévoit des mesures (notamment des contrôles de sécurité relatifs aux personnes et la procédure de sécurité relative aux entreprises) qui ne sont pas du tout réglées ou réglées différemment sur le plan cantonal (et communal). Par conséquent, les cantons (et les communes) devraient pouvoir solliciter les services spéciaux de la Confédération. BE propose un al. 4 complémentaire à cet article, qui devrait avoir la teneur suivante: «[4] Les autorités et services cantonaux peuvent solliciter les prestations des services spécialisés de la Confédération prévus par la présente loi. Le Conseil fédéral peut édicter que, lorsque des prestations sont fournies à d'autres autorités et services que ceux prévus à l'al. 1, il sera perçu des émoluments couvrant les frais administratifs.» BE considère qu'il ne serait pas judicieux et difficilement possible de mettre en place dans les cantons et communes, souvent de façon décentralisée, le savoir-faire spécifique indispensable aux tâches des services spécialisé CSP et PSE. C'est pourquoi les cantons doivent pouvoir solliciter les prestations des services spécialisés de la Confédération. Dans la mesure où les dispositions de la LSI assujettissent directement les services cantonaux et communaux à cette loi (art. 2, al. 2, let. f, respectivement art. 89, al. 1, LSI), les prestations fournies (par exemple la réalisation d'un contrôle CSP) devraient être financées par la Confédération. Mais, dans la mesure où les cantons mettent en œuvre les dispositions de la LSI dans leur propre domaine de compétences et de manière autonome, par exemple en introduisant un contrôle CSP pour d'autres employés du canton, il semble approprié qu'ils prennent à leur charge, par le biais d'émoluments, les frais encourus par la Confédération.

ZH relève que l'art. 89, al. 2, let. a, LSI autorise le Conseil fédéral de régler les contrôles de sécurité relatifs aux personne, pour les organes cantonaux. Mais du fait qu'avec les contrôles de sécurité relatifs aux personnes, on commet une ingérence dans les droits fondamentaux des personnes concernées, cette réglementation doit se faire à l'échelon de la loi, tout au moins pour ses lignes essentielles. Il conviendrait dès lors de modifier en ce sens le projet de LSI.

OW considère qu'il est judicieux que les cantons doivent désigner un service en tant qu'interlocuteur des autorités fédérales en matière de sécurité de l'information (art. 89, al. 3, LSI). Ainsi, on peut partir de l'idée que l'échange d'information aura lieu systématiquement et que la mise en œuvre des mesures interviendra aussi de manière coordonnée.

NW déclare qu'il désignera un service cantonal en tant qu'interlocuteur des autorités fédérales par voie d'ordonnance d'introduction à la LSI. Dans ce canton, la sécurité de l'informatique a été attribuée au centre de prestations informatiques, *Informatikleistungszentrum ILZ OVV/NW*, qui a son siège à Sarnen.

GL désigne, en tant qu'interlocuteur des autorités fédérales en matière de sécurité de l'information, le service de l'informatique *Informatikdienst*, Rathaus, 8750 Glaris.

ZG demande de modifier, respectivement de compléter l'art. 89, al. 1 et 3, de la manière suivante:

> «[1] Dans la mesure où des autorités et services cantonaux exercent des activités sensibles, ~~sur mandat et sous la surveillance de la Confédération,~~ en collaboration avec la Confédération, les cantons veillent à appliquer les mesures en se fondant sur la présente loi.
> [2] …(inchangé)
> [3] Chaque canton désigne, pour des questions de sécurité de l'information, un service en tant qu'interlocuteur des autorités fédérales et des organes cantonaux de coordination.»

De leur côté, les cantons doivent désigner un organe centralisé en tant qu'antenne et service de coordination, par exemple la Conférence des gouvernements cantonaux CdC, qui a une activité intersectorielle. De cette manière, les incidences sur les cantons et les questions de collaboration et de coordination entre la Confédération et les cantons pourraient être abordées de manière fondée et précoce. D'une manière générale, ZG suggère que la Confédération recherche suffisamment tôt la collaboration avec les cantons, tel que le prévoit le règlement-cadre sur le mode de travail de la CdC et la Conférence des directeurs relative à la coopération entre la Confédération et les cantons, du 28 septembre 2012.

