Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

17.028

Message concernant la loi sur la sécurité de l'information

du 22 février 2017

Messieurs les Présidents,
Mesdames, Messieurs,

Par le présent message, nous vous soumettons le projet d'une loi sur la sécurité de l'information, en vous proposant de l'adopter.

Nous vous prions d'agréer, Messieurs les Présidents, Mesdames, Messieurs, l'assurance de notre haute considération.

22 février 2017

Au nom du Conseil fédéral suisse:

La présidente de la Confédération, Doris Leuthard
Le chancelier de la Confédération, Walter Thurnherr

Condensé

Se fondant sur des normes reconnues sur le plan international, le présent projet crée une base légale uniforme pour la sécurité de l'information au sein de la Confédération. Il met l'accent sur les informations et systèmes les plus critiques et sur la standardisation des mesures, dans le but d'améliorer de façon durable la sécurité de l'information au sein de la Confédération et son économicité.

Contexte

Plusieurs attaques contre des systèmes d'information de la Confédération ont montré que la protection des informations de la Confédération présentait des lacunes, qui sont notamment dues à des bases légales obsolètes. Les bases légales de la sécurité de l'information sont disséminées dans une multitude d'actes. Les diverses prescriptions sont conçues de façon sectorielle: elles ne sont guère harmonisées et présentent souvent des lacunes et des contradictions. Il s'ensuit que la Confédération exploite aujourd'hui, sous l'angle tant juridique qu'organisationnel, des structures parallèles pour les divers secteurs de la sécurité de l'information. L'évolution vers une société de l'information accentue la complexité et le caractère dynamique des menaces: ces dernières doivent être abordées globalement, en réseau et avec professionnalisme. La pratique a montré que l'approche sectorielle au sein de la Confédération n'est plus adaptée et n'est plus efficace. Les mesures de sécurité de l'information doivent être conçues pour répondre aux besoins de la société de l'information, être mises en œuvre autant que possible en fonction des risques et être coordonnées entre les différentes autorités. Il faut dès lors regrouper les mesures dans un seule cadre réglementaire moderne, ce qui correspond aussi aux normes internationales qui règlent la sécurité de l'information dans une perspective globale.

Le Conseil fédéral a chargé le DDPS d'élaborer des bases légales au sens formel pour la sécurité de l'information au sein de la Confédération. Il a donné pour instruction que des normes minimales de sécurité s'appliquent à toutes les autorités fédérales. Durant les travaux, le Conseil fédéral a pris de nombreuses mesures dont le projet devait tenir compte. Les résultats majoritairement favorables de la procédure de consultation ont confirmé que des mesures s'imposaient dans le domaine de la sécurité de l'information et que le projet offrait une solution adéquate.

Contenu du projet

Par le présent projet, le Conseil fédéral poursuit deux objectifs ambitieux. D'une part, il entend regrouper en un seul acte les bases légales principales régissant la sécurité des informations et des moyens informatiques de la Confédération (acte unique), ce qui devrait permettre de combler les lacunes du droit en vigueur et de tenir compte de nombreuses demandes des autorités parlementaires de surveillance. D'autre part, la réglementation s'appliquera à l'ensemble des autorités et organisations de la Confédération, afin d'atteindre un niveau de sécurité aussi homogène que possible. La réglementation reste cependant très modeste à deux égards: premièrement, le projet se fonde sur des normes internationales éprouvées; deuxièmement, il ne fixe aucune mesure précise pour garantir la sécurité de l'information,

mais pose uniquement un cadre formel sur la base duquel les autorités fédérales prendront les mesures de sécurité de l'information par voie d'ordonnance et de directive.

La loi règle en particulier la gestion des risques, la classification des informations, la sécurité des moyens informatiques, les mesures applicables au personnel et la protection physique des informations et des moyens informatiques. Pour atteindre un niveau de sécurité aussi homogène que possible et réduire les coûts, les exigences et les mesures seront standardisées. Le principe de la transparence de l'administration n'est pas remis en cause, raison pour laquelle le projet prévoit expressément la primauté de la loi sur la transparence.

Les contrôles de sécurité relatifs aux personnes seront désormais réglés dans la présente loi, et non plus par la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure. Les dispositions réglant ces contrôles sont adaptés par la même occasion aux besoins actuels de la sécurité de l'information. Le Conseil fédéral entend restreindre les contrôles de sécurité au strict minimum nécessaire à l'identification des risques considérables. Les contrôles devraient ainsi être nettement moins nombreux.

Pour garantir la sécurité de l'information lors de l'adjudication de mandats sensibles à des tiers, y compris pour l'acquisition de moyens informatiques critiques, le Conseil fédéral entend étendre au domaine civil le champ d'application de la procédure de sécurité relative aux entreprises et recourir à ce nouvel instrument de manière ciblée et non bureaucratique. Il entend également créer une base légale à la délivrance de déclarations de sécurité au profit d'entreprises suisses qui soumissionnent pour des mandats étrangers et ont besoin à cet effet d'une déclaration de sécurité nationale.

Pour soutenir les exploitants d'infrastructures critiques en matière de sécurité technique de l'information, les organes fédéraux compétents doivent traiter des ressources d'adressage du domaine des télécommunications. Or, selon les circonstances, les ressources d'adressage peuvent être considérées comme des données sensibles. Le projet crée la base légale de leur traitement et de leur échange.

La loi s'adresse en premier lieu aux autorités de la Confédération. Toutefois, le Conseil fédéral entend également améliorer la collaboration avec les cantons. Ces derniers doivent veiller à assurer une sécurité équivalente de l'information lorsqu'ils traitent des informations classifiées de la Confédération ou recourent à ses moyens informatiques. Pour renforcer la collaboration, les cantons seront représentés au sein de l'organe de coordination de la Confédération et participeront à la standardisation des mesures.

Les coûts de mise en œuvre dépendent largement du niveau de sécurité visé par les autorités fédérales et de la législation d'exécution. Les charges engendrées par le personnel supplémentaire nécessaire pour améliorer la sécurité de l'information seront dans une large mesure compensées par la réduction des charges de personnel liées aux contrôles de sécurité relatifs aux personnes. Globalement, selon les estimations les plus récentes, entre quatre et onze postes supplémentaires pourraient être nécessaires à moyen terme.

Table des matières

Message

1 Présentation du projet

1.1 Contexte

1.1.1 Évolution vers une société de l'information

Depuis quelques décennies, le monde connaît un profond changement sociétal provoqué par le développement rapide et continu de l'informatique. Les nouvelles possibilités d'accéder à des informations en tout temps et en tout lieu, et de pouvoir les échanger, concernent tous les secteurs de la société: la culture, l'économie, la formation et la recherche, la santé, les transports et l'énergie, la défense, etc. Cette évolution est une conséquence inévitable et une condition indispensable de la mondialisation en cours. Toutes les sociétés sont bien plus interconnectées, plus mobiles et, pour la plupart, plus transparentes que jamais. Au regard de l'histoire, notre façon de vivre a radicalement changé en très peu de temps.

Le recours à l'informatique offre à la Suisse de multiples chances dans son évolution vers une société de l'information. Les nouvelles possibilités et mises en réseau présentent toutefois des risques que l'on ne peut ignorer. Les informations peuvent en effet avoir une valeur considérable. La perte, le vol, la divulgation et l'usage abusif d'informations, ou encore la perturbation des moyens de traitement de l'information (moyens informatiques), peuvent mettre gravement en péril des intérêts essentiels de l'État ou des droits de tiers, occasionner des préjudices financiers substantiels, voire entraver l'accomplissement de tâches critiques de la Confédération.

Stratégie «Suisse numérique»

Le Conseil fédéral est conscient de l'importance capitale de l'informatique pour la place économique suisse et les citoyens. Il a ainsi adopté une Stratégie pour une société de l'information en Suisse[1] en 1998 déjà, qui a été mise à jour en 2006[2] puis en 2012[3]. Le 20 avril 2016, le Conseil fédéral a adopté la Stratégie «Suisse numérique»[4] en remplacement de la stratégie de 2012. La nouvelle stratégie vise en priorité à saisir les opportunités de la numérisation afin de positionner la Suisse comme un espace de vie attractif et un pôle économique et scientifique innovant tourné vers l'avenir. Elle fixe à cet effet les lignes directrices régissant l'action de l'État et indique comment les autorités, l'économie, les milieux scientifiques, la société civile et les acteurs politiques doivent collaborer afin que la Suisse puisse tirer pleinement profit de ce processus de transformation.

Prenant la mesure de ce changement sociétal, le Conseil fédéral a lancé de nombreux projets (par ex. dans le domaine de la cyberadministration, de la cyberjustice, de la

1 FF **1998** III 2052
2 FF **2006** 1845
3 FF **2012** 3505
4 FF **2016** 3801

cybersanté, de la gestion électronique des affaires). De plus, il a confié au DFJP plusieurs mandats visant à établir les bases légales requises. Ces projets ont débouché sur un réseau de plus en plus complexe et dynamique d'échanges d'informations des citoyens avec les autorités, d'une part, et des autorités entre elles, d'autre part.

Stratégie suisse de cyberadministration

Le 24 janvier 2007, le Conseil fédéral a adopté la Stratégie suisse de cyberadministration[5]. Cette stratégie nationale a été conçue sous la direction de l'UPIC, en étroite collaboration avec les cantons et les communes. Elle fixe des objectifs communs à la Confédération, aux cantons et aux communes et elle définit des principes, des procédures et des instruments pour la mise en œuvre de la cyberadministration. Elle poursuit trois objectifs stratégiques:

- la population peut régler ses affaires importantes, répétitives ou complexes, avec les autorités par voie électronique;
- l'économie effectue les transactions administratives avec les autorités par voie électronique;
- les autorités ont modernisé leurs processus et communiquent entre elles par voie électronique.

La nouvelle mouture de la Stratégie suisse de cyberadministration a été adoptée à la fin de l'année 2015[6].

Principe de la transparence dans l'administration fédérale

Dans son message relatif à la LTrans, le Conseil fédéral a reconnu que le principe du secret en vigueur dans l'administration ne répondait plus aux exigences d'un réel contrôle démocratique de l'activité de l'administration par les citoyens. La LTrans a été adoptée à la fin de l'année 2004: elle autorise toute personne à consulter des documents officiels sans devoir apporter la preuve d'un intérêt particulier et à obtenir des unités administratives des informations sur le contenu de documents officiels. Le principe de la transparence a une portée qui dépasse le simple cadre juridique. Il signifie que l'État traite ses informations sur mandat et au nom du peuple suisse et que ce dernier est habilité en tout temps à exercer son contrôle. Des exceptions existent, mais elles sont énumérées de manière exhaustive dans la loi. Lorsque l'accès à un document est exceptionnellement restreint, ajourné ou refusé au nom de la protection d'intérêts publics ou privés prépondérants, le document concerné doit être protégé en conséquence.

Stratégie en matière de libre accès aux données publiques (Stratégie OGD Suisse)

L'expression «données publiques en libre accès» (*open government data,* OGD) renvoie à un modèle visant à garantir le libre accès aux données produites par l'administration et à permettre leur réutilisation. La publication et la libre réutilisa-

5 La stratégie peut être consultée à l'adresse suivante: www.egovernment.ch > Mise en œuvre > La cyberadministration suisse 2008–2015.

6 La stratégie peut être consultée à l'adresse suivante: www.egovernment.ch > Mise en œuvre > Stratégie suisse de cyberadministration.

tion de données des autorités peuvent offrir des avantages économiques, politiques et internes à l'administration. L'appréciation des chances et des risques montre ainsi que mettre les données publiques en libre accès recèle un potentiel intéressant pour une conduite transparente et efficace de l'administration et la création d'une plus-value économique. Le Conseil fédéral a donc adopté le 16 avril 2014 une Stratégie en matière de libre accès aux données publiques en Suisse pour les années 2014 à 2018[7], dans laquelle il expose sa vision et ses objectifs stratégiques, de même que les principes autour desquels la stratégie s'articule et les mesures à mettre en œuvre pour atteindre les objectifs. Seules les données qui sont détenues par l'administration fédérale et dont la réutilisation ne contrevient pas au droit de la protection des données, au droit d'auteur ou au droit de la protection des informations peuvent être publiées en vertu du modèle OGD. De plus, les autorités doivent veiller à l'intégrité (l'exactitude) des données rendues accessibles et à ce qu'elles soient compréhensibles; elles doivent donc définir et appliquer les mesures juridiques, organisationnelles et techniques nécessaires.

1.1.2 Risques que recèle la société de l'information

Le Conseil fédéral entend limiter les risques de voir le changement sociétal désavantager la population et l'économie ou mettre en péril les droits individuels. En effet, certains risques ne sont pas directement liés aux conséquences du changement (par ex. la fracture numérique), mais aux informations elles-mêmes et aux réseaux d'information et de communication. Souvent, la valeur réelle des informations n'apparaît malheureusement qu'après un incident aux conséquences négatives. La perte, le vol, la diffusion non autorisée ou l'utilisation abusive d'informations peut avoir des conséquences extrêmement déplaisantes, tant pour les pouvoirs publics que pour les entreprises et les particuliers. Les infrastructures d'information et de communication et les moyens informatiques dont les autorités et les entreprises se servent dans leurs processus sont tout aussi vulnérables. Ainsi, la défaillance d'un système informatique peut avoir des conséquences financières considérables selon les affaires qu'il sert à traiter. Lorsqu'une telle défaillance touche l'exploitant d'une infrastructure critique qui fournit des services indispensables au fonctionnement de la société, de l'économie ou de la Confédération, les effets peuvent être catastrophiques voire entraîner mort d'homme.

Risques pour les informations et les moyens informatiques

Chaque jour ou presque, les médias relatent des cas d'espionnage, d'attaques ou de défaillances touchant des services informatiques ou d'autres événements en rapport avec la sécurité de l'information. Ces dangers sont décrits dans la Stratégie nationale de protection de la Suisse contre les cyberrisques. Pour en prendre une mesure réaliste, il faut tenir compte de trois éléments.

Les menaces doivent être prises au sérieux. Si les spécialistes ont souvent tendance à dramatiser les risques et leurs effets potentiels, on ne saurait non plus les sous-estimer. Ainsi, les organisations criminelles peuvent investir énormément d'argent et

7 FF **2014** 3347

de savoir-faire pour dérober des données en ligne de clients (notamment les données bancaires et les données des cartes de crédit) ou pour faire chanter des particuliers, mais leurs moyens sont insignifiants par rapport aux ressources financières et humaines engagées par certains acteurs étatiques dans l'espionnage politique, diplomatique, scientifique et économique. Certains États accordent même la priorité à des activités ciblées d'espionnage économique et industriel en vue de favoriser l'industrialisation et le développement de leur propre économie ou de moderniser leurs forces armées.

De plus, les menaces qu'il faut prendre au sérieux ne concernent pas seulement la protection de la confidentialité des informations, mais également la disponibilité d'infrastructures et de services publics ou privés, en raison de leur dépendance à l'égard de l'informatique. Des sabotages tels l'attaque découverte en juin 2010 contre des installations iraniennes d'enrichissement d'uranium par le logiciel malveillant Stuxnet figurent parmi les scénarios les plus cités. Cependant, les perturbations ou interruptions de l'activité dues à des défaillances techniques, à de fausses manipulations ou à des événements naturels, par exemple une panne d'électricité ou un incendie, sont nettement plus fréquentes et peuvent avoir des conséquences tout aussi graves.

Enfin, la surveillance à grande échelle du trafic sur Internet, notamment par le détournement de services informatiques très répandus, ne saurait être passée sous silence, pas plus que la corruption systématique des normes de chiffrement. Nous savons aujourd'hui que la présomption d'intégrité d'Internet et des services de base est erronée, notamment en ce qui concerne la sécurité du traitement des informations.

On assiste à une course aux armements informatiques. La plupart des pays développés sont conscients de leur dépendance à l'égard de l'informatique, de même que des dangers qu'ils courent, et ils prennent des mesures de protection. Les États sont cependant loin de tous se contenter de stratégies purement défensives: nombreux sont ceux qui se dotent de capacités offensives de nature militaire ou dans le domaine du renseignement. Des voix s'élèvent également en Suisse pour renforcer de telles capacités offensives. Contrairement à la course classique aux armements, la participation ne se limite pas aux acteurs étatiques ou financés par l'État. Étant donné que les solutions ne sont pas toujours particulièrement complexes et coûteuses et qu'elles ne demandent pas nécessairement des installations d'envergure, nombre d'informaticiens, de mathématiciens et d'autres spécialistes des nouvelles technologies travaillent inlassablement au développement de programmes techniques de protection ou de programmes malveillants. Eu égard aux moyens engagés et à l'hétérogénéité des acteurs, la course aux armements informatiques semble n'en être qu'à ses débuts. Enrayer cette dynamique constituera un défi de taille pour lequel les réponses font encore défaut: la seule certitude est qu'aucun pays ne parviendra à la maîtriser à lui seul.

Une trop grande concentration sur le domaine informatique est dangereuse. L'informatisation du traitement de l'information et la mise en réseau des systèmes, notamment par Internet, ont créé de nouveaux types de menaces. L'attention et l'action se focalisent donc naturellement sur la protection contre ces nouveaux risques. Pour autant, on ne saurait réduire la protection des informations et des moyens informa-

tiques à la seule prévention des cyberattaques: il est en effet des menaces significatives qui n'ont que peu à voir avec Internet ou les logiciels malveillants, ou alors indirectement seulement. Par exemple, l'espionnage applique toujours des méthodes anciennes. Certes, le recours à des techniques électroniques d'espionnage est relativement moins coûteux et moins risqué que le recours à des espions en chair et en os. La composante humaine reste toutefois indispensable à l'acquisition d'informations de qualité. En effet, des informations continuent d'être échangées oralement ou d'être traitées sur support papier. Les risques qui en découlent ne sauraient par conséquent être ignorés du point de vue de la sécurité de l'information.

Stratégie nationale de protection de la Suisse contre les cyberrisques

Le Conseil fédéral entend minimiser, en collaboration avec les autorités, les milieux économiques et les exploitants d'infrastructures critiques, les cyberrisques auxquels ces acteurs sont quotidiennement exposés. La stratégie nationale développée à cet effet considère que les cyberrisques émergent en fonction des processus et responsabilités en place, raison pour laquelle ils doivent être intégrés dans les processus existants de gestion des risques.

Par sa stratégie, le Conseil fédéral poursuit trois buts:

- la détection précoce des menaces et des dangers dans le cyberespace;
- l'augmentation de la capacité de résistance des infrastructures critiques;
- la réduction des cyberrisques.

Il entend consolider à cette fin la collaboration entre les autorités et les milieux économiques dans le domaine informatique et renforcer les bases existantes. La collaboration entre l'UPIC et le SRC au sein de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information, qui couvrait déjà cette tâche sous forme de partenariat public-privé, a été renforcée. De plus, le Conseil fédéral a chargé les départements de mettre en œuvre diverses mesures, dans leur domaine de compétence et en concertation avec les autorités cantonales et les milieux économiques. Ces mesures vont de l'analyse des risques auxquels sont exposées les infrastructures informatiques critiques à une défense plus soutenue des intérêts suisses sur le plan international. Un organe a été créé au DFF pour assurer la coordination de la mise en œuvre de la SNPC. Le Conseil fédéral s'appuie ainsi sur des structures existantes et renonce à un organe national central de pilotage et de coordination semblable à ceux que d'autres États mettent en place.

La stratégie sera mise à jour dans le courant de l'année 2017.

Risques pour les autorités fédérales

Les autorités fédérales sont elles aussi exposées aux risques évoqués dans la SNPC. Elles exploitent en effet des infrastructures d'information et de communication dont les perturbations, la défaillance ou la destruction peuvent mettre en péril l'accomplissement de tâches critiques que leur confie la loi et causer des préjudices considérables à la société, à l'économie ou à l'État.

Dans l'accomplissement de ses tâches, la Confédération traite quotidiennement des volumes importants d'informations, parmi lesquelles se trouvent des informations

particulièrement importantes pour la sécurité intérieure et extérieure, les relations internationales ou les intérêts économiques de la Suisse. Ces informations doivent être protégées et donc classifiées. Les informations classifiées ne sont toutefois pas les seules informations qui nécessitent une protection renforcée. Certes, l'espionnage visait par le passé essentiellement la recherche de renseignements militaires ou d'informations de politique extérieure. De nos jours, cependant, il vise de plus en plus souvent l'économie. Dans un contexte de forte concurrence internationale, quiconque réussit à se procurer le savoir de ses concurrents (résultats de recherche et développement, savoir-faire, etc.) obtient un avantage décisif. Aussi les activités d'espionnage se multiplient-elles depuis quelques années dans les secteurs économique et industriel, notamment dans les domaines de haute technologie. L'administration fédérale constitue un centre névralgique très sensible à cet égard: elle réglemente l'économie privée, vérifie certains produits et en autorise la diffusion, contrôle des entreprises, acquiert elle-même des biens et services de valeur, etc. Pour accomplir sa mission, l'administration fédérale est par ailleurs en dialogue permanent avec des partenaires publics et privés, en Suisse comme à l'étranger. Dans le cadre de ces activités, elle traite de nombreuses informations qui contiennent des secrets d'affaires et de fabrication de tiers. Elle peut donc se trouver dans le viseur de ceux qui veulent se procurer de telles informations. Les tiers qui confient leurs informations aux autorités fédérales en vertu d'une obligation légale ou d'un contrat attendent de ces autorités qu'elles protègent leurs informations avec toute la diligence requise.

La Confédération traite également un volume important de données personnelles qui, en vertu de la législation sur la protection des données, doivent être utilisées de façon licite, conformément au but recherché et dans le respect du principe de la 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: il existe un marché florissant pour l'acquisition et la diffusion de données personnelles.

Ces risques pour la Confédération ne sont pas des hypothèses abstraites ou invraisemblables. Ainsi, au début de l'année 2016, un logiciel d'espionnage a été découvert au sein de l'entreprise d'armement RUAG, qui appartient à la Confédération. Le maliciel était resté longtemps caché dans le réseau de RUAG. Auparavant, le DFAE avait été victime d'attaques similaires. On ne doit pas non plus oublier les menaces que peuvent représenter les collaborateurs de la Confédération: un cas grave de vol de données a été découvert en mai 2012 au SRC: un collaborateur de ce service avait copié sur des supports amovibles de grandes quantités d'informations sensibles auxquelles il avait accès grâce à ses autorisations et les avait transportées hors des locaux de l'administration. Avant son arrestation, il a tenté de vendre les informations dérobées.

Des cas moins graves se produisent fréquemment. Ils concernent le vol ou la perte d'ordinateurs, de téléphones portables ou de supports d'informations classifiées, la divulgation non autorisée, généralement pour des motifs politiques, d'informations confidentielles et les perturbations liées à la défaillance d'un serveur, aux surcharges

du réseau ou à la mauvaise configuration d'un logiciel. Étant donné que la plupart de ces incidents ne sont pas systématiquement consignés ou au moins transmis aux services spécialisés pour examen, il est difficile d'estimer le préjudice global subi par la Confédération. Si des incidents graves ou répétés devaient se produire, la confiance en nos autorités fédérales pourrait s'en trouver fortement ébranlée, au point que des informations pourraient ne pas être transmises à la Confédération aussi longtemps que cette dernière n'apporte pas la preuve qu'elle les protège de manière fiable.

1.1.3 Nécessité d'une nouvelle loi fédérale

Dans quelle mesure une loi au sens formel est-elle nécessaire pour assurer la sécurité de l'information des autorités fédérales? Les trois raisons principales sont présentées ci-après. Le dispositif détaillé est exposé au ch. 1.2.

Informatisation de l'échange d'informations et mise en réseau

Pour accomplir les tâches qui leur incombent en vertu de la Constitution et des lois, les autorités fédérales échangent des informations entre elles et avec des tiers. Cet échange se fait de plus en plus par voie électronique. Simultanément, la mise en réseau des systèmes informatiques des autorités de la Confédération gagne constamment en importance, d'où une multiplication des interfaces entre les systèmes informatiques des autorités fédérales. Dès lors, le risque augmente que les menaces et les attaques contre une autorité se propagent à d'autres autorités participantes. Lorsque des informations sont traitées hors de l'organisation, on ne peut plus se satisfaire de la seule protection dans son domaine de compétence, car les mesures de protection doivent déployer leurs effets au-delà de son propre périmètre. Les mesures de protection doivent par conséquent être liées à l'information. C'est pourquoi il est indispensable que les autorités concernées soient tenues d'harmoniser leurs mesures de sécurité de l'information, tant sur les plans organisationnel, technique et physique que vis-à-vis du personnel, et que les tiers qui traitent des informations de la Confédération respectent les exigences de la Confédération.

Les bases légales régissant la sécurité de l'information sont disséminées, généralement sans précision, dans une multitude d'actes (par ex. LOGA, LParl, LAAM, CP, LMSI, LPers, LMP, LAr, LPD, LTrans) qui ne s'appliquent qu'à certaines autorités. En voici quelques exemples.

- Bien que la classification des informations soit déterminante pour les contrôles de sécurité relatifs aux personnes (cf. art. 19, al. 1, LMSI), les critères de classification sont définis dans un acte (OPrI) qui s'applique à l'administration fédérale et à l'armée, mais non aux autres autorités de la Confédération. Ces dernières sont en principe libres de définir leurs propres échelons de classification. Tant les critères que les mesures de protection sont par conséquent hétérogènes entre les autorités fédérales.
- La réglementation visant à assurer la sécurité des moyens informatiques est presque exclusivement conçue de manière sectorielle, selon le principe de la

protection du périmètre (LOGA pour l'administration fédérale, LParl pour le Parlement, etc.).

- Les contrôles de sécurité relatifs aux personnes ne peuvent en principe être menés qu'auprès des employés de l'administration fédérale, des militaires et des tiers participant à des projets classifiés de la Confédération. Or, dans quelques cas, des employés des cantons doivent être contrôlés. On peut même se demander si les employés des autres autorités fédérales relèvent du champ d'application de la LMSI.
- En raison de son champ d'application, la procédure de sauvegarde du secret ne peut actuellement être utilisée que pour les acquisitions militaires classifiées, et non pour les acquisitions critiques des autorités civiles.

Le champ d'application des instruments de la sécurité de l'information doit s'étendre à toutes les personnes et organisations traitant des informations de la Confédération sur mandat de cette dernière ou ayant accès à ses systèmes et réseaux informatiques. C'est la seule manière de garantir le niveau de sécurité nécessaire et la confiance mutuelle.

Inefficacité de la réglementation actuelle

Outre des lacunes dans leur champ d'application, les bases légales de la sécurité de l'information présentent plusieurs carences et faiblesses matérielles. Ainsi, la plupart des instruments restent sectoriels, manquent de coordination et ne répondent pas aux besoins d'une société de l'information. En voici quelques exemples.

- La protection des données, la protection des informations classifiées, la sécurité informatique, les contrôles de sécurité relatifs aux personnes, les procédures de sauvegarde du secret, la gestion des risques et la sécurité physique sont tous réglés dans des actes distincts. La Confédération a mis en place de ce fait des structures organisationnelles parallèles pour chacun de ces secteurs de la sécurité de l'information. Les efforts de coordination sont considérables et empêchent une vision globale de l'efficacité et de l'économicité de ces structures. La coordination des affaires politiques en lien avec la sécurité de l'information et la collaboration avec les cantons et les partenaires internationaux sont également très difficiles.
- En matière de traitement sécurisé des informations, la législation met généralement l'accent sur la protection de la confidentialité. Bien que les effets d'une non-disponibilité des informations ou des systèmes informatiques puissent être beaucoup plus graves que ceux d'une perte de confidentialité, aucun contrôle de sécurité relatif aux personnes ni aucune procédure de sauvegarde du secret ne peuvent s'appliquer aujourd'hui aux personnes et aux entreprises qui exploitent des moyens informatiques critiques de la Confédération ou qui exploitent de tels moyens pour son compte.
- Certains actes prévoient que les informations (et les données) doivent être protégées en fonction de l'état de la technique (cf. art. 8, al. 2, let. d, LPD et art. 3, let. k, OPrI), mais aucune disposition ne précise qui détermine l'état de la technique.

L'évolution vers une société de l'information accentue la complexité et le caractère dynamique des menaces: ces dernières doivent être abordées globalement, en réseau et avec professionnalisme. La pratique a montré que l'approche sectorielle au sein de la Confédération n'est plus adaptée et n'est plus efficace. Il faut dès lors regrouper les mesures principales de sécurité de l'information dans un seul cadre réglementaire moderne afin de pouvoir les gérer de manière globale, ce qui correspond aux normes internationales qui règlent aussi la sécurité de l'information dans une perspective globale.

Limitation de droits constitutionnels et traitement de données sensibles

En vertu des art. 36, al. 1, 2e phrase, et 164, al. 1, let. b, Cst., toute restriction des droits constitutionnels doit être fondée sur une base légale au sens formel. Son degré de détail dépend de l'importance de la restriction. De plus, en vertu de l'art. 17, al. 2, LPD, les organes de la Confédération ne peuvent traiter des données sensibles ou des profils de la personnalité que si une loi au sens formel le prévoit expressément. Des bases légales au sens formel sont ainsi nécessaires pour les opérations suivantes:

- le recours à des systèmes d'information pour le contrôle central des données d'identification, car des données sensibles sont traitées dans ce cadre;
- le contrôle de sécurité relatif aux personnes, car un tel contrôle constitue une atteinte considérable aux droit fondamentaux des personnes physiques;
- la procédure de sécurité relative aux entreprises, car une telle procédure constitue une atteinte considérable aux droits fondamentaux des personnes physiques et morales;
- le soutien aux exploitants d'infrastructures critiques, car il implique le traitement de données sensibles;
- la classification d'informations, l'attribution d'une catégorie de sécurité aux moyens informatiques et la délimitation de zones de sécurité, car ces mesures conditionnent les contrôles de sécurité relatifs aux personnes et les procédures de sécurité relatives aux entreprises et déterminent à ce titre les atteintes aux droits constitutionnels.

1.1.4 Mandats du Conseil fédéral

Compte tenu de ces évolutions et des nouveaux risques, le Conseil fédéral a confié nombre de mandats liés à la sécurité de l'information au sein de la Confédération. Seuls ceux qui sont en lien direct avec le projet de loi ou qui ont sensiblement pesé sur sa préparation sont commentés ci-après. Les recommandations des organes parlementaires de surveillance dont le projet a également tenu compte complètent cette liste.

Adoption de l'ordonnance concernant la protection des informations et mandat d'étude

Au milieu de l'année 2007, le Conseil fédéral a adopté la nouvelle OPrI. Cette dernière a remplacé les deux ordonnances en vigueur dans les domaines civil et militaire et a supprimé la distinction obsolète entre informations civiles et militaires.

Les prescriptions qu'elle contient sur la classification et le traitement des informations ont permis d'instaurer pour la première fois un niveau de protection uniforme dans l'ensemble de l'administration fédérale. L'OPrI a été conçue comme un acte transitoire et sa durée de validité est donc limitée. En l'adoptant, le Conseil fédéral a chargé le DDPS de lui remettre avant la fin de 2009 un rapport sur l'exécution, l'efficacité et l'économicité de la mise en œuvre de l'ordonnance et de lui présenter des propositions visant la création de bases légales au sens formel.

Décision du Conseil fédéral relative à des mesures visant à améliorer la sécurité de l'information dans l'administration fédérale

Dans le sillage de l'attaque contre les systèmes informatiques du DFAE, le Conseil fédéral a pris les 16 décembre 2009 et 4 juin 2010 des mesures visant à améliorer la sécurité de l'information dans l'administration fédérale. Il a défini à cet effet une série de mesures organisationnelles et techniques censées améliorer à court et moyen termes la protection des informations lors de leur traitement par des moyens informatiques de l'administration fédérale. Par ailleurs, il a proposé au Contrôle fédéral des finances d'examiner l'avancement de la mise en œuvre de ces mesures. Le premier rapport d'audit du Contrôle fédéral des finances a été remis au Conseil fédéral le 2 décembre 2011[8]. Malgré sa portée limitée, ce rapport fournit une bonne vue d'ensemble des mesures à prendre.

Mandat du Conseil fédéral visant la création de bases légales au sens formel pour la protection et la sécurité de l'information

Le rapport demandé par le Conseil fédéral parallèlement à l'adoption de l'OPrI devait rendre compte de l'efficacité de l'ordonnance en question. Il a montré que le délai transitoire (fin 2009) prévu par l'ordonnance pour les adaptations permettant de garantir la protection technique des informations n'avait généralement pas été respecté. Des lacunes importantes ont été constatées, notamment en matière de protection électronique des informations classifiées.

Le 12 mai 2010, après avoir pris acte du rapport du DDPS et tiré les conséquences de l'attaque contre le DFAE évoquée ci-avant, le Conseil fédéral a chargé le DDPS d'élaborer des bases légales au sens formel pour la protection des informations. La nouvelle réglementation devait notamment remplir les objectifs suivants:

- élargir le champ d'application des prescriptions de sécurité à toutes les personnes chargées par la Confédération de traiter des informations protégées;
- créer des bases légales uniformes pour des procédures de protection du secret dans les domaines civil et militaire;
- établir une compétence uniforme pour le Conseil fédéral de conclure des traités internationaux en matière de protection des informations.

Le Conseil fédéral a également chargé le DDPS d'examiner dans quelle mesure d'autres problèmes matériels dans le domaine de la protection des informations

8 www.cdf.admin.ch > Publications > Audits transversaux > Audit transversal sur la sécurité TI dans l'administration fédérale

requerraient des bases légales au sens formel et si les compétences et responsabilités en matière de sécurité de l'information satisfaisaient aux exigences actuelles.

Élargissement du mandat du Conseil fédéral du 12 mai 2010

Le 14 janvier 2011, le chef du DDPS a institué un groupe d'experts dirigé par M. Markus Müller, docteur en droit, professeur ordinaire de droit public et de droit administratif à l'Université de Berne. Le chef du DDPS l'a chargé d'élaborer une esquisse d'acte normatif et de rédiger sur cette base un projet de loi. Le groupe d'experts a soumis son esquisse d'acte normatif au chef du DDPS le 29 juin 2011. Une fois informé des résultats du groupe de travail, le Conseil fédéral a étendu par décision du 30 novembre 2011 la portée de la réglementation envisagée d'une simple protection des informations classifiées à une sécurité exhaustive de l'information. Il a constaté par ailleurs qu'en raison de la multiplication des échanges électroniques d'informations avec les autres autorités et de l'interconnexion croissante des systèmes informatiques, une sécurité efficace de l'information ne pouvait être garantie que si des normes minimales de sécurité uniformes étaient imposées à l'ensemble des autorités fédérales. Il a donc décidé que le projet devait s'appliquer à l'ensemble des autorités et organisations de la Confédération, les modalités d'exécution restant de la compétence des diverses autorités fédérales. Enfin, il a chargé le DDPS de coordonner les travaux législatifs avec les mandats concernant l'élaboration de la SNPC et la Stratégie pour une société de l'information en Suisse.

L'extension du champ d'application et de la portée de la réglementation, de même que la coordination avec les projets susmentionnés, ont conduit à un élargissement du groupe d'experts, qui a réuni depuis lors des représentants de la ChF, du DFAE, du DFJP (SG, OFJ, fedpol), du DDPS (SG, État-major de l'armée), du DFF (SG, UPIC, OFIT), du DETEC (OFCOM), du PFPDT, des Services du Parlement, des tribunaux fédéraux et des cantons (Conférence suisse sur l'informatique). La Centrale d'enregistrement et d'analyse pour la sûreté de l'information et le SRC y participent ponctuellement.

Mandat complémentaire et élargissement à un groupe de travail interdépartemental

Après la découverte d'un incident au SRC, le Conseil fédéral a confié le 24 octobre 2012 un mandat complémentaire au groupe d'experts, à savoir l'élaboration d'un rapport sur les risques et les lacunes en matière de sécurité de l'information au sein de l'administration fédérale et de propositions sur les mesures urgentes à prendre. Le groupe d'experts a été élargi à cet effet à des représentants du DFI et du DEFR, devenant un groupe de travail interdépartemental (GTI LSI). Celui-ci a remis son rapport et ses recommandations au DDPS le 29 janvier 2013. Le Conseil fédéral a décidé le 15 mars 2013 de former l'ensemble des cadres dirigeants de l'administration fédérale à la problématique de la sécurité de l'information et confié la responsabilité de cette formation à l'OFPER.

Mandat du Conseil fédéral visant l'harmonisation et la restriction des CSP

Le 1er février 2012, le Conseil fédéral a chargé le DDPS d'examiner les moyens d'harmoniser et de restreindre les fonctions soumises à des CSP et les degrés de

contrôle afférents et d'identifier d'autres mesures d'optimisation des ressources. Après avoir pris acte du rapport établi par le groupe de travail interdépartemental institué pour l'occasion, le Conseil fédéral a notamment chargé le GTI LSI le 29 novembre 2013 de tenir compte dans ses travaux des recommandations du rapport et de les intégrer de façon appropriée au projet de loi (cf. ch. 1.2.5).

Adoption de l'ordonnance concernant la procédure de sécurité relative aux entreprises dans le cadre des programmes européens de navigation par satellite Galileo et EGNOS

Par décision du 13 décembre 2013, le Conseil fédéral a approuvé l'accord de coopération avec l'UE relatif aux programmes européens de navigation par satellite[9]. Cet accord permet aux entreprises suisses de soumissionner à armes égales pour les mandats en lien avec les deux programmes. En le concluant, la Suisse s'est engagée à protéger les deux programmes, plus particulièrement contre les utilisations abusives, les perturbations de fréquences et les activités hostiles: elle doit garantir à cet égard un niveau de sécurité comparable à celui de l'UE. Les entreprises et instituts de recherche suisses intéressés par des acquisitions ou des mandats de recherche sensibles ont dès lors besoin d'une déclaration de sécurité relative aux entreprises (DSE) nationale. Étant donné que les procédures qui permettent de les délivrer ne sont admissibles à l'heure actuelle que dans le domaine militaire, sur la base de l'ordonnance dépassée du DMF du 29 août 1990 concernant la sauvegarde du secret[10], le Conseil fédéral a approuvé le 6 juin 2014 une ordonnance[11] fondée directement sur la Constitution à titre de solution transitoire jusqu'à l'entrée en vigueur de la LSI. L'ordonnance permet aux services compétents du DDPS de délivrer des DSE pour des acquisitions dans le cadre de Galileo et d'EGNOS.

Mandat visant la création d'une base légale pour la gestion des données d'identification et des accès de la Confédération (GIA Confédération)

Les autorités et organisations de la Confédération exploitent de nombreux systèmes informatiques dans l'accomplissement de leurs tâches. Pour chaque système, il faut s'assurer que les bonnes personnes ou les bonnes applications obtiennent les droits d'accès adéquats au moment opportun, ce qui exige une gestion adéquate des données d'identification et des accès. La consultation de plus en plus fréquente d'informations hors des organisations concernées implique une coordination transversale des systèmes pour répondre aux exigences en matière de protection et de fonctionnalité. Le programme GIA Confédération doit permettre d'authentifier les utilisateurs et de contrôler certains attributs et autorisations non plus séparément pour chaque application spécialisée, mais de façon groupée. Certains aspects du traitement centralisé de données personnelles nécessitent une base légale au sens formel en vertu de la législation sur la protection des données. Une gestion efficace des données d'identification et des accès étant une condition essentielle de la sécurité de l'information, le Conseil fédéral a chargé le DDPS le 14 janvier 2015 de com-

9 RS **0.741.826.8**
10 RS **510.413**
11 RS **510.661**

pléter le projet de LSI, en collaboration avec le DFF, en y ajoutant une base légale pour les systèmes de gestion des données d'identification.

Recommandations des organes parlementaires de surveillance

Les CdG et la DélCdG traitent régulièrement de thèmes en rapport avec la sécurité de l'information. Récemment, elles ont recommandé diverses améliorations dont le Conseil fédéral a tenu compte dans la préparation du présent projet.

- *Rapport de la CdG-E du 3 décembre 2010 sur la gestion par les autorités fédérales de la crise diplomatique entre la Suisse et la Libye*[12]*, recommandation 12:* dans le cadre de son examen de la gestion par les autorités fédérales de la crise diplomatique entre la Suisse et la Libye, la CdG-E a constaté une série de lacunes en matière de protection des informations. Dans son rapport, elle affirme que *«de tels incidents sont la preuve qu'en ce qui concerne la protection des informations et des moyens techniques mis à disposition des collaborateurs, de graves lacunes existent aujourd'hui au niveau de l'administration fédérale, lacunes auxquelles il est impératif de remédier rapidement»*. Elle recommande au Conseil fédéral de *«prendre les mesures nécessaires, dans son domaine de compétences, pour pouvoir garantir à l'avenir le secret aussi aux plus hauts niveaux de l'administration fédérale. Ce faisant, le Conseil fédéral s'attache également aux aspects techniques des appareils mis à disposition des collaborateurs»*.
- *Rapport de la CdG-N du 12 avril 2013 sur le contrôle de suivi de l'inspection relative aux circonstances de la nomination de Roland Nef au poste de chef de l'armée*[13]
  - *Recommandation 1:* la CdG-N demande au Conseil fédéral d'examiner attentivement, dans le cadre de l'élaboration de la LSI, l'opportunité de définir dans la loi au sens formel d'une part ce qui constitue un risque pour la sécurité au sens des CSP, et d'autre part quel est l'objectif final de ce type de contrôles.
  - *Recommandation 5:* la CdG-N demande au Conseil fédéral de veiller à ce que la situation des personnes sans nationalité suisse soit éclaircie rapidement, et à ce que les deux services spécialisés CSP suivent une pratique uniforme en la matière, basée sur des bases légales claires.
- *Rapport de la DélCdG du 30 août 2013 sur la sécurité informatique au sein du SRC (résumé):* le 15 octobre 2012, la DélCdG a décidé de mener une inspection formelle de la sécurité informatique au sein du SRC. Au début du mois de juillet 2013, elle a établi un rapport exhaustif à l'intention du Conseil fédéral et publié un résumé assorti de onze recommandations. Trois d'entre elles sont particulièrement importantes pour le projet de LSI.
  - *Recommandation 5:* la DélCdG recommande au Conseil fédéral de réviser l'OCSP de sorte que les collaborateurs externes soient soumis au même degré de contrôle de sécurité que les employés de la Confédération qui exercent la même activité qu'eux. Le service de la Confédéra-

12 FF **2011** 3901
13 FF **2013** 5619

tion qui est le destinataire final des prestations fournies par les entreprises externes doit être responsable du respect, par ces entreprises et par leurs collaborateurs, des prescriptions applicables. À l'occasion du contrôle de suivi de l'inspection, la DélCdG a demandé au Conseil fédéral, par lettre du 30 juin 2014, de veiller à ce que la LSI règle le CSP de manière aussi complète et précise pour les collaborateurs externes que pour le personnel interne de la Confédération (cf. rapport annuel 2014 de la CdG/DélCdG du 30 janvier 2015[14], ch. 4.3.4).

- *Recommandation 6:* la DélCdG recommande au Conseil fédéral de présenter dans son message une explication détaillée des rôles des CSP et de la conduite du personnel dans la sécurité de l'information et de les différencier clairement. Parallèlement, elle demande un rapport séparé comportant une estimation des effectifs que la Confédération doit affecter à la réalisation des CSP, d'une part, et une description de la contribution que la Confédération entend ainsi apporter à la protection des informations, d'autre part.
- *Recommandation 9:* la DélCdG recommande au Conseil fédéral d'élaborer des propositions visant à améliorer le processus de contrôle de la sécurité informatique au sein de la Confédération. Ces mesures devront permettre au Conseil fédéral d'identifier les risques liés à la sécurité informatique suffisamment tôt, d'adopter les mesures requises pour réduire ces risques et de suivre leur mise en œuvre dans le cadre d'un processus institutionnalisé.

- *Rapport de la CdG-E du 7 octobre 2014 sur les collaborateurs externes de la Confédération*[15]*:* dans ce rapport, la CdG-E commente les résultats d'une évaluation menée par le Contrôle parlementaire de l'administration à propos de l'ampleur, de la légalité, de la transparence et de l'opportunité du recours à des collaborateurs externes à l'administration fédérale. Elle a émis six recommandations à l'intention du Conseil fédéral. Par sa recommandation 6, la CdG-E invite le Conseil fédéral à prêter une attention particulière aux CSP des collaborateurs externes travaillant dans le domaine informatique, en raison de leur accès à des informations ou à du matériel classifiés «confidentiel» ou «secret». Elle l'invite également à prévoir une modification des bases légales régissant le CSP, afin de prescrire que le résultat dudit contrôle soit connu avant l'entrée en service du collaborateur.

1.2 Dispositif proposé

Par le dispositif qu'il propose, le Conseil fédéral entend créer un cadre juridique uniforme pour la gestion et la mise en œuvre de la sécurité de l'information par toutes les autorités de la Confédération. Tous les principes et toutes les mesures de sécurité de l'information doivent être regroupés en un acte unique de sorte que la mise en œuvre puisse être globale et le niveau de sécurité aussi homogène que

14 FF **2015** 4763
15 FF **2015** 3311

possible. Le projet permet parallèlement de combler certaines lacunes du droit en vigueur: les autorités fédérales disposeront ainsi de bases légales modernes répondant aux besoins de la société de l'information. De plus, une base légale au sens formel donnera à la Confédération les compétences centrales dont elle a besoin pour la mise en œuvre de la Stratégie nationale de protection de la Suisse contre les cyberrisques. Enfin, l'organisation de la sécurité de l'information sera plus professionnelle et plus efficace.

Le dispositif détaillé et les solutions proposées au sujet des points essentiels de la nouvelle législation sont commentés ci-après.

1.2.1 Sécurité de l'information

La plupart des informations sont aujourd'hui traitées sous forme électronique. Leur protection dépend dès lors de plus en plus des procédures et moyens informatiques utilisés dans leur traitement. La protection électronique des informations présente aujourd'hui d'importantes lacunes en matière de sécurité. Dans ce contexte, il faut relever que les tâches des services chargés d'élaborer les prescriptions de sécurité informatique et de les mettre en œuvre sont devenues bien plus complexes en peu de temps, du fait des innovations technologiques permanentes, des nouvelles menaces et faiblesses qui y sont liées ainsi que du manque de personnel et de ressources financières. Au vu de l'ampleur des défis techniques, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information préconisait déjà une réorientation dans son rapport semestriel en été 2008:

> «Les mesures techniques de sécurité et le bon sens ne suffisent plus pour déjouer les cyberattaques ciblées d'aujourd'hui. D'où la nécessité d'une redéfinition des priorités axée sur la protection de l'information et non plus seulement sur la protection des ordinateurs et des réseaux. [...] la gestion de l'information et des données, la classification de l'information, etc., joueront un rôle accru»[16].

Ce point est capital pour la compréhension du dispositif proposé. La seule sécurité technique de l'informatique ne suffit plus: une protection plus efficace des informations requiert des mesures organisationnelles. Au sein de la Confédération, les lacunes dans ce domaine concernent en particulier les bases légales et la gestion de la sécurité de l'information.

Le cadre juridique présente les principales lacunes. Les bases légales de la protection des informations sont en effet très sectorielles, peu harmonisées et souvent incomplètes. La Confédération exploite ainsi, aux niveaux tant juridique qu'organisationnel, des systèmes parallèles de protection des données, de protection des informations classifiées, de sécurité informatique, de sécurité physique et de gestion des risques. Par ailleurs, les CSP et les PSE s'appliquent uniquement aux personnes et entreprises qui traitent des informations classifiées de la Confédération, mais non aux personnes qui gèrent ou exploitent des moyens informatiques critiques. De plus,

16 Le rapport peut être consulté à l'adresse suivante: www.melani.admin.ch > Documentation > Rapports sur la situation.

les bases légales ne sont pas toujours adaptées aux besoins concrets du traitement électronique des informations.

Dans le secteur privé, on prend conscience au plus tard après qu'un dommage a eu lieu et qu'on s'est efforcé de limiter les dégâts du fait que la sécurité est de la responsabilité de la hiérarchie et qu'une gestion efficace de la sécurité de l'information est économiquement rentable. Dans les administrations publiques en revanche, la sécurité est souvent considérée comme une simple génératrice de coûts et comme un obstacle, notamment parce que les pouvoirs publics ne peuvent pas subir un dommage concurrentiel en cas d'incident. Par conséquent, la perte de productivité, due par exemple à une panne de services informatiques, n'est généralement pas évaluée, pas plus qu'elle n'est comparée aux coûts qu'entraîneraient des mesures de limitation du risque.

Cette situation prévaut à la Confédération. Par exemple, la sécurité informatique est souvent considérée comme une affaire purement technique, et non comme une tâche de direction. Ainsi, les supérieurs hiérarchiques ne prêtent généralement qu'une attention minime à leur propre rôle dans le processus de sécurité et les tâches habituelles de direction (par ex. la définition d'objectifs, le contrôle de la mise en œuvre ou l'évaluation de l'efficacité des mesures) incluent rarement le domaine de la sécurité. Les coûts de la sécurité ne peuvent pas non plus être exposés de manière transparente, ce qui empêche toute appréciation de l'économicité des mesures (analyse coût-utilité). Enfin, en cas d'incident ou de violation des prescriptions, les responsables ne sont que rarement amenés à rendre des comptes.

Si les informations peuvent nécessiter une protection pour diverses raisons, les mesures organisationnelles et techniques permettant de répondre aux besoins de protection ne se distinguent guère les unes des autres. Lorsque leur mise en œuvre est réglée et organisée de manière uniforme, on peut bénéficier d'effets de synergie tout en améliorant la protection. À cet effet, les bases légales doivent impérativement s'aligner sur les besoins de la société de l'information et les supérieurs hiérarchiques doivent mieux assumer leurs tâches.

Le Conseil fédéral est conscient de l'interdépendance croissante de la protection technique et organisationnelle des informations, de même que des lacunes organisationnelles évoquées plus haut. Il a aiguillé en conséquence les travaux législatifs concernant la LSI. Le but est une *sécurité intégrale de l'information*, tenant compte des exigences tant organisationnelles que techniques. De plus, la nouvelle réglementation doit, sur le plan de l'organisation, s'inspirer de *normes internationales reconnues*. Cette sécurité intégrale de l'information correspond à ce qui a déjà cours selon les règles de l'art dans le secteur privé et dans de nombreuses administrations publiques dans le monde entier. Elle est formalisée par quelques normes internationales, notamment les normes ISO/IEC 27001 et 27002[17]. Celles-ci n'ont que peu à voir avec la sécurité technique: l'accent est mis presque exclusivement sur les tâches de *gestion* de la protection des informations et sur les mesures organisationnelles qui s'imposent à cette fin. Toutefois, les normes contiennent également de *bonnes pratiques* de sécurité applicables et éprouvées en matière de technique, de personnel

17 Les normes peuvent être consultées sur le site de l'Organisation internationale de normalisation à l'adresse suivante: www.iso.org/iso/fr > Store > Normes ISO.

et de constructions. Elles sont régulièrement adaptées pour tenir compte des nouvelles connaissances, notamment empiriques, acquises dans le cadre d'études ou à la faveur d'incidents. Elles correspondent donc aux connaissances scientifiques et techniques les plus récentes.

La LSI crée des bases légales uniformes pour la gestion de la sécurité de l'information au sein de la Confédération. Sa structure et son contenu se fondent pour l'essentiel sur les normes évoquées, si bien que le projet opère une transposition sur mesure dans le droit national. Ainsi, la *sécurité de l'information est considérée dans son intégralité*, c'est-à-dire que tous ses aspects sont autant que possible pilotés, mis en œuvre, analysés et améliorés en un bloc. Le projet regroupe à cet effet en une seule réglementation les mesures organisationnelles les plus importantes afin de protéger toutes les informations d'assurer la sécurité des moyens informatiques.

1.2.2 Champ d'application et collaboration avec les cantons

Champ d'application matériel

Le champ d'application matériel découle de la notion de sécurité de l'information. Au cœur du dispositif de protection se trouvent toutes les informations relevant de la compétence des autorités fédérales, à savoir principalement les informations que les autorités produisent elles-mêmes, mais également celles qu'elles obtiennent de tiers et dont le traitement sûr et licite relève de leur compétence. Les informations que les autorités fédérales confient pour traitement à des tiers entrent également dans le champ d'application de la loi. La LSI s'applique aux informations de toute nature (par ex. non seulement les informations textuelles, mais également les représentations graphiques), quelle que soit leur forme, c'est-à-dire tant les informations électroniques que les documents papier.

Le projet couvre tous les moyens informatiques engagés par les autorités fédérales ou dont elles confient l'exploitation à des tiers. Certes, les moyens techniques de traitement des informations ne doivent pas être protégés pour eux-mêmes: c'est bien plus à eux d'assurer la sécurité des informations qu'ils traitent ou des processus auxquels ils servent. Toutefois, puisque la pratique considère les moyens informatiques comme des *objets à protéger*, la LSI les mentionne expressément.

Champ d'application institutionnel

Par maints aspects, le présent acte est une loi d'organisation. Elle doit cependant être appliquée par toutes les autorités fédérales et organisations qui leur sont subordonnées dans leur domaine de compétence respectif: c'est en effet la seule façon d'assurer une sécurité efficace de l'information. Les unités de l'administration fédérale décentralisée et les organisations de droit public ou de droit privé chargées de tâches administratives doivent également y être soumises en tout ou partie dans la mesure où elles exercent une activité sensible de la Confédération ou lorsqu'elles doivent recourir ou accéder à des moyens informatiques de la Confédération. Cette solution correspond à la volonté du Conseil fédéral d'étendre en fonction du risque le champ d'application de la réglementation sur la protection des informations à

toutes les personnes que la Confédération charge de traiter des informations protégées.

Nombreuses sont les raisons pour lesquelles la présente loi doit s'appliquer à toutes les autorités fédérales, y compris aux autorités législatives et judiciaires. Tout d'abord, dans l'accomplissement de leurs tâches constitutionnelles et légales, les autorités fédérales échangent régulièrement des informations. L'un des objectifs du Conseil fédéral est de favoriser et de renforcer l'échange électronique d'informations et les services électroniques (cyberadministration). Parmi ces informations, on trouve également des informations classifiées ou d'autres informations nécessitant une protection renforcée. Bien que la classification soit déterminante pour les CSP, les autorités fédérales ne se sont pas dotées d'un système de classification unique. Les mesures de sécurité prises par les diverses autorités sont donc très hétérogènes et guère harmonisées. Toutes les autorités fédérales doivent appliquer les mêmes principes de classification et prendre des mesures de protection équivalentes: ce n'est que de cette façon que l'on instaurera la confiance mutuelle dans le traitement de ces informations.

Il ne faut pas oublier que la mise en réseau des systèmes informatiques des autorités fédérales se poursuit sans discontinuer. Inexorablement, il y aura de plus en plus d'interfaces entre les systèmes des diverses autorités de la Confédération: le risque augmente ainsi de voir des attaques et des menaces contre une autorité se répercuter dans les domaines de compétence d'autres autorités. Il est donc indispensable que toutes les autorités fédérales soumises à la présente loi appliquent les mêmes critères et méthodes d'évaluation des risques et qu'elles harmonisent leurs mesures de sécurité relatives aux moyens informatiques, tant sur les plans organisationnel, technique et physique que dans le domaine du personnel.

Enfin, en vertu de l'art. 3, al. 1, LRCF, la Confédération répond du dommage causé sans droit à un tiers par un membre du personnel d'une autorité ou d'une organisation soumise à la loi dans l'exercice de ses fonctions. Le champ d'application de la LSI correspond par conséquent à celui de la LRCF. Seuls le Parlement et l'armée viennent s'y ajouter.

Collaboration avec les cantons

Pour pouvoir accomplir leurs tâches, la Confédération et les cantons doivent travailler en étroite collaboration. Aussi échangent-ils de nombreuses informations, de plus en plus sous forme électronique. Les infrastructures et systèmes informatiques de la Confédération et des cantons sont par ailleurs de plus en plus interconnectés, ce qui renforce le risque de voir des menaces dans le domaine de compétence d'une autorité se répercuter sur les domaines de compétence d'autres autorités.

Les cantons répondent eux-mêmes de leur sécurité de l'information. Pour des raisons constitutionnelles, le Conseil fédéral ne veut ni ne peut imposer aux cantons des prescriptions générales. Toutefois, la Confédération a un intérêt direct à ce que les cantons et leurs services garantissent une protection équivalente lorsqu'ils traitent des informations protégées de la Confédération ou recourent à ses moyens informatiques. Par analogie avec la législation sur la protection des données (cf. art. 37, al. 1, LPD), les prescriptions de la Confédération ne s'appliquent toutefois que si les prescriptions et mesures cantonales ne répondent pas aux exigences de

la Confédération en matière de sécurité (subsidiarité). Les cantons devront de surcroît examiner périodiquement l'efficacité de leurs mesures de protection et informer les services fédéraux compétents des résultats de leurs contrôles (cf. également art. 37, al. 2, LPD).

Enfin, le Conseil fédéral veut associer les cantons à la mise en œuvre pour atteindre un niveau de sécurité aussi homogène que possible. Deux représentants des cantons siégeront par conséquent au sein de l'organe transversal de coordination. Ils coordonneront ainsi l'exécution de la LSI avec les services fédéraux compétents et participeront à la standardisation.

1.2.3 Relation avec la loi sur la transparence et la législation sur la protection des données

Relation avec la loi sur la transparence

L'un des buts du projet est de protéger adéquatement les informations qui doivent rester confidentielles, pour des raisons légales et contractuelles. Il fixe à cet effet les critères régissant la classification des informations pour protéger la Suisse et la Confédération. Cette classification entre cependant en conflit avec la LTrans, qui autorise tout un chacun à consulter des documents officiels sans avoir à prouver un intérêt particulier et à obtenir des unités administratives des informations sur le contenu de documents officiels. La LSI fournit une solution à ce problème en établissant la primauté de la LTrans. Elle précise ainsi clairement que le champ d'application de la LTrans n'est d'aucune manière limité par la réglementation sur la sécurité de l'information. L'art. 4 LTrans, en vertu duquel les dispositions spéciales d'autres lois qui déclarent certaines informations secrètes sont réservées, ne peut donc pas s'appliquer aux dispositions de la LSI relatives à la classification. Pour toutes les autorités soumises à la LTrans, les dispositions que contient cette loi sur l'accès à des documents officiels s'appliquent également aux informations classifiées en vertu de la LSI. L'appréciation des documents dans le cadre de la procédure prévue par la LTrans intervient donc indépendamment de la LSI. Dès lors, face à une demande de consultation de documents officiels, le service compétent examine indépendamment de toute classification si l'accès doit être autorisé, limité, ajourné ou refusé. Une mention de classification peut cependant fournir un indice sur la non-publicité d'un document au sens de la LTrans. En effet, la décision de classification suppose une appréciation du besoin de protéger des informations qui risquent de compromettre des intérêts public au sens de la LSI: sur le plan matériel, cette décision doit correspondre à une décision de limiter, différer ou refuser l'accès en vertu de l'art. 7, al. 1, LTrans.

Les intérêts dignes de protection au sens de la LSI ne recouvrent toutefois pas totalement le catalogue d'exceptions de l'art. 7 LTrans: la LSI met en effet l'accent non seulement sur le maintien de la confidentialité, mais aussi sur la disponibilité, l'intégrité et la traçabilité de l'information. Les dispositions relatives à la classification sont cependant conçues pour ne pas contredire le catalogue des exceptions. On retiendra par ailleurs que le champ d'application personnel de la LSI est plus large

que celui de la LTrans parce que la LSI doit s'appliquer à toutes les autorités fédérales.

Relation avec la législation sur la protection des données

La législation sur la protection des données règle, tant pour les particuliers que pour les organes de la Confédération, la protection de la personnalité et des droits fondamentaux des personnes dont les données sont traitées (art. 1 LPD). Elle dispose notamment que des données personnelles ne peuvent être traitées que de façon licite et dans le respect du principe de la proportionnalité et du but indiqué, et que la collecte des données et les finalités de leur traitement doivent être reconnaissables pour la personne concernée (art. 4 LPD). Il va de soi que dans le champ d'activités des autorités fédérales, les données personnelles doivent être traitées conformément à la législation sur la protection des données, qui revêt ainsi le statut de législation spéciale dans son rapport à la LSI. Cependant, la législation sur la protection des données fixe également des exigences pour la protection concrète de la confidentialité, de la disponibilité et de l'intégrité des données. Ainsi, l'art. 7 LPD dispose que les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées. Le Conseil fédéral a défini en particulier aux art. 8 à 11 OLPD des exigences en matière de protection des données personnelles, notamment que les mesures techniques et organisationnelles doivent tenir compte du développement technique. On n'y précise toutefois pas ce qu'il faut entendre par développement technique et qui en décide.

Les prescriptions de la LSI relatives au traitement des données personnelles s'appliquent à titre complémentaire. En effet, au sens de la LSI, les données personnelles sont des informations dont les autorités fédérales doivent protéger la confidentialité, la disponibilité, l'intégrité et la traçabilité. Généralement, les données personnelles ne sont pas formellement classifiées. La classification est réservée à des intérêts publics de la Confédération strictement définis. Toutefois, les dispositions d'exécution attribueront un *niveau de protection* aux informations et données pour assurer leur confidentialité, leur disponibilité, leur intégrité et leur traçabilité. La standardisation des mesures en fonction des connaissances scientifiques et techniques les plus récentes, liée aux niveaux de protection, contribuera également à répondre aux exigences de la législation sur la protection des données pour la sécurité de ces dernières et à renforcer la protection des données au sein de la Confédération.

1.2.4 Mesures générales

Principes de la sécurité de l'information

La sécurité de l'information incombe aux dirigeants: la direction de l'autorité concernée en porte la responsabilité. Le projet précise par conséquent certaines obligations spécifiques, par exemple l'obligation faite aux plus hautes autorités d'organiser, de gérer, de mettre en œuvre et de contrôler la sécurité de l'information conformément aux connaissances scientifiques et techniques les plus récentes. Les dispositions concernées portent sur le niveau de sécurité requis et les compétences

en matière de gestion des risques. Par ailleurs, le projet renforce le rôle opérationnel des plus hautes instances dirigeantes dans divers domaines tels que la sécurité des moyens informatiques ou les CSP.

Il n'est plus possible aujourd'hui de protéger les informations et les systèmes d'information contre tous les dangers et toutes les menaces. La priorité doit être donnée aux aspects les plus importants et les plus critiques. Cette situation exige que les autorités fédérales mettent davantage l'accent sur l'évaluation systématique des besoins de protection des informations et sur l'appréciation continue des risques en la matière. Une gestion efficace des risques dans le domaine de la sécurité de l'information s'impose par conséquent, de même qu'un examen régulier de la mise en œuvre, de l'efficacité et de l'économicité des mesures de réduction des risques. Or, ces deux éléments font aujourd'hui largement défaut. Les audits sont l'un des principaux points faibles en matière de sécurité de l'information au sein de la Confédération: les contrôles n'interviennent que ponctuellement ou après un incident. Pourtant, seuls des audits adéquats permettent aux autorités et organisations de connaître le niveau de sécurité de leurs informations et de savoir quels risques elles encourent et quelles mesures correctives s'imposent le cas échéant. En l'absence presque totale d'audits, le savoir-faire et les ressources nécessaires font largement défaut. On doit dès lors s'attendre à ce que les autorités soumises à la LSI ne puissent éviter d'affecter des ressources supplémentaires à cette tâche (cf. également ch. 1.1.4: rapport de la DélCdG sur la sécurité informatique au sein du SRC, recommandation 9).

Classification des informations

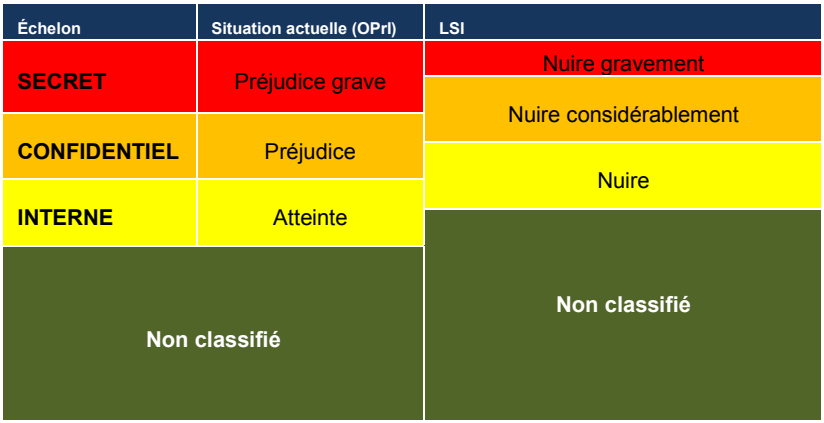
La classification est une mesure appliquée de longue date pour protéger les informations propres à une organisation qui peuvent nuire aux buts de l'organisation ou lui causer un préjudice si elles sont portées à la connaissance de personnes non autorisées. Bien qu'elle soit déterminante pour les CSP, chaque autorité concernée est en principe libre de définir, au besoin, son propre système de classification, ses propres motifs de classification et ses propres prescriptions de traitement. Certains incidents survenus au cours des dernières années ont montré qu'une différence dans le traitement des informations classifiées peut accroître la méfiance. L'un des buts du présent projet est donc de mettre sur pied un système de classification qui s'applique à toutes les autorités et qui puisse être mis en œuvre en suivant des principes aussi uniformes que possible. Le système à trois échelons proposé permet de protéger les informations en fonction des risques. Il permet également d'atteindre un niveau de sécurité homogène sur le plan international. Une réserve concernant le droit de procédure garantit que la classification ne constituera pas un obstacle pour l'Assemblée fédérale, les tribunaux et les ministères publics.

En élaborant le système de classification, on a tenu compte des attentes croissantes de la population quant à la transparence de l'action des autorités fédérales. La classification doit dès lors être conçue comme une exception fondée au principe de la transparence, étant entendu que la LTrans restera applicable sans restriction aux informations classifiées pour l'ensemble des autorités et organisations concernées. Les valeurs seuils de la classification sont par ailleurs relevées, de sorte que l'on

classifiera de façon plus ciblée et que le nombre des informations classifiées se réduira.

Illustration 1

Relèvement des valeurs seuils de classification de la LSI



Sécurité des moyens informatiques

Depuis quelques années, la sécurité des moyens informatiques a fortement gagné en importance en raison de la mise en réseau de plus en plus prononcée des systèmes et de la dépendance croissante des autorités fédérales vis-à-vis de ces moyens dans l'accomplissement de leurs tâches légales. De nombreux incidents, survenus dans le monde et en Suisse, ont montré la vulnérabilité des moyens informatiques et ses conséquences potentielles. On ne peut se dispenser aujourd'hui d'inscrire formellement dans une loi certaines valeurs de référence en matière de sécurité informatique, compte tenu notamment de la mise en réseau des autorités et de la multiplication des échanges électroniques d'informations: des solutions et processus applicables à toutes les autorités s'imposent donc. De plus, les dispositions relatives au niveau de sécurité des moyens informatiques seront également déterminantes pour les CSP et les PSE. En raison de la rapidité des évolutions technologiques, la plupart des mesures concrètes de protection continueront d'être définies dans des ordonnances ou dans des directives.

La sécurité des moyens informatiques est souvent considérée comme une affaire technique, ce qui n'est vrai que dans une faible mesure: la majorité des mesures de sécurité informatique sont en effet de nature organisationnelle. Les autorités et organisations qui décident de l'engagement de moyens informatiques (bénéficiaires de prestations) sont les premières compétentes en la matière, et non les organisations qui exploitent ces moyens sur mandat des autorités et organisations (fournisseurs de prestations). Le domaine de l'organisation est donc celui qui réclame le plus d'attention.

Le projet se fonde sur des processus et des procédures en place et les adapte aux besoins identifiés. La LSI poursuit trois objectifs principaux à cet égard:

- *atteindre un niveau de sécurité transversal aussi homogène que possible:* Le projet ne contient pratiquement aucune mesure de sécurité détaillée, mais il exige des autorités soumises à la loi qu'elles définissent les processus, compétences et mesures nécessaires. Bien que la mise en œuvre reste de la compétence de chacune des autorités, la loi part du principe qu'elles règleront ces processus, compétences et mesures d'un commun accord et de façon si possible uniforme;
- *répartir clairement les compétences et responsabilités entre bénéficiaires et fournisseurs de prestations:* La responsabilité principale en matière de sécurité dans l'engagement des moyens informatiques incombe aux bénéficiaires de prestations. Ils sont compétents pour l'évaluation des besoins en matière de sécurité de l'information et pour la définition des mesures qui s'imposent. En revanche, les fournisseurs de prestations sont tenus de garantir la sécurité lors de l'exploitation des moyens informatiques. Ils doivent respecter et appliquer les exigences et mesures prévues par la présente loi et répondre aux exigences supplémentaires convenues avec les bénéficiaires de prestations;
- *mettre l'accent sur les moyens informatiques les plus critiques:* Le projet exige qu'une catégorie de sécurité soit attribuée aux moyens informatiques en fonction des informations qu'ils sont appelés à traiter et des tâches de l'autorité ou de l'organisation concernée. L'attribution d'une catégorie de sécurité aux moyens informatiques sert d'une part à permettre aux autorités d'évaluer le caractère critique (criticité) de leurs informations et moyens informatiques et, par la suite, de mettre l'effort principal sur les informations et moyens informatiques les plus critiques lorsqu'elles décideront des mesures de sécurité. D'autre part, les autorités devront définir des exigences et mesures de sécurité standard minimales pour chaque catégorie de sécurité et les appliquer avant la mise en exploitation du moyen informatique.

Mesures concernant le personnel et mesures physiques de protection

Les membres du personnel et les tiers mandatés sont responsables du respect des prescriptions régissant l'utilisation des informations et des moyens informatiques. Il est donc indispensable de les former de manière appropriée. A cet égard, les besoins sont considérables. Par exemple, on a constaté que de nombreuses personnes qui ont été soumises à un CSP n'ont jamais été formées au traitement d'informations classifiées. Un autre principe important de la sécurité de l'information est de ne délivrer les autorisations de traiter des informations, les autorisations d'utiliser des moyens informatiques et les autorisations d'accéder aux locaux que si les les personnes concernées en ont effectivement besoin pour l'accomplissement de leurs tâches. Pour l'heure, ce principe n'est pas respecté partout et son application n'est guère contrôlée. Aussi la LSI retient-elles ces deux principes comme critères minimaux de sécurité envers le personnel. L'informatisation croissante de l'accomplissement des tâches impose également de nouvelles méthodes d'identification des personnes (authentification) souhaitant accéder aux informations ou aux systèmes d'informa-

tion de la Confédération. La LSI habilite donc les autorités à recourir à des méthodes de vérification biométriques.

Les contrôles à l'entrée des locaux et d'autres mesures physiques de protection sont des mesures efficaces de sécurité de l'information. La LSI fixe à cet égard les exigences minimales de protection. Elle crée également une base légale permettant d'établir des zones de sécurité, à savoir des locaux et des secteurs bénéficiant d'une protection particulière parce que l'on y traite souvent des informations classifiées «confidentiel» ou «secret» ou qu'on y exploite des moyens informatiques des catégories de sécurité «protection élevée» ou «protection très élevée». Dans la pratique, ces zones sont surtout délimitées pour des locaux destinés aux serveurs, à la conduite ou à la sécurité. Ces zones de sécurité sont usuelles dans les autres pays, mais peu répandues au sein de la Confédération. Une base légale au sens formel s'impose parce que ces zones peuvent être liées à des mesures qui portent gravement atteinte aux droits individuels (par ex. la vidéosurveillance, le CSP ou la PSE).