SO part de l'idée que très peu de collaborateurs cantonaux seraient soumis aux règles de la présente loi. Le rapport explicatif ne comporte pas d'autres détails qui permettraient d'y voir plus clair. Même si quelques-uns seulement des collaborateurs des services cantonaux accomplissent des mandats pour la Confédération, cela aurait pour conséquence que tous les systèmes TIC cantonaux devraient répondre aux exigences de la LSI. Mais cela impliquerait des charges élevées. SO demande dès lors d'étudier si l'on ne peut déléguer aux cantons la compétence en matière de sécurité de l'information – dans la mesure où les cantons respecteraient des standard minimaux – par analogie avec les dispositions de l'art. 37, al. 1 de la loi sur la protection des données. Ces normes minimales devraient figurer exhaustivement dans la LSI ou dans l'ordonnance d'exécution.

BS ne se considère concerné par les dispositions de la LSI que lorsqu'il accomplira une activité sensible définie par l'art. 2, al. 3, sur mandat de la Confédération en vertu de l'art. 2, al. 2, let. f, LSI. Dans ce cas, les mesures ordonnées à l'art. 89, al. 1, LSI devraient être appliquées. La division Informatiksteuerung und Organisation (ISO) (pilotage et organisation de l'informatique) a entamé des travaux préliminaires en vue de préparer systématiquement l'ISMS.BS (système de gestion de la sécurité de BS), ceci afin de pouvoir mettre en œuvre dans le canton les dispositions de la loi et les mesures qu'elle prévoit. Selon la loi, les cantons seraient tenus de désigner un service en tant qu'interlocuteur des autorités fédérales en matière de sécurité de l'information (art. 89, al. 3, LSI). De par la désignation d'un responsable cantonal en matière de sécurité de l'information au sein de l'ISO, cette exigence serait d'ores et déjà satisfaite.

AI requiert de régler, à l'art. 89, que la Confédération, qui mandaterait sous sa surveillance les cantons en vue d'accomplir des activités sensibles, prendra à sa charge intégralement les coûts, y compris ceux de l'infrastructure nécessaire pour ces tâches. Les cantons qui accompliraient ainsi des mandats au nom de la Confédération devraient en effet être indemnisés intégralement pour leurs dépenses dans ce contexte. AI répète que la loi doit inscrire ce principe expressément et sans ambiguïté dans la loi. Par ailleurs, les cantons devraient pouvoir s'adresser directement et gratuitement aux services spécialisés de la Confédération pour obtenir des prestations relevant de la loi sur la sécurité de l'information. Il conviendrait de compléter l'art. 89 dans ce sens.

TG demande de biffer purement et simplement l'al. 2 de l'art. 89 de la LSI. Les cantons n'ont pas de compte à rendre dans la sélection de leur propre personnel. Il ne convient pas que la Confédération dicte au canton comment sélectionner son propre personnel. Même s'il est seulement question ici des activités sensibles que les cantons effectuent sur mandat de la Confédération, chaque canton devrait garder la compétence de décider quel personnel il veut affecter à telle ou telle tâche. En outre, les cantons, vu leur proximité à l'égard de leur propre personnel, sont bien mieux à même d'évaluer les potentiels de risques dans leurs propres rangs. TG invite dès lors la Confédération à bien vouloir tenir compte de leur souveraineté.

VD veut préciser l'al. 2 «Le Conseil fédéral, en concertation avec les cantons règle: ...». L'ordonnance fédérale devrait tenir compte du fait qu'une entité indépendante, telle que le Contrôle cantonal des finances (cf. ad art. 11, al. 2, ci-dessus), peut être habilitée, sur mandat spécial de l'autorité exécutive cantonale, à effectuer le contrôle des mesures.

Conformément à la demande (l'art. 89, al. 3), GE désigne la direction générale des systèmes d'information (DGSI) en qualité d'interlocuteur cantonal pour la sécurité de l'information.

La CSI demande de compléter l'art. 89 par un nouvel al. 4 ayant la teneur suivante:

«[4] Des autorités et services cantonaux peuvent solliciter des prestations auprès des services spécialisés de la Confédération prévus dans la présente loi. Le Conseil fédéral peut édicter que lorsque des prestations sont fournies à d'autres autorités et services que ceux prévus à l'al. 1, il sera perçu des émoluments couvrant les frais administratifs.»