Systèmes d'information destinés au contrôle central des données d'identification (systèmes GIA)

L'une des mesures opérationnelles les plus efficaces de la sécurité de l'information est une gestion et un contrôle efficaces des données d'identification et des accès. Étant donné que les informations proviennent de plus en plus de diverses sources, y compris hors de l'organisation concernée, les exigences en matière de protection et de fonctionnalités ne peuvent être satisfaites que grâce à des systèmes coordonnés transversaux. Le programme GIA Confédération introduit un tel système pour l'administration fédérale. Le Conseil fédéral et les autres autorités fédérales sont certes habilités à introduire des systèmes GIA, mais certains aspects du traitement des données personnelles exigent une base légale au sens formel pour des raisons liées à la protection des données. L'un des buts du projet est de régler l'architecture et le fonctionnement des systèmes de gestion des données d'identification sur lequel se fondent les compétences et les limites du traitement des données personnelles. Les dispositions d'exécution préciseront les droits et obligations des participants, de même que les exigences en matière de protection et de sécurité des données, contiendront une liste détaillée des données à traiter et règleront la transmission des données.

1.2.5 Contrôles de sécurité relatifs aux personnes

Les bases légales au sens formel autorisant les CSP se trouvent actuellement dans deux lois, dont la LMSI pour la Confédération. L'art. 24 LENu prévoit quant à lui des contrôles de loyauté pour le personnel des exploitants de centrales nucléaires. Bien que l'art. 113, al. 1, let. d, LAAM prévoie également un contrôle de sécurité relatif aux personnes, il ne s'agit pas d'un CSP au sens de la LMSI, mais d'une évaluation du potentiel de violence en vue de la remise de l'arme personnelle. La LRens videra la LMSI de presque toute sa substance, et l'on n'y trouvera plus que les dispositions régissant les CSP et les tâches ressortissant à la compétence de fedpol. La réglementation de la LMSI relative aux CSP servant presque exclusivement à la protection des informations (cf. art. 19, al. 1, LMSI), il est judicieux de

transférer ces dispositions dans la LSI. Le Conseil fédéral veut saisir cette occasion pour procéder à des adaptations en profondeur des dispositions légales formelles régissant les CSP, notamment en précisant le but qu'il poursuit par les CSP et en les simplifiant.

But des CSP

Ces derniers temps, les CSP ont fait l'objet de critiques répétées. On a régulièrement exigé le contrôle de personnes qui n'étaient pas chargées de tâches fédérales particulièrement sensibles (par ex. le personnel des services de nettoyage). Dans quelques cas, la décision de risque sur laquelle le contrôle a débouché a été jugée disproportionnée (cf. l'arrêt du Tribunal administratif fédéral A-6797/2013, de même que l'interpellation 14.3085 et le postulat 14.4076 intitulés «La gestion du risque lié au personnel de l'administration fédérale»). De plus, on a regretté qu'aucun contrôle ne soit mené pour certaines fonctions, notamment dans le domaine informatique, ou que des collaborateurs internes ou externes ne soient pas traités de la même manière pour la même fonction (cf. rapport de la CdG-E sur les collaborateurs externes de la Confédération, mentionné ci-avant au ch. 1.1.4, et motion 14.3031 «FINMA. Enquête de sécurité concernant les dirigeants avant leur nomination»). Enfin, régulièrement, la critique porte sur les délais de contrôle qui peuvent être très longs. Dans ce contexte, la DélCdG a recommandé au Conseil fédéral dans son rapport sur la sécurité informatique au sein du SRC (cf. ch. 1.1.4) de définir clairement, dans le cadre du présent message, les rôles des CSP et de la gestion du personnel dans le domaine de la sécurité de l'information, et de les distinguer rigoureusement. Elle l'a par ailleurs invité à préciser les effectifs qu'il entendait affecter aux CSP et l'apport qui en résulterait pour la sécurité de l'information.

Le CSP est une mesure destinée à prévenir des malveillances internes. Il vise à identifier le risque d'une atteinte intentionnelle ou par négligence à d'importants intérêts publics lorsqu'une personne donnée exerce une activité sensible. L'autorité ou l'organisation qui engage la personne concernée porte seule la responsabilité de décider si elle prend un risque accru, si elle assortit l'engagement de conditions pour réduire le risque ou si, pour éviter ou supprimer le risque, elle renonce à engager la personne ou la licencie. Déterminer si une personne est digne de confiance nécessite en premier lieu un entretien direct entre la personne responsable de l'engagement et le candidat, auquel s'ajoute le dossier de candidature. Pour la plupart des engagements, des affectations à des tâches militaires et des emplois dans le cadre de mandats militaires, les données collectées lors de la procédure directe de sélection suffisent; de plus, un abus de confiance n'entraîne généralement que des dommages mineurs pour les intérêts publics au sens de la présente loi. Si le dommage potentiel est considérable, un CSP peut mettre en lumière des facteurs de risque tirés des antécédents ou de l'environnement de la personne contrôlée. Une évaluation menée par les services compétents (services spécialisés CSP) qui conclut à l'absence de risque pour la sécurité ne saurait en aucun cas dégager la responsabilité des supérieurs hiérarchiques. Ceux-ci sont tenus d'identifier et de gérer les risques associés à leur personnel. Le CSP a donc une portée similaire à celle d'une évaluation des compétences (*assessment*), souvent ordonnée par un employeur avant l'engagement de dirigeants ou de personnes destinées à exercer une fonction clé.

Le CSP est une mesure étatique de sécurité de l'information: à ce titre, le recours au CSP doit être adapté au risque et rester économique. Étant donné que le CSP porte par nature une atteinte relativement lourde aux droits individuels, il doit répondre à des exigences sévères du point de vue de la proportionnalité. Lorsqu'il a établi sa première liste des personnes à contrôler en vertu de l'ordonnance du 15 avril 1992 relative aux contrôles de sécurité dans l'Administration fédérale[18] (abrogée le 1er février 1999), le Conseil fédéral s'était résolu pour des raisons politiques à limiter les CSP à un nombre restreint de fonctions, retenant un ordre de grandeur de quelque 1200 fonctions. Depuis l'entrée en vigueur de la LMSI en 1998, le nombre des personnes contrôlées n'a cependant cessé de croître, jusqu'à atteindre 70 000 à 80 000 annuellement depuis 2012. Plus de 60 000 CSP concernent des conscrits et des militaires, ce chiffre incluant la nouvelle évaluation du potentiel de violence au sens de l'art. 113 LAAM. Les ressources des services spécialisés CSP ont donc été régulièrement revues à la hausse, ce qui n'a pas empêché la hausse du nombre de cas en suspens.

Face à cette évolution, le Conseil fédéral juge que les CSP ne sont aujourd'hui plus adaptés au risque ni conformes au principe de la proportionnalité. Le CSP ne saurait être compris comme une mesure de protection de base appliquée systématiquement à tous les collaborateurs internes et externes. La charge qu'il occasionne et l'atteinte aux droits individuels qui l'accompagne ne se justifient en effet que si la fonction ou le mandat pour lesquels un CSP est prévu permet effectivement de nuire gravement aux intérêts de la Confédération. C'est pourquoi le Conseil fédéral entend restreindre le recours au CSP au strict minimum nécessaire à l'identification et à la maîtrise de risques considérables pour la sécurité de l'information. La nouvelle réglementation proposée devrait réduire significativement le nombre des fonctions soumises à un CSP.

Le projet de loi prévoit plusieurs mesures qui devraient globalement contribuer à cette réduction. En voici quelques exemples.

– Les valeurs seuils de la classification «confidentiel» ou «secret» sont relevées. À l'avenir, moins de fonctions seront associées au traitement d'informations de ces catégories.

– Les activités pour lesquelles un contrôle est nécessaire seront plus clairement définies que dans la LMSI. Les motifs de contrôle seront strictement limités aux besoins de la sécurité de l'information grâce à la notion d'*activité sensible*. Certains motifs de contrôle sont ainsi supprimés. Il s'agit notamment de l'accès régulier à des données sensibles dont la révélation pourrait porter gravement atteinte aux droits individuels des personnes concernées (art. 19, al. 1, let. e, LMSI). Dans la pratique, il n'est guère possible de déterminer quelles sont les informations qui répondent à ce critère.

  La LSI assure un contrôle à plusieurs niveaux des CSP. Le service spécialisé de la Confédération pour la sécurité de l'information présidera ainsi à l'élaboration et à l'examen régulier des listes de fonctions, ce qui garantira une application restrictive des critères fixés dans la loi et une vérification du

18 RO **1992** 1022

respect de ces critères. Les préposés à la sécurité de l'information assureront également un contrôle au sein des autorités fédérales et des départements. Par ailleurs, les éventuels problèmes d'exécution seront traités par la Conférence des préposés à la sécurité de l'information, qui s'appliquera à les résoudre de manière uniforme.

– Pour éviter un vide en matière de sécurité, il faudra enfin mettre à la disposition des employeurs d'autres moyens plus proportionnés pour répondre à leurs besoins légitimes de sécurité: si la préservation de leurs intérêts le requiert, ils seront autorisés à exiger des candidats et des membres de leur personnel des extraits du casier judiciaire et du registre des poursuites. Une révision de la LPers est proposée à cette fin.

Suppression de lacunes juridiques

De nombreuses adaptations ont été apportées au système régissant les CSP dans le but de combler des lacunes. Les principales modifications sont présentées ci-après.

– *Densité réglementaire accrue:* Le principe constitutionnel de la légalité exige que toute atteinte grave aux droits de la personnalité se fonde sur une base légale au sens formel et que celle-ci soit détaillée. La réglementation proposée est à cet égard bien plus précise que la LMSI. Elle répond également aux attentes du Parlement visant à ce que la notion de risque pour la sécurité soit définie dans une loi (cf. ch. 1.1.4);

– *Contrôles selon la législation spéciale:* Bien que les dispositions de la LMSI relatives aux CSP aient été conçues pour répondre presque exclusivement aux besoins de protection des informations dans le domaine de la sûreté intérieure ou extérieure, les motifs justifiant un CSP ont été étendus dans l'OCSP au-delà des critères de la LMSI. Par exemple, rares sont les directeurs d'office de l'administration fédérale qui assument des tâches liées à la sûreté intérieure ou extérieure ou qui accèdent régulièrement à des informations de la Confédération classifiées «secret». Ils doivent toutefois se soumettre à un CSP élargi avec audition, soit l'échelon de sécurité le plus élevé prévu par l'OCSP, avant d'être nommés par le Conseil fédéral. Le CSP élargi s'applique aux personnes en mission à l'étranger qui représentent officiellement la Suisse. On comprend aisément que les titulaires de ce type de fonction doivent répondre à des exigences sévères pour s'assurer de leur loyauté. On peut néanmoins se demander quel est le lien avec la préservation de la sûreté intérieure ou extérieure au sens de la LMSI.

  Le Conseil fédéral veut davantage de rigueur. La LSI ne prévoit de CSP que pour des activités se rapportant clairement à la sécurité de l'information au sein de la Confédération. Par conséquent, les dommages que les CSP au sens de la LSI doivent permettre d'éviter ou de réduire doivent également être compris comme des dommages à la sécurité de l'information. Une probabilité accrue de mise en péril de la réputation de la Confédération ne suffit donc plus en principe à justifier un risque pour la sécurité au sens de la LSI. Si un contrôle s'impose pour d'autres activités, il doit être justifié dans la législation spéciale. Pour être en mesure de distinguer sans équivoque un CSP au sens de la LSI et un CSP en vertu d'autres textes législatifs, une

autre terminologie est utilisée pour les seconds (*contrôle de loyauté*): à cet égard, des modifications de la LPers et de la LAAM sont proposées. Ainsi, des personnes qui représentent régulièrement la Suisse à l'étranger, disposent de compétences décisionnelles ou assument des tâches de surveillance dans des dossiers financiers importants pourront être soumises à un contrôle de loyauté. Le Conseil fédéral n'ordonnera ces nouveaux contrôles que de manière très restrictive.

– *Suppression du critère de la régularité pour les CSP:* Le critère de la régularité (cf. art. 19, al. 1, LMSI) repose, entre autres, sur une appréciation du SRC: celui-ci juge que le risque pour la protection de l'État est particulièrement élevé lorsque des collaborateurs ont régulièrement et durablement accès à des informations classifiées. Les personnes qui ne disposent que d'un accès ponctuel et temporaire sont moins menacées parce qu'elles sont moins intéressantes pour des services désireux de se procurer des informations. Le critère de la régularité pose toutefois deux problèmes. D'une part, les activités de renseignement ne constituent qu'une menace parmi d'autres pour la sécurité de l'information. En n'accédant ne serait-ce qu'une seule fois à une information classifiée «secret», une personne est déjà en mesure de nuire gravement aux intérêts de la Confédération. Ce pourrait être le cas, par exemple, si elle divulguait des informations sur la stratégie de négociation de la Suisse dans un dossier particulièrement important. Le dommage découle ainsi avant tout du contenu de l'information. D'autre part, la notion de régularité est ambiguë et a déjà conduit à des interprétations divergentes. Pour soumettre un membre du personnel de la Confédération à un CSP, il est bien plus important de savoir si la personne qui exerce une fonction donnée doit traiter des informations classifiées «confidentiel» ou «secret» dans l'accomplissement de ses tâches, *doit* administrer, exploiter, entretenir ou vérifier des moyens informatiques des catégories de sécurité «protection élevée» ou «protection très élevée» ou *doit* accéder à des zones de sécurité. C'est uniquement lorsqu'une telle activité est *indispensable* à l'accomplissement des tâches liées à la fonction – que la fonction doit figurer dans la liste des fonctions à contrôler. Les autorités et organisations soumises à la loi doivent veiller à ce que le nombre des personnes chargées de tâches sensibles soit limité au strict nécessaire.

– *Passage de trois à deux degrés de contrôle:* Le droit en vigueur (art. 9 à 12 OCSP) prévoit trois degrés de contrôle, à savoir un contrôle de sécurité de base, un contrôle de sécurité élargi et un contrôle de sécurité élargi avec audition. Alors que les deux premiers degrés au sens de l'OCSP visent un objectif compréhensible, on peut se demander quelles informations ou activités devraient être mieux protégées que les informations classifiées «secret». Pour accéder à ces dernières, en effet, un CSP élargi au sens de l'art. 11 OCSP est requis. La Confédération ne connaît pas cependant d'échelon de classification «très secret», pour lequel un contrôle élargi avec audition au sens de l'art. 12 OCSP serait nécessaire. La présente loi ramène donc de trois à deux le nombre des degrés de contrôle. Pour renforcer l'efficacité des CSP, elle réorganise en revanche la collecte des données dans le cadre des deux degrés restants et la complète si nécessaire.

Le système actuel des listes de fonctions, qui doivent être définies dans un acte, a également fait l'objet de discussions. Ce système présente les inconvénients suivants: l'établissement des listes occasionne de lourdes charges, les listes ne sont guère harmonisées entre les départements et la Chancellerie fédérale et elles doivent être adaptées en permanence en raison des changements organisationnels et des nouvelles dénominations données aux fonctions. Elles posent également problème pour des raisons de sécurité: elles donnent en effet une image complète de toutes les fonctions des autorités comportant des activités sensibles. Leur publication permet ainsi à tout un chacun d'y accéder dans le monde entier, y compris aux services de renseignement étrangers. Les listes présentent malgré tout un avantage décisif par rapport à d'autres solutions possibles: elles garantissent la sécurité du droit et limitent le cercle des personnes à contrôler, de sorte que l'on évite une multiplication sauvage des contrôles. Avant d'adopter les dispositions d'exécution, le Conseil fédéral devra encore déterminer si la publication des listes sans restriction d'accès est adéquate.

1.2.6 Procédure de sécurité relative aux entreprises

La PSE (appelée jusqu'ici «procédure de maintien du secret») a pour objet la sécurité de l'information dans le cadre de l'attribution de mandats des autorités fédérales à des tiers (ci-après entreprises) non soumis à leur surveillance directe. La procédure vise à vérifier si l'entreprise est digne de confiance et à permettre le contrôle et l'application des mesures nécessaires à la sécurité de l'information durant toute la durée d'exécution du mandat. La PSE n'a pas pour objectif la sécurité des produits, pour laquelle la compétence revient au seul adjudicateur.

La PSE vise entre autres à empêcher que des entreprises qui pourraient par exemple être pilotées ou significativement influencées par des services de renseignement étrangers ou des organisations poursuivant des buts criminels en raison de leurs rapports de propriété, de leur nature juridique, de leur structure organisationnelle ou de leurs relations d'affaires (entreprises sous contrôle ou influence de l'étranger) aient accès à des informations sensibles ou à des vecteurs permettant de lancer des attaques contre des moyens informatiques critiques de la Confédération. L'évaluation de la loyauté d'entreprises prestataires de services, notamment l'exclusion potentielle des procédures d'adjudication des entreprises sous contrôle ou influence de l'étranger, a gagné en importance politique depuis les révélations d'Edward Snowden. En effet, certains services de renseignement sont en mesure de contraindre l'industrie informatique de leur pays, par des moyens légaux et répressifs, de manquer à leurs obligations contractuelles ou légales de maintien du secret. Les entreprises sous la coupe des services de renseignement de ces pays ne peuvent fournir de garantie crédible qu'elles accorderont la priorité au respect des obligations de maintien du secret imposées par le droit national. Par ailleurs, les dommages que peuvent causer des entreprises contrôlées ou influencées de la sorte ne se limitent pas à la confidentialité des informations: des menaces planent également sur la disponibilité et l'intégrité des moyens informatiques. Dans ce contexte, les États excluent de leurs appels d'offres un nombre croissant de fournisseurs étrangers de services informatiques critiques. Il est important de préciser à cet égard que l'évaluation du risque

pour la sécurité se fonde toujours sur la sensibilité du mandat pour la sécurité et la situation concrète de l'entreprise. La LSI ne saurait justifier a priori l'exclusion globale de fournisseurs étrangers, en violation du principe de la concurrence.

La PSE est adéquate et usuelle dans le contexte international (cf. par ex. l'art. 11 de la décision 2013/488/UE[19] ou la section VII du règlement de sécurité de l'Agence spatiale européenne du 15 décembre 2011[20]). Elle ne pose pas de problème par rapport au droit international des marchés publics puisque l'accord du 15 avril 1994 sur les marchés publics[21] prévoit une exception pour les mesures de cette nature (cf. art. XXIII). La PSE est appliquée en Suisse depuis la fin des années 1970 aux mandats de la Confédération à contenu militaire classifié. Le champ d'application restreint de l'ordonnance du DMF du 29 août 1990 concernant la sauvegarde du secret ne permet cependant d'y recourir que pour les mandats militaires classifiés. Le Conseil fédéral déplore depuis longtemps l'absence d'une PSE uniforme, c'est-à-dire également applicable aux mandats de la Confédération ressortissant au domaine civil. C'est pourquoi des mesures de sécurité spéciales ont été prises dans les cas d'espèce pour les mandats classifiés de la Confédération dans le domaine non militaire. En outre, cette lacune a empêché plusieurs fois des entreprises suisses de soumissionner avec succès pour des projets étrangers non militaires classifiés, par exemple la confection de documents d'identité ou de moyens de paiement pour le compte d'États tiers ou la participation à des projets scientifiques. La compétitivité de l'économie suisse s'en trouve affaiblie. Le Conseil fédéral entend combler cette lacune.

La PSE se déroule grosso modo de la manière suivante: l'adjudicateur demande au service chargé de la procédure de sécurité relative aux entreprises (service spécialisé PSE) d'ouvrir une procédure. Après l'ouverture de la procédure, le service spécialisé PSE définit tout d'abord en accord avec l'adjudicateur les exigences de sécurité, puis examine la qualification des entreprises concernées sous l'angle de la sécurité. Il cherche en particulier à savoir si les entreprises concernées sont contrôlées par d'autres États ou se trouvent sous leur influence, et le cas échéant si cette dépendance ou cette influence sont compatibles avec la sécurité de l'information de la Confédération. L'adjudicateur attribue par la suite le mandat à une entreprise jugée qualifiée. L'entreprise définit alors dans un plan de sécurité, sous la surveillance du service spécialisé PSE, la façon dont elle entend satisfaire aux exigences en matière de sécurité de l'information. Après la mise en œuvre des mesures de sécurité nécessaires, une déclaration de sécurité pour les entreprises (DSE) est délivrée à l'entreprise. Puis, lorsque les déclarations de sécurité relatives aux personnes ont été établies à l'issue des CSP qui s'imposaient, l'adjudicateur est autorisé à mettre à la disposition de l'entreprise les moyens (informations, données, etc.) nécessaires à l'accomplissement du mandat sensible. La DSE a des effets particuliers tant pour l'entreprise que pour le service spécialisé PSE: ce dernier est notamment habilité à inspecter l'entreprise à l'improviste et à prendre d'autres mesures.

19 Décision 2013/488/UE du Conseil du 23 septembre 2013 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne, JO L 274 du 15.10.2013, p. 1.

20 Le règlement peut être consulté sur le site de l'Agence spatiale européenne à l'adresse suivante: www.esa.int > About us > Security at ESA > Règlement de sécurité.

21 RS **0.632.231.422**

La réglementation proposée est proche de celle qui régit les CSP, mais elle s'en distingue sur des points importants. En principe, la procédure vise dans les deux cas à vérifier si la personne ou l'entreprise est digne de confiance. Selon le résultat de l'évaluation, une DSE est établie. Celle-ci confirme que l'entreprise est digne de confiance et lui permet d'exercer des activités sensibles de la Confédération (ou d'autorités étrangères). Contrairement au CSP, la procédure applicable aux entreprises ne se termine pas par une fois que la des est délivrée: le respect des mesures imposées peut en effet être vérifié en tout temps. À la différence du CSP, l'évaluation de l'autorité chargée de la procédure lie en principe l'adjudicateur, raison pour laquelle le service spécialisé PSE rend une décision formelle sujette à recours. Une exception est prévue pour le cas où toutes les entreprises qui entrent en considération pour le mandat représentent un risque pour la sécurité. Elle vise principalement les prestations dans le domaine informatique, car certaines entreprises de ce secteur détiennent une position de quasi-monopole. Si un mandat doit être confié à une telle entreprise en l'absence d'autre solution, aucune DSE suisse ne lui est délivrée: la procédure est classée et l'adjudicateur assume la responsabilité de l'application et du contrôle des mesures de sécurité. En vertu de la loi, l'adjudicateur dispose des mêmes droits que le service spécialisé PSE pour exécuter cette tâche.

Le Conseil fédéral souhaite un recours ciblé à la PSE et une procédure aussi peu bureaucratique que possible. Le projet prévoit ainsi la possibilité de renoncer à une PSE lorsque le risque peut être réduit par d'autres moyens. Le Conseil fédéral précisera ce principe au niveau de l'ordonnance.

1.2.7 Infrastructures critiques

Dans sa Stratégie nationale de protection de la Suisse contre les cyberrisques, le Conseil fédéral a retenu le principe de la réglementation décentralisée des infrastructures critiques (cf. ch. 1.1.2). Ce principe signifie qu'il faut adapter la législation spéciale lorsque l'on identifie un besoin sectoriel. L'examen des besoins incombe ainsi aux départements qui, dans l'accomplissement de leurs tâches, disposent de compétences réglementaires vis-à-vis des exploitants d'infrastructures critiques (par ex. le DETEC pour le secteur des infrastructures d'approvisionnement en énergie). Il est cependant des tâches transversales qui, ne peuvent être assumées de manière décentralisée, notamment pour des raisons d'efficacité et de coût. Il s'agit essentiellement du soutien aux exploitants des infrastructures critiques par l'échange d'informations sur les menaces en matière de sécurité de l'information, qui sert notamment à la détection précoce des risques et à la prévention des dangers. Dans ce domaine, la pratique a montré que les exploitants d'infrastructures critiques souhaitent expressément disposer d'un interlocuteur unique auprès de la Confédération. Cette tâche est actuellement assumée par la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI).

En accord avec les décisions du Conseil fédéral des 29 octobre 2003 et 24 janvier 2007, MELANI est exploitée conjointement par l'UPIC et le SRC, conformément à leurs bases légales respectives. La direction stratégique de MELANI et le centre de compétences technique sont rattachés à l'UPIC, tandis que la plaque tournante

d'information est exploitée par le SRC. Le partenariat public-privé mis en place dans le cadre de MELANI s'est révélé très performant, notamment en raison de l'accès aux informations du SRC. Outre les informations mises à disposition, les exploitants d'infrastructures critiques apprécient particulièrement que les fournisseurs de renseignements relatifs à des incidents restent maîtres de leurs informations (ils décident à qui l'information peut être transmise), que la collaboration repose sur une base volontaire et que la sécurité de l'information et la gestion des risques reposent sur l'information, éventuellement sur des recommandations, plutôt que par sur des mesures contraignantes.

Dans l'accomplissement de ses tâches, MELANI doit régulièrement traiter des ressources d'adressage au sens de l'art. 3, let. f, LTC (en particulier des noms de domaine, des adresses IP et des adresses de messagerie) qui sont liés des dangers ou des menaces réels et qu'elle échange avec les exploitants d'infrastructures critiques. Les infrastructures criminelles sont souvent constituées d'ordinateurs infectés par des logiciels malveillants à l'insu de leur propriétaire, de noms de domaine enregistrés sous de faux noms, de sites Internet légitimes mais modifiés illicitement et de serveurs loués sous des identités usurpées. Grâce aux informations fournies par MELANI, les exploitants d'infrastructures critiques peuvent protéger leurs systèmes, par exemple en bloquant les demandes de communication émanant d'ordinateurs infectés. Cependant, comme les ressources d'adressage se rapportent à des personnes identifiées ou identifiables (ou à des installations ou raccordements attribuables à des personnes identifiées ou identifiables), elles peuvent être considérées comme des données personnelles. Dès qu'une plainte pénale est déposée ou que des informations sont recueillies dans le cadre d'une enquête de police, les données concernées sont liées à des poursuites pénales et peuvent devenir des données sensibles au sens de l'art. 3, let. c, ch. 4, LPD. Toutefois, étant donné qu'une plainte pénale ne peut écarter à elle seule le danger, du moins pas à court terme, informer les exploitants d'infrastructures critiques à propos de ces vecteurs d'attaque est essentiel pour leur permettre de protéger leurs systèmes et d'identifier le cas échéant les attaques qui sont déjà survenues. Pour traiter ces informations et ces données, et les échanger avec les exploitants d'infrastructures critiques, MELANI doit toutefois disposer d'une base légale au sens formel qui fait aujourd'hui défaut (cf. art. 17, al. 2, LPD).

Par décision du 30 novembre 2011, le Conseil fédéral a chargé le DDPS d'intégrer à la présente loi les bases légales nécessaires au traitement des données dans le cadre du soutien aux exploitants d'infrastructures critiques. La LSI règle tout d'abord les tâches essentielles de MELANI en matière de soutien aux exploitants d'infrastructures critiques. Elle crée ensuite les bases légales au sens formel permettant le cas échéant de traiter et d'échanger ces données dans la mesure où la sécurité technique de l'information des infrastructures critiques l'exige. Il est impératif que cet échange d'informations soit également garanti avec les partenaires étrangers et internationaux de la Suisse, raison pour laquelle la LSI définit les principes et les limites nécessaires de la coopération internationale. Ce dispositif permet par exemple d'échanger des ressources d'adressage avec l'office fédéral allemand de la sécurité technique des informations (*Bundesamt für Sicherheit in der Informationstechnik*), l'Agence nationale de la sécurité des systèmes d'information en France ou les centres nationaux néerlandais et finlandais de la cybersécurité (*National Cyber Security Centers*).

Les unités organisationnelles chargées de la protection des infrastructures critiques (d'information) diffèrent selon les pays: elles peuvent être autonomes ou alors rattachées à la police, à un service de renseignement, à l'armée ou au régulateur des télécommunications.

La collaboration avec les partenaires en Suisse et à l'étranger repose sur le volontariat et la transparence. Les services compétents ne peuvent prendre aucune mesure de contrainte; ils doivent s'identifier en bonne et due forme à chaque demande d'informations ou de données et ils doivent communiquer au fournisseur potentiel des données le but de la demande et l'utilisation qui sera faite des données. Néanmoins, des données sont également livrées spontanément à des organisations partenaires lorsqu'elles paraissent utiles pour identifier des incidents dans leur domaine de compétence ou y remédier.

Bien que le Conseil fédéral ait désigné le SRC service (co-)compétent pour les tâches relatives à la présente loi, la LSI ne lui accorde aucun autre droit de traiter des données dans le cadre des autres attributions que lui confère la LRens. Le champ d'application de la LSI concerne essentiellement la sécurité technique de l'information et le fonctionnement des infrastructures d'information conformément à leur but, y compris Internet et les systèmes qui y sont raccordés. À l'avenir, ces tâches seront assumées par les services compétents indépendamment de leur rattachement administratif et des bases légales qui régissent les organisations dont ils dépendent. Le recours aux connaissances et aux aptitudes de l'UPIC et du SRC ont sans conteste contribué au succès de MELANI, raison pour laquelle cette collaboration doit être maintenue. La législation d'exécution règlera de manière transparente l'échange des données entre les divers acteurs de la sécurité de l'information. Par ailleurs, le Conseil fédéral veille à un contrôle périodique du traitement des données par un service externe. Dans la mesure où le SRC traite des données dans le champ d'application de la LSI, le Conseil fédéral peut donc ordonner un contrôle par un autre service que ses propres organes de surveillance et de contrôle.

1.2.8 Exécution

La réglementation de l'exécution doit relever le défi d'une application aussi uniforme que possible de la loi, afin d'éviter des lacunes de sécurité dans l'échange d'informations entre les autorités qui, autrement, ne manqueraient pas d'apparaître. L'autonomie des autorités soumises à la loi en matière d'organisation et d'exécution doit toutefois être maintenue. Par ailleurs, les compétences constitutionnelles des diverses autorités pour l'accomplissement de leurs tâches ne doivent pas être remises en cause par les prescriptions d'exécution d'une seule autorité (par exemple le Conseil fédéral). La LSI prend en compte ces exigences contradictoires en prévoyant trois mécanismes.

– *Réglementation selon le principe de subsidiarité:* Chaque autorité exécute la loi dans son domaine de compétence et édicte les dispositions d'exécution afférentes. La législation d'exécution du Conseil fédéral s'appliquera toutefois par analogie aux autres autorités de la Confédération aussi longtemps qu'elles n'auront pas édicté leur propre réglementation.

- *Normes:* Le Conseil fédéral est habilité à définir des exigences et mesures de sécurité standard conformes aux connaissances scientifiques et techniques les plus récentes, qui vaudront recommandations pour les autres autorités fédérales. Il ne réglera pas à cet égard des problèmes organisationnels de fond, mais des processus, moyens et prestations qui y sont subordonnés (par ex. la détermination des besoins de protection des informations, les méthodes d'évaluation des risques, le chiffrement, etc.). L'objectif est de parvenir à un niveau uniforme de sécurité tout en réduisant les coûts de projet et de mise en œuvre. Le Conseil fédéral pourra déléguer la définition de ces exigences et mesures à des organes spécialisés.
- *Création d'un organe de coordination:* L'institution d'une Conférence des préposés à la sécurité de l'information, qui regroupera des représentants de toutes les autorités fédérales, des cantons et du PFPDT, est une mesure centrale du dispositif. Les préposés à la sécurité de l'information, chargés de contrôler la mise en œuvre de la loi, auront en effet des connaissances approfondies des problèmes de sécurité de l'information dans leurs domaines de compétence, notamment à propos de l'applicabilité, de l'efficacité et de l'économicité des prescriptions et des mesures prises. La conférence devra garantir l'exécution uniforme de la loi par toutes les autorités concernées en fonction des risques, de même que la coordination avec les cantons et le PFPDT. Elle devra également être associée de manière décisive à la standardisation des exigences et des mesures.

La solution proposée préservera l'indépendance des autorités de la Confédération en matière d'exécution. Cette dernière se fera de manière décentralisée. Le niveau de sécurité uniforme recherché sera atteint par la définition commune des principes applicables, par l'élaboration de mesures standard et par le soutien professionnel d'organes spécialisés.

Le projet pose essentiellement le cadre général applicable à toutes les autorités. L'exécution par l'administration fédérale est de la compétence du Conseil fédéral, dont l'autonomie en matière d'exécution n'est guère restreinte. Sur le plan organisationnel, il laisse une grande latitude. Le Conseil fédéral décidera à cet égard s'il entend s'en tenir à l'exécution majoritairement décentralisée ou s'il veut centraliser certaines compétences et responsabilités. L'exécution par les unités décentralisées de l'administration fédérale et les organisations de droit public ou privé soumises à la loi et qui assument des tâches de l'administration dépendra de la portée de leur degré de subordination et de leur autonomie.

1.2.9 Organisation

Lors de l'élaboration du projet, on a examiné dans quelle mesure les compétences et les responsabilités en matière de sécurité de l'information répondaient aux exigences actuelles. Ce mandat ne concernait en principe que l'administration fédérale, mais les résultats de l'analyse fournissent des informations importantes qui valent également pour l'organisation de la sécurité de l'information au niveau transversal (entre les autorités).

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

Au sein de l'administration fédérale, les compétences et les responsabilités en matière de protection des informations sont réglées dans divers actes et par diverses instances habilitées à édicter des directives, en fonction de la nature des informations (par ex. les informations classifiées ou les données personnelles) ou du type de traitement et des mesures de protection (électronique ou physique). En conséquence, la Confédération a institué plusieurs organisations parallèles chargées de tâches principales ou partielles dans le domaine de la sécurité de l'information (protection des informations, protection des données, sécurité informatique, etc.).

Organisation de la protection des informations

La protection des informations est pour l'essentiel réglée dans l'OPrI. Des règles supplémentaires figurent dans les traités internationaux dits de protection des informations. L'OPrI ne s'applique qu'à l'administration fédérale et à l'armée. La mise en œuvre de la protection des informations se fait de manière décentralisée, tout en étant coordonnée au niveau central par des organes non habilités à donner des instructions. La Conférence des secrétaires généraux (CSG) a la compétence d'édicter des prescriptions détaillées (catalogue de classification et directives de traitement). Les prescriptions de traitement contiennent également des règles de comportement pour le traitement électronique d'informations classifiées, de même que des exigences concernant la sécurité des moyens informatiques. Les départements et la ChF doivent désigner un préposé à la protection des informations. Bien que l'OPrI ne l'impose pas, tous les départements ont désigné des conseillers en protection des informations au sein des unités administratives. Un comité de coordination veille à une exécution homogène au niveau de la Confédération et élabore les prescriptions à l'intention de la CSG. Il est assisté d'un organe de coordination.

Organisation de la protection des données

Les bases légales du traitement des données personnelles sont fournies par les lois spéciales afférentes. En revanche, l'organisation de la protection des données au sein de la Confédération est réglée principalement dans la LPD et l'OLPD. Contrairement à l'OPrI, ces actes normatifs s'appliquent également aux particuliers. La mise en œuvre de la protection des données est décentralisée, mais elle est coordonnée de façon centrale par le PFPDT et par le groupe Protection des données, un organe informel non habilité à donner des instructions. Les départements et la ChF doivent désigner un préposé à la protection des données. Bien qu'ils n'y soient pas contraints, tous les départements ont désigné des conseillers en protection des données au sein des unités administratives.

Organisation de la sécurité informatique

L'organisation de la sécurité informatique est principalement réglée dans l'OIAF, mais de nombreux autres actes normatifs ont une incidence sur les compétences et les responsabilités en la matière (OPrI, traités internationaux de protection des informations, OLPD, O-GEVER, etc.). Le Conseil fédéral édicte des prescriptions en matière de sécurité informatique, dont l'exécution est décentralisée. Les départements et la ChF sont eux-mêmes responsables dans leur domaine de compétence.

L'exécution est toutefois pilotée de façon centralisée par un organe habilité à donner des instructions (l'UPIC). L'UPIC décide de réglementations particulières sur l'attribution des droits et des mandats en matière de sécurité, notamment en lien avec les pare-feu, les droits d'accès et les privilèges. Lorsque l'administration fédérale est menacée, elle décide des mesures de sécurité informatique. Elle peut enquêter en qualité d'expert, sur mandat d'un département ou de la ChF, sur des événements supposés ou avérés en rapport avec la sécurité. Elle désigne le délégué à la sécurité informatique de la Confédération.