La CSI considère qu'il serait peu judicieux et difficilement possible de mettre en place dans les cantons et communes, souvent de façon décentralisée, le savoir-faire spécifique indispensable aux tâches des services spécialisé CSP et PSE. C'est pourquoi les cantons devraient pouvoir prétendre aux prestations des services spécialisés en la matière de la Confédération. Dans la mesure où les dispositions de la LSI assujettissent directement les services cantonaux et communaux à cette loi (art. 2, al. 2, let. f, respectivement art. 89, al. 1, LSI), les prestations fournies (par ex., la réalisation d'un contrôle CSP) devraient être à la charge de la Confédération. Mais dans la mesure où les cantons mettent en œuvre les dispositions de la LSI dans leur propre domaine de compétences et de manière tout à fait autonome, par exemple en introduisant un contrôle CSP pour d'autres employés du canton, il semble approprié qu'ils prennent à leur charge, par le biais d'émoluments, les frais encourus par la Confédération. S'il n'est pas possible de répondre à cette demande, l'art. 2, al. 2, let. f et l'art. 89 devront être biffés et il conviendra de leur préférer la solution proposée par la loi fédérale sur la protection des données, qui dit que, dans la mesure où les normes minimales sont respectées, les cantons sont aussi compétents en matière de protection des données lorsqu'ils exécutent des tâches que leur ont confiées des autorités fédérales (art. 37 LPD).

Art. 90 Conventions de droit international

Le SRC fait observer que l'échange d'informations en matière de renseignement se fonde sur l'art. 12 du projet de loi sur le renseignement (LRens).

Chapitre 7 Dispositions finales

Art. 93 Dispositions transitoires

BE et la CSO demandent de compléter l'art. 93 par un nouvel al. 3 ayant la teneur suivante: «[3]Les autorités concernées des cantons mettent en œuvre la présente loi au plus tard cinq ans après son entrée en vigueur, dans la mesure où le Conseil fédéral ne détermine pas une période transitoire plus longue». C'est en particulier dans le domaine des systèmes TIC que la mise en œuvre de mesures de sécurité pourrait impliquer des frais élevés, du fait que des adaptations de matériel informatique et de logiciels seront indispensables. Il n'est souvent plus rentable d'adapter un ancien système à de nouvelles exigences en matière de sécurité parce que l'acquisition d'un nouveau système est plus avantageuse. Mais il se pourrait aussi que l'adaptation requise soit impossible à mettre en œuvre parce que le fabricant d'ordinateurs ou de logiciels aurait renoncé au support ou n'existerait simplement plus. Pour pouvoir répondre aux exigences de la LSI et mettre en œuvre les mesures qu'elle prévoit, il conviendra en règle générale de remplacer les anciens systèmes par de nouveaux. Par conséquent, la période transitoire devra être déterminée en fonction du cycle de vie des systèmes TIC. Il faudra en tenir compte. Par ailleurs, la CSI souhaite ajouter une deuxième phrase: «En dérogation aux dispositions de la Confédération, le droit cantonal peut prévoir une période transitoire allant jusqu'à dix ans si une mise en œuvre plus précoce engendrait des frais disproportionnés.»

L'AS-MPC est d'avis qu'il n'existe encore pas de solution satisfaisante pour des personnes qui n'ont actuellement pas subi un contrôle de sécurité relatif aux personnes mais qui devraient certainement s'y soumettre en vertu des nouvelles dispositions. En effet, ces personnes occupent actuellement des fonctions comportant des activités sensibles et l'AS-MPC se demande s'il ne faut pas prévoir explicitement une réglementation à leur intention. Et si ces personnes devaient se soumettre après coup à un contrôle CSP, il conviendrait également de déterminer un délai à ce propos dans les dispositions transitoires.

5.2 Modification d'autres actes législatifs

Insecor déplore l'absence, dans le projet de loi, d'autres harmonisations avec des lois fédérales ayant un rapport avec la sécurité de l'information, (par ex., LPD, SCSE, LTC ou CP) – en particulier au vu des risques et des dangers actuels. Insecor recommande d'examiner instamment cette proposition et de vérifier s'il n'y a pas des dispositions de certaines ordonnances (notamment OIAF, OPri, OLPD) qui devraient être enlevées à l'échelon de la loi. Insecor considère que la phrase suivante figurant en p. 15 du rapport explicatif est contradictoire: «[…] Les responsables ne sont que rarement sommés de rendre des comptes.» En effet, le présent projet de loi ne contient ni des dispositions pénales ni une adaptation pertinente du Code pénal (CP; RS 311.0). Insecor suggère que l'on reconsidère cette possibilité.