Deux organes consultatifs accompagnent l'UPIC. Le Comité de la sécurité informatique assiste ainsi l'UPIC pour toutes les questions relatives à la sécurité informatique et assure la coordination interdépartementale. Le Conseil informatique de la Confédération assiste également l'UPIC dans les affaires informatiques (y compris les affaires concernant la sécurité) qui nécessitent une entente entre les départements et la ChF, notamment pour ce qui est de l'édiction de prescriptions et de l'approbation de dérogations. Pour l'exécution, les départements, la ChF et toutes les unités administratives sont tenues de désigner un délégué à la sécurité informatique qui assume des tâches de coordination.

Outre cette organisation de base, de nombreux autres organes ou services se préoccupent également de la sécurité informatique au sein de la Confédération, notamment la Protection des informations et des objets au sein de l'état-major de l'armée, le CERT militaire et la Sécurité de l'information et cryptologie de la BAC, armasuisse Sciences et technologie (armasuisse est un centre d'achats de la Confédération pour des biens et services en matière de cryptologie), MELANI, l'État-major pour la sûreté de l'information et le CSIRT (*Computer Security Incident Response Team*, autre nom des CERT) de l'OFIT. Le Contrôle fédéral des finances est chargé pour sa part de la révision dans le domaine informatique au sein de l'administration fédérale.

Lacunes et faiblesses organisationnelles

L'organisation actuelle présente de nombreuses lacunes et de nombreux points faibles. En voici quelques exemples.

- Des points de vue tant juridique qu'organisationnel, la Confédération exploite aujourd'hui des structures parallèles pour plusieurs secteurs de la sécurité de l'information. Les compétences des divers domaines ne sont pas toujours clairement définies et leurs recoupements ne bénéficient pas d'une attention suffisante, ce qui nuit non seulement à la sécurité effective de l'information, mais encore à la coordination des dossiers politiques liés à la sécurité de l'information de même qu'à la collaboration avec les cantons et les partenaires internationaux.
- De trop nombreux acteurs ne disposent pas de connaissances spécialisées suffisantes, parce qu'ils n'exercent leurs tâches en matière de sécurité de l'information qu'à titre accessoire.
- Les actuels préposés ne disposent souvent pas de ressources suffisantes pour accomplir leur tâches. La masse critique n'est atteinte nulle part. Pourtant, dans nombre d'organisations, les ressources suffiraient, mais elles sont mal

utilisées parce qu'elles sont réparties entre un nombre trop élevé de personnes.

- Les coûts de la sécurité sont généralement exposés de manière peu transparente, ce qui empêche toute appréciation de l'économicité des mesures.
- Les pouvoirs des spécialistes sont insuffisants. La plupart du temps, ils ne sont chargés que de tâches de coordination et ne peuvent ni mener des audits, ni intervenir lorsqu'ils constatent des lacunes. Les spécialistes, notamment dans le domaine informatique, relèvent par ailleurs souvent d'un domaine spécialisé dont ils devraient évaluer les risques en toute indépendance, ce qui provoque des conflits d'intérêts.
- La gestion de la sécurité est lacunaire. La sécurité de l'information est considérée comme une affaire purement technique. Par conséquent, les activités usuelles de gestion (par ex. définition d'objectifs, contrôle de la mise en œuvre et examen de l'efficacité) ne s'étendent que rarement au domaine de la sécurité. Les responsables hiérarchiques doivent être conseillés, accompagnés et formés de manière plus compétente à tous les échelons.
- La conscience de la nécessité de garantir la sécurité est lacunaire. Souvent, les mesures mises en place en matière de formation ne touchent pas les personnes chargées de tâches sensibles. De nombreuses personnes sont soumises à un CSP mais ne sont pas formées en conséquence aux problèmes de la sécurité de l'information.

L'organisation actuelle s'est mise en place, au fil des ans, en fonction de besoins juridiques et matériels sectoriels. Durant de longues années, ses résultats étaient satisfaisants. L'évolution vers une société de l'information a toutefois complexifié les menaces qui pèsent sur l'information et les moyens informatiques et accentué leur caractère dynamique. Il est nécessaire d'affronter ces dangers de manière globale et professionnelle, ce qui implique des mesures sur les plans juridique et organisationnel, de même que des connaissances et compétences approfondies. Il est indubitable que l'organisation actuelle au sein de la Confédération ne répond pas à ces exigences.

Les divers organes spécialisés doivent être regroupés dans la mesure du possible, afin que l'on puisse exploiter les synergies et dégager des économies d'échelle. Ce regroupement doit également permettre de régler les problèmes de compétences et de renforcer le savoir interdisciplinaire. Pour ce qui est des divers préposés, leurs compétences peuvent être renforcées par une professionnalisation plus marquée. Le professionnalisme pourrait être amélioré en concentrant diverses tâches de gestion de la sécurité de l'information auprès d'un petit nombre de personnes.

Nouvelle organisation à l'échelon de la Confédération

Le projet jette les bases d'une clarification et d'une simplification des compétences et des responsabilités. Il met l'accent sur l'acquisition des qualifications nécessaires par les services chargés de la mise en œuvre, notamment grâce à l'appui d'experts et à un échange plus soutenu d'informations. En conséquence, le projet prévoit un seul rôle de préposé, un seul organe de coordination et un service spécialisé de la Confédération, qui assumeront tous des tâches transversales dans le domaine de la sécurité

de l'information. La nouvelle réglementation permettra de regrouper les structures d'exécution actuelles de la protection des informations et de la sécurité informatique.

Préposés à la sécurité de l'information

La nouvelle fonction de préposé à la sécurité de l'information est d'une importance capitale pour l'exécution. Ce nouveau rôle est essentiellement une fonction de gestion. Les préposés à la sécurité de l'information ne traiteront pas en priorité de questions hautement techniques en lien avec la sécurité de l'information mais piloteront, sur mandat de leur autorité (ou des départements et de la ChF), la sécurité de l'information et vérifieront l'application des mesures prises. Ils devront aussi mettre l'accent sur la gestion des risques et la coordination avec d'autres domaines. Pour assumer leurs tâches de façon efficace, les préposés à la sécurité de l'information devront non seulement bénéficier du soutien affirmé de leur direction, mais encore collaborer étroitement avec les services chargés de la gestion générale des risques, de la protection des données et de la sécurité. Ils serviront ainsi de plaque tournante entre la direction et les services chargés de la mise en œuvre des mesures.

Dans les départements et à la ChF, cette nouvelle fonction remplacera les rôles jusqu'ici distincts des préposés à la protection des informations et des délégués à la sécurité informatique. Le Conseil fédéral devra décider lorsqu'il adoptera l'ordonnance si un regroupement des fonctions est utile et nécessaire au sein des unités administratives subordonnées.

Conférence des préposés à la sécurité de l'information

En raison de l'indépendance constitutionnelle des autorités fédérales, un niveau uniforme de sécurité ne peut être atteint qu'à la condition de développer une des principes communs, malgré des besoins pour partie hétéroclites. En raison de leur statut, les préposés à la sécurité de l'information auront une bonne connaissance de la situation et des problèmes de la sécurité de l'information dans leur domaine de compétence, notamment quant à l'applicabilité et à l'efficacité des prescriptions et mesures prises. Il est donc judicieux d'instituer un organe de coordination sous la forme d'une conférence de ces préposés à la sécurité de l'information.

La conférence s'occupera principalement de la coordination transversale de l'exécution et de l'évaluation des normes proposées. Elle jouera de ce fait un rôle non négligeable dans le développement de principes uniformes. Les cantons et le PFPDT sont également représentés au sein de la conférence, qui pourra recourir à des experts des milieux scientifiques et économiques pour des questions stratégiques. La conférence remplacera les actuels Comité de coordination pour la protection des informations au sein de la Confédération (OPrI) et Comité de la sécurité informatique (OIAF), les aspects techniques restant du ressort d'organes spécialisés subordonnés.

Service spécialisé de la Confédération pour la sécurité de l'information

L'organisation de la sécurité de l'information doit être pilotée et contrôlée comme un tout. Plusieurs tâches prévues par la présente loi existent déjà et seront assumées par divers organes spécialisés: elles sont conçues et accomplies de manière sectorielle et guère harmonisée. Une simple coordination renforcée ne suffit pas à garantir

une approche intégrale, raison pour laquelle un service spécialisé central est institué. Celui-ci sera conçu comme un centre de compétences pour les tâches transversales au niveau des autorités fédérales. Il ne sera pas habilité à donner des instructions: il agira toujours sur proposition ou sur mandat d'une autorité soumise à la loi, et ses tâches relèveront pour l'essentiel du soutien et du conseil.

La loi énumère de façon exhaustive les tâches transversales concrètes du service spécialisé. Outre le conseil et le soutien, il pourra, sur proposition des autorités soumises à la loi, évaluer les risques liés à l'introduction de nouvelles technologies ou piloter et coordonner des projets transversaux importants en matière de sécurité de l'information. Une autre de ses tâches essentielles sera d'examiner les aspects de sécurité de l'information pour certains processus, moyens et services (sur proposition des autorités soumises à la loi). S'il s'avère que les processus, moyens et services en question répondent aux exigences de la Confédération, ils pourront être normalisés, puis utilisés plus simplement par d'autres autorités ou organisations de la Confédération (réduction des charges). Par ailleurs, le service spécialisé pourra aussi être appelé à mener des contrôles de sécurité et des audits. Enfin, il sera l'interlocuteur privilégié pour des contacts avec les services étrangers et internationaux dans le domaine de la sécurité de l'information: cette fonction est indispensable pour la mise en œuvre de traités internationaux (cf. ch. 5.2).

Le Conseil fédéral règlera l'organisation du service spécialisé au niveau de l'ordonnance, en définissant quelles tâches il assumera seul ou en collaboration avec d'autres services fédéraux. De nombreux services de l'administration fédérale sont actuellement chargés de tâches transversales figurant dans le cahier des charges du futur service spécialisé. Ce dernier se verra par exemple confier des tâches aujourd'hui assumées par l'UPIC-Sec et la Protection des informations et des objets pour le compte de l'administration fédérale. Les tâches des unités administratives existantes seront par conséquent redéfinies au niveau de l'ordonnance et certains recoupements devront être réexaminés.

Nouvelle réglementation pour l'administration fédérale

Compte tenu de ce qui précède, le service spécialisé de la Confédération pour la sécurité de l'information n'aura aucun pouvoir d'exécution au niveau transversal. En revanche, le Conseil fédéral pourra lui attribuer d'autres compétences pour l'administration fédérale et définir de manière différenciée ses relations avec les responsables hiérarchiques et les préposés à la sécurité de l'information. Bien que la hiérarchie reste en principe responsable de l'édiction et de l'application des prescriptions, une forte majorité des participants aux travaux s'est prononcée en faveur d'un renforcement des compétences d'exécution du service spécialisé, notamment en matière d'audits. Le Conseil fédéral étudiera l'organisation de la sécurité de l'information au sein des unités décentralisées de l'administration fédérale soumises à la loi et des organisations au sens de l'art. 2, al. 4, LOGA dans le cadre de la législation d'exécution. La LSI prévoit toutefois que le Conseil fédéral leur ménagera une autonomie suffisante.

1.3 Appréciation de la solution retenue

Le dispositif proposé est détaillé au ch. 1.2. L'accent est mis ci-après sur les autres solutions étudiées et sur les avantages et inconvénients de la solution retenue.

1.3.1 Autres solutions étudiées

Acte unique

Les bases légales de la Confédération relatives à la protection des informations sont conçues de façon très sectorielle: elles ne sont guère harmonisées et présentent souvent des lacunes. De plus, elles ne répondent pas aux besoins d'une société de l'information. La dimension sectorielle complique la gestion des affaires politiques et opérationnelles liées à la protection des informations. Les compétences étant réglées en fonction des domaines spécialisés, les besoins de coordination se sont fortement accrus. Dès lors, toutes les mesures que la Confédération doit prendre pour protéger les informations doivent être regroupées en un acte unique. Cette approche intégrale correspond aux normes internationales.

On a étudié la possibilité de créer une loi autonome pour les CSP et les PSE. Cette solution aurait pour avantage que les mesures générales de sécurité de l'information (chap. 2 de la loi) auraient plus de poids par le nombre de dispositions qu'elles occupent. On a toutefois renoncé à cette voie car tant les CSP que les PSE sont aujourd'hui des mesures de sécurité de l'information et parce qu'elles dépendent des réglementations sur la classification, sur les catégories de sécurité des moyens informatiques et sur les zones de sécurité. De plus, il faudrait définir de nouvelles compétences et responsabilités, ce qui compliquerait la coordination des points de vue juridique et organisationnel.

On a aussi envisagé de compléter ou d'adapter des lois en vigueur (par ex. la LOGA, la LParl, la LAAM, la LPers, etc.), ce qui aurait permis de renoncer à une nouvelle loi. La solution présente toutefois des inconvénients majeurs. Toutes les lois à adapter n'ont qu'un champ d'application très sectoriel, ce qui empêcherait pratiquement toute exécution globale. Les lacunes constatées ne pourraient être comblées qu'au prix d'efforts de coordination disproportionnés ou ne pourraient tout simplement pas être éliminées. Dans la pratique, cette option empêcherait également l'application transversale de critères et de mesures uniformes. Le Conseil fédéral a par conséquent très rapidement rejeté cette solution.

La sécurité de l'information (y compris les CSP et les PSE) est très étroitement liée à la protection des objets, actuellement couverte par diverses dispositions légales aménagées de manière relativement hétéroclite et traitant la matière de façon disparate. L'analyse a montré qu'une certaine harmonisation de ces dispositions ou la création d'une base légale uniforme serait souhaitable, mais qu'elle dépasserait le cadre de la LSI en raison de sa portée matérielle et organisationnelle. Le projet comporte néanmoins deux dispositions sur la protection physique.

On a également renoncé à définir des éléments matériels constitutifs d'infractions. Les dispositions du CP et du CPM sur la protection du secret de fonction et sur la

protection des informations classifiées ou sensibles de la Confédération ne doivent pas être révisées de façon accessoire dans le cadre d'une loi d'organisation particulière, mais par un projet législatif séparé.

Champ d'application

Champ d'application matériel

Le projet couvre toutes les informations et vise à les protéger en fonction de leurs besoins de confidentialité, de disponibilité, d'intégrité et de traçabilité. Le champ d'application matériel exhaustif correspond aux connaissances scientifiques les plus récentes et à la pratique. Une limitation aux informations sensibles ne serait pas judicieuse. L'appréciation du caractère sensible d'une information présuppose en effet des critères et des mécanismes d'évaluation qui doivent nécessairement s'appliquer à toutes les informations. De plus, on ne pourrait obtenir l'efficacité accrue et les synergies attendues qui constituent l'objectif de la standardisation des mesures envisagée.

Champ d'application institutionnel

Les raisons pour lesquelles toutes les autorités de la Confédération doivent être soumises à la loi sont exposées en détail au ch. 1.2.2. Une limitation à l'administration fédérale et à l'armée réduirait considérablement l'étendue de la LSI, car le Conseil fédéral serait alors seul compétent pour l'exécution. En revanche, elle ne comblerait pas les lacunes au niveau transversal. De plus, les autres autorités fédérales ne pourraient bénéficier d'importantes ressources de l'administration fédérale (par ex. CSP ou PSE). L'objectif de garantir un niveau de sécurité homogène ne pourrait être atteint qu'au prix de lourdes charges administratives. Pour ces raisons, le Conseil fédéral juge que le champ d'application élargi assorti d'une exécution décentralisée est la solution la plus efficace et la plus économique.

Classification

Le Conseil fédéral a rejeté un autre modèle de classification à deux échelons pour deux raisons: d'une part, le modèle à trois échelons permet de faciliter la collaboration avec des partenaires étrangers et internationaux, qui connaissent pour la plupart un système à quatre échelons; d'autre part, il garantit une protection de ses propres informations qui soit davantage en adéquation avec le risque. On a également rejeté la classification des données personnelles ou des secrets d'affaire et de fabrication, soit parce que les critères de classification sont fixés par la législation sectorielle (LPD), soit parce qu'ils doivent être convenus avec les propriétaires des informations.

On s'est encore demandé si l'on ne devait pas réserver en principe à des ressortissants suisses le traitement d'informations de la Confédération classifiées «secret». De telles limitations sont habituelles dans le contexte international. Le Conseil fédéral y a toutefois renoncé étant donné que les autorités de la Confédération sont aussi tributaires, dans le domaine de la sécurité, de spécialistes étrangers.

Systèmes de gestion des données d'identification

On a envisagé de renoncer à l'utilisation du numéro AVS. Le Conseil fédéral reste toutefois convaincu que la solution proposée reste la plus économique et la plus simple tout en permettant une protection des données au moins équivalente.

CSP

Le Conseil fédéral estime que la réglementation proposée répond mieux aux besoins actuels de la sécurité de l'information et permet simultanément de réduire significativement le nombre des CSP, et partant les coûts financiers et les charges de personnel. On a envisagé de ne plus autoriser de CSP en Suisse que pour le traitement d'informations classifiées «secret», pour la gestion et l'exploitation de moyens informatiques de la catégorie «protection très élevée» et pour l'accès aux zones de sécurité correspondantes, tout en aménageant la possibilité de procéder à des CSP pour l'accès à des informations étrangères classifiées «confidentiel». Une procédure analogue s'appliquerait au contrôle de loyauté au sens de la LPers et de la LAAM. Cette solution réduirait encore les charges, mais elle a été abandonnée parce qu'elle constituerait une exception dans le contexte international et qu'elle contredirait l'harmonisation visée en matière de coopération internationale.

PSE

Le Conseil fédéral juge que la réglementation proposée permet de mener des PSE de manière ciblée et non bureaucratique. Les charges afférentes seront limitées au strict nécessaire.

Comme pour les CSP, on a envisagé de ne plus mener de PSE en Suisse que pour le traitement d'informations classifiées «secret», pour la gestion et l'exploitation de moyens informatiques de la catégorie «protection très élevée» et pour l'accès aux zones de sécurité correspondantes, tout en étendant le champ d'application dans le contexte international. Cette solution a été écartée pour les mêmes raisons que pour les CSP.

On a également étudié la possibilité que l'évaluation du service spécialisé PSE ne lie pas l'adjudicateur. Ce système correspondrait au régime appliqué aux CSP. Il aurait pour avantage de laisser l'entière responsabilité de l'attribution du mandat à l'adjudicateur, qui pourrait ainsi prendre des risques plus importants. Cette solution n'a pas été retenue pour diverses raisons. Premièrement, la DSE est un «sceau de sécurité» officiel qui doit être l'apanage d'une autorité nationale de sécurité. On ne peut garantir l'intégrité de ce sceau que si la décision est prise par des spécialistes. Deuxièmement, contrairement au CSP, la PSE ne prend pas fin après l'inspection de l'entreprise mais s'étend au contrôle de l'application des mesures. Si l'adjudicateur n'était pas lié par l'évaluation, ces pouvoirs de contrôle seraient sans objet. Troisièmement, dans la pratique, il est rare qu'une entreprise soit déclarée problématique sous l'angle de la sécurité. Dans un cas exceptionnel de cette nature, on doit pouvoir s'assurer que l'entreprise n'exercera aucun mandat sensible pour la Confédération.

Infrastructures critiques

Les raisons pour lesquelles on a renoncé à des prescriptions et obligations de déclaration centralisées pour les infrastructures critiques sont exposées dans la SNPC.

Exécution

Le champ d'application institutionnel ne doit pas limiter l'indépendance que la Constitution garantit aux autorités concernées. C'est pourquoi les autorités fédérales sont chargées de l'exécution de la LSI, le projet prévoyant par ailleurs divers instruments visant à garantir des prescriptions et mesures homogènes. L'exécution en toute autonomie présente un désavantage: les exigences minimales en matière d'organisation, qui valent pour toutes les autorités de la Confédération, doivent impérativement être consignées au niveau de la loi. Le projet comporte dès lors diverses dispositions qui relèvent généralement plutôt du niveau de l'ordonnance.

On a également envisagé une délégation de compétences législatives transversales à l'Assemblée fédérale (ordonnance du Parlement) ou au Conseil fédéral. Une délégation de cette nature permettrait de transférer de nombreuses dispositions au niveau de l'ordonnance, ce qui allégerait d'autant le projet. Les autorités fédérales concernées se sont toutefois opposées dans le cadre des diverses consultations à toute subordination au droit d'exécution d'une autre autorité. On a renoncé pour la même raison à un organe de pilotage transversal habilité à donner des instructions. La solution de l'exécution décentralisée garantit l'indépendance constitutionnelle des diverses autorités de la Confédération. Elle permet une exécution souple, adaptée aux risques et conforme aux besoins de sécurité de chaque autorité. De l'avis du Conseil fédéral, les avantages de la solution proposée l'emportent largement sur ses inconvénients.

Organisation

L'organisation proposée améliore le professionnalisme dans le domaine de la sécurité de l'information, définit clairement les compétences et respecte le principe de l'exécution décentralisée. Elle repose pour l'essentiel sur des structures et des organes existants, qui seront regroupés pour partie et qui seront chargés de tâches répondant aux exigences de la société de l'information. Renoncer à ces organes, notamment au service spécialisé de la Confédération pour la sécurité de l'information, entraverait considérablement une mise en œuvre efficace et uniforme de la loi. Les autorités et organisations soumises à la loi devraient en outre développer leurs propres capacités (par ex. cryptologie et audits techniques) alors que celles-ci devraient plutôt être disponibles au niveau central pour des raisons économiques.

1.3.2 Procédure de consultation

Avis exprimés dans le cadre de la procédure de consultation

Le 26 mars 2014, le Conseil fédéral a adopté l'avant-projet de loi sur la sécurité de l'information et a ouvert la procédure de consultation, qui s'est achevée le 4 juillet 2014.

Le DDPS à invité 62 destinataires à s'exprimer; il a reçu 55 réponses au total (26 cantons, 4 partis politiques, 24 organisations et autres milieux concernés).

La plupart des participants à la consultation approuvent dans son principe une loi sur la sécurité de l'information. Certains participants ont toutefois exprimé des réserves

sur divers points de l'avant-projet. Seul un parti (l'UDC) l'a rejeté dans sa totalité. Un canton et une association faîtière suisse de l'économie pourraient éventuellement souscrire au projet moyennant une révision substantielle de certains aspects réglementaires ou des documents annexes.

Les améliorations souhaitées concernaient notamment:

- la collaboration entre la Confédération et les cantons;
- la réglementation relative aux infrastructures critiques;
- les conséquences financières pour la Confédération et les cantons.

Adaptation du projet mis en consultation

Le 5 novembre 2014, le Conseil fédéral a pris connaissance des résultats de la procédure de consultation[22] et chargé le DDPS d'élaborer un message.

Les principales modifications apportées au projet mis en consultation sont présentées ci-après.

- La réglementation de la collaboration entre la Confédération et les cantons se fonde désormais sur la législation sur la protection des données. De plus, les cantons seront étroitement associés à l'élaboration des dispositions d'exécution et des normes. Par ailleurs, ils seront représentés au sein de la Conférence des préposés à la sécurité de l'information et ils pourront bénéficier des conseils et de l'assistance du service spécialisé de la Confédération pour la sécurité de l'information. Enfin, le Conseil fédéral pourra autoriser les cantons à recourir pour leurs propres besoins aux prestations des services spécialisés prévus par le projet.
- Les dispositions relatives aux infrastructures critiques ont été revues, notamment la réglementation du traitement des données.
- La LSI a été complétée d'une section consacrée aux systèmes d'information concernant la gestion centralisée des données d'identification.
- La protection pénale du secret de fonction au sens de l'art. 320 CP et du secret de service au sens de l'art. 77 CPM a été élargie aux personnes auxiliaires externes. Étant donné que ni la Confédération ni les cantons ne peuvent se passer à l'heure actuelle de prestations informatiques externes, le Conseil fédéral estime que cette extension doit entrer en vigueur rapidement.
- Quelques dispositions ont été adaptées de manière à garantir uen marge de manœuvre des autorités soumises à la présente loi, en particulier du Conseil fédéral, s'agissant des coûts de mise en œuvre et de l'organisation.

Enfin, on a procédé à de nombreuses simplifications., Les compléments et précisions apportés ont permis de tenir compte de quantité de remarques.

22 www.admin.ch > Droit fédéral > Procédures de consultation > Procédures de consultation terminées > 2014 > DDPS > Loi fédérale sur la sécurité des informations

1.3.3 Appréciation générale

La sécurité de l'information a récemment fortement gagné en importance, y compris sur le plan politique. De nombreux incidents et les évolutions au niveau international ont montré que notre société est devenue très vulnérable en raison de la dépendance croissante vis-à-vis de l'informatique. L'obligation pour la Confédération de mieux se protéger des nouvelles menaces n'est pas contestée au niveau politique. Il s'agit finalement de garantir l'accomplissement de tâches fondamentales telles la sûreté intérieure et extérieure, la défense des intérêts économiques, financiers et monétaires de la Suisse et la préservation de la capacité de décision et d'action des autorités fédérales. Le Conseil fédéral juge qu'il crée par le présent projet un cadre légal formel équilibré et ciblé pour une sécurité de l'information moderne au sein de la Confédération, ce que les résultats de la procédure de consultation confirment dans leur majorité. Les souhaits les plus importants exprimés par les participants à la consultation, notamment ceux des cantons, ont été pris en compte.

1.4 Comparaison avec le droit étranger, notamment européen

Généralités

Face aux développements dans le domaine informatique, la plupart des États limitrophes de la Suisse et les organisations internationales avec lesquelles la Suisse entretient des relations étroites revoient leurs prescriptions en matière de sécurité. Il n'est pas possible d'offrir une vue d'ensemble de ces travaux. Par ailleurs, les réglementations dans ce domaine sont souvent difficilement accessibles. Les réglementations et prescriptions de quelques pays européens font l'objet d'une analyse comparative de certains aspects regroupés par thème. Les États suivants ont été retenus: l'Allemagne, la France, l'Italie et l'Autriche en tant que voisins directs de la Suisse, auxquelles s'ajoutent le Royaume-Uni, les Pays-Bas et la Suède. Quant aux points étudiés, ils concernent en particulier la nature de la réglementation en matière de sécurité de l'information et son champ d'application institutionnel, le système de classification, le CSP, la PSE et l'organisation des autorités.

Nature de la réglementation de la sécurité de l'information

L'Allemagne règle les principes de la sécurité de l'information au niveau de la loi, par le biais de prescriptions et de directives administratives exhaustives. En France, divers actes règlent le domaine de la sécurité de l'information aux niveaux de la constitution, de la loi et de l'ordonnance. En Italie, celui-ci est régi par une loi, deux décisions du premier ministre et des directives de l'autorité nationale de sécurité. Aux Pays-Bas, la sécurité de l'information est réglée dans plusieurs textes aux niveaux les plus divers. Plusieurs lois suédoises comportent des règles de sécurité de l'information, mais aucun acte ne traite de la sécurité industrielle. L'Autriche ne dispose pas d'une réglementation homogène qui couvrirait l'ensemble du domaine de la sécurité de l'information. La loi autrichienne sur la sécurité de l'information règle toutefois la classification et les CSP. Au niveau des provinces, on ne trouve que des dispositions du droit de la fonction publique, par exemple à propos du secret

de fonction. Au Royaume-Uni, on ne trouve pas non plus de législation spéciale sur la sécurité de l'information, mais plusieurs textes constituent une base. Les directives de la politique nationale de sécurité sont précisées dans le *Security Policy Framework*, qui définit les conditions auxquelles l'administration, le gouvernement, les autorités et les adjudicateurs sont tenus de répondre.

L'UE règle la protection de ses informations classifiées de façon presque exhaustive. Tant la décision 2013/488/UE que la décision (UE, Euratom) 2015/444[23] règlent la classification et la protection du secret au niveau du personnel (y compris les CSP) et sur le plan matériel, la sécurité informatique et la protection du secret dans le domaine industriel. En ce qui concerne la sécurité technique de l'information, on citera également le règlement nº 526/2013[24].

Champ d'application institutionnel

En Allemagne, les autorités fédérales et les établissements relevant directement de l'État fédéral sont soumis à la réglementation. Parallèlement, on y trouve des directives applicables aux entreprises chargées de traiter des informations classifiées (*Verschlusssachen* ou *VS*). En France, une réglementation de la protection des informations vaut pour tous les ministères, mais ces derniers peuvent édicter des prescriptions plus détaillées. En Italie, les exigences en matière de sécurité de l'information s'appliquent à l'ensemble des pouvoirs publics, à l'industrie et aux particuliers chargés de traiter des informations classifiées. Les parlementaires, les ministres et les juges qui doivent pouvoir prendre connaissance d'informations classifiées ne sont pas contrôlés. En Autriche, la réglementation s'applique exclusivement aux services de l'État fédéral. L'industrie est tenue de reconnaître et d'appliquer les dispositions du droit fédéral par le biais de conventions de droit privé. Au Royaume-Uni, le *Security Policy Framework* vaut pour tous les services des autorités, les agences et les adjudicateurs traitant des mandats classifiés. Certaines de ses dispositions s'appliquent également aux forces de police. Le *Security Investigation Act* néerlandais vaut pour toutes les unités administratives de même que pour l'industrie. Les prescriptions concernant le traitement d'informations classifiées et la sécurité de l'information ne s'appliquent cependant qu'à l'administration: les dispositions régissant la sécurité industrielle dans le domaine militaire valent pour les entreprises concernées. En Suède, certains actes s'appliquent à toutes les autorités, alors que d'autres ne valent pas pour le gouvernement et le parlement.

Dans l'UE, les prescriptions sont certes largement harmonisées, mais chaque organe indépendant (Parlement, Conseil et Commission) édicte ses propres prescriptions.

23 Décision (UE, Euratom) 2015/444 de la Commission du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne, JO L 72 du 17.3.2015, p. 53.

24 Règlement (UE) nº 526/2013 du Parlement européen et du Conseil du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) nº 460/2004, JO L 165 du 18 juin 2013, p. 41.

Système de classification

La France et le Royaume-Uni connaissent un système de classification à trois échelons, l'Allemagne, l'Italie, l'Autriche et les Pays-Bas un système à quatre échelons. On trouve deux systèmes de classification en Suède: un système à quatre échelons pour le domaine militaire et un système à deux échelons pour les autres autorités.

L'UE connaît les quatre échelons suivants:

- *TRÈS SECRET UE / EU TOP SECRET*: la divulgation non autorisée pourrait causer un préjudice exceptionnellement grave aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres;
- *SECRET UE / EU SECRET*: la divulgation non autorisée pourrait nuire gravement aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres;
- *CONFIDENTIEL UE / EU CONFIDENTIAL*: la divulgation non autorisée pourrait nuire aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres;
- *RESTREINT UE / EU RESTRICTED*: la divulgation non autorisée pourrait être défavorable aux intérêts de l'Union européenne ou d'un ou de plusieurs de ses États membres.

CSP

En Allemagne, les conditions d'un CSP sont l'accès effectif et à court terme ou la possibilité d'un accès à des informations classifiées. Le contrôle est effectué par l'Office fédéral de protection de la constitution, dont l'appréciation est contraignante. En France, la fonction de la personne concernée au sein de l'administration ou de l'économie privée doit figurer sur une liste. L'autorisation de sécurité est délivrée par une autorité donnée en fonction de l'échelon de classification. L'appréciation du risque n'est pas contraignante. En Italie, la demande de CSP doit indiquer les raisons pour lesquelles la personne doit accéder à des informations classifiées et l'échelon de classification. La personne contrôlée doit confirmer qu'elle est informée de la nécessité du CSP et qu'elle y a consenti. La procédure est menée par l'autorité concernée en collaboration avec la police, la police financière, les forces armées et l'administration. L'appréciation est contraignante.

En Autriche, une personne peut être contrôlée à la demande d'une entreprise lorsqu'elle est appelée à assumer une fonction sensible ou à travailler dans un domaine critique pour la sécurité et qu'elle a consenti au CSP. Dans le domaine militaire, l'accès prévu à des informations classifiées est déterminant. Des autorités différentes sont compétentes dans les domaines civil et militaire. Au Royaume-Uni, un CSP est mené pour certifier l'identité d'une personne et évaluer sa loyauté avant de lui donner accès à des informations ou du matériel classifiés ou à des infrastructures nationales critiques. En Suède, l'accès à des informations classifiées est également déterminant. Aux Pays-Bas, les fonctions nécessitant un CSP figurent sur une liste. Chaque ministère définit les fonctions en question, en prenant pour critère le dommage potentiel que la personne revêtant l'une de ces fonctions peut causer. Les CSP

sont menés par le service de renseignement général et le service de renseignement militaire, dont l'appréciation du risque est contraignante.

Dans l'UE, un CSP est mené en cas d'accès à des objets ou informations classifiés CONFIDENTIEL UE / EU CONFIDENTIAL ou à un échelon supérieur. Le contrôle est opéré par l'autorité de sécurité de l'État membre selon le droit interne. Les autorités de l'UE sont liées par la décision de l'autorité nationale de sécurité.

PSE

En Allemagne, la condition d'une PSE est l'attribution concrète d'un mandat classifié confidentiel ou d'un échelon supérieur ou la participation à un appel d'offres classifié aux mêmes échelons. Le Ministère fédéral de l'économie et de l'énergie procède à l'évaluation du risque, dont le résultat lie l'adjudicateur. En France, une PSE présuppose l'existence d'un contrat en vertu duquel l'entreprise doit produire des informations ou du matériel classifiés ou y accéder. L'appréciation du risque n'est pas contraignante. En Italie, il incombe à l'adjudicateur d'ouvrir une PSE s'il confie un mandat classifié «secret» à une entreprise. L'appréciation du risque est contraignante. En Autriche, l'accès prévu à des informations classifiées est déterminant pour une PSE. L'appréciation du risque n'est pas contraignante. Au Royaume-Uni, la condition de l'ouverture d'une PSE est qu'une entreprise traite en un endroit donné des informations ou du matériel classifiés «secret» ou à un échelon supérieur en lien avec un mandat classifié du gouvernement.

Aux Pays-Bas, une PSE est menée lorsqu'une entreprise peut être appelée à exercer un mandat classifié dans le domaine militaire. La procédure est menée par un service du Ministère de la défense. Lorsque l'entreprise peut être désignée pour un mandat international classifié, la procédure est menée par le Ministère de l'intérieur et des territoires d'outre-mer, dont l'appréciation est contraignante. En Suède, le *Protective Security Act* fait obligation aux autorités qui lancent un appel d'offres en lien avec la sécurité nationale de conclure une convention de sécurité écrite avec l'entreprise pressentie. Avant l'adjudication du mandat, l'entreprise doit se soumettre à un audit selon les critères de l'*Industrial Security Manual*. L'agence suédoise de l'armement mène ensuite des contrôles auprès de l'entreprise.

Dans l'UE, une PSE est menée pour les mandats assortis d'un accès à des objets ou informations classifiés CONFIDENTIEL UE / EU CONFIDENTIAL ou à un échelon supérieur. La procédure est régie par les dispositions du droit interne de l'État membre. Les autorités de l'UE sont liées par la décision de l'autorité nationale de sécurité.

Organisation des autorités

En Allemagne, le Ministère fédéral de l'intérieur est l'autorité de sécurité nationale. Le Ministère fédéral de l'économie et de l'énergie est seul compétent en matière de protection du secret dans l'économie. En France, le Secrétaire général de la défense et de la sécurité nationale est la seule autorité de sécurité nationale. La sécurité informatique relève de l'Agence nationale de la sécurité des systèmes d'information. En Italie, le premier ministre est l'autorité de sécurité nationale. Il peut déléguer une partie de ses compétences au secrétaire d'État et il est assisté d'un organe de sécurité nationale dirigé par le directeur général du *Dipartimento Informazioni per la Sicu-*

rezza. En Autriche, on trouve une commission pour la sécurité de l'information dans le domaine civil, alors que l'office de la défense est compétent dans le domaine militaire. Au Royaume-Uni, bien que le *Cabinet Office* soit l'autorité de sécurité nationale, les diverses unités administratives et agences gouvernementales sont responsables, dans leur domaine de compétence, de la sécurité de leurs informations et de celles qu'elles confient à leurs mandataires.