6 Prises de position sur les conséquences exposées dans le rapport explicatif

Sont exposées ci-après les prises de position à propos des conséquences mentionnées dans le rapport explicatif. Cependant, seules figurent les conséquences ayant fait l'objet d'une prise de position explicite ou implicite.

Généralités

TI tient à relever que les conséquences des procédures au niveau institutionnel, en particulier les implications en matière de procédure pour les échelons visés, ne sont qu'insuffisamment abordées même si elles ne sont pas en lien direct avec le thème de la sécurité et qu'au surplus aucune consigne spécifique ne figure dans le rapport.

Le PSS s'attend à ce que les conséquences de la LSI en matière d'organisation, de personnel et de finances soit bien expliquées dans le message et que la Confédération veille à ce que toutes les autorités concernées disposent de ressources financières suffisantes pour pouvoir mettre en œuvre cette loi dans les règles de l'art. Le PSS est d'avis qu'aujourd'hui, les plus graves lacunes en matière de sécurité de l'information et de protection des structures TIC ne se situent pas à l'échelon conceptuel ou législatif, mais bien plutôt dans les déficiences en matière d'organisation ainsi que dans la dotation financière et en personnel insuffisantes des services concernés.

6.1 Conséquences pour la Confédération

Le PDC demande que le Conseil fédéral explique en détail dans son futur message – comme il s'y engage dans son rapport explicatif – quels seront les coûts qu'engendrera la mise en vigueur de cette loi. Le Conseil fédéral est donc prié d'exposer quels seront les coûts découlant d'une Conférence des préposés à la sécurité de l'information ainsi que ceux du service spécial de la Confédération pour la sécurité de l'information. Le PDC demande en outre que l'édification et l'exploitation du nouveau système interviennent sans augmentation de l'effectif du personnel.

Le PLR souligne que les coûts réels que pourrait engendrer cette loi, tant techniques qu'organisationnels ne sont pas encore estimables et ne le seront pas avant la fin de la procédure de consultation. Pour Le PLR, il est important qu'un équilibre soit trouvé entre le niveau de sécurité et les coûts nécessaires pour l'obtenir, afin d'éviter une explosion des dépenses.

Le PSS est d'avis que l'allocation des moyens doit clairement revenir en priorité au domaine civil et quotidien. Les départements civils compétents n'ont ni assez de personnel ni assez de ressources financières pour passer de la parole aux actes. Une chose est claire pour le PSS: la compétence principale doit continuer à se situer de manière décentralisée dans les départements civils. Il est nécessaire de procéder à une redistribution des ressources provenant de domaines de la politique de sécurité militaire devenus obsolètes vers de nouveaux domaines d'une politique de sécurité civile qu'il y a lieu de mettre en place en urgence. De fait, quiconque voudrait gagner en sécurité devrait engager les 250 à 300 millions de francs par an – devenus disponibles à la suite du refus de l'acquisition d'avions de combat Gripen – dans le domaine des risques liés à la société de l'information, des cyberrisques et dans la

protection d'infrastructures critiques. Le rapport explicatif de la LSI, qui occulte complètement l'importance des frais subséquents et les postes de travail supplémentaires qu'implique la LSI, montre à l'évidence combien la question de ressources est précaire. Sans réponse claire à cette question, même la meilleure des nouvelles lois n'amènera pas un gain effectif en matière de sécurité.

Dans le contexte de cette nouvelle loi pour le moins conflictuelle, le PSS réaffirme sa demande de donner enfin les ressources nécessaires au Préposé fédéral à la protection des données et à la transparence (PFPDT). Le PFPDT joue en effet un rôle-clé pour l'établissement d'une bonne pratique juridique en matière de classification et de transparence. Il ne serait utile à personne de ne donner que des recommandations superficielles lors de litiges en raison de ressources insuffisantes. En effet, dans la mesure où la LSI confère de nouvelles tâches au PFPDT, la Confédération se doit de lui fournir des moyens financiers et en personnel supplémentaires. Le PSS escompte dès lors que le message du Conseil fédéral au sujet de la LSI mentionnera le nombre de nouveaux postes de travail qui seront attribués au PFPDT afin qu'il soit en mesure d'accomplir cette tâche supplémentaire importante qui vient s'ajouter à celles qu'il effectue déjà.