Aux Pays-Bas, on trouve deux autorités de sécurité nationale: l'autorité civile de sécurité nationale est le service général de renseignement et de sécurité rattaché au Ministère de l'intérieur et des territoires d'outre-mer, tandis que l'autorité militaire de sécurité nationale relève du Ministère de la défense. En Suède, il n'existe pas non plus d'autorité de sécurité globale. Les tâches sont réparties entre les forces armées et le Ministère des affaires étrangères (pour les informations classifiées de l'ASE, de l'UE et de l'OTAN). Ce dernier coordonne néanmoins les diverses compétences de manière à ce que toutes les tâches d'une autorité nationale de sécurité soient assurées.

L'UE dispose également de plusieurs autorités de sécurité. Ainsi, en ce qui concerne le Conseil, le Bureau de sécurité du secrétariat général est responsable des règlements techniques de protection des objets et informations classifiés. Pour ce qui est la Commission européenne, la direction de la sécurité assume cette tâche. L'ENISA est compétente pour sa part en matière de sécurité des réseaux et de l'information.

Infrastructures critiques

Le domaine de la sécurité de l'information pour les infrastructures critiques a fait l'objet d'une comparaison exhaustive dans la SNPC, aussi ne la répétera-t-on pas ici en détail. Cependant, depuis l'approbation de la SNPC, l'UE et l'Allemagne ont développé de nouvelles règles succinctement exposées ci-après.

Union européenne

La directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union[25] est entrée en vigueur le 8 août 2016. L'UE considère qu'une infrastructure informatique sûre est nécessaire au fonctionnement fiable du marché intérieur. Pour ce faire, les États membres sont tenus de renforcer leur capacité de défense et leur coopération. De plus, les exploitants d'infrastructures critiques et certains fournisseurs de services numériques (places de marché en ligne, moteurs de recherche en ligne et services d'informatique en nuage) sont tenus de prendre des mesures minimales visant la maîtrise des risques en matière de sécurité et de déclarer les incidents graves aux autorités nationales compétentes. Les exigences de sécurité applicables aux fournisseurs de services numériques sont toutefois moins incisives que celles qui s'appliquent aux exploitants d'infrastructures critiques. Les petites et moyennes entreprises et les administrations publiques sont en principe libérées de ces obligations.

25 JO L 194 du 19.7.2016. p. 1.

La directive impose une série de mesures organisationnelles aux autorités nationales. Ainsi, chaque État membre doit prendre les mesures suivantes:

- adopter une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information;
- désigner une ou plusieurs autorités nationales chargées de contrôler l'application de la directive par les exploitants d'infrastructures critiques et les fournisseurs de services numériques;
- désigner un point de contact national unique pour assurer une coopération transfrontalière entre les États membres;
- désigner un ou plusieurs centres nationaux chargés d'assurer un service national d'alerte précoce et un service d'assistance en matière de sécurité technique de l'information pour les exploitants d'infrastructures critiques et les fournisseurs de services numériques (cf. art. 75 LSI).

La directive fixe en outre des exigences en matière de coopération nationale et internationale et pour les ressources des autorités compétentes.

Les États membres doivent mettre en œuvre la directive dans leur droit national d'ici au mois de mai 2018. Par conséquent, nombre d'entre eux seront contraints d'adapter bientôt leur législation nationale en matière de sécurité de l'information.

Allemagne

La loi allemande du 17 juillet 2015 visant la sécurité renforcée des systèmes techniques d'information (*Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*) vise des objectifs similaires à ceux de la directive de l'UE évoquée plus haut. Elle est toutefois entrée en vigueur avant cette directive. La loi allemande porte en premier lieu sur les infrastructures critiques. Leurs exploitants doivent respecter des exigences minimales en matière de sécurité de l'information et signaler les incidents à l'Office fédéral de la sécurité des technologies de l'information (*Bundesamt für Sicherheit in der Informationstechnik*, BSI). Le BSI exploite les informations collectées et les met à la disposition des exploitants pour leur permettre de mieux protéger leurs infrastructures. Simultanément, le rôle de conseil du BSI a été renforcé dans ce domaine. Les fournisseurs de services de télécommunication sont tenus de garantir la sécurité *conformément aux techniques les plus récentes*. De plus, ils doivent déclarer sans délai certains incidents touchant la sécurité et informer les utilisateurs concernés d'incidents connus.

Contrairement à la directive de l'UE qui exclut les autorités publiques de son champ d'application, la loi allemande assujettit également les autorités fédérales allemandes, à l'exception du *Bundestag* (Diète fédérale allemande).

Résultats de l'analyse de droit comparé

Dans de nombreux pays européens, les bases légales de la sécurité de l'information sont adaptées aux nouvelles réalités de la société de l'information. En raison des ordres juridiques pour partie très hétérogènes et des structures des États, la hiérarchie normative des réglementations en question et leur champ d'application ne peuvent que difficilement être comparés. En revanche, on peut affirmer que les

dispositions de la LSI correspondent globalement aux réglementations des divers États analysés ou qu'elles sont pour le moins coordonnées avec elles. Sur le plan organisationnel, grâce au service spécialisé de la Confédération pour la sécurité de l'information, la Confédération dispose d'un interlocuteur unique au niveau international. La coopération internationale en matière de sécurité de l'information devrait s'en trouver simplifiée et gagner en efficacité.

En revanche, pour ce qui est des infrastructures critiques, le Conseil fédéral est nettement moins exigeant vis-à-vis des exploitants d'infrastructures critiques avec la SNPC et la LSI que ne le sont l'UE ou l'Allemagne. Le Conseil fédéral compte sur la responsabilité des exploitants et sur une assistance ciblée de la Confédération en fonction des besoins. Il n'entend donc pas fixer d'exigences minimales pour les infrastructures critiques ni obliger leurs exploitants à signaler les incidents graves.

1.5 Mise en œuvre

La réglementation de l'exécution par les autorités soumises à la présente loi est exposée au ch. 1.2.9. Celles-ci exécutent la loi en toute autonomie et édicteront les dispositions d'exécution nécessaires. Toutefois, les dispositions d'exécution du Conseil fédéral s'appliqueront aux autres autorités fédérales aussi longtemps qu'elles n'auront pas édicté leurs propres dispositions (subsidiarité). Ce principe a été convenu avec les autorités concernées.

Dans le cadre de la procédure de consultation, on s'est demandé si l'avant-projet était exécutable au niveau cantonal. Certains participants ont notamment regretté que les critères d'application du projet aux cantons fussent peu clairs, et partant que les conséquences pour ces derniers n'étaient guère prévisibles. La collaboration avec les cantons a dès lors été revue en s'inspirant du modèle éprouvé de la législation sur la protection des données (cf. art. 37 LPD). La plupart des autres souhaits des cantons ont également été pris en compte (participation à l'élaboration des dispositions d'exécution, accès aux ressources de la Confédération pour les CSP, conseils du service spécialisé de la Confédération pour la sécurité de l'information, etc.; cf. ch. 1.2.2).

Sur le plan pratique, le service spécialisé de la Confédération pour la sécurité de l'information préparera les projets de dispositions d'exécution et de normes et les soumettra à la Conférence des préposés à la sécurité de l'information en lui demandant d'en examiner l'efficacité, l'économicité et l'applicabilité. Les propositions consolidées seront ensuite approuvées par le Conseil fédéral. Les autorités fédérales et les cantons devront être consultés à propos de toutes les dispositions importantes et susceptibles d'engendrer des coûts. On pourra ainsi atteindre un degré de sécurité aussi homogène que possible et répondre à satisfaction aux besoins de toutes les autorités fédérales et des cantons.

Pour certains points de la réglementation, le droit d'exécution sera édicté rapidement et sans complications. Cela concerne avant tout le CSP (chap. 3), la PSE (chap. 4) et la sécurité de l'information dans les infrastructures critiques (chap. 5), mais également les systèmes d'information concernant le contrôle centralisé des données d'identification (chap. 2, sect. 6). En revanche, l'exécution des mesures générales de

sécurité de l'information (chap. 2) nécessitera d'autres éclaircissements: il s'agit en effet de processus essentiels et d'exigences qui devront être adaptées aux connaissances scientifiques et techniques les plus récentes et être harmonisées entre toutes les autorités concernées.

La LSI prévoit suffisamment de temps pour une mise en œuvre raisonnable. Le Conseil fédéral n'entend la mettre en vigueur que lorsque les dispositions d'exécution et autres bases nécessaires seront prêtes. Une mise en vigueur par étapes reste possible. Le Conseil fédéral entend vérifier périodiquement l'efficacité du projet et faire rapport aux commissions de surveillance compétentes. Il incombe aux cantons de mener leurs propres contrôles.

2 Commentaire des dispositions

2.1 Loi sur la sécurité de l'information

Titre

L'acte ne constitue pas une loi générale sur la sécurité de l'information. Il concerne au premier chef les autorités fédérales et certaines organisations de droit public ou privé effectuant des tâches dévolues à la Confédération. Il peut aussi s'appliquer à des tiers lorsque ceux-ci traitent des informations de la Confédération ou utilisent ses moyens informatiques. Cet effet sur les tiers ne se concrétise cependant que par l'application par une autorité ou une organisation de la Confédération des dispositions concernées.

La notion de *sécurité de l'information* repose, en principe, sur les normes techniques reconnues. La sécurité de l'information englobe donc toutes les exigences et mesures visant à protéger la confidentialité, l'intégrité, la disponibilité et la traçabilité des informations, de même que la disponibilité et l'intégrité des moyens informatiques (cf. art. 6). Elle ne doit pas être réduite à la sécurité informatique, parce qu'elle englobe toutes les procédures de traitement, documents papier et déclarations orales comprises, et non le traitement électronique uniquement. La sécurité de l'information couvre également la sécurité des données au sens de l'art. 7 LPD ou d'autres lois imposant une protection de l'information.

L'intégration au projet du CSP et de la PSE signifie que les deux instruments sont des mesures *particulières* de la sécurité de l'information. Les motifs justifiant la réalisation de ces contrôles découlent des mesures générales de sécurité de l'information.

Préambule

Cf. ch. 5.1.

Chapitre 1 Dispositions générales

Art. 1 But

L'al. 1 dispose que la loi porte non seulement sur les informations en tant que telles, mais également sur les moyens informatiques. La notion d'*information* n'est pas définie car elle correspond à son acception dans le langage courant. La loi ne fait pas non plus de différence fondamentale entre *informations* et *données*: les deux notions sont regroupées dans celle d'*informations*. La loi ne recourt à la notion de données que dans le cas de données personnelles au sens de la LPD. La notion de *moyens informatiques* est définie à l'art. 5.

Al. 2: la sécurité n'est pas une fin en soi. La protection des informations sert certains intérêts publics ou des intérêts de la Confédération en sa qualité d'institution. Ce sont donc les intérêts de la Confédération et de la Suisse qui sont protégés en priorité, et non ceux de tiers. Une liste exhaustive énumère ces intérêts (let. a à e). La liste s'inspire, pour l'essentiel, de celle de l'art. 7, al. 1, LTrans, qui précise les domaines dans lesquels le droit d'accès à des documents officiels peut être limité, différé ou refusé. La liste de l'art. 1, al. 2, LSI n'est toutefois pas entièrement identique à celle de la LTrans car le but et le champ d'application de cette dernière diffèrent de ceux de la LSI (cf. ch. 1.2.3).

La présente loi protège les intérêts présentés ci-après.

- La protection, par des mesures de sécurité de l'information, de la capacité des autorités fédérales à décider et à agir (let. a) est l'un des intérêts centraux de la présente loi. Dans l'accomplissement de leurs tâches constitutionnelles et légales, les autorités fédérales dépendent de plus en plus de la disponibilité, de l'intégrité et, dans certains cas, de la confidentialité de leurs informations, de même que du bon fonctionnement de l'infrastructure informatique (cf. art. 7, al. 1, let. a et b, LTrans et ch. 2.2.2.1.1 et 2.2.2.1.2 MCF LTrans).
- La défense des intérêts visés à la let. b concerne en priorité la protection des informations émanant de la police, des douanes, des services de renseignement et de l'armée, de même que des services chargés de l'approvisionnement du pays, ainsi que des moyens engagés par les autorités fédérales pour assurer la sûreté intérieure et extérieure du pays. De telles informations présentent souvent un haut besoin de confidentialité dans la mesure où leur utilisation abusive peut représenter une menace existentielle pour l'État, la population et certains individus ou groupes de personnes. La même raison justifie que les moyens informatiques des autorités engagés pour appuyer les tâches critiques liées à la sécurité doivent être continuellement disponibles et fonctionnels en temps de crise (cf. art. 7, al. 1, let. c, LTrans et ch. 2.2.2.1.3 MCF LTrans).
- Les relations extérieures (let. c), tout comme les questions de sécurité, comptent parmi les domaines sensibles des activités de l'État. L'objectif principal à cet égard est de préserver la confidentialité des informations. L'acquisition d'informations sur la situation et les événements à l'étranger ainsi que sur les intentions des autorités étrangères ou internationales revêtent, en particulier, une grande importance pour la conduite de la politique

étrangère et pour l'entretien des relations extérieures. Un point décisif du succès de toute négociation est de ne pas porter à la connaissance des autres parties ou du public les stratégies poursuivies et les intentions qui les sous-tendent. Il en va de même des processus diplomatiques dans les rapports entre États. Enfin, il faut mentionner que la Suisse peut être tenue, sur la base de traités internationaux ou de pratiques étatiques reconnues, de ne pas publier certains documents émanant de l'étranger (cf. art. 7, al. 1, let. d, LTrans et ch. 2.2.2.1.4 MCF LTrans).

– Let. d: la communication non autorisée ou la falsification de certaines informations et la perturbation des systèmes d'information des autorités fédérales peuvent porter un préjudice considérable aux intérêts économiques, financiers et monétaires de la Suisse. La concurrence internationale étant sans merci, ces intérêts économiques gagnent en importance (cf. art. 7, al. 1, let. f, LTrans et ch. 2.2.2.1.6 MCF LTrans).

– La let. e concerne le domaine de la conformité (*compliance*), c'est-à-dire celui de l'accomplissement des obligations légales et contractuelles des autorités fédérales en matière de protection des informations qui ne relèvent pas des let. a à d. Dans l'accomplissement de leurs tâches légales, les autorités fédérales traitent en effet un très grand nombre d'informations qu'elles doivent protéger en vertu des dispositions légales les plus variées (par ex. LPD, LOGA, LParl, LBN, LMP, LFC, etc.) ou qu'elles ont obtenues de tiers à la condition expresse d'assurer une protection appropriée. Les secrets professionnels, d'affaires et de fabrication ou la préservation de la confidentialité et de l'intégrité des données personnelles ne comptent pas parmi les intérêts directs de la Confédération. Cependant, la loi ou des conventions font obligation à la Confédération de protéger ces informations. S'il devait être établi que les autorités fédérales ne respectaient pas leur devoir de protection, la confiance dont elles bénéficient en pâtirait sérieusement et leur responsabilité pourrait être engagée. La let. e couvre donc toutes les informations que les autorités fédérales traitent et doivent protéger, sans nécessairement classifier les informations concernées. Elle protège aussi l'intérêt des autorités fédérales à préserver le haut degré de de confiance dont elles bénéficient (cf. art. 7, al. 1, let. e, g et h, LTrans et ch. 2.2.2.1.5, 2.2.2.1.7 et 2.2.2.1.8 MCF LTrans).

Art. 2 Autorités et organisations concernées

Les autorités soumises à la présente loi au sens de l'al. 1 sont l'Assemblée fédérale, c'est-à-dire les Chambres fédérales, le Conseil fédéral, les tribunaux fédéraux (Tribunal fédéral, Tribunal pénal fédéral, Tribunal administratif fédéral, Tribunal fédéral des brevets, de même que les tribunaux militaires, les tribunaux militaires d'appel et le Tribunal militaire de cassation), le Ministère public de la Confédération et son autorité de surveillance et, dans l'intérêt de la politique monétaire et économique de la Confédération, la Banque nationale suisse. Dans les activités qu'elles déploient en leur qualité d'autorité, ces institutions ne reçoivent pas directement d'instructions de la part d'une autre autorité. Néanmoins, en raison du flux d'informations qu'elles échangent, elles sont tenues d'appliquer la présente loi dans leur propre domaine de

compétence organisationnelle. Dans la mesure où la loi contient des délégations de compétence, elle se réfère toujours à ces autorités en les désignant par *autorités soumises à la présente loi*. Les raisons pour lesquelles toutes les autorités fédérales sont soumises à la loi sont exposées au ch. 1.2.2.

Il va de soi que la LSI doit tenir compte, dans certaines dispositions, du statut constitutionnel et des particularités des diverses autorités et institutions. Elle prévoit ainsi des exceptions à l'obligation d'un CSP pour les personnes élues par le peuple, de même que des exceptions pour certaines compétences d'exécution, en particulier dans le domaine des tribunaux fédéraux. Lorsque les obligations ne s'appliquent qu'à certaines autorités ou organisations, la loi les nomme expressément (cf. par ex. art. 7 ou 10, al. 2). La loi ne précise pas toute la structure que les diverses autorités doivent mettre en place pour l'exécution ni l'ensemble des compétences de leurs organes ou services: la législation d'exécution des diverses autorités y pourvoira.

L'al. 2 prend en compte le fait que les autorités mentionnées à l'al. 1 n'assument que dans une mesure marginale leurs propres tâches d'exécution et que les organisations qui leur sont subordonnées doivent être elles-mêmes directement tenues d'appliquer la loi dans leur domaine de compétence. La répartition entre les autorités et les organisations qui leur sont subordonnées doit, en particulier, garantir que le droit administratif spécifique à chaque autorité énumérée ne soit pas perturbé par la nouvelle réglementation. Les autorités soumises à la loi ne doivent pas assumer elles-mêmes des tâches d'exécution mineures; quant aux organisations énumérées, elles ne peuvent endosser de compétences législatives ou décisionnelles qui dépassent les dispositions organisationnelles auxquelles elles sont soumises. Les organisations concernées sont en particulier les Services du Parlement et les administrations des tribunaux fédéraux, des départements, de la ChF et de l'armée et l'administration fédérale, y compris ses unités décentralisées au sens de l'art. 2, al. 3, LOGA.

Les organisations de droit public ou privé qui assument des tâches administratives de la Confédération au sens de l'art. 2, al. 4, LOGA (cf. à ce sujet l'art. 8, al. 4 et 5, LOGA) sont en principe également soumises à la présente loi. Il s'agit notamment d'organisations qui, en vertu de la loi, sont habilitées à donner des instructions à des particuliers. La Confédération est responsable des organisations de cette nature à titre subsidiaire (cf. art. 19 LRCF). L'application de la loi aux unités administratives décentralisées et aux organisations externes chargées de tâches de la Confédération n'est pas absolue. Étant donné que leurs rapports avec la Confédération sont pour partie très hétérogènes en raison des actes organisationnels qui les régissent, les soumettre à la loi ne se justifie que lorsqu'elles peuvent représenter un risque de sécurité pour la Confédération. L'al. 3 précise ces cas, à savoir lorsqu'elles accomplissent des tâches sensibles de la Confédération, lorsqu'elles ont recours des moyens informatiques de la Confédération ou lorsque leurs moyens informatiques sont fortement interconnectés avec ceux de la Confédération. Le Conseil fédéral évaluera le risque pour la sécurité de chacune des organisations dans le cadre de la législation d'exécution et définira au niveau de l'ordonnance si elles sont soumises pour tout ou partie à la LSI. Il pourra le faire dans la législation d'exécution de la LSI ou dans les dispositions d'exécution de lois spéciales. En cas de nécessité, le Conseil fédéral pourra autoriser les organisations en question à appliquer une partie seulement de la loi (par ex. les dispositions concernant la classification, la sécurité

des moyens informatiques ou le CSP). Il décidera également à cet égard, en vertu de l'al. 4, dans quelle mesure ces organisations devront exécuter la loi de façon autonome. Une organisation exclue du champ d'application de la LSI est considérée comme un tiers.

L'al. 5 précise à titre liminaire que le soutien aux exploitants d'infrastructures critiques est régi par les dispositions du chap. 5. Quiconque exploite des infrastructures critiques à l'extérieur de la Confédération peut conclure sur une base volontaire un partenariat avec la Confédération et solliciter dans ce cadre un soutien, raison pour laquelle les articles concernés s'appliquent aux exploitants d'infrastructures critiques sans qu'il n'en résulte pour autant une obligation quelconque. Il va de soi que la LSI s'applique sans restriction aux infrastructures critiques exploitées par la Confédération elle-même. Grâce à la LSI, la Confédération se dote d'instruments spécifiques en matière de sécurité de l'information qu'elle met à la disposition de certains régulateurs et exploitants d'infrastructures critiques . Les CSP suscitent un intérêt particulier, mais parfois également certaines dispositions relatives à la classification ou à la sécurité des moyens informatiques. Certains exploitants d'infrastructures critiques utilisent déjà ces instruments de la Confédération, par exemple les centrales nucléaires pour lesquelles la Confédération prescrit des mesures de sécurité de l'information (cf. art. 5 et 24 LENu). La LSI dispose dès lors qu'en cas de nécessité la législation spéciale peut soumettre certains exploitants d'infrastructures critiques à la LSI ou à une partie de ses dispositions.

Art. 3 Application de la loi aux cantons

Pour la collaboration avec les cantons, on se référera au ch. 1.2.2;. pour ce qui est des CSP pour les employés des cantons, aux art. 30 et 32; et pour l'exécution par les cantons, à l'art. 87.

Art. 4 Rapport avec d'autres lois fédérales

Pour le rapport avec la LTrans et la législation sur la protection des données, cf. ch. 1.2.3. L'al. 1 dispose que la LTrans prime la LSI et qu'elle n'est aucunement limitée par la LSI. L'al. 2 règle le rapport du nouvel acte avec les nombreuses lois fédérales qui imposent des exigences en matière de protection de la confidentialité, de la disponibilité, de l'intégrité ou de la traçabilité des information, ou en matière de disponibilité et d'intégrité des moyens informatiques. L'application à titre complémentaire des dispositions de la LSI signifie qu'elle crée un cadre uniforme à l'évaluation du besoin de protection lié à ces informations et à la mise en œuvre des exigences de sécurité fixées par les lois spéciales pour ces informations.

Art. 5 Définitions

Quelques notions ou expressions importantes pour le projet ne peuvent être définies plus précisément dans la loi, car elles limiteraient trop fortement la marge de manœuvre des autorités, organisations et services concernés. Il s'agit notamment des expressions *nuire*, *nuire considérablement* et *nuire gravement* aux intérêts définis à l'art. 1, al. 2.

Let. a: l'expression *moyen informatique* est utilisée comme notion générique pour tous les moyens des techniques de l'information et de la communication. On utilisera et définira si nécessaire au niveau de l'ordonnance et des directives d'autres notions plus précises (par ex. système d'information, réseau, application, communication vocale, téléphonie, etc.). Un moyen informatique peut regrouper plusieurs systèmes ou moyens en une unité fonctionnelle.

Let. b: l'*activité sensible* est une notion centrale de la loi. L'exercice d'une activité de cette nature est la condition non seulement de l'application de la loi aux organisations visées à l'art. 2, al. 3 et 4, LOGA, mais également des CSP et des PSE. Elle est strictement définie dans le contexte de la sécurité de l'information au sens de la présente loi.

- L'adoption de l'échelon de classification «confidentiel» comme point de départ pour la définition d'une activité sensible (ch. 1) implique que le caractère sensible d'une activité n'est admis que si les intérêts visés à l'art. 1, al. 2, peuvent, pour le moins, subir un préjudice *considérable*. De plus, la notion de sensibilité ne s'applique pas à l'*accès* à ces informations, mais à leur *traitement* effectif et justifié. En d'autres termes, en prenant pour exemple le personnel de nettoyage, celui-ci n'exerce généralement pas une activité sensible au sens de la présente loi, bien que la probabilité soit élevée qu'il puisse parfois accéder pendant ses travaux à des informations classifiées dès lors que certains collaborateurs ne respectent pas toujours les prescriptions de sécurité. L'utilisation du *matériel classifié* à partir de l'échelon «confidentiel» n'est pas expressément mentionnée mais elle est implicitement comprise. Le matériel ne doit pas être confondu avec le *support d'information* qui contient l'information immatérielle à de multiples fins. On entend par matériel classifié des appareils et des objets dont les propriétés permettent de diffuser des informations classifiées: le matériel *est* ou *contient de manière indissociable* les informations (immatérielles) qui doivent être protégées. Il s'agit avant tout de biens d'armement et de systèmes intégrés de communication du domaine militaire. Il est fréquent qu'un État tiers qui en a autorisé la livraison à la Suisse exige leur classification.
- Le ch. 2 couvre les activités impliquant des droits d'accès étendus aux moyens informatiques des deux catégories de sécurité supérieures ou à des activités particulières relatives à ces moyens dont l'exercice permettrait à des personnes de nuire considérablement aux intérêts définis à l'art. 1, al. 2, par exemple en volant des données ou en commettant des actes de sabotage. La simple utilisation de ces moyens informatiques n'est donc pas jugée sensible (seul le contenu des informations à traiter détermine si l'utilisateur exerce une activité sensible ou non). Sont concernés avant tout certains administrateurs ou responsables d'application des systèmes nécessitant une protection élevée ou très élevée. La notion d'*exploitation* se réfère à l'activité des fournisseurs de prestations au sens de l'art. 19 LSI. Elle doit être clairement distinguée de l'expression «exploiter un système d'information» que l'on trouve dans la législation sur la protection des données. Elle ne vise en fait qu'à régler le *recours* à un système d'information par un bénéficiaire de prestations (cf. par ex. art. 24, al. 1, LSI).

– Enfin, aux termes du ch. 3, l'accès aux zones de sécurité (art. 23) est réputé sensible, car les dommages que l'espionnage ou le sabotage peuvent occasionner dans ces zones sont potentiellement considérables en raison des informations et des moyens informatiques qui s'y trouvent. Le ch. 3 couvre également l'accès aux zones de sécurité 2 et 3 au sens de la législation sur la protection des ouvrages militaires (cf. art. 19, al. 1, let. c, LMSI).

Par rapport à la réglementation en vigueur et aux conditions imposant un CSP (cf. art. 19, al. 1, LMSI), la notion d'*activité sensible* est plus vaste parce qu'elle tient compte des besoins de sécurité accrus dans le domaine informatique. Elle est cependant aussi plus étroite parce qu'elle ne couvre plus l'accès régulier aux données sensibles dont la divulgation peut nuire gravement aux droits de la personnalité des personnes concernées (cf. ch. 1.2.5).

Let. c: cette définition est identique à celle de l'art. 6, al. 1, let. a, ch. 4, LRens. Les deux définitions se fondent sur la terminologie de la protection de la population.

Chapitre 2 Mesures générales

Section 1 Principes

Art. 6 Sécurité de l'information

L'art. 6 expose le contenu matériel de la sécurité de l'information et les principes selon lesquels elle doit être concrétisée. En détaillant les objectifs de protection, il complète l'article portant sur le but de la loi (art. 1).

Le besoin de protection des informations (al. 1) est établi en fonction du préjudice potentiel porté aux intérêts visés à l'art. 1, al. 2, et défini sur la base des critères détaillés de l'al. 2. Le besoin spécifique de protection à raison de la matière est très souvent implicitement déterminé par d'autres lois (cf. également art. 1, al. 2, let. e, et art. 4, al. 2).

Sur le plan matériel, la doctrine et la pratique retiennent généralement quatre critères de protection pour la sécurité de l'information, dont la pondération peut varier selon les circonstances: la préservation de la confidentialité, de l'intégrité, de la disponibilité et de la traçabilité des informations. Souvent, d'autres critères de protection sont également cités, mais ceux-ci sont, en principe, repris implicitement par les critères énumérés à l'al. 2, voire combinés entre eux, par exemple l'authenticité (reprise sous la notion d'intégrité), l'imputabilité ou l'incontestabilité (découlant des critères d'intégrité et de traçabilité).

– *Confidentialité:* ce principe veut que seules les personnes autorisées aient accès aux informations. Le cercle de ces personnes est défini par le contexte dans lequel les tâches légales sont exécutées, de même que par le contenu et l'importance des informations. Le cercle de ces personnes peut ainsi être très étendu ou extrêmement restreint.
– *Disponibilité:* la capacité de décision et d'action des autorités et organisations exige qu'elles puissent consulter à temps les informations nécessaires à l'accomplissement de leurs tâches légales. Les exigences de disponibilité

sont d'autant plus élevées lorsque les informations doivent être disponibles en permanence pour l'accomplissement de tâches essentielles.

– *Intégrité:* la préservation de l'intégrité et de l'exactitude des informations est particulièrement importante lorsque les informations sont destinées au public ou destinées à être réutilisées (cf. ch. 1.1.1 de la Stratégie OGD Suisse). Les données personnelles (art. 5 LPD) ou les informations comptables (art. 38 LFC) doivent être exactes. De plus, la préservation de l'intégrité est indispensable au bon fonctionnement de certains moyens informatiques.

– *Traçabilité:* la traçabilité du traitement des informations est non seulement importante pour les procédures publiques (procédure pénale, procédure de recours, etc.), mais aussi pour l'exercice des contrôles et de la surveillance, ainsi que pour la procédure en cas d'utilisation abusive d'informations.

En vertu des al. 1 et 2, les autorités et organisations soumises à la loi doivent donc évaluer le besoin de protection des informations et déterminer l'objectif et l'ampleur de cette protection. Par exemple, le maintien de la confidentialité n'est nécessaire que si elle doit être garantie pour une raison légale. Certaines informations peuvent justifier des exigences accrues en matière de protection de leur intégrité ou de leur disponibilité, sans pour autant que de telles exigences figurent explicitement dans la législation, notamment lorsque ces informations doivent impérativement être exactes ou disponibles pour l'accomplissement des tâches d'une autorité. Cela concerne en particulier les informations et les moyens informatiques qui soutiennent des processus critiques des autorités.

Bien que découlant en principe de l'al. 2, let. b et c, l'exigence d'une protection adéquate contre les abus et les perturbations est une nouvelle fois expressément mentionnée, car l'appui technique des moyens informatiques aux processus d'affaires ne cesse de gagner en importance. Désormais, leur bon fonctionnement est une condition sine qua non de l'accomplissement efficient des tâches des autorités fédérales.

Il va de soi qu'une sécurité absolue est un idéal inatteignable et que le coût de l'élimination des lacunes mineures qui subsistent au niveau de la sécurité peut être disproportionné. Les autorités et organisations soumises à la loi doivent donc veiller à ce que leurs mesures soient appropriées et économiques. Les supérieurs hiérarchiques sont ainsi tenus, dans leur suivi des mesures de protection, d'évaluer le rapport coût-utilité de la sécurité. Force est cependant de constater que si les mesures de sécurité entravent trop le personnel dans l'accomplissement de ses tâches, il est fort probable qu'elles ne seront pas respectées ou qu'elles seront intentionnellement contournées.

Art. 7 Responsabilité des autorités soumises à la présente loi

La sécurité est de la responsabilité de la hiérarchie. Les autorités soumises à la loi doivent organiser, mettre en œuvre et contrôler la sécurité de l'information dans leur domaine de compétence, en tenant compte des connaissances scientifiques et techniques les plus récentes. Plusieurs normes formulent ce qui est communément appelé *bonnes pratiques* dans la gestion de la sécurité de l'information et fixent des exigences pour l'application de mesures de sécurité adaptables aux besoins des

diverses autorités ou organisations, ou pour des parties d'entre elles. Par exemple, la loi ne commande pas aux autorités de mettre en place un système de gestion de la sécurité de l'information selon la norme DIN ISO/IEC 27001, mais leur organisation devrait au moins s'en inspirer. Des organisations à effectifs réduits ne pourront évidemment mettre sur pied une organisation de ce type, raison pour laquelle la loi permet, par exemple, que les tribunaux fédéraux décident de mettre sur pied une seule organisation commune tout en conservant l'indépendance des divers tribunaux. Pour garantir une application uniforme, les autorités doivent décider d'un modèle d'organisation commun. La matérialisation de la sécurité de l'information touchant de nombreux domaines (par ex. les finances, les services du personnel, le droit, l'informatique, la gestion des risques, etc.), les domaines spécialisés concernés doivent cautionner la sécurité de l'information et être associés aux décisions.

Les autorités sont aussi tenues de régler le contrôle de la sécurité de l'information. En principe, les supérieurs hiérarchiques en sont chargés. Les préposés à la sécurité de l'information mèneront également des contrôles sur mandat de leurs autorités (cf. art. 82, al. 2, let. c), par exemple en proposant un plan annuel d'audits qui précise les priorités et les ressources nécessaires. Les normes exigent par ailleurs qu'un service externe (indépendant) évalue périodiquement l'efficacité de l'organisation et des mesures. La périodicité et le service chargé des contrôles sont déterminés par l'autorité concernée. Au sein de l'administration fédérale, ils peuvent être menés par les structures de surveillance internes des départements, par le Contrôle fédéral des finances, qui assure déjà la révision dans le domaine informatique, ou par une entreprise externe.

En vertu de l'al. 2, les autorités sont tenues de définir certains principes.

- Les objectifs des autorités soumises à la loi en matière de sécurité de l'information déterminent le niveau de sécurité qui doit être atteint (niveau exigé de sécurité de l'information). Ils impliquent une analyse coût-utilité (quel niveau de sécurité les autorités souhaitent-elles et à quel prix?) et sont déterminants pour l'attribution des ressources nécessaires. L'efficacité des mesures de sécurité de l'information doit être mesurée à l'aune du niveau de sécurité visé.
- Chaque autorité doit également déterminer la façon dont les organisations subordonnées doivent gérer les risques, déterminer les risques qui peuvent être supportés sans mesure particulière et ceux qui doivent être rapportés aux autorités elles-mêmes (acceptation du risque). Même si la plupart des risques pour la sécurité de l'information peuvent être traités et assumés au niveau opérationnel (département, office, voire unité subordonnée), certains peuvent avoir une portée stratégique. De tels risques doivent à tout le moins être communiqués à l'autorité concernée, notamment ceux liés aux moyens informatiques de la catégorie «protection très élevée» (art. 17, al. 3).
- Il n'est pas une organisation qui ne compte, parmi ses membres, des personnes qui ne prennent pas au sérieux la sécurité de l'information et qui utilisent les moyens informatiques mis à leur disposition négligemment ou en enfreignant les consignes de sécurité. Très souvent, de tels manquements sont excusés sans aucune investigation. Ils peuvent néanmoins avoir

d'importantes répercussions. Les autorités soumises à la loi doivent ainsi appliquer les consignes de manière conséquente et indiquer, en les expliquant, les conséquences de leur violation.

Art. 8 Gestion des risques

Une gestion efficace des risques est une condition sine qua non d'une sécurité adéquate et économique de l'information. L'accent doit être mis là où se trouvent les plus grands risques et il faut les juguler par les mesures les plus efficaces. C'est pourquoi les autorités et organisations de la Confédération sont tenues de garder les risques sous contrôle, tant dans leur propre domaine de compétence que dans le cadre de leur collaboration avec des tiers. L'évaluation des risques présuppose une solide connaissance des tâches légales et des processus d'affaires qui s'y rapportent, une appréciation régulière des menaces, l'analyse des vulnérabilités, la détermination de la probabilité de survenance d'un événement et l'estimation des dommages potentiels liés à des risques donnés. Même si la gestion des risques exigée est spécifique à la matière et doit par conséquent être pilotée et exercée par des spécialistes, la sécurité de l'information reste un élément de la gestion ordinaire des risques, raison pour laquelle elle doit être intégrée à la gestion globale des risques de l'autorité ou de l'organisation concernée.

Un objectif important de la gestion des risques est de prendre les mesures les plus efficaces pour éviter ou réduire les risques. Les risques peuvent être évités dans la mesure où l'on peut renoncer totalement à une activité trop risquée (par ex. renoncer à un projet informatique pour lequel l'application de mesures de prévention des risques n'est pas défendable économiquement). Bien évidemment, les risques peuvent également être pris en compte ou supportés, mais ils ne devraient pas être ignorés. Les risques subsistant après l'application des mesures de sécurité prévues (appelés risques résiduels) et les risques ne devant pas être minimisés doivent être clairement signalés. Les décideurs doivent être pleinement avisés de ces risques et de leurs conséquences potentielles. Les risques résiduels doivent être clairement acceptés et supportés.

Des mesures organisationnelles, plus efficaces ou plus économiques, sont régulièrement développées dans le domaine de la sécurité de l'information. Les évolutions techniques sont encore plus rapides, notamment en ce qui concerne les moyens informatiques, mais également dans le domaine de la sensorique (par ex. les détecteurs de feu, de chaleur ou de mouvement) et des techniques de fermeture (par ex. les systèmes de fermeture des portes). Il est très important que les mesures de sécurité ne reposent pas sur des technologies obsolètes et qu'elles agissent contre les menaces d'aujourd'hui. Les normes doivent donc être élaborées selon les connaissances scientifiques et techniques les plus récentes (cf. art. 86), tout en sachant que les critères d'acceptation des risques déterminants pour l'évaluation des risques sont fixés par chaque autorité soumise à la loi en fonction de ses propres besoins en matière de sécurité de l'information.

Art. 9 Collaboration avec les tiers

Au sens de la présente loi, sont réputées tiers les autorités, organisations et personnes de droit public ou privé qui ne sont pas des autorités ou organisations soumises à la loi (y compris les cantons) et qui agissent donc, en principe, indépendamment de ces autorités et organisations. Les autorités fédérales ont souvent besoin de l'appui des acteurs de l'économie privée ou d'autres organes pour accomplir leurs tâches. Dans ces cas, les autorités et organisations qui attribuent des mandats à des tiers doivent veiller à ce que les mesures prévues par la loi soient respectées lors de l'attribution et de l'exécution des mandats. Les mesures de sécurité à respecter sont généralement réglées contractuellement. En principe, les tiers ne devraient être habilités à accéder aux informations ou aux moyens informatiques de la Confédération que lorsque les mesures de sécurité nécessaires ont été mises en œuvre. La LSI contraint également les autorités et organisations soumises à la loi à contrôler de manière adéquate (c'est-à-dire en tenant compte des risques) l'application effective de telles mesures, par exemple en procédant à une visite des lieux ou en demandant une confirmation écrite de la tierce partie. Lorsque le mandat implique l'exercice d'une activité sensible, ces autorités et organisations doivent demander l'ouverture d'une procédure de CSP (cf. art. 28 ss) ou, le cas échéant, d'une procédure de PSE (cf. art. 50 ss).

Art. 10 Procédure en cas de violation de la sécurité de l'information

Des incidents sont inévitables dans le domaine de la sécurité de l'information. Il faut dès lors appliquer une procédure efficace et uniforme pour faire face à ces incidents. Les autorités et organisations soumises à la loi doivent, dans un premier temps, prendre les mesures nécessaires pour être capables, avant toute chose, d'identifier rapidement ces incidents (par ex. contrôles réguliers, capteurs, installations d'alarme, surveillance des réseaux, analyses régulières des fichiers journaux). Elles doivent également fixer une procédure dictant le comportement à adopter lorsque des incidents ou des vulnérabilités sont identifiés et attribuer des compétences claires pour leur traitement. Le personnel impliqué, qu'il soit interne ou externe, doit aussi savoir comment réagir face à de tels événements pour pouvoir limiter au maximum leurs effets. Pour pouvoir tirer les enseignements des incidents survenus, les autorités et organisations soumises à la loi doivent veiller à ce que ses causes soient identifiées et analysées.

Les autorités fédérales, et plus particulièrement le Conseil fédéral, doivent de plus prendre toutes les dispositions nécessaires pour assurer sans retard l'accomplissement de leurs tâches essentielles, même en situation extraordinaire (gestion de la continuité des affaires, cf. art. 6, al. 3, LOGA). On peut aujourd'hui partir du principe que l'accomplissement des tâches les plus critiques de la Confédération dépend de l'engagement fiable de moyens informatiques. La LSI exige dès lors des autorités soumises à la loi qu'elles identifient leurs tâches essentielles de leur point de vue stratégique, qu'elles établissent à titre préventif des plans d'action dans l'éventualité d'une grave violation de la sécurité de l'information (par ex. défaillance durable d'un système) des et qu'elles organisent des exercices. Pour les moyens informatiques engagés pour l'accomplissement de ces tâches essentielles, la catégorie de sécurité «protection très élevée» au sens de l'art. 17, al. 3 sert de modèle.

Section 2 Classification des informations

Art. 11 Principes régissant la classification

La classification est obligatoire dès lors que les critères afférents sont remplis. Eu égard au principe de la transparence et compte tenu des coûts qu'elle occasionne, la classification d'informations doit être l'exception et non la règle. Souvent, les besoins de protection s'amenuisent avec le temps ou après un événement déterminé (par ex. publication d'un rapport ou levée d'une mesure spécifique). La classification de ces informations (par ex. devenues désuètes) ne se justifie dès lors plus et n'entraînerait que des dépenses inutiles. Par ailleurs, les informations devant rester classifiées durant une longue période requièrent des mesures de sécurité techniques différentes de celles applicables aux informations dont le besoin de protection est plus limité dans le temps. Lorsqu'une classification provisoire n'est pas d'emblée possible, il faut veiller à ce que les informations ne restent pas inutilement classifiées. Une vérification du besoin de protection doit avoir lieu au moins lorsque les documents sont annoncés aux Archives fédérales.

Les informations classifiées doivent être protégées aussi longtemps que le besoin de protection est avéré. Les mesures nécessaires sont définies au niveau de l'ordonnance. Si la Suisse a signé avec un État ou une organisation internationale un traité sur l'échange d'informations classifiées (cf. art. 88, let. b), le traitement des informations relevant du champ d'application de ce traité suivra les dispositions particulières du traité. En l'absence de traité, les informations classifiées seront traitées selon les prescriptions de la LSI et de sa législation d'exécution.

Il arrive également que du *matériel* soit classifié (cf. commentaire de l'art. 5, let. b, ch. 1). La classification de matériel est un cas particulier de la classification des informations: c'est pourquoi les mêmes méthodes d'évaluation et les mêmes mesures de protection s'appliquent en principe (y compris les CSP et les PSE).

Art. 12 Compétences

Au sein de l'administration fédérale, la compétence de la classification revient à l'auteur du document car il est celui qui peut le mieux estimer le besoin de protection des informations et les risques éventuels. Les autorités soumises à la loi peuvent toutefois décider que la classification relève par exemple de la direction de l'autorité, d'un service centralisé ou exclusivement des supérieurs hiérarchiques. La classification est en principe contraignante. Lorsqu'une information est classifiée, ce statut l'accompagnera pour ainsi dire toute sa vie. Quiconque accède à une information de cette nature est tenu de respecter les prescriptions liées à la classification. En principe, une modification ou une suppression de la classification ne peut être le fait que de l'auteur de la classification lui-même. Bien évidemment, les dispositions régissant la hiérarchique, la surveillance des services et le droit de donner des instructions des supérieurs et des autorités de surveillance s'appliquent. Ces dernières peuvent, le cas échéant, corriger les décisions du service auteur de la classification. L'art. 12 n'exclut pas que la mise en œuvre des prescriptions de classification et de déclassification puissent prendre place dans des systèmes d'information (par ex. GEVER).

L'al. 3 habilite le Conseil fédéral à régler spécialement la déclassification de documents en vue de leur archivage, de même que la déclassification de fonds d'archives classifiés. Il ne dote pas le Conseil fédéral d'une compétence générale de réglementation en matière de déclassification des informations: l'art. 85, al. 1, confère cette compétence à chaque autorité soumise à la loi pour son propre domaine.

Cette disposition vise à assurer, d'une part, que seules les informations qui nécessitent durablement une protection élevée soient classifiées dans les archives (archives classifiées). Les informations classifiées doivent si possible être déclassifiées avant leur versement aux Archives fédérales (cf. commentaire de l'art. 11, al. 3). Le besoin de protection doit donc être vérifié au plus tard lorsque les documents sont annoncés aux Archives fédérales. La disposition vise aussi, d'autre part, à éviter que des archives classifiées restent classifiées pour toujours. Ainsi, les documents classifiés devraient en règle générale être automatiquement déclassifiés à l'échéance du délai de protection prévu par la LAr. Le Conseil fédéral veillera dans les dispositions d'exécution à ce que les mécanismes de déclassification n'imposent ni aux Archives fédérales ni aux services versants une charge de travail disproportionnée.

Cette disposition montre également que la LSI et la LAr présentent des recoupements. En effet, tant la LSI que la LAr s'appliquent à toutes les informations pour lesquelles les autorités fédérales sont compétentes. Il faut donc s'assurer que les objectifs poursuivis par les deux législations et les compétences qu'elles définissent n'entrent pas en conflit. En principe, les rapports entre les deux systèmes sont simples: la LAr règle de manière uniforme l'archivage des documents de la Confédération et l'accès à ces documents archivés, tandis que la LSI s'applique aux mesures usuelles de protection des informations et de moyens informatiques, à savoir celles qui ne sont pas spécifiques aux techniques d'archivage. Dans la mesure où des règles spéciales régissent les fonds d'archives, ces normes sont fixées dans la LSI (cf. art. 14, al. 2, LSI). Juridiquement, l'exécution de cette réglementation ne pose pas de problème car le Conseil fédéral est compétent aussi bien pour l'exécution de la LAr que pour la législation d'exécution de la LSI, dans la mesure où l'administration fédérale est concernée.

Dans la pratique, la protection des documents archivés sur papier qui ont un besoin élevé de protection n'est pas problématique. L'archivage croissant de documents sensibles sous forme électronique pose toutefois de nouveaux défis tant aux services versants qu'aux Archives fédérales. Les organes chargés de la planification de la mise en oeuvre de la LSI examineront en collaboration avec les Archives fédérales si les mesures de protection organisationnelles et techniques prévues par la LAr suffisent ou si elles doivent être adaptées. Le cas échéant, le Conseil fédéral demandera une augmentation du plafond des dépenses des Archives fédérales pour les postes et les ressources nécessaires.

Art. 13 Échelons de classification

L'art. 13 règle les conditions matérielles de la classification des informations et fixe les échelons de classification correspondants pour toutes les autorités et organisations soumises à la loi. Le texte proposé se limite à des critères assez généraux et prend directement en compte les intérêts publics à protéger définis à l'art. 1, al. 2,

let. a à d. La référence à ces intérêts est toutefois limitée: la protection des intérêts publics définis à la let. e n'est pas un motif de classification en soi. Cette protection doit, notamment, assurer le traitement conforme au droit des informations dont la protection est prévue dans le cadre d'autres lois ou d'accords conclus avec des tiers. Par conséquent, les données personnelles au sens de la LPD ou les secrets d'affaires, de fabrication ou professionnels ne sont en principe pas classifiés, à moins que certaines informations ne doivent l'être pour protéger un intérêt au sens de l'art. 1, al. 2, let. a à d. Il en va de même des informations traitées par les tribunaux ou les ministères publics lors de leurs procédures ordinaires. La plupart d'entre elles sont des données personnelles, et donc sensibles, qui ne sont toutefois pas soumises à classification en vertu de la présente loi. Par contre, les mesures particulières prises pour protéger ces informations peuvent être classifiées (par exemple un plan de sécurité de l'information).

Les échelons de classification à proprement parler sont déterminés par la *gravité du préjudice* que la divulgation des informations à une personne non autorisée peut porter aux intérêts définis à l'art. 1, al. 2, let. a à d. Ils sont attribués comme suit:

- lorsque la divulgation est susceptible de *nuire à ces intérêts:* échelon de classification «interne»;
- lorsque la divulgation est susceptible de *nuire considérablement à ces intérêts:* échelon de classification «confidentiel»;
- lorsque la divulgation est susceptible de *nuire gravement à ces intérêts:* échelon de classification «secret».

Ces qualifications sont des notions juridiques indéterminées qui devront encore être concrétisées en tenant compte de la politique de gestion des risques.

Bien que le critère de la gravité du préjudice que peuvent subir les intérêts définis à l'art. 1, al. 2, let. a à d, soit déterminant pour la classification, il ne suffit pas: un lien de causalité raisonnable doit également être établi entre la divulgation des informations à une personne non autorisée et le préjudice potentiel pour les intérêts à protéger. Il faut donc tenir compte de la probabilité du dommage. La classification d'une information correspond dès lors au résultat d'une évaluation du risque et doit refléter le *besoin effectif de protection* de l'information classifiée.

Une retenue toute particulière est nécessaire lors de l'appréciation du besoin de protection des informations de *nature politique*. Certes, la protection de la libre formation de l'opinion et de la volonté des autorités et organisations soumises à la loi est prise en compte à l'art. 1, al. 2, let. a (capacité de décision). Dans une démocratie moderne, cependant, la discussion sur la place publique, voire la critique (même sévère) des idées, propositions, projets et décisions d'ordre politique relève des activités normales du gouvernement. La classification ne doit donc pas servir à soustraire certains sujets du débat public lorsqu'aucun intérêt public prépondérant n'est en jeu.

Al. 1: l'échelon «interne» représente la limite entre une information devant être classifiée et celle qui ne doit pas l'être. Même si le préjudice exigé pour la classification n'est pas défini plus précisément dans la loi, il faut que la classification soit justifiée par des indices d'un dommage potentiel qualifié. Ainsi, le dommage poten-

tiel aux intérêts définis à l'art. 1, al. 2, let. a à d, ne peut être simplement négligeable: il doit être *sensible*. Par rapport à l'actuel art. 7 OPrI, qui n'évoque qu'un préjudice, la nouvelle réglementation est beaucoup plus sévère. Lorsque les informations touchent la sécurité au sens de l'art. 1, al. 2, let. b, les valeurs seuils permettant une classification «interne» sont, dans la plupart des cas, relativement vite atteintes. Cet échelon de classification est aussi celui qui est le plus souvent utilisé lorsque de tels cas se présentent. Ainsi, divers documents relatifs à la sécurité des moyens informatiques ou de simples plans d'engagement établis pour les forces de sécurité sont généralement classifiés «interne».

Al. 2: par rapport à la situation actuelle, où seul un *dommage* non qualifié est exigé (art. 6 OPrI), la réglementation proposée se traduit par une élévation des exigences en matière de classification. L'expression retenue exige un dommage plus perceptible et plus important, par exemple:

- la libre formation de l'opinion et de la volonté des autorités soumises à la loi se trouve provisoirement entravée de manière illicite;
- une organisation soumise à la loi est temporairement dans l'incapacité d'agir;
- l'accomplissement de certaines tâches par une autorité ou une organisation est sensiblement entravé sur le long terme;
- certaines ressources de l'armée ou des organes de sécurité de la Confédération ne peuvent temporairement être engagées;
- la position de la Suisse dans des négociations internationales est considérablement affaiblie;
- la sécurité de personnes ou de groupes de personnes est menacée;
- la Confédération subit un préjudice financier considérable.

Al. 3: la formulation retenue introduit une notion de dommage particulièrement grave, voire catastrophique, pour la Confédération, par exemple:

- une autorité soumise à la loi est temporairement dans l'incapacité de prendre des décisions ou d'agir ou est très sérieusement entravée dans l'accomplissement de ces tâches sur le long terme;
- une organisation soumise à la loi est momentanément empêchée d'accomplir ses tâches essentielles ou sérieusement entravée dans l'accomplissement de ces tâches sur le long terme;
- des ressources importantes de l'armée ou des organes de sécurité de la Confédération sont inaptes à l'engagement;
- la vie et l'intégrité de certains groupes de population sont menacées;
- la fourniture par des infrastructures critiques de prestations indispensables est interrompue;
- certaines fonctions sensibles d'une centrale nucléaire sont hors d'usage à la suite d'un sabotage;
- la Confédération subit un grave préjudice financier.

La classification doit être perçue immédiatement sans risque de confusion avec d'autres mentions. Dans le contexte international, la règle est de la faire figurer en lettres grasses majuscules. L'al. 4 impose cette règle à toutes les autorités de la Confédération.

Art. 14 Accès aux informations classifiées

L'al. 1 décrit les conditions d'accès à des informations classifiées, cet accès étant indispensable pour traiter les informations concernées. Le principe du *besoin* de connaître les informations vaut pour chaque information classifiée. Il n'existe donc pas de droit général à accéder à toutes les informations classifiées. Ce principe s'applique également aux organes de vérification, de contrôle et de surveillance: bien qu'ils disposent d'un droit général à l'information dans les cas d'espèce, ils doivent justifier pour chaque information classifiée que les informations visées sont effectivement nécessaires à l'accomplissement de leurs tâches. Si le droit d'accès est convenu contractuellement, les accords conclus à cet effet doivent prévoir l'accès aux informations classifiées et régler leur traitement. La *garantie* d'un traitement correct des informations classifiées implique que les personnes qui doivent les traiter ont été formées en conséquence. En outre, ces dernières doivent, le cas échéant, apporter la preuve de leur capacité à respecter les mesures techniques et physiques de sécurité. Pour les informations classifiées «confidentiel» ou «secret», la conduite d'un CSP peut aussi constituer une condition supplémentaire.

Al. 2: la réglementation de l'accès aux fonds d'archives (art. 9 à 16 LAr) a fait ses preuves en ce qui concerne les archives classifiées. Elle continuera donc de s'appliquer (cf. également commentaire de l'art. 12, al. 3).

Al. 3: la plupart des pays et des organisations internationales avec lesquels la Suisse a conclu un traité sur l'échange d'informations classifiées exigent que leurs informations soient traitées exclusivement par des personnes de leur propre nationalité ou de nationalité suisse (clause d'exclusion des États tiers). De telles informations ne sont en principe pas accessibles à des personnes d'une autre nationalité, sous réserve d'un accord préalable avec l'auteur de ces informations.

Art. 15 *Accès à des informations classifiées dans le cadre de procédures spéciales*

Le droit de procédure de l'Assemblée fédérale et celui des tribunaux et des ministères publics sont réservés. Pour l'accès aux informations classifiées (par ex. dans le cadre de leur utilisation comme bases de décision ou moyens de preuve), le droit de procédure concerné doit s'appliquer. Le droit de procédure de la Confédération contient également des dispositions réglant la manière dont ces informations peuvent être ouvertes à la consultation des participants à la procédure, dans quelle mesure elles peuvent être divulguées dans le cadre de procédures publiques ou dans quelle mesure les témoins peuvent refuser de s'exprimer compte tenu des obligations légales de maintien du secret (cf. par ex. art. 47, 150, 153 et 154 LParl, 56, al. 2, et 59, al. 2, LTF, 16, al. 2, 18, al. 2, 27 et 28 PA, 40, al. 3, LTAF, ou 70, 170, 173, al. 2, et 194, al. 2, CPP, de même que les art. 45, 48, al. 2, et 77 CPM; voir également l'art. 58 de l'ordonnance du 24 octobre 1979 concernant la justice pénale

militaire[26]). Avant toute décision relative à la divulgation d'informations classifiées, l'occasion peut néanmoins être donnée à l'auteur de la classification de s'exprimer sur les motifs de la classification et les conséquences possibles d'une telle divulgation. L'organe ou le tribunal compétent décide de la suite de la procédure en fonction de son appréciation de la situation.

Section 3 Sécurité des moyens informatiques

Art. 16 Procédure de sécurité

Le temps où les offices fédéraux et les tribunaux exploitaient leurs propres moyens informatiques dans leurs propres locaux est bien lointain. En règle générale, les autorités et organisations de la Confédération se procurent leurs prestations informatiques auprès de fournisseurs externes hautement spécialisés. Il en résulte une séparation organisationnelle entre l'engagement et l'exploitation de moyens informatiques qui se répercute significativement sur la sécurité, notamment parce que la sécurité de l'information est le plus souvent considérée comme un problème purement technique de la responsabilité du fournisseur de prestations. La loi définit en principe les tâches incombant aux autorités et organisations pour qu'elles assument leurs responsabilités en matière de sécurité. Les autorités soumises à la loi (et non les organisations) doivent préciser ces tâches dans une procédure dite de sécurité. Toutes les autorités fédérales recourent déjà à ce type de procédure. Cependant, ces procédures doivent être systématisées et, si nécessaire, complétées. Les principales étapes de la procédure doivent être uniformisées entre les différentes autorités au niveau de l'ordonnance. La procédure de sécurité doit notamment préciser les tâches, les compétences et les responsabilités en matière de sécurité pour les services qui planifient l'engagement de moyens informatiques et qui en prennent la décision. L'al. 2 mentionne quelques points que la procédure de sécurité doit contenir.

– Let a: les moyens informatiques sont engagés à certaines fins et pour une certaine durée de vie. La première étape de la mise en application de la sécurité de l'information est de déterminer, en même temps que l'objectif du recours aux moyens informatiques, les processus d'affaires qu'ils sont appelés à soutenir, de même que les informations qui seront traitées. À ce moment, c'est-à-dire durant la planification, le bénéficiaire de prestations doit recenser les besoins de protection des informations au sens de l'art. 6, al. 1, et évaluer les conséquences possibles d'une perturbation ou d'une utilisation abusive pour les intérêts visés à l'art. 1, al. 2. Il procède fondamentalement à une analyse de l'impact économique et celle-ci doit impérativement être menée par le service responsable du processus d'affaires. L'évaluation des besoins de protection doit également tenir compte du fait que, généralement, les moyens informatiques sont insérés et exploités dans un certain environnement technique et logique (architecture). L'identification précoce des interconnexions et interdépendances permet aussi d'appliquer les mesures où elles seront les plus efficaces. De l'analyse des besoins de protection décou-

26 RS **322.2**

lent les exigences en matière de protection des informations. Cette analyse est également déterminante pour l'attribution des moyens informatiques à une catégorie de sécurité au sens de l'art. 17.

- Let. b: les autorités soumises à la loi doivent définir les mesures qui devront être appliquées (cf. également l'art. 18) et comment leur application sera contrôlée. En principe, on choisira des mesures standard (cf. art. 86). Le contrôle de l'application des mesures est particulièrement important à cet égard. Ainsi, les autorités et organisations compétentes doivent disposer, avant même d'engager un moyen informatique, d'une preuve que la procédure de sécurité s'est déroulée correctement et que les mesures nécessaires ont été effectivement appliquées (conformité).
- Let. c: des moyens informatiques sont régulièrement mis en exploitation sans que les besoins de sécurité de l'information soient couverts. L'autorisation relative à la sécurité doit garantir que l'autorité ou l'organisation compétente connaît les risques résiduels identifiés avant d'utiliser un moyen informatique et qu'elle est prête à les assumer. Si elle juge qu'ils sont trop élevés, elle peut refuser l'autorisation et demander des mesures susceptibles de réduire encore les risques.
- Let. d: la sécurité de l'information est en constante mutation. Les autorités doivent dès lors définir une procédure permettant de prendre en compte l'évolution des risques pour les moyens informatiques qui sont déjà en exploitation.

En vertu de l'al. 3, la compétence de conduire la procédure de sécurité incombe à l'autorité ou à l'organisation qui décide de recourir aux moyens informatiques (bénéficiaire de prestations). Le bénéficiaire de prestations est en effet responsable des processus d'affaires et de la mise en œuvre des exigences de sécurité. Il doit donc communiquer clairement ses exigences en la matière au service chargé de l'exploitation des moyens informatiques en question (fournisseur de prestations).

Art. 17 Catégories de sécurité

Les catégories de sécurité visent à identifier, sous l'angle des intérêts publics au sens de l'art. 1, al. 2, la criticité d'un moyen informatique déterminé. La criticité découle de la gravité du préjudice que peuvent causer les informations traitées avec le moyen informatique concerné ou le moyen informatique lui-même lorsqu'ils sont utilisés abusivement ou perturbés. Dès lors, la catégorisation dépend tant des besoins de protection de la confidentialité, de la disponibilité, de l'intégrité et de la traçabilité des informations que de la criticité du déroulement adéquat et sans retard des processus d'affaires soutenus par le moyen informatique. En ce qui concerne l'évaluation de la gravité du préjudice, on se référera par analogie au commentaire de l'art. 13.

Les prescriptions actuelles de l'administration fédérale ne prévoient que deux catégories: un besoin général et un besoin élevé. Le nouveau modèle à trois catégories s'inspire de la norme de l'office fédéral allemand chargé de la sécurité informatique.

- La catégorie de sécurité «protection de base» s'applique aux moyens informatiques ne devant pas satisfaire à des exigences particulières de protection. La grande majorité des systèmes de la Confédération devrait relever de cette catégorie de sécurité. Les données personnelles, les informations classifiées «interne» et d'autres informations dont la confidentialité doit être protégée, mais qui ne requièrent pas une protection particulièrement élevée, peuvent être traitées par les moyens de cette catégorie.
- Les moyens informatiques sont classés dans la catégorie «protection élevée» lorsque l'utilisation abusive des informations qu'ils servent à traiter ou du moyen informatique lui-même est susceptible de causer un préjudice considérable. Les moyens informatiques servant au traitement d'informations classifiées «confidentiel» relèvent ainsi de cette catégorie, de même que les moyens informatiques servant au traitement de données sensibles ou de secrets d'affaires ou de fabrication dans la mesure où l'utilisation abusive de ces informations peut occasionner un préjudice considérable à la Confédération. Lorsqu'un moyen informatique soutient un processus d'affaires dont la défaillance ou la perturbation peut entraver considérablement la marge d'action d'une autorité, le moyen informatique est également classé dans cette catégorie.
- Les moyens informatiques sont classés dans la catégorie «protection très élevée», lorsqu'ils peuvent entraîner un préjudice *grave* ou lorsque l'usage abusif d'informations qu'ils servent à traiter peut entraîner un tel préjudice. Il s'agit des moyens informatiques dont la défaillance ou la perturbation peut nuire gravement aux intérêts définis à l'art. 1, al. 2 (cf. également art. 10, al. 2) ou de ceux qui servent au traitement d'informations classifiées «secret».

L'attribution à une catégorie de sécurité détermine également les exigences de sécurité requises et comment les mesures de sécurité doivent être conçues. Des exigences et des mesures sont définies pour chaque catégorie de sécurité (art. 86) afin d'assurer la protection de la confidentialité, de la disponibilité, de l'intégrité et de la traçabilité. La standardisation est indispensable pour un échange efficace et sécurisé des informations entre les autorités. Elle présente d'importants avantages: des exigences de sécurité claires sont ainsi communiquées en amont aux services de développement et d'achat, qui en tiennent compte lors de l'intégration de la sécurité aux moyens informatiques de manière à garantir la transparence des coûts de la sécurité dans les projets et à faciliter leur calcul et leur planification.

Un tableau de concordance qui précise les catégories de sécurité auxquelles les informations et les processus d'affaires sont attribués ne peut encore être établi, parce que les critères d'attribution de l'art. 17 sont nouveaux et ne sont pas encore entrés dans la pratique. Par ailleurs, les autorités et organisations ne traitent pas tous les mêmes informations, ce qui empêche d'évaluer le besoin effectif de protection des diverses informations dans l'absolu. Un niveau de protection donné sera néanmoins attribué aux informations et données en fonction de leur besoin de confidentialité, de disponibilité, d'intégrité et de traçabilité. Grâce à des tableaux de concordance, les niveaux de protection permettront de standardiser les mesures.

Art. 18 Mesures de sécurité

Les autorités soumises à la loi doivent définir les exigences de sécurité minimales auxquelles doivent satisfaire leurs moyens informatiques pour chaque catégorie de sécurité. La pratique a montré qu'avec un certain nombre d'exigences et de mesures de sécurité prédéfinies, on peut réduire le risque dans une proportion acceptable pour une majorité de moyens informatiques. Toutes ces exigences et mesures constituent la protection de base. L'avantage d'une protection de base prédéfinie et standardisée réside dans le fait que les autorités, et organisations ne doivent pas mener d'analyses du risque détaillées et coûteuses pour les moyens informatiques concernés par cette catégorie. Les mesures de protection de base conditionnent aussi les mesures de «protection élevée» et de «protection très élevée». Les mesures applicables à la protection de base doivent donc être relativement souples et modulables: si certaines d'entre elles ne sont pas applicables pour un moyen informatique en particulier, d'autres mesures permettant une protection équivalente doivent être prises.

Les catégories «protection élevée» et «protection très élevée» ne peuvent souvent se satisfaire des exigences et des mesures de sécurité de la protection de base. Aussi procède-t-on aujourd'hui, dans un premier temps, à une analyse du risque que présente le moyen informatique concerné. Le point central de cette analyse réside dans la protection des critères soumis à des exigences élevées de protection. Lorsqu'un moyen informatique atteint la catégorie «protection élevée» parce que sa disponibilité doit être très élevée alors que sa confidentialité n'est soumise à aucune exigence particulière, l'analyse du risque se concentre en priorité sur sa disponibilité. Une fois l'analyse du risque terminée, le système actuel exige qu'un plan de sécurité de l'information et de protection des données soit établi. Ce plan de sécurité atteste de la mise en place des mesures de protection de base et décrit les mesures de sécurité supplémentaires qui ont été décidées.

Il est prévu de maintenir le système actuel (analyse du risque et plan de sécurité) pour les moyens informatiques des deux catégories plus élevées, mais rien dans le texte de loi ne s'opposerait à d'autres solutions..

Une analyse de l'efficacité au sens de l'al. 3 est la seule mesure permettant de déterminer dans quelle mesure la sécurité de l'information est effectivement garantie. Le moyen informatique fait l'objet d'un audit exhaustif. De plus, il est exposé à des attaques réelles qui ont pour but d'identifier les éventuelles lacunes de sécurité et les vulnérabilités exploitables (par ex. au moyen de tests d'intrusion). L'analyse de l'efficacité n'est exigée que pour les moyens informatiques les plus critiques, car son coût est loin d'être négligeable (de 0,5 à 2 % de l'investissement total).

Art. 19 Sécurité de l'exploitation de moyens informatiques

En vertu des art. 16 à 18, les bénéficiaires de prestations portent la responsabilité principale de la sécurité des moyens informatiques. Pour leur part, les fournisseurs de prestations sont chargés d'assurer la sécurité durant l'exploitation selon les connaissances scientifiques et techniques actuelles. Ils doivent donc respecter et transposer les exigences et mesures prévues par la présente loi, de même que les exigences complémentaires des bénéficiaires de prestations. Les fournisseurs internes de prestations sont tous soumis à la présente loi et sont donc tenus de l'appliquer

dans le cadre de leurs activités. Par contre, les fournisseurs externes de prestations sont considérés comme des tiers au sens de l'art. 9 et doivent être tenus contractuellement de respecter les mesures prévues par la présente loi.

Chaque fournisseur de prestations est tenu de surveiller ses réseaux. Des anomalies, des attaques ou des perturbations doivent être identifiées à temps et évaluées pour permettre d'y réagir. En cas de soupçon d'une mise en danger ou en cas de violation concrète de la sécurité de l'information, il se peut que les activités électroniques de certains collaborateurs (ou machines) internes ou externes doivent être analysées plus en détail. À cet égard, lorsque l'identification nominative d'une personne s'impose, les dispositions de la LOGA sur le traitement des données personnelles produites dans le cadre de l'utilisation de l'infrastructure informatique s'appliquent par analogie. Les processus dits forensiques de l'administration fédérale se fondent déjà sur ces dispositions lorsque des données personnelles doivent être exploitées.

Section 4 Mesures relatives aux personnes

Art. 20 Conditions d'accès

Les personnes qui doivent pouvoir accéder à des informations, des moyens informatiques ou des infrastructures de la Confédération doivent se plier à certaines exigences. Il incombe à l'employeur ou à l'adjudicateur de veiller à ce que l'employé ou le mandataire réponde à ces exigences.

- Lors du choix des employés ou des mandataires, les critères de sélection doivent tenir compte des besoins de protection des informations ou de la criticité des moyens informatiques. Les employeurs sont responsables du choix de leur personnel. L'assujettissement d'une personne à un CSP ne les délie pas de cette responsabilité.
- La gestion des accès aux systèmes d'information, aux locaux et aux infrastructures est de plus en plus informatisée. Les personnes qui souhaitent recourir aux ressources de la Confédération doivent s'identifier électroniquement (authentification) de manière que l'on puisse déterminer s'ils disposent d'une autorisation d'accès. Selon le caractère critique de l'accès, des systèmes plus ou moins sophistiqués d'authentification sont utilisés. Par exemple, on exige en sus du mot de passe une carte à puce ou le contrôle d'une caractéristique biologique (empreintes digitales, reconnaissance oculaire, etc.).
- Let. c: les autorités et organisations soumises à la loi doivent suffisamment former les membres de leur personnel et leurs mandataires. Dans le domaine de la sécurité de l'information, une formation unique ne suffit pas. Le personnel et les mandataires doivent régulièrement être formés et sensibilisés à cette problématique. Une attention particulière doit être accordée à la formation des cadres et des personnes qui exercent une activité sensible.
- En vertu des art. 22 LPers et 320 CP, le personnel de la Confédération est soumis au secret de fonction. En ce qui concerne les tiers chargés d'exécuter des mandats pour la Confédération, l'obligation du maintien du secret doit

être stipulée contractuellement par écrit et assortie de sanctions claires en cas de non-respect, car les tiers échappent au champ d'application de l'art. 320 CP. Notons au surplus qu'une obligation contractuelle de préserver le secret ne disculpe pas le fonctionnaire qui l'a révélé en l'absence de consentement écrit interne de l'autorité supérieure au sens de l'art. 320, al. 2, CP. En ce qui concerne la violation du secret de fonction, on se référera au commentaire de l'art. 320 CP.

Le recours à des méthodes de vérification biométriques pour l'authentification peut apporter un complément de sécurité. Il ne s'agit pas d'identifier quelqu'un parmi un nombre indéterminé de personnes, mais uniquement de vérifier si une personne donnée qui demande d'accéder à des ressources de la Confédération est réellement la personne qu'elle prétend être. Les autorités soumises à la loi doivent pouvoir recourir à cette méthode pour l'accès à leurs ressources. Elles l'utilisent d'ailleurs déjà dans certains domaines. Pour des raisons liées à la protection des données, les données biométriques doivent impérativement être détruites à l'expiration de l'autorisation d'accès.

Art. 21 Délivrance restrictive des autorisations

L'art. 21 pose un principe essentiel de la sécurité de l'information. Quiconque travaille ou exerce un mandat pour la Confédération doit, selon les circonstances, avoir accès à des informations, des moyens informatiques ou des locaux pour effectuer ses tâches. Le personnel et les mandataires ne doivent obtenir que les autorisations dont ils ont effectivement besoin pour l'accomplissement de leurs tâches. Le risque d'abus peut être fortement réduit lorsqu'une personne ne peut pas traiter, sans motif, des informations d'un autre domaine. Il arrive que d'anciens membres du personnel ou mandataires ne reçoivent pas l'ordre de rendre leur clé ou leur badge à l'échéance de leurs rapports de travail, de leur contrat ou à la fin d'une tâche particulière ou que leur compte d'utilisateur ne soit pas bloqué. De telles autorisations devenues *caduques* peuvent être utilisées par la suite contre les intérêts de l'employeur ou de l'adjudicateur. Lorsqu'un engagement, un contrat ou une tâche arrive à son terme, les autorisations correspondantes doivent être retirées. Lorsque des indices donnent à penser que la sécurité de l'information est menacée, les autorisations doivent être immédiatement bloquées ou retirées. Ces deux mesures doivent en particulier contribuer à réduire le risque de délits commis en interne.

Section 5 Protection physique

Art. 22 Principe

Les mesures physiques de protection servent à réduire les risques engendrés par des menaces physiques. Les infractions commises par des personnes comptent parmi ces menaces (par ex. l'espionnage, le vol, le vandalisme ou le sabotage). Tombent également dans cette catégorie les dommages provoqués par des éléments naturels (par ex. la chaleur, le feu, l'eau, la poussière, les vibrations). L'art. 22 fixe le principe selon lequel les autorités et organisations soumises à la loi doivent assurer la

protection physique de leurs informations et moyens informatiques. L'objectif est en particulier d'empêcher tout accès non autorisé aux informations et moyens informatiques, par exemple au moyen de contrôles d'accès, de caméras vidéo, de systèmes de verrouillage, de conteneurs sécurisés, d'appareils de destruction de documents, etc. Pour prévenir les dommages causés par des éléments naturels, on préconise par exemple de poser des installations d'alarme incendie et d'extinction automatique. Les mesures de protection physique concernent aussi bien les informations et moyens informatiques se trouvant dans les locaux de l'autorité ou de l'organisation concernée que ceux auxquels le public peut accéder. Dans le second cas, il s'agit d'une part d'informations et de moyens informatiques emmenés hors de leur endroit habituel (bureau) et qui doivent être protégés en dehors du périmètre de sécurité usuel et, d'autre part, d'informations et d'installations, de câbles et de conduites d'alimentation qui ne sont pas soumis à un contrôle permanent de l'autorité ou de l'organisation. Une attention toute particulière doit être accordée aux points d'accès, par exemple aux zones de livraison et de chargement.