Pour swico, le fait que le rapport explicatif à la LSI ne mentionne aucun chiffre à la p. 76 au sujet des conséquences financières et de l'effectif du personnel montre à l'évidence que ce projet de loi n'est pas suffisamment mûri.

6.2 Conséquences pour les cantons et les communes

ZH demande que les conséquences pour les cantons et leur implication soient clarifiées au plus tard lors de la mise en œuvre de cette loi et de l'élaboration des dispositions d'exécution y relatives. Dans ce contexte, il conviendra impérativement de tenir compte des besoins des cantons en général et de l'autonomie qui leur revient en matière d'organisation en particulier.

Afin que les cantons et les communes sachent avec précision dans quelle mesure ils sont soumis à la LSI, BE demande que cela figure dans une liste à l'échelon de l'ordonnance. Le message du Conseil fédéral concernant la LSI devrait comporter une liste de ces activités dans la perspective actuelle pour permettre aux cantons et aux communes d'évaluer les conséquences qu'auront pour eux la LSI.

BE souhaite aussi que la Confédération implique étroitement les cantons et leurs autorités spécialisées pour l'élaboration des dispositions d'exécution de la loi, en particulier lorsque ces dispositions concernent également les cantons.

Pour LU, le coût de ces mesures pour les cantons n'est pas clair. Tant que l'on ne connaîtra pas les dispositions d'exécution de l'ordonnance fédérale, les cantons pourront difficilement évaluer les dépenses qui les attendent. Aussi LU demande-t-il qu'avant d'adopter cette loi, les conséquences financières pour les cantons soient précisés. Tant la loi que les ordonnances d'exécution devront être aménagées de telle manière que les cantons puissent mettre en œuvre la loi sans devoir faire face à des charges administratives élevées.

UR estime aussi qu'il est difficile d'évaluer les conséquences financières pour les cantons dans le cadre de la gestion des risques et des mesures nécessaires en matière de sécurité et de protection. Ici, c'est surtout à la Confédération de faire preuve du discernement nécessaire pour que la sécurité de l'information soit également abordable pour les cantons à plus faible capacité financière. Si la Confédération dispose déjà d'éléments concernant les coûts auxquels les cantons doivent s'attendre et le financement en général, ils devraient encore être communiqués.

En considération du rapport explicatif et du projet de loi, SZ arrive à la conclusion que la LSI n'aura fondamentalement aucune conséquence pour le canton de SZ. Toutefois, les dispositions d'exécution suivantes se fondant sur la loi pourraient tout de même avoir certaines conséquences pour SZ dans le domaine du contrôle de sécurité élargi en vertu de l'art. 39, al. 2, let. a, en corrélation avec l'art. 40, al. 1, LSI. Voilà pourquoi SZ part de l'idée que SZ sera aussi invité en temps voulu à se prononcer sur les dispositions d'exécution.

OW ne peut pas encore, en l'état actuel des choses, évaluer les conséquences concrètes de cette nouvelle loi sur son canton, respectivement sur les charges financières supplémentaires à assumer. Mais vu la proportion relativement modeste des tâches fédérales qui lui ont été confiées par rapport à l'ensemble des tâches administratives d'OW, la charge supplémentaire devrait se limiter à cadre plutôt étroit. Selon OW, les autorités de poursuite pénale sont tributaires d'informations provenant des autorités fédérales pour accomplir les tâches qui lui sont dévolues. Afin que les informations qui parviendront aux autorités cantonales soient protégées aux termes des dispositions contenues dans le projet de loi, OW devra peut-être prendre des dispositions pour renforcer la sécurité, ce qui pourrait générer des charges financières supplémentaires pour les autorités plus modestes. Cela devrait être examiné ultérieurement.

NW part de l'idée que si cette loi présentée en procédure de consultation entrait en vigueur, les dispositions d'exécution de la LSI pourraient constituer pour NW une énorme charge financière sur le plan opérationnel. NW retient que la loi comporte quelques articles qui, en fonction du champ d'application, concernerait certains services ou toute l'administration cantonale, ce qui pourrait impliquer diverses adaptations en matière de lois, d'ordonnances et de directives. NW part donc de l'idée qu'il sera invité en temps voulu à se prononcer sur les dispositions d'exécution respectives.