Art. 23 Zones de sécurité

La délimitation de zones ou de locaux en zones de sécurité constitue une mesure physique en faveur de la sécurité de l'information. Cette mesure est déjà en partie appliquée au sein de la Confédération, notamment pour protéger les locaux abritant des serveurs ou certaines salles de conduite. Une zone de sécurité doit être prédéfinie, identifiable et protégée en conséquence. La législation d'exécution du Conseil fédéral définira vraisemblablement deux types de zones de sécurité en tenant compte, pour chacune d'elles, de la criticité des informations qui y sont traitées ou des moyens informatiques qui y sont exploités. Les mesures à prendre dans ces deux types de zones devront être définies en fonction du risque. Contrairement aux dispositions de la législation d'autres pays ou organisations internationales et de celle relative à la protection des ouvrages militaires (cf. également al. 4), les autorités et organisations soumises à la loi ne sont pas tenues de désigner de tels emplacements comme zones de sécurité. Elles instituent ces zones à l'issue d'une évaluation des risques.

Les al. 2 et 3 règlent les pouvoirs particuliers de l'autorité ou de l'organisation qui institue une zone de sécurité.

- L'introduction de certains objets dans une zone de sécurité peut être limitée. Les appareils de prises de vues ou de sons (téléphones et ordinateurs portables y compris) requièrent généralement une autorisation spéciale.
- Les domaines des zones de sécurité jugés particulièrement importants pour la sécurité de l'information (par ex. la zone d'accès à un local spécial pour serveurs, le poste de travail de l'administrateur ou la salle des archives contenant des informations classifiées «secret») peuvent être surveillés par des appareils vidéo.
- À l'entrée ou à la sortie d'une zone de sécurité, l'autorité ou l'organisation peut ordonner un contrôle des sacs ou des fouilles afin d'éviter que des personnes amènent sans autorisation des appareils ou repartent avec des informations (par ex. avec une clé USB).

– Pour une mise en œuvre efficace des prescriptions, il est également nécessaire de pouvoir contrôler les bureaux. Lors de ces contrôles, le respect de ce que l'on appelle la «politique du bureau bien rangé» est aussi vérifié (aucune information sensible ne doit traîner sur le bureau ou ailleurs, l'ordinateur doit être verrouillé ou éteint, les supports de données doivent être mis sous clé, les tiroirs doivent être fermés, la corbeille ne doit pas contenir d'informations classifiées, etc.). Le contrôle peut avoir lieu en l'absence de la personne concernée, par exemple de nuit.
– L'autorité ou l'organisation peut exploiter une installation de télécommunication perturbatrice lorsque la zone de sécurité est particulièrement critique. Le besoin réel d'une telle installation ainsi que les conditions de son exploitation sont appréciés à l'aune de la LTC.

Section 6 Systèmes de gestion des données d'identification

Art. 24 Exploitation de systèmes de gestion des données d'identification

Les systèmes centralisés de gestion des données d'identification sont le cœur d'un système de gestion global des données d'identification (système GIA). Les al. 1 et 2, qui décrivent dans les grandes lignes le but et le mode de fonctionnement des systèmes GIA centraux, constituent ainsi le socle sur lequel repose le reste du dispositif normatif. La LSI confère aux autorités soumises à la loi la compétence d'exploiter des systèmes GIA pour contrôler de manière centralisée les personnes, les machines et les systèmes qui requièrent un accès à des systèmes d'information et à d'autres ressources. Le nombre des systèmes GIA n'est pas précisé à dessein. En ce qui concerne l'administration fédérale, il reviendra au Conseil fédéral de décider quels services ou unités administratives exploiteront ce type de système. On peut par exemple imaginer que l'on crée d'abord plusieurs groupements GIA au sein de l'administration fédérale, avant de les consolider partiellement avec le temps. Pour chaque système de gestion des données d'identification, un organe responsable devra être désigné. Il n'est pas possible de désigner les organes responsables dans la loi elle-même, puisque le nombre de systèmes qui seront exploités et l'organisation des groupements GIA sont laissés à la libre appréciation des autorités soumises à la loi.

Art. 25 Échange et harmonisation des données

Un système GIA échange des données personnelles avec d'autres systèmes dans trois cas de figure bien précis.

– Lors de la création d'un nouveau système GIA, ce dernier se procure les informations requises concernant l'identité des collaborateurs dans les répertoires de personnes et d'utilisateurs du domaine couvert. Par la suite, en cours d'exploitation, les mutations effectuées dans les systèmes raccordés doivent être communiquées périodiquement au système GIA.

– Lorsqu'une application informatique qui authentifie elle-même les utilisateurs est raccordée au système GIA, les données utilisées jusque-là pour l'authentification des utilisateurs sont transmises au système GIA central, où elles sont intégrées aux autres données. Les exigences mentionnées à l'al. 2 sont également contrôlées lors de cette transmission. Par la suite, les mutations des données des utilisateurs sont normalement communiquées par l'application au système GIA. Selon les circonstances et l'attribution des tâches, on peut cependant aussi envisager une gestion centralisée des données d'identification pour certains cercles d'utilisateurs.
– Dans le cas le plus fréquent, des données sur l'utilisateur sont transmises lors de chaque ouverture de session. Le système GIA authentifie alors l'utilisateur, complète les données d'identification exigées par l'application à partir de son répertoire (par ex. l'appartenance à un service administratif) ou d'une source externe (par ex. la fonction d'officier public ou de médecin) et met ces données à la disposition de l'application sous forme de confirmations que celle-ci sait interpréter pour octroyer concrètement les droits d'accès.

Art. 26 Utilisation du numéro AVS

Il est très important, pour un système GIA, de pouvoir identifier sans erreur les personnes dont il traite les données. On ne peut tolérer ni la confusion entre deux personnes, ni la fusion des données les concernant à la suite d'une erreur de correspondance. On ne peut non plus admettre l'enregistrement à double des données d'une même personne en raison d'un problème de correspondance. Ce genre de situation peut se présenter lors de la création et de la mise à jour des répertoires d'utilisateurs, mais aussi lors de chaque accès, avec la transmission des données concernant la personne identifiée du système GIA à l'application. L'identifiant personnel le plus sûr, permettant de reconnaître sans erreur son détenteur, est le numéro AVS visé à l'art. 50*c* LAVS. Presque toutes les personnes qui seront enregistrées dans les systèmes GIA prévus disposent de cet identifiant. L'art. 50*e*, al. 1, LAVS exige qu'une base légale au sens formel règle le but de l'utilisation et définisse les utilisateurs légitimés pour que le numéro AVS puisse être utilisé systématiquement en dehors des assurances sociales fédérales.

La communication entre les systèmes GIA et les applications ou d'autres ressources se fait sans numéro AVS. Celui-ci peut en effet être remplacé sans restrictions ni surcoûts disproportionnés par un identifiant personnel sectoriel. En revanche, lors de la maintenance du répertoire des utilisateurs du système GIA, il doit être possible d'utiliser *temporairement* le numéro AVS afin de garantir l'attribution correcte des données personnelles. Dans le cadre de cette comparaison, il est prévu de convertir par un processus irréversible le numéro AVS en un identifiant personnel sectoriel, spécifique au système GIA,. Cet identifiant personnel dérivé sera, d'une part, utilisé pour l'identification des données et, d'autre part, stocké dans le système de gestion des données d'identification pour des harmonisations ultérieures des données. Ce processus permet de garantir un niveau de qualité élevé des données au sein des systèmes GIA, niveau qui ne pourrait être obtenu autrement que moyennant un effort disproportionné. De plus, divers garde-fous limitent l'utilisation du numéro AVS:

– il ne peut être utilisé que si le système qui fournit les données contient et a lui-même le droit d'utiliser le numéro AVS;
– il n'est utilisé que brièvement pour générer l'identifiant sectoriel dérivé et n'est pas enregistré dans le système GIA;
– il n'est utilisé que lors de la reprise ou de l'enregistrement de nouvelles personnes, donc en dehors du système GIA.

Lorsque, dans un cas concret, l'harmonisation des données peut être garantie par un autre moyen sûr et plus simple, par exemple à l'aide d'un numéro personnel interne, on renoncera bien entendu à l'utilisation du numéro AVS. Au besoin, ces cas de figure pourront être précisés dans les ordonnances.

Art. 27 Dispositions d'exécution

Les autorités soumises à la loi se voient conférer le mandat et la compétence d'édicter des dispositions d'exécution étendues sur l'engagement de systèmes GIA.

Chapitre 3 Contrôle de sécurité relatif aux personnes

Section 1 Dispositions générales

Art. 28 But et objet du contrôle

Le CSP est une mesure préventive de protection contre les infractions intentionnelles venant de l'intérieur. Il doit permettre d'identifier le risque de voir les intérêts définis à l'art. 1, al. 2, menacés par une personne donnée dans l'exercice d'une activité sensible. Le CSP consiste donc à déterminer la probabilité qu'une personne donnée puisse menacer, intentionnellement ou par négligence, la sécurité de l'information au sein de la Confédération. Des données sur le parcours de cette personne sont récoltées à cet effet. C'est en effet sur cette base que le risque est évalué ou le pronostic établi . L'appréciation du risque ne repose pas uniquement sur des faits avérés: par la nature des choses, les conclusions tirées des données recueillies peuvent aussi être des hypothèses ou des présomptions (cf. arrêt du Tribunal administratif fédéral A-5617/2013 du 25 mars 2013, consid. 3.4). Après avoir pris connaissance de cette évaluation, l'autorité ou l'organisation soumise à la loi décide seule si elle entend assumer un éventuel risque aggravé, le réduire en posant certaines conditions ou l'éviter en n'engageant pas la personne concernée ou en la licenciant.

Les al. 2 et 3 définissent de manière générale le contenu du contrôle et ses limites, c'est-à-dire quelles données doivent être traitées pour évaluer le risque et quelles données ne peuvent en principe pas être traitées afin de garantir le respect des droits de la personnalité des personnes contrôlées. La pratique a montré qu'un catalogue de données pertinentes pour la sécurité est un bon moyen d'interpréter le contenu matériel d'un CSP. Souvent, une mise en péril ou une violation de la sécurité de l'information par une personne donnée trouve son origine dans des antécédents de la personne ou des circonstances particulières. Par exemple, des difficultés personnelles ou financières ou des relations nouées à l'étranger sur lesquelles la personne concernée garde le silence en Suisse peuvent créer des situations susceptibles de

causer un préjudice considérable à l'État. C'est pourquoi le mode de vie de la personne contrôlée est passé à la loupe. Le catalogue de données évoqué à l'al. 2, concernant le mode de vie de la personne concernée, n'est pas exhaustif et correspond sur le fond à l'art. 20, al. 1, LMSI. La notion d'«activités illégales menaçant la sûreté intérieure et extérieure» est toutefois supprimée: d'une part, ces activités sont déjà couvertes par la notion de mode de vie et, d'autre part, elle met une condition à la collecte de ces données (ces activités doivent être illégales et menacer la sûreté); or leur appréciation ne peut intervenir que dans le cadre de l'évaluation du risque pour la sécurité. Par rapport au droit en vigueur, les droits dont disposent les services spécialisés CSP de collecter des données ne sont pas restreints par cette suppression. Les limites posées par les art. 3, al. 1, et 20, al. 1, 2e phrase, LMSI, sont toutefois maintenues.

Art. 29 Liste des fonctions

L'art. 29 définit, en relation avec l'art. 30, le personnel assujetti au CSP. Les autorités soumises à la loi (mais non les organisations) doivent édicter, dans leur domaine, une liste des fonctions qui impliquent l'exercice d'une activité sensible et dont les titulaires doivent dès lors faire l'objet d'un contrôle. S'agissant des conditions matérielles permettant l'inscription d'une fonction dans cette liste, le système actuel de la LMSI n'est pas repris purement et simplement. Le critère de la *régularité* est écarté, en particulier dans le cadre du traitement d'informations classifiées (cf. ch. 1.2.5). Le point déterminant pour l'assujettissement du personnel fédéral et des militaires au CSP est de savoir si la personne titulaire d'une fonction *doit* exercer une activité sensible pour accomplir sa tâche. C'est uniquement si l'exercice d'une telle activité est effectivement *nécessaire* que la fonction doit être inscrite dans la liste des fonctions à contrôler.

Quelques exemples fictifs permettent d'illustrer l'application de ce principe.

- Une collaboratrice de l'Office fédéral de l'environnement est, dans le cadre de ses tâches, responsable de l'étude de l'impact des constructions et des ouvrages militaires sur l'environnement. À cette fin, elle doit traiter des informations classifiées dès l'échelon «confidentiel» et, parfois, accéder à des zones de protection 2 d'ouvrages militaires. Sa fonction doit figurer dans la liste.
- Un collaborateur de l'AFF doit, à titre exceptionnel, évaluer les effets d'une demande classifiée «confidentiel» adressée au Conseil fédéral. En situation normale, d'autres collaborateurs sont responsables du traitement de telles affaires, mais ils sont soit en vacances, soit en arrêt maladie. Cette tâche n'entre normalement pas dans le cahier des charges de ce collaborateur et, par conséquent, sa fonction ne doit pas être inscrite dans la liste.
- De temps en temps, le personnel de nettoyage employé par une autorité accède involontairement à des informations classifiées lorsque, dans le cadre de ses activités ordinaires de nettoyage des bureaux, il tombe sur des supports d'informations que les membres du personnel de la Confédération n'ont pas rangés ou détruits conformément aux prescriptions. Le personnel de nettoyage n'a pas pour tâche de traiter des informations classifiées. Les

fonctions en question ne doivent donc pas être reprises dans la liste, à moins que la fonction particulière implique des travaux de nettoyage à l'intérieur d'une zone de sécurité.

Le critère de la *régularité*, qui est de facto presque toujours rempli, n'est pas pertinent sous l'angle juridique. Même si la description d'un poste ne prévoit que 5 % du temps de travail pour accomplir des tâches sensibles, cette fonction doit être inscrite dans la liste, même lorsque la personne titulaire de cette fonction n'a, peut-être, pas dû accomplir de telles tâches pendant un temps relativement long. L'éventualité de l'exercice d'une activité sensible dans le cadre de cette fonction ne justifie par contre en aucun cas son inscription dans la liste.

Cette approche restrictive implique que les autorités et organisations soumises à la loi possèdent une claire vue d'ensemble des processus d'affaires et des domaines d'activité, tant internes que transversaux, impliquant l'exercice d'activités sensibles. Prendre du recul dans ce domaine et garder une vue d'ensemble constitue une mesure de base dans le domaine de la gestion des risques pour la sécurité de l'information. Les raisons menant à l'inscription d'une fonction dans la liste correspondante doivent être justifiables: les descriptifs de postes des différentes fonctions doivent décrire précisément les tâches dont l'exécution nécessite l'exercice d'une activité sensible. En outre, les autorités et organisations soumises à la loi sont tenues, indépendamment de tout assujettissement à un CSP, de prendre les mesures qui s'imposent afin de réduire au strict minimum le cercle des personnes devant exercer des activités sensibles.

L'utilisation du verbe *édicter* indique clairement qu'il s'agit d'une délégation formelle du pouvoir législatif aux autorités soumises à la loi. Ainsi, les listes des fonctions devront figurer dans des ordonnances ou des règlements. Pour l'administration fédérale, il s'agira grosso modo de maintenir le système actuel. Le Conseil fédéral pourra habiliter les départements et la ChF à établir leurs propres listes détaillées en se fondant sur la répartition des compétences prévues par la LOGA.

Al. 2: en vertu l'al. 1, seules les autorités soumises à la loi sont responsables de l'appréciation du caractère sensible des fonctions. Les listes de fonctions lient en principe les services spécialisés CSP: ces derniers ne peuvent vérifier pour chaque CSP si la fonction est véritablement sensible sous l'angle de la sécurité: la charge de travail serait disproportionnée. Il faut dès lors s'assurer que les autorités en question garantissent l'actualité de leurs listes et, partant, la correspondance entre les fonctions répertoriées et leur sensibilité effective.

Art. 30 Personnes soumises au contrôle

Les al. 1 à 3 définissent les personnes soumises au contrôle. Dans le contexte international, les conditions relatives au CSP sont réglées par les traités internationaux correspondants. Le principe de l'al. 1, let. c, s'applique aussi aux personnes devant exercer une activité sensible sur mandat d'une autorité étrangère ou d'une organisation internationale. Dans le cas exceptionnel d'une fonction qui remplit les critères visés à l'art. 29 sans être encore répertoriée dans la liste correspondante, le contrôle peut être réalisé avec l'accord exprès de l'autorité soumise à la loi. En ce qui concerne l'administration fédérale, le Conseil fédéral peut déléguer sa compétence

décisionnelle en la matière au chef du département concerné. Après le contrôle, la liste doit être modifiée. Les membres des autorités élus par le peuple ou les magistrats nommés par l'Assemblée fédérale ne sont en principe pas soumis à un CSP, même s'ils exercent souvent une activité sensible dans le cadre de leurs fonctions. L'exception est toutefois liée à la fonction et n'est donc que relative: par exemple, si un membre de l'Assemblée fédérale est astreint au service militaire et doit exercer à ce titre une activité sensible, il sera soumis à un CSP par rapport à ses fonctions militaires. Bien qu'ils ne soient pas explicitement mentionnés, les magistrats exerçant la fonction de chancelier auprès d'un canton ne sont pas non plus contrôlés.

Art. 31 Degrés de contrôle

La LMSI ne fixe pas de règles pour les degrés de contrôle. Le principe de la légalité exige cependant, en raison de la grave atteinte aux droits fondamentaux des personnes assujetties à un CSP, que les modalités les plus importantes de cette atteinte soient définies dans une loi au sens formel. Étant donné que les degrés de contrôle déterminent l'ampleur de l'atteinte, ils doivent être réglés dans la LSI. Le projet prévoit désormais (cf. ch. 1.2.5) deux degrés de contrôle.

– Le contrôle de sécurité de base s'applique aux activités sensibles dont l'exercice inadéquat ou contraire aux prescriptions est susceptible de nuire considérablement aux intérêts définis à l'art. 1, al. 2. Compte tenu du potentiel de dommage mentionné, il s'agit implicitement: (a) du traitement d'informations classifiées «confidentiel»; (b) de l'administration, de l'exploitation, du contrôle ou de la maintenance des moyens informatiques relevant de la catégorie de sécurité «protection élevée»; (c) de l'accès à des zones de sécurité où les activités visées aux let. (a) et (b) sont exercées. Un CSP est également nécessaire pour accéder aux zones de protection 2 d'un ouvrage militaire.
– En toute logique, le CSP élargi est réalisé dans le cas: (a) du traitement d'informations classifiées «secret»; (b) de l'administration, de l'exploitation, du contrôle ou de la maintenance de moyens informatiques relevant de la catégorie de sécurité «protection très élevée»; (c) de l'accès à des zones de sécurité où les activités visées aux let. (a) et (b) sont exercées. Un CSP élargi est également nécessaire pour accéder aux zones de protection 3 d'un ouvrage militaire.

L'élément déterminant du degré de contrôle n'est pas seulement la sensibilité effective de la fonction concernée. Il incombe aux autorités soumises à la loi de définir les degrés de contrôle pour les fonctions et mandats concernés et de veiller à ce que les collaborateurs internes et externes soient soumis au même degré de contrôle lorsque les fonctions sont de sensibilité égale (cf. ch. 1.1.4). L'appréciation des responsables hiérarchiques lie en principe le service spécialisé CSP. Ce dernier collecte les données pour le degré de contrôle requis (cf. art. 35) et applique dans l'évaluation du risque les critères du degré de contrôle concerné. Étant donné que le dommage potentiel justifiant un CSP élargi est bien plus important que dans le cas d'un CSP de base, les mêmes faits peuvent conduire à un risque de sécurité plus élevé dans un CSP élargi que dans un CSP de base.

Section 2 Procédure

Art. 32 Services compétents

L'al. 1 confère aux autorités soumises à la loi et aux cantons une compétence formelle pour déterminer les responsabilités pour l'ouverture de la procédure de contrôle et la décision concernant l'exercice de l'activité sensible.

- Les services spécialisés CSP ne peuvent en aucun cas ouvrir et réaliser un CSP de leur propre chef; ils doivent toujours être mandatés à cet effet. Les autorités soumises à la loi désignent dès lors, dans leur domaine de compétence, les services habilités à ouvrir une procédure de contrôle et à attribuer aux services spécialisés CSP le mandat afférent. Généralement, il s'agit du service du personnel, mais dans de nombreuses unités administratives la compétence a été attribuée à d'autres détenteurs de fonction (par ex. aux préposés à la sécurité de l'information). Le Conseil fédéral peut aussi, s'il l'estime utile, habiliter certains tiers à ouvrir un CSP, en particulier les entreprises qui exercent souvent des activités sensibles au profit de la Confédération et qui sont au bénéfice d'une DSE au sens de l'art. 62.
- La compétence de décider de l'exercice d'une activité sensible est nécessairement liée à la responsabilité de la prise en charge du risque éventuel. Il s'agit donc fondamentalement d'une affaire de personnel, soumise aux règles du droit du personnel. Des exceptions sont néanmoins possibles, notamment pour décider de l'exercice d'une activité sensible par des collaborateurs externes. On notera à cet égard que les services décidant de l'attribution de l'activité ne sont souvent pas les mêmes que les services qui ouvrent la procédure.

Pour les contrôles, le Conseil fédéral recourt aujourd'hui à deux services spécialisés CSP. L'un relève du DDPS et est compétent pour la plupart des contrôles; l'autre est subordonné administrativement à la ChF et contrôle les cadres de haut niveau de la Confédération de même que les employés de l'autre service spécialisé CSP. Globalement, le système en vigueur sera maintenu, mais il reviendra au Conseil fédéral de décider de l'organisation et de la subordination des services spécialisés (cf. également art. 49, let. b, et l'avis du Conseil fédéral du 22 avril 2009 à propos de la recommandation 3 de la CdG-N dans son rapport du 28 novembre 2008 sur le contrôle de suivi de l'inspection relative aux circonstances de la nomination de Roland Nef au poste de chef de l'armée[27]). Les services spécialisés CSP doivent pouvoir évaluer le risque pour la sécurité de l'information de la manière la plus objective possible, c'est-à-dire en se fondant sur les données collectées et conformément à la jurisprudence et aux connaissances scientifiques les plus récentes. Les responsables hiérarchiques ne sauraient donc s'immiscer dans la procédure de contrôle; dans le cas contraire, un CSP pourrait être utilisé abusivement à des fins personnelles ou politiques. La LSI dispose dès lors que les services spécialisés CSP mènent leurs évaluations en toute indépendance (sans aucune instruction), ce qui correspond au droit en vigueur (cf. art. 21, al. 1, LMSI).

27 FF **2009** 3045

Art. 33 Consentement et collaboration

En principe, la réalisation d'un CSP nécessite le consentement exprès de la personne concernée. Les services spécialisés CSP ont un devoir implicite d'information à cet égard: dans la pratique, la personne concernée reçoit une notice qui précise les bases légales du CSP (y compris celles régissant la collecte des données) et explique la procédure de contrôle. Seules l'armée et la protection civile peuvent réaliser des CSP sans l'accord des personnes concernées. Cette exception s'impose: à défaut, certains militaires ou membres de la protection civile pourraient refuser de donner leur consentement pour se soustraire à leur obligation de servir en empêchant le contrôle.

L'al. 3 renvoie implicitement à l'art. 13, al. 1, let. c, PA: la jurisprudence et la doctrine afférentes s'appliquent. Dans le cadre de l'obligation de collaborer à la procédure, la personne contrôlée doit participer à l'établissement des faits. Outre la communication des renseignements lors de l'audition, l'obligation s'étend à des documents complémentaires utiles au CSP. La personne contrôlée doit notamment participer à la clarification de sa situation personnelle lorsque les services spécialisés CSP manquent d'informations à ce propos et qu'elles ne sont pas en mesure d'établir les faits sans prendre d'autres mesures. La personne interrogée est tenue de dire la vérité. Le contrôle de sécurité serait illusoire si, sous le couvert des droits fondamentaux, la personne concernée pouvait refuser de répondre à des demandes de renseignements sur d'éventuels abus d'alcool ou de stupéfiants, des dettes personnelles, des occupations accessoires, etc., et si des faits de cette nature n'entraient pas dans l'appréciation du risque pour la sécurité (cf. également le message relatif à la LMSI, FF *1994* II 1123, 1188). Elle peut toutefois déclarer ne pas vouloir répondre à certaines questions. Il appartient alors au service spécialisé d'apprécier le refus de répondre ou le refus de fournir d'autres documents: elle dispose d'une certaine liberté pour poser des questions en rapport avec la vie privée de la personne concernée. Si cette dernière refuse de collaborer dans une mesure telle qu'une appréciation correcte n'est plus possible, le service spécialisé CSP établit une constatation (art. 40, al. 1, let. d).

Art. 34 Moment du contrôle

Le droit en vigueur (art. 19, al. 3, LMSI) exige que le CSP soit effectué avant l'attribution de la fonction ou du mandat. Cette règle (en soi logique) ne peut toutefois être appliquée car elle entraînerait une augmentation importante des ressources en personnel des services spécialisés CSP. C'est pourquoi l'al. 1 n'applique cette règle qu'au personnel des autorités et organisations soumises à la loi et des cantons. Les employeurs conservent naturellement le droit d'attendre la déclaration du service CSP avant de confier une activité sensible à la personne concernée. Dans les faits, ils vont probablement introduire dans les contrats de travail une clause selon laquelle l'établissement d'une déclaration de sécurité assortie de réserves, d'une déclaration de risque ou d'une constatation (cf. art. 40, al. 1, let. b à d) peut être un motif de retrait de l'activité sensible, voire de résiliation immédiate des rapports de travail. Pour réduire provisoirement les risques, les employeurs peuvent demander un extrait du casier judiciaire ou du registre des poursuites (art. 20*a* LPers).

Pour les personnes nommées par le Conseil fédéral, la réglementation correspond au droit en vigueur (art. 19, al. 3, LMSI). Il en va de même des tiers chargés d'exécuter un mandat sensible: le CSP doit être terminé avant que la personne puisse être chargée d'exercer l'activité sensible concernée (cf. également ch. 1.1.4: rapport de la CdG-E 2014 sur les collaborateurs externes de la Confédération, recommandation 6). La raison qui justifie de traiter, sur le plan juridique, le personnel fédéral différemment des tiers tient aux conditions particulières qui le lient à la Confédération. En principe, on peut attendre de lui une grande loyauté pour défendre les intérêts de cette dernière. En outre, le personnel fédéral travaille, la plupart du temps, directement auprès de l'employeur, ce qui facilite les contrôles.

Dans le contexte international, même si le traité applicable ne le règle pas expressément, une déclaration de sécurité est toujours exigée avant qu'une activité sensible puisse être exercée.

Art. 35 Collecte des données

La collecte des données s'inspire largement de la législation en vigueur (cf. art. 20 LMSI). Les al. 1 et 2 règlent les modalités de la collecte des données, qui est réorganisée en raison du passage de trois à deux degrés de contrôle. Pour les deux degrés de contrôle, la collecte des données fait l'objet d'une disposition *potestative*. Les services spécialisés CSP ne doivent pas obligatoirement recourir à tous les moyens disponibles pour évaluer le risque. Cette règle est particulièrement importante pour le contrôle élargi, parce que la réduction du nombre des degrés de contrôle ne doit pas entraîner une augmentation massive des coûts des CSP. Dans ses dispositions d'exécution, le Conseil fédéral pourra aussi déterminer quelles données *devront* être collectées et à quel moment.

Pour le contrôle de base, les sources ci-après peuvent être consultées.

– Le casier judiciaire, les dossiers des autorités pénales (cf. art. 12 CPP), y compris ceux des autorités pénales des mineurs, et les banques de données du SRC, des autorités de police et de sécurité de la Confédération et des cantons peuvent donner des indications sur la loyauté et sur les éventuels antécédents d'une personne. La LSIP habilite les services spécialisés CSP à consulter en ligne l'index national de police. Ils pourront aussi prendre connaissance, aisément et efficacement, des données des organes de police cantonaux qui y sont reliés. Il va de soi que les résultats doivent être pondérés en fonction de l'activité envisagée pour la personne concernée et remis dans leur contexte. Il ne revient pas aux autorités pénales de décider quels documents sont nécessaires à un CSP. Le service spécialisé CSP doit avoir accès à tous les documents disponibles pour se faire une idée complète de la personne contrôlée.
– Les informations obtenues à partir des registres des offices des poursuites et faillites sont nécessaires pour pouvoir évaluer la situation financière de la personne concernée: des risques de corruption, par exemple, peuvent en effet représenter un risque pour la sécurité.
– Désormais, les documents et résultats des CSP antérieurs peuvent aussi être utilisés. D'une part, le service spécialisé doit apprécier les mêmes faits de

manière cohérente. Dès lors, une personne donnée ne devrait en principe pas être jugée sur les mêmes faits différemment qu'à l'occasion d'un contrôle antérieur de même degré. D'autre part, la collecte des données s'en trouve facilitée, car certains faits ont déjà été établis à la faveur de contrôles antérieurs. En raison des délais de répétition du contrôle, il peut arriver qu'une déclaration antérieure contienne des données qui ont été détruites dans le système en vertu de l'art. 48: il va de soi qu'elles ne peuvent alors plus être traitées.

– Les informations émanant de réseaux sociaux non destinés au public et réservés à un cercle fermé de personnes ne sont pas réputées d'accès public et ne peuvent être collectées.

Lors d'un CSP élargi, les services spécialisés peuvent consulter les sources ci-après, en sus de celles qui viennent d'être mentionnées:

– les données des registres fiscaux fédéraux et cantonaux peuvent fournir des informations complémentaires sur la situation économique de la personne concernée, par exemple si l'on constate un écart significatif entre son train de vie et ses déclarations fiscales;

– les données des registres du contrôle des habitants ne sont pas toujours collectées car elles n'apportent souvent qu'une plus-value marginale; elles peuvent néanmoins, dans certains cas, livrer des indices précieux pour l'appréciation de la situation personnelle de la personne concernée;

– lors du contrôle élargi, la situation financière de la personne concernée est analysée en détail; c'est pourquoi les données des établissements financiers et des banques avec lesquels la personne concernée entretient des relations d'affaires peuvent être systématiquement collectées;

– l'audition de la personne concernée sert à vérifier des faits qui ne ressortent pas ou pas clairement de la consultation des registres. L'audition au sens de l'al. 2, let. d, ne doit pas être confondue avec celle de l'al. 3: elle peut être menée sans indice d'un risque pour la sécurité et sa portée n'est pas limitée.

L'al. 3 prévoit que les services spécialisés CSP peuvent auditionner les personnes concernées, indépendamment du degré de contrôle lorsque, dans le cadre de la collecte de données, ils découvrent des indices laissant penser que la personne est susceptible d'engendrer un risque pour la sécurité. La portée de l'audition est limitée aux données qui peuvent être collectées selon le degré de contrôle concerné. Une telle audition peut également avoir lieu lorsque le service spécialisé CSP n'a pu obtenir de données suffisantes sur une période suffisamment longue. Ce peut être le cas par exemple lorsque la personne contrôlée a séjourné longtemps dans un pays où une collecte de données est impossible ou peu fiable. La notion de période suffisante est formulée à dessein de façon peu précise. La réglementation actuelle de l'art. 19, al. 3, OCSP, en vertu duquel les services spécialisés CSP doivent au moins disposer de données couvrant la période de cinq ans précédant l'engagement de la procédure de contrôle de base et la période de dix ans précédant l'engagement de la procédure de contrôle élargi a été critiquée parce qu'elle s'est révélée disproportionnée et trop absolue. On peut envisager deux solutions à cet égard: soit le Conseil fédéral précise dans les dispositions d'exécution l'expression en question, soit son interprétation est

laissée aux services spécialisés CSP. Pour faire la lumière sur des éléments particulièrement pertinents pour la sécurité ou pour obtenir un complément de données sur une plus longue période, les services spécialisés CSP peuvent aussi interroger des tiers. De telles auditions ne peuvent être menées qu'avec le consentement de la personne contrôlée et celui des tiers concernés, ces derniers restant libres de donner des renseignements. Les tiers concernés peuvent donc refuser en tout temps de communiquer des informations, même s'ils ont donné leur consentement.

Par la nature des choses, des questions très personnelles sont posées dans le cadre des auditions au sens de l'al. 2, let. d, ou du présent alinéa. La pertinence des questions dépend toujours du contexte de l'audition ou de la fonction, de la tâche ou de la situation personnelle de la personne soumise au contrôle. Ainsi, certaines questions peuvent se concentrer sur des aspects indispensables à l'appréciation du risque. D'autres en revanche servent à la structuration de l'entretien ou à l'établissement d'une culture du dialogue. Cependant, aucune question étrangère au mandat n'est posée. On ne peut évidemment exclure que la personne contrôlée perçoive l'audition comme un désagrément, ce dont on tient compte en menant l'entretien d'une façon aussi agréable que le but de l'audition le permet. Toutes les informations nécessaires à l'évaluation doivent néanmoins être collectées.

Il arrive que les données nécessaires à l'évaluation du risque concernent non seulement les personnes contrôlées, mais aussi des tiers, par exemple les extraits de comptes bancaires d'une personne mariée. En vertu de l'al. 4, ces données personnelles peuvent également être traitées dans la mesure où elles sont indissociablement liées à la personne faisant l'objet du contrôle et indispensables à l'évaluation du risque. La charge que représenterait l'assentiment des tiers pour traiter des données serait disproportionnée pour les services spécialisés CSP. Pour des raisons de transparence, ceux informeront néanmoins les tiers concernés du traitement des données. Si l'obligation d'information est impossible à respecter ou est disproportionnée, l'art. 18*a*, al. 4, let. b, LPD s'applique.

Art. 36 Assistance administrative

Les services spécialisés CSP ne collectent pas eux-mêmes toutes les données, notamment les données recueillies à l'étranger. Cette collecte passe usuellement par fedpol et le SRC. La loi doit donc faire obligation aux autorités concernées d'accorder l'assistance administrative aux services spécialisés CSP. L'al. 2 règle les modalités particulières de l'assistance administrative de fedpol pour des données étrangères dans le domaine de la poursuite pénale. Selon le droit international, les canaux d'information de police dans le cadre de Schengen et Europol ne sont disponibles que pour l'échange d'informations entre autorités de poursuite pénale. Il en va de même du canal Interpol. Étant donné que les services spécialisés ne sauraient être des autorités de poursuite pénale, même en interprétant largement la notion, et que leurs activités relèvent exclusivement des tâches de police de sécurité, les canaux policiers par lesquels transitent les demandes internationales non liées à des soupçons ne sont en principe pas disponibles dans le cadre des CSP. Toutefois, si les premières investigations du service spécialisé CSP dans les systèmes d'information à sa disposition (notamment l'interrogation automatique des registres au sens de l'art. 46, al. 6) révèlent des indices d'un acte pénalement répréhensible relevant de la

compétence de la police judiciaire fédérale en tant que service central, les canaux cités peuvent être utilisés. Dans ce cas, le service central concerné (fedpol) examine si les données sont pertinentes sous l'angle de la sécurité et peuvent par conséquent être transmises. L'al. 2 a été introduit pour donner une base légale tant aux demandes du service spécialisé CSP qu'aux travaux des services d'analyse de fedpol.

Art. 37 Prise en charge des coûts

La participation des autorités à la procédure reste gratuite. C'est la pratique en vigueur, à l'exception des extraits des registres cantonaux des poursuites et des faillites qui étaient jusqu'ici payants. Les tiers, par exemple des banques ou des instituts de crédit associés à la procédure, doivent être indemnisés si leur participation leur occasionne une charge considérable. Une charge est réputée considérable notamment lorsqu'elle dépasse l'établissement d'extraits de comptes ou d'autres documents similaires et qu'elle exige des recherches particulièrement intensives de la part des tiers sollicités. Le Conseil fédéral réglera les conditions et les montants de ces indemnités dans les dispositions d'exécution.