GL estime que la nouvelle loi sur la sécurité d'information est très claire en ce qui concerne les autorités fédérales. Elle l'est moins pour les cantons et une récapitulation de leurs tâches essentielles, de leurs compétences et de leurs responsabilités serait judicieuse. En plus de cette récapitulation, certaines définitions devraient être plus concrètes. Il convient en particulier de clarifier sous quelle forme exactement les différents cantons sont concernés par les exigences de la loi et par les formations nécessaires.

Selon ZG, les conséquences pour les différents cantons sont trop peu élaborées, tant dans le projet de loi que dans le rapport explicatif.

SO part de l'idée que très peu de collaborateurs cantonaux seront concernés par les dispositions de la loi. Mais le rapport explicatif ne comporte pas d'indications détaillées à ce sujet. Même si quelques-uns seulement des collaborateurs des services cantonaux accomplissent des mandats pour la Confédération, cela signifie que tous les systèmes TIC cantonaux devraient répondre aux exigences de la LSI, ce qui implique des charges élevées. SO demande dès lors d'examiner si l'on pourrait déléguer aux cantons la compétence en matière de sécurité de l'information par analogie à la réglementation de l'art. 37, al. 1, de la loi sur la protection des données – dans la mesure où les cantons respecteraient des standard minimaux. Ces normes minimales devraient dès lors figurer exhaustivement dans la LSI ou dans l'ordonnance d'exécution.

BS estime que l'on n'est informé ni dans le texte de loi proposé (art. 2, al. 2, let. f, LSI) ni dans les commentaires des activités tombant dans le champ d'application de cette loi. BS suggère dès lors de compléter l'art. 87 LSI par une disposition selon laquelle le Conseil fédéral doit déterminer par voie d'ordonnance les activités que recouvre l'art. 2, al. 2, let. f. Afin que les cantons puissent évaluer les conséquences qu'ils devront assumer, le message du Conseil fédéral déjà devrait comporter une liste de ces activités dans une perspective actuelle. Le message devra également clarifier ce qu'il convient d'entendre par «sous sa surveillance».

BL estime qu'aucun coût ne devrait être à la charge des cantons assujettis à cette nouvelle loi car le rapport ne dit strictement rien à ce propos.

Etant donné que la nouvelle loi fédérale fixe certes un cadre pour l'exercice d'activités sensibles, mais qu'il confère des marges de manœuvre pour l'exécution, AI estime qu'il est d'autant plus important que les cantons puissent se prononcer également au sujet des ordonnances d'exécution. AI souhaite aussi pouvoir se prononcer au sujet de l'ordonnance du Conseil fédéral.

Pour GR, le projet de LSI ne règle pas suffisamment clairement les interfaces entre la Confédération et les cantons. Il manque notamment une description exacte des activités sen-

sibles et on ne sait comment les cantons seront impliqués. Pour qu'aucune difficulté ne surgisse lors de la mise en œuvre pratique, il convient de régler ces points de manière différenciée déjà au niveau de la loi. Selon que les cantons sont tenus d'appliquer la LSI directement en tant qu'autorité concernée ou dans le cadre de l'intégration des dispositions de la LSI dans leur droit cantonal, ils doivent avoir la possibilité de pouvoir mandater les services spécialisés centraux de la Confédération – qui doivent encore être créés en vertu de la LSI (en particulier les services chargés des contrôles de sécurité relatifs aux personnes et ceux qui effectuent la procédure de contrôle de sécurité des entreprises). L'adaptation des systèmes aux mesures de sécurité pourrait par ailleurs impliquer des frais élevés. La durée de vie des systèmes TIC est de cinq à dix ans. Voilà pourquoi il convient d'établir des périodes transitoires appropriés de cinq à dix ans au moins pour la mise en œuvre de la loi.

AG estime qu'à l'heure actuelle, plusieurs questions concernant des domaines importants pour les cantons sont encore en suspens. Ainsi, par exemple, il est dit que la Confédération réglera par voie d'ordonnance comment elle entend aménager les contrôles de sécurité relatifs aux personnes pour les employés cantonaux. Par conséquent, aujourd'hui, les cantons n'ont aucune indication quant au mode d'exécution et aux incidences du contrôle de sécurité sur le personnel de l'administration cantonale. AG déplore aussi que rien ne soit mentionné concernant le contrôle, par la Confédération, de la mise en œuvre des dispositions fédérales au sein des cantons. AG estime que l'aménagement de la procédure et notamment le flux de données dans cette procédure de surveillance sont flous. Selon AG, le projet de loi ne comporte guère d'interfaces entre le droit en matière de sécurité de l'information et la surveillance de la protection des données des cantons. Quoi qu'il en soit, AG ne peut pas apprécier définitivement cette question, car les rapports réciproques entre la protection des données et la sécurité de l'information ne sont que marginalement évoqués dans le rapport. Le rapport explicatif comporte néanmoins une réserve implicite en faveur du droit fédéral en matière de protection des données (cf. rapport explicatif, chiffre 1.3.1.2, en p. 28). AG part dès lors de l'idée qu'une telle réserve s'appliquera d'autant plus au droit cantonal en matière de protection des données, notamment dans les domaines où les cantons soumis à la LSI devront mettre en œuvre le droit fédéral. Les questions en suspens mentionnées ici devront encore être éclaircies au cours de la procédure législative et expliquées dans le message du Conseil fédéral relatif à la LSI.

De l'avis de TI, la LSI aura naturellement des conséquences opérationnelles à l'échelon des cantons. Il conviendra d'examiner les conséquences de la nouvelle loi – en particulier la classification des informations – sur les systèmes et les procédures habituelles de l'administration cantonale tessinoise. Pour satisfaire aux nouvelles règles, la mise en réseau des systèmes canton – Confédération devra vraisemblablement être adaptée. Il conviendra aussi de lancer sans tarder les éventuelles modifications des lois sectorielles à apporter pour les domaines dans lesquels les services de l'administration cantonale fournissent des informations à l'administration fédérale. Par exemple: les réglementations pour la sécurité des entreprises doivent-elles être appliquées pour le choix des produits informatiques utilisés dans la mise en réseau avec la Confédération? Y a-t-il une relation entre la loi cantonale sur l'archivage et le droit supérieur, en l'occurrence la loi fédérale sur l'archivage, impliquant alors des modifications à l'échelon cantonal?

6.3 Conséquences pour l'économie

La plupart des conséquences économiques de cette loi vont dans le sens des exigences du *PLR*. Elle laisse en effet escompter un renforcement de la compétitivité des entreprises et une meilleure protection des secrets économiques qu'elles placeront sous la protection du gouvernement.

Pour le CP et la CVAM il est difficile, à ce stade, de se prononcer sur l'efficacité des mesures proposées, on peut toutefois se réjouir du fait qu'en lieu et place de normes et mesures disparates s'appliquant dans les divers services fédéraux, un dispositif légal de référence s'appliquera à l'avenir. Cela affermira la sécurité des flux d'information tout en les facilitant, renforcera la sécurité juridique et favorisera, paradoxalement, le principe de transparence

dans l'administration. Celui-ci sera en effet réservé pour autant qu'aucune mesure de sécurité basée sur la LSI ou l'une des autres lois spéciales ne s'applique (art. 3, al. 1, LSI).

7 Prises de position concernant les aspects juridiques

TI considère qu'il est nécessaire que le futur message du Conseil fédéral précise, éventuellement en se référant à l'art. 89 du projet de loi, que la haute surveillance par la Confédération ne touche aucunement les compétences des autorités cantonales pour la surveillance et le contrôle de la protection des données et que ces dernières seront dès lors maintenues telles quelles. TI estime qu'il importe de préciser que les organes cantonaux publics ne deviendront pas des organes de la Confédération, ceci indépendamment du genre d'acte juridique par lequel la Confédération leur aura attribué ou délégué une tâche publique (mandat ou délégation de fonction). Sauf en ce qui concerne le droit spécial de la Confédération qui détermine et délimite le mandat ou la délégation de fonction, ces organes cantonaux publics restent soumis au droit cantonal, à savoir aussi au droit en matière de protection des données.

Pour le CP et la CVAM, le projet LSI ne soulève de problèmes ni en matière de constitutionnalité, ni sous l'angle du fédéralisme.