Art. 38 Classement de la procédure

Une procédure engagée est classée lorsque la personne concernée revient sur son consentement ou lorsque, pour une autre raison, elle n'entre plus en considération pour la fonction prévue ou pour l'exécution du mandat (par ex. parce la personne soumise au contrôle a résilié ses rapports de travail ou en cas d'insolvabilité de l'entreprise pour laquelle la personne concernée aurait dû travailler). Dans un tel cas de figure, tant la personne concernée que le service requérant doivent être informés du classement de la procédure et les données et documents collectés doivent être détruits. La personne concernée est dès lors réputée non contrôlée et ne peut exercer l'activité sensible en question ou la fonction envisagée. Le classement de la procédure est un acte matériel au sens de l'art. 25*a* PA.

Section 3 Évaluation du risque pour la sécurité

Art. 39 Risque pour la sécurité

Le fait que la LMSI ne précise pas explicitement ce qu'il faut entendre par «risque pour la sécurité» a fait l'objet de critiques (cf. ch. 1.1.4: rapport de la CdG-N sur le contrôle de suivi de l'inspection relative aux circonstances de la nomination de Roland Nef au poste de chef de l'armée, recommandation 1). Une disposition fondée sur la jurisprudence du Tribunal administratif fédéral et du Tribunal fédéral est introduite dans le projet pour y remédier. Il va de soi qu'il n'existe pas de méthode purement quantitative permettant d'évaluer le risque que posent les agissements ou les omissions d'êtres humains. D'où le recours à une méthode qualitative qui repose sur la présence et la convergence de facteurs de risque.

La doctrine définit le risque comme le produit de la probabilité de survenance d'un incident et des conséquences de la survenance de ce dernier. La notion d'*activité*

sensible, déterminante pour tout assujettissement à un CSP, renferme dans sa définition les conséquences qui doivent être évitées. En l'occurrence, il s'agit d'un *préjudice considérable ou grave porté aux intérêts définis à l'art. 1, al. 2*. Si la personne assujettie au CSP effectue correctement et dans le respect des prescriptions les tâches qui lui sont confiées, aucun dommage ne peut survenir par sa faute. *A contrario*, l'incident à éviter est celui qui résulte de l'exercice inadéquat ou contraire aux prescriptions d'une activité sensible donnée par la personne faisant l'objet du contrôle. Un risque pour la sécurité existe donc, au sens l'al. 1, lorsque *la probabilité est élevée* de voir la personne concernée exercer l'activité sensible de manière inadéquate ou contraire aux prescriptions, causant de ce fait, pour le moins, une atteinte considérable aux intérêts définis à l'art. 1, al. 2.

Les services spécialisés CSP doivent exclusivement se concentrer sur la probabilité de survenance d'un incident. L'appréciation d'une telle probabilité restera toujours une prévision assortie d'incertitudes: par nature, l'appréciation ne repose pas uniquement sur des faits *avérés* et les conclusions tirées des données recueillies peuvent aussi être des hypothèses ou des présomptions. L'appréciation se fonde sur l'ensemble des éléments disponibles, par exemple la personnalité de la personne concernée, ses antécédents et son train de vie, dans la mesure où ils permettent d'en tirer des conclusions quant à son comportement futur. L'al. 2 énumère donc les facteurs de risque permettant de conclure à un haut degré de probabilité d'un préjudice, à savoir les caractéristiques personnelles particulièrement porteuses de risque. L'énumération s'inspire de la pratique actuelle des services spécialisés CSP, de même que de la jurisprudence du Tribunal administratif fédéral et du Tribunal fédéral. Elle se fonde en principe sur des caractéristiques qui sont autant que possible objectives, mais qui ne peuvent souvent être tirées que d'indices ou déduites du contexte; de plus, ces caractéristiques se recoupent partiellement. L'intégrité et la loyauté d'une personne se jugent en premier lieu par le caractère de celle-ci, ses habitudes et les relations qu'elle a avec son entourage. Ces caractéristiques ne sont ni plus ni moins que les aptitudes de base nécessaires à l'exercice d'une activité sensible. Lorsqu'elles sont présentes, il y a de fortes chances que la personne à qui l'activité sensible sera confiée assumera loyalement ses tâches et veillera aux intérêts de l'employeur ou de l'institution en matière de sécurité. Il est impossible de spécifier au niveau de la loi les indices et corrélations qui pourraient témoigner du manque de loyauté d'une personne, de sa vulnérabilité au chantage ou de l'insuffisance de ses capacités de jugement et de décision: il faut les mettre en lumière lors de chaque appréciation concrète.

En vertu de l'al. 3, le CSP se fonde sur une menace objective, et non sur un comportement fautif, contrairement par exemple au droit pénal pour lequel la faute est une condition sine qua non de la peine. En cas de doute, et contrairement au droit pénal (*in dubio pro reo*), la sécurité de l'État ou les intérêts du pays priment les intérêts de la personne concernée. L'existence d'un risque pour la sécurité doit être justifiée par des faits et des circonstances réelles touchant de près la personne concernée. De pures conjectures, en particulier sur les opinions politiques de cette personne, ne sont pas recevables.

Art. 40 Résultat de l'évaluation

L'al. 1 règle les diverses déclarations des services spécialisés CSP dans lesquelles figurent les résultats des appréciations. Lorsqu'une personne ne peut être évaluée correctement en raison de données insuffisantes au sens de l'art. 35, al. 3, le service spécialisé CSP établit une constatation. Le cas échéant, la personne concernée est entendue au préalable.

Juridiquement, les déclarations des services spécialisés CSP ne sont pas des décisions mais des actes matériels au sens de l'art. 25*a*, al. 1, PA. Tout comme la LMSI (cf. art. 21, al. 3 LMSI), la LSI institue une protection juridique directe au profit de la personne contrôlée (cf. art. 45). Ainsi, la voie de doit prévue à l'art. 25*a*, al. 2, PA n'est pas ouverte (décision relative à des actes matériels). L'al. 2 donne formellement à la personne contrôlée le droit de donner son avis. Concrètement, cela signifie que lorsque le projet de déclaration visé aux let. b à d est rédigé, la personne concernée doit être informée en bonne et due forme de son contenu et disposer d'un délai approprié pour faire valoir son point de vue.

Art. 41 Notification

Les al. 1 et 2 correspondent sur le fond au droit en vigueur (art. 21, al. 2 à 4, LMSI). L'instance décisionnelle reçoit également la déclaration dans son intégralité, car dans le cas contraire elle ne serait pas en mesure de prendre une décision fondée.

L'al. 3 règle le cas où un CSP est mené alors que la personne concernée est soumise à un contrôle en rapport avec une autre activité au sens des let. a à c (par ex. en vertu de l'art. 20*b* LPers). Dans ce cas, le service spécialisé CSP compétent doit pouvoir informer l'instance décisionnelle concernée de la déclaration rendue lors du contrôle principal. Les dispositions concernant le contrôle de loyauté au sens des art. 20*b* LPers et 113 LAAM exigent que les deux procédures soient réunies si la personne concernée doit aussi faire l'objet d'un CSP en vertu de la présente loi. Les dispositions de l'al. 3 n'exigent pas qu'un autre contrôle soit en cours ou doive être immédiatement répété. La précision est importante notamment pour les contrôles au sens de l'art. 113 LAAM, auxquels tous les militaires peuvent être soumis. Si l'on constate dans le cadre d'un CSP un risque par rapport à l'arme personnelle, les services spécialisés CSP sont autorisés à communiquer la déclaration aux autorités militaires compétentes. L'al. 4 permet aux services spécialisés CSP d'informer l'organe compétent pour statuer sur la remise ou le retrait de l'arme à des militaires potentiellement violents au sens de l'art. 113 LAAM des résultats de leur évaluation afin que celui-ci puisse trancher la question de la remise de l'arme personnelle.

Lorsque les services spécialisés CSP disposent d'indices fondés d'un risque pour la sécurité et qu'il y a urgence, ils peuvent informer à titre préventif les instances compétentes avant même l'achèvement de la procédure. Ces instances peuvent alors prendre les mesures de sécurité provisoires nécessaires.

Section 4 Conséquences de la déclaration

Art. 42 Exercice de l'activité sensible

L'al. 1 correspond à l'art. 21, al. 4, LMSI. Il n'est pas dans les attributions des services spécialisés CSP d'assumer ou de limiter la responsabilité des supérieurs hiérarchiques pour les décisions concernant le personnel, mais uniquement d'informer l'instance de décision d'un risque éventuel. Avant toute décision, l'instance décisionnelle doit prendre connaissance de la déclaration du service spécialisé CSP, seule façon pour elle de décider en tenant compte du risque éventuel.

Les conditions visées à l'al. 3 sont des mesures visant à réduire le risque identifié et relevant généralement du droit du personnel. L'instance décisionnelle peut par exemple exiger que la personne concernée rende compte régulièrement de sa situation financière ou se soumette régulièrement à des tests de dépistage de consommation de stupéfiants. Ces conditions s'appliquent exclusivement à l'exercice de l'activité sensible et non à d'autres tâches. Généralement, les conditions les mieux adaptées à la situation sont recommandées par le service spécialisé CSP. L'instance décisionnelle n'est toutefois pas liée par ces recommandations et peut fixer elle-même ses propres conditions.

La communication de la décision en vertu de l'al. 4 se fait par le système d'information visé à l'art. 46. Elle est avant tout déterminante pour l'autorisation d'accès à certaines zones de sécurité. Les services spécialisés CSP ne tirent aucune conclusion des décisions et ces dernières n'influent d'aucune manière sur leur pratique.

Art. 43 Utilisation de la déclaration pour d'autres activités sensibles

En règle générale, lorsque la personne concernée est au bénéfice d'une déclaration pour un degré de contrôle au moins équivalent et que celle-ci est encore valable, un nouveau contrôle doit être évité pour des raisons d'économies. La condition qui permet d'éviter un nouveau CSP est une approche standardisée lors du contrôle et d'évaluation du risque (cf. commentaire de l'art. 31). Dans la pratique, cette disposition ne pose pas de problèmes lorsqu'une déclaration de sécurité est émise pour un degré de contrôle similaire ou supérieur. Mais des problèmes peuvent par exemple surgir lorsqu'une personne obtient, en particulier pour un degré supérieur de contrôle, une déclaration de sécurité assortie de réserves ou une déclaration de risque. Il est en effet tout à fait possible qu'un risque pour la sécurité soit établi pour le traitement d'informations classifiées «secret», alors que ce risque peut être acceptable pour le traitement d'informations classifiées «confidentiel». Le Conseil fédéral concrétisera cette disposition potestative au niveau de l'ordonnance.

Art. 44 Répétition du contrôle

La LSI ne prescrit aucun intervalle fixe pour ces répétitions: elle se contente de fixer des lignes directrices. La raison est que la répétition des contrôles dépendra davantage du besoin réel de sécurité. Les modalités seront réglées dans les dispositions d'exécution. Le Conseil fédéral doit pouvoir renoncer au contrôle d'un militaire ou

d'un membre de la protection civile lorsque, par exemple, il serait inutile ou disproportionné de répéter le contrôle au vu de la période de service restante.

L'al. 3 règle la répétition extraordinaire. La répétition anticipée du contrôle est motivée par l'apparition de risques nouveaux, par exemple lorsque la personne concernée fait l'objet d'une procédure pénale qui présente un lien potentiel avec l'activité sensible qu'elle exerce.

Art. 45 Voies de droit

Malgré une formulation revue, les al. 1 et 2 correspondent au droit en vigueur (cf. art. 21, al. 2, LMSI). Par rapport à la situation actuelle, le délai d'exercice des droits de consultation et de rectification passe de 10 à 30 jours. La personne contrôlée disposant en vertu de l'al. 3 d'un délai de 30 jours pour former recours auprès du Tribunal administratif fédéral, elle doit pouvoir exercer tous les droits visés à l'al. 1 durant cette période.

Sur le fond, l'al. 3 correspond également au droit en vigueur (cf. art. 21, al. 3, LMSI), étant précisé que les déclarations du service spécialisé CSP sont des actes matériels au sens de l'art. 25*a* PA. L'art. 22 OCSP qualifie les déclarations des services spécialisés CSP de décisions au sens de l'art. 5 PA. Sous l'angle matériel, cette qualification n'est toutefois pas pertinente, car les déclarations n'ont que valeur de recommandation (cf. art. 21, al. 4, LMSI et art. 42 LSI). Compte tenu de la gravité de l'atteinte aux droits de la personnalité de la personne contrôlée, la protection juridique ordinaire pour les actes matériels au sens de l'art. 25*a* PA est remplacée par une voie de droit directe auprès du Tribunal administratif fédéral.

La LSI permet dorénavant au Tribunal administratif fédéral et au Tribunal fédéral d'ouvrir une procédure de CSP pour leurs propres employés et pour les tiers qu'ils mandatent. Dans ces cas, ils seront également compétents pour la décision concernant l'exercice d'une activité sensible et, simultanément, pour une éventuelle procédure de recours. Comme pour les litiges relevant du droit du travail, il en découle un conflit d'intérêts que permet de prévenir la réglementation prévue à l'art. 36 LPers, qui a fait ses preuves.

Section 5 Traitement des données personnelles

Art. 46 Système d'information sur le contrôle de sécurité relatif aux personnes

L'art. 46 correspond sur le fond au droit en vigueur (cf. art. 144 à 149 LSIA). Les deux services spécialisés recourent aujourd'hui à un système (SICSP) utilisé et exploité par le DDPS. Les données récoltées, et notamment les évaluations de risques, sont des données personnelles ou des profils de la personnalité au sens de l'art. 3, let. c et d, LPD. Le système ne sera bien sûr pas utilisé pour les seuls CSP au sens de la LSI, mais également pour les contrôles de loyauté exigés par la législation spéciale et pour l'évaluation du potentiel de violence au sens de la LAAM. Le Con-

seil fédéral définira les compétences en matière de protection des données (cf. art. 49, let. d).

Pour le contrôle d'identité, le système utilise son propre numéro d'enregistrement. Le numéro AVS n'est utilisé que si un autre système y recourt systématiquement. Il s'agit en premier lieu du système d'information SIPA du Groupement de l'armement. Étant donné que le SIPA utilise systématiquement le numéro AVS, ce dernier est repris à l'ouverture d'un CSP par l'armée. Dans le cadre de ce système d'information, le numéro d'enregistrement propre au système est à nouveau utilisé. Lors de l'harmonisation avec le SIPA, la concordance avec le numéro AVS doit toutefois être rétablie.

Al. 6: en vertu de l'art. 19, al. 3, LPD, les données sensibles ne peuvent être rendues accessibles en ligne que si une loi au sens formel le prévoit expressément. L'efficacité de la procédure de contrôle peut être renforcée si les accès aux systèmes d'information de la Confédération, concédés par la législation aux services spécialisés CSP, se traduisent par une consultation automatique en ligne. Les bases légales formelles des trois systèmes d'information évoqués prévoient d'ores et déjà l'accès des services spécialisés CSP. Les prérogatives de ces derniers ne changent donc pas. Jusqu'ici toutefois, les employés des services spécialisés devaient consulter manuellement chacun des systèmes. À l'avenir, seuls les systèmes dont le consultation automatique aura fourni un résultat (c'est-à-dire qui contiennent une mention de la personne concernée) devront encore être consultés manuellement (cf. également art. 36, al. 2). Cette procédure, qui devra être détaillée au niveau de l'ordonnance, réduit par ailleurs sensiblement les risques d'erreurs lors de la saisie manuelle. Il va de soi que les cantons pourront ménager aux services spécialisés CSP un accès automatique à leurs banques de données.

Art. 47 Consultation et communication des données

Les al. 1 à 3 de l'art. 47 correspondent au droit en vigueur (cf. art. 144 à 149 LSIA), mais ils sont plus explicites en raison de l'art. 19, al. 3, LPD. Les listes au sens de l'al. 4 ne sont communiquées qu'en cas de besoin prouvé. Elles sont remises hors du système d'information.

Art. 48 Conservation, archivage et destruction des données

L'art. 48 correspond sur le fond au droit en vigueur (cf. art. 144 à 149 LSIA et OCSP). L'al. 1 crée la base légale de l'enregistrement sonore des auditions. En vertu de l'al. 2, la durée de conservation des données ne peut dépasser dix ans. Si une personne a déjà subi plusieurs contrôles, les données remontant à plus de dix ans doivent être détruites. Les Archives fédérales jugent quelles informations contenues dans le système sont dignes d'archivage (al. 3); il s'agit notamment de statistiques sur les cas à risques et le nombre de CSP réalisés. Si la procédure est classée au sens de l'art. 38, il est possible (bien que cela semble improbable) que la personne concernée exige une décision et forme ensuite un recours devant le Tribunal administratif fédéral. Les services spécialisés ne peuvent dès lors détruire immédiatement les données.

Section 6 Dispositions édictées par le Conseil fédéral

Art. 49

Le Conseil fédéral devra édicter des dispositions complémentaires ou des normes primaires. Ces dispositions vont au-delà des dispositions d'exécution pour lesquelles le Conseil fédéral est compétent en vertu de l'art. 182 Cst. L'art. 85, al. 1, donne en effet aux autorités au sens de l'art. 2, al. 1, la compétence d'édicter les dispositions portant exécution de la présente loi.

- Let. c: les autorités de sécurité étrangères n'autorisent l'accès à des informations classifiées, à du matériel classifié et à des zones de sécurité qu'aux personnes disposant d'un certificat de sécurité. L'autorité suisse compétente (probablement le service spécialisé de la Confédération pour la sécurité de l'information au sens de l'art. 84) doit être habilitée à délivrer les certificats de sécurité aux personnes concernées. La décision de l'instance décisionnelle est déterminante, et non la déclaration rendue par le service spécialisé.
- Let. d à f: l'art. 16, al. 2, LPD fait obligation au Conseil fédéral d'édicter des dispositions complémentaires sur l'organisation des compétences et des responsabilités pour la protection des données (y compris la sécurité des données) traitées dans le système d'information visé à l'art. 46. Les données traitées dans le cadre des CSP étant sensibles, la légalité de leur traitement doit être vérifiée périodiquement par un service indépendant des services spécialisés CSP.

Chapitre 4 Procédure de sécurité relative aux entreprises

Section 1 Dispositions générales

Art. 50 But de la procédure

Pour le but poursuivi par la PSE, on se référera au ch. 1.2.6.

Art. 51 Entreprises concernées

Le sens donné par la LSI au terme «entreprise» ne correspond pas nécessairement à celui d'une entreprise considérée dans sa globalité. Il s'applique surtout aux parties d'une entreprise et aux personnes effectivement chargées d'exécuter un mandat sensible.

- La let. a concerne le cas principal visé par la procédure: celui où une autorité ou une organisation soumise à la loi envisage d'adjuger à une entreprise un mandat sensible pour lequel cette dernière a soumissionné. La PSE est, en principe, une affaire d'ordre national. C'est pourquoi les entreprises dont le siège est à l'étranger et qui entendent obtenir un mandat émanant des autorités suisses doivent se faire contrôler par l'État dans lequel elles ont leur siège. Les compétences et les modalités de la procédure sont réglées par des traités internationaux au sens de l'art. 88.

– À l'inverse, la let. b traite le cas des entreprises qui ont leur siège en Suisse et soumissionnent pour des mandats émanant de l'étranger, dès lors qu'elles doivent présenter aux autorités étrangères une déclaration de sécurité établie par les autorités suisses. Cette procédure et la certification qui s'y rapporte constituent une tâche officielle qui ne peut être confiée au secteur privé, car les autorités étrangères exigent systématiquement un «sceau officiel de sécurité» de l'État où l'entreprise a son siège. La Confédération n'ayant dans ce cas aucun intérêt immédiat à la procédure, l'entreprise en assume les coûts (al. 3). Le Conseil fédéral réglera ce point au niveau de l'ordonnance.

Dans la pratique, le consentement exigé de l'entreprise ne pose jamais de problèmes puisque cette dernière est intéressée financièrement à l'adjudication du mandat.

Art. 52 Classement de la procédure

La PSE n'est menée que si certains critères et conditions (par ex. l'assentiment) sont remplis. Si l'entreprise ne remplit plus ces critères alors que la PSE est en cours, la procédure est classée et toutes les données et documents afférents sont détruits. Selon la let. c, ce peut aussi être le cas lorsque l'entreprise ne peut plus du tout remplir le mandat, par exemple en raison de sa mise en faillite ou de la destruction de son site de production par un incendie. L'al. 2 dispose que la PSE est menée par un service spécialisé chargé de la procédure de sécurité relative aux entreprises (service spécialisé PSE). Au sein de la Confédération, un seul service mènera ces procédures, ce qui correspond à la situation actuelle. Le service spécialisé PSE doit notifier le classement de la procédure à l'entreprise et à l'adjudicateur.

Section 2 Ouverture de la procédure

Art. 53 Demande d'ouverture de la procédure

Le service spécialisé PSE n'agit que sur demande (et non sur mandat) des autorités ou organisations soumises à la loi. Ces dernières sont toutefois tenues de déposer une demande lorsqu'elles entendent confier un mandat sensible à une entreprise. Les autorités doivent régler les compétences relatives à la demande. Selon leurs besoins organisationnels, il peut s'agir d'un service central ou de tout organe compétent pour attribuer des mandats sensibles à des entreprises du secteur privé (cf. également ordonnance du 24 octobre 2012 sur l'organisation des marchés publics de l'administration fédérale[28]).

Dans le contexte international, l'ouverture de la procédure est généralement requise par les autorités étrangères de sécurité au moyen du formulaire *Facility Security Clearance Information Sheet* adressé aux autorités de sécurité suisses et d'une confirmation de l'entreprise concernée. La réponse est apportée dans le cadre d'une procédure standard. Les modalités de ces procédures seront réglées par voie d'ordonnance.

28 RS **172.056.15**

Art. 54 Examen de la demande

Après le dépôt de la demande, le service spécialisé PSE vérifie tout d'abord que les conditions sont réunies (par ex. l'attribution d'un mandat sensible) avant d'engager, le cas échéant, la procédure. Lorsque le risque pour la sécurité de l'information peut, dans un cas particulier, être suffisamment réduit par d'autres mesures, le service spécialisé PSE peut, en accord avec l'adjudicateur, renoncer à la procédure, ce qui permet d'éviter des dépenses inutiles et des contraintes bureaucratiques. Lorsque le mandat placé sous le contrôle de l'adjudicateur est exécuté dans les locaux de ce dernier et qu'aucun document n'a été remis à l'entreprise, des CSP peuvent souvent s'avérer suffisants. Si le service spécialisé renonce à la PSE, il recommande aussi les mesures de sécurité qu'il juge adéquates. Dans ce cas, il n'a plus la compétence d'imposer quoi que ce soit.

Art. 55 Définition des exigences en matière de sécurité

Après l'ouverture de la procédure, le service spécialisé PSE fixe, en accord avec l'adjudicateur, les exigences en matière de sécurité de l'information qui s'imposent pour l'exécution du mandat. Dans la mesure où l'exercice d'une activité sensible est déjà nécessaire lors de la procédure d'adjudication, les mesures de sécurité sont également fixées pour cette phase-là. Cette situation se produit souvent lorsque la divulgation d'informations classifiées ou l'accès à des zones de sécurité est nécessaire en vue de l'établissement d'une offre.

Section 3 Évaluation des entreprises

Art. 56 Qualification

La notion de *qualification* est prise dans le sens du droit des marchés publics. Le maintien de la sécurité de l'information n'est certes pas un critère formel de qualification au sens de l'art. 9 LMP, mais le projet l'introduit pour l'exécution de mandats sensibles. L'examen de la qualification sous l'angle de la sécurité équivaut à une évaluation du risque. Pour des raisons économiques et de protection des données, cet examen du risque ne doit pas être mené auprès de tous les soumissionnaires, mais uniquement auprès de ceux qui entrent en ligne de compte pour l'adjudication. Si un risque pour la sécurité de l'information au sens de l'art. 58 est décelé, l'entreprise concernée n'est pas qualifiée. Le service spécialisé PSE ne doit être soumis à aucune instruction pour l'évaluation de la qualification. En l'occurrence, il doit pouvoir procéder à cette évaluation en faisant abstraction des intérêts de politique économique (cf. également art. 32, al. 2).

Art. 57 Collecte des données

L'art. 57 crée la base légale formelle de la collecte des données pour l'examen de la qualification des entreprises. L'al. 1 énumère les données permettant au service spécialisé PSE d'évaluer la qualification. Les données nécessaires sont surtout recueillies auprès de l'entreprise elle-même, avec son consentement. Les résultats

des recherches auprès du SRC revêtent également une importance particulière. Enfin, le service spécialisé PSE peut encore recueillir des données concernant l'entreprise auprès du registre du commerce ou sur Internet: ces recherches peuvent livrer des renseignements précieux sur la loyauté de l'entreprise (cf. art. 35, al. 1, let. g, pour le CSP). De nombreuses entreprises ayant des liens avec l'étranger, il est nécessaire de recueillir des informations sur ces relations. Plus particulièrement, des informations fournies au SRC par les services de renseignement étranger peuvent donner des indications très utiles sur les risques pour la sécurité. Les modalités de ces demandes et la transmission des renseignements seront réglées au niveau de l'ordonnance.

Art. 58 Évaluation du risque pour la sécurité

Cette disposition correspond à l'évaluation du risque pour la sécurité dans le cadre du CSP. Les mécanismes d'évaluation du risque sont en principe identiques (cf. commentaire de l'art. 39). Un risque pour la sécurité existe lorsque des indices concrets donnent à penser que l'entreprise exécutera selon une probabilité élevée le mandat sensible de manière inadéquate ou contraire aux prescriptions. Ce peut être le cas par exemple lorsque des données collectées montrent que l'entreprise a commis des actes punissables qui ont un effet sur la sécurité de l'information ou lorsque l'entreprise ne compte qu'une personne (raison individuelle) ou encore lorsque certaines personnes sont indispensables (c'est-à-dire qu'il s'agit d'experts qui ne peuvent être remplacés ou qui gèrent l'entreprise et que le mandat ne pourrait être accompli sans leur participation): une déclaration de risque dans le cadre d'un CSP pour ces personnes peut avoir pour conséquence que l'entreprise dans son ensemble doive être réputée représenter un risque pour la sécurité. La PSE vise toutefois principalement à empêcher que des entreprises qui pourraient par exemple être pilotées ou significativement influencées par des services de renseignement étrangers ou des organisations poursuivant des buts criminels en raison de leurs rapports de propriété, de leur nature juridique, de leur structure organisationnelle ou de leurs relations d'affaires aient accès à des informations sensibles ou à des vecteurs permettant de lancer des attaques contre des moyens informatiques critiques de la Confédération (cf. ch. 1.2.6).

L'al. 3 dispose que le risque pour la sécurité doit se fonder sur des faits, indépendamment de toute faute de l'entreprise elle-même ou de son personnel, par exemple lorsque l'entreprise à laquelle elle appartient est contrôlée ou influencée par des personnes liées à un service de renseignement étranger ou à une organisation criminelle (cf. le commentaire de l'art. 39, al. 3).

Art. 59 Notification de l'évaluation et exclusion de la procédure d'adjudication

Le service spécialisé PSE notifie à l'entreprise concernée l'évaluation de son aptitude. Si l'entreprise n'est pas d'accord avec l'évaluation du risque, elle peut faire recours devant le Tribunal administratif fédéral (art. 70, al. 1, let. d). L'adjudicateur peut poursuivre la procédure de soumission ou les négociations contractuelles avec les entreprises ne représentant pas de risque pour la sécurité. Il n'est pas autorisé à

recourir et n'est donc qu'informé de l'évaluation. Lorsque le service spécialisé PSE décèle qu'une entreprise pose un risque intolérable pour la sécurité, l'adjudicateur ne peut conclure de contrats avec elle ou lui adjuger le mandat. Il l'exclut de la procédure d'adjudication. Contrairement au CSP, l'adjudicateur est en principe lié par l'évaluation du service spécialisé PSE, car une entreprise au bénéfice d'une déclaration de sécurité (DSE) reçoit de l'État un «sceau officiel de sécurité». L'intégrité de ce «sceau» ne peut être assurée que si la décision relative à la qualification est prise par des spécialistes, raison pour laquelle le service spécialisé PSE rend une décision formelle sujette à recours.

L'al. 3 prévoit une exception pour le cas où où toutes les entreprises qui entrent en considération pour le mandat posent un risque pour la sécurité. La disposition vise principalement les prestations dans le domaine informatique, car certaines entreprises de ce secteur détiennent une position de quasi-monopole. Si un mandat doit être confié à une telle entreprise en l'absence d'autre solution, aucune DSE suisse ne lui est délivrée: la procédure est classée et l'adjudicateur assume la responsabilité de l'application et du contrôle des mesures de sécurité. En vertu de la loi, l'adjudicateur dispose des mêmes droits que le service spécialisé PSE pour exécuter cette tâche.

Section 4 Plan de sécurité

Art. 60 Adjudication et plan de sécurité

Dès que l'adjudicateur a procédé à l'adjudication, il en informe le service spécialisé PSE. Ce dernier entame alors les autres étapes de la procédure. Pour que la sécurité de l'information soit assurée, des mesures adéquates doivent être prises au niveau de l'organisation et du personnel, de même que sur les plans technique et physique. L'entreprise décrit ainsi dans un plan de sécurité comment elle entend répondre aux exigences de sécurité de l'information (cf. également art. 55). En règle générale, les entreprises ont déjà pris des mesures de sécurité dans les domaines les plus variés; en tel cas, le service spécialisé PSE se contente de les vérifier ou, le cas échéant, de les compléter. Toutes les mesures sont définies dans le plan. Le service spécialisé PSE collecte directement auprès de l'entreprise les données nécessaires au contrôle et à l'approbation du plan de sécurité.

Art. 61 Contrôles de sécurité relatifs aux personnes

Le personnel de l'entreprise est contrôlé conformément aux art. 30, al. 1, let. c, ou 30, al. 2. L'art. 31 détermine le degré de contrôle, qui doit être le même pour les collaborateurs internes et externes. Le service spécialisé PSE décide ensuite de manière contraignante si l'activité sensible peut être confiée à la personne contrôlée. Lorsque la procédure est classée en application de l'art. 59, al. 3, il revient à l'adjudicateur de prendre cette décision.

Section 5 Déclaration de sécurité relative aux entreprises

Art. 62 Établissement de la déclaration de sécurité relative aux entreprises

Contrairement à la déclaration de sécurité rendue dans le cadre d'un CSP, la délivrance ou le refus d'une DSE fait l'objet d'une décision au sens de l'art. 5 PA, car elle a des effets juridiques directs pour les participants. Il est rarement arrivé qu'une entreprise n'ait pas appliqué les mesures de sécurité ou qu'elle se soit vu refuser une DSE. Lorsqu'un tel cas se produit, le service spécialisé PSE doit lui accorder un délai lui permettant de remplir ses obligations avant de prendre sa décision de refus. Si l'entreprise n'est pas d'accord avec la décision prise par le service spécialisé PSE, elle peut faire recours devant le Tribunal administratif fédéral (art. 70, al. 1, let. d). La décision est également notifiée à l'adjudicateur, car celui-ci ne doit pas confier le mandat sensible à l'entreprise qui s'est vu refuser la déclaration de sécurité (art. 63). À ce moment de la procédure, l'adjudicateur aura probablement déjà investi des sommes considérables dans le projet. Aussi est-il également en droit de déposer un recours (contrairement à l'art. 59, al. 1).

La limitation à cinq ans de la validité de la DSE vise à garantir une réévaluation à intervalles réguliers de la qualification. De cette façon, on peut tenir compte des changements importants qui surviennent dans l'entreprise et qui influent sur la sécurité de l'information.

Art. 63 Exécution d'un mandat sensible

L'adjudicateur est lié par la décision du service spécialisé PSE. Il ne peut pas confier de mandat sensible à l'entreprise qui s'est vu refuser la DSE (cf. art. 62, al. 2). Inversement, les entreprises au bénéfice d'une DSE sont habilitées à exécuter des mandats sensibles lorsqu'elles remportent l'adjudication correspondante ou obtiennent le contrat. La DSE doit être établie avant que l'adjudicateur confie le mandat à l'entreprise. Cette disposition correspond, sur le fond, à l'art. 34, al. 3, dans le domaine des CSP.

Art. 64 Obligations de l'entreprise

Les entreprises au bénéfice d'une DSE sont tenues de collaborer. Elles ont pour principale obligation d'appliquer dans le cours régulier de leurs affaires les mesures prévues par le plan de sécurité. Elles doivent aussi informer le service spécialisé PSE de toute modification importante pour la sauvegarde de la sécurité de l'information survenant lors de l'accomplissement du mandat sensible. Elles doivent, par exemple, annoncer les nouveaux collaborateurs appelés à exercer des activités sensibles pour qu'ils puissent être soumis à un CSP. En outre, l'entreprise doit immédiatement signaler tout incident dans le domaine de la sécurité.

Art. 65 Contrôles et mesures de protection

Le service spécialisé PSE doit surveiller, au sein de l'entreprise, le respect des mesures relatives au mandat prévues par le plan de sécurité. Le contrôle peut, par nature, être inopiné. Il ne peut se dérouler qu'en présence d'un membre de l'entre-

prise, généralement le préposé à la sécurité. Le service spécialisé PSE, face à des, peut prendre les mesures de protection qui s'imposent s'il trouve des indices concrets donnant à penser que la sécurité de l'information est menacée. Il peut, par exemple, décider la reprise ou la mise en lieu sûr immédiates de certains documents ou matériels. Lorsque la sécurité de l'information ne peut être garantie autrement, il est aussi autorisé à mettre lui-même certains documents ou matériels en lieu sûr. Cette disposition s'applique également aux cas où une entreprise fait faillite et où des documents ou des moyens informatiques doivent être retirés rapidement de la masse de la faillite.

Art. 66 Procédure simplifiée en cas d'adjudication d'autres mandats sensibles

Les entreprises qui disposent d'une DSE en cours de validité sont en principe réputées sûres et leur qualification n'est pas réévaluée. Le service spécialisé PSE doit néanmoins contrôler, le cas échéant, s'il faut adapter le plan de sécurité, par exemple si une entreprise qui ne devait traiter jusque-là que des informations classifiées «confidentiel» est également chargée du traitement d'informations classifiées «secret». Une procédure simplifiée est appliquée. Le Conseil fédéral en règlera les modalités au niveau de l'ordonnance.

Art. 67 Certificat international de sécurité

Les entreprises qui ont leur siège en Suisse et qui entendent soumissionner pour un mandat sensible à l'étranger doivent de plus en plus souvent présenter aux autorités du lieu une attestation de sécurité officielle émise par les autorités suisses. L'art. 67 crée les bases nécessaires à l'établissement de telles attestations, qui pourront ouvrir aux entreprises suisses l'accès à des mandats étrangers.

Art. 68 Révocation de la déclaration de sécurité

La révocation de la DSE durant l'exécution d'un mandat sensible est extrêmement rare. Lorsque le cas se produit, une décision est rendue, contre laquelle un recours peut être formé auprès du Tribunal administratif fédéral. Le droit de recours s'étend également à l'adjudicateur dans la mesure où une telle révocation peut aussi lui être défavorable: il peut avoir grand intérêt, financièrement, à ce que la DSE ne soit pas révoquée. L'adjudicateur doit toutefois retirer immédiatement le mandat en vue de limiter les risques. L'entreprise n'a droit à aucune indemnité financière, mais les travaux exécutés doivent lui être payés. L'application de l'art. 59, al. 3, est réservée (adjudication à une entreprise représentant un risque pour la sécurité), car il se peut que l'adjudicateur ne dispose d'aucune solution de rechange acceptable du point de vue économique. Dans ce cas, les pouvoirs de contrôle et d'exécution sont transférés du service spécialisé PSE à l'adjudicateur.

Section 6 Répétition de la procédure et voies de droit

Art. 69 Répétition de la procédure

Durant la répétition de la procédure, l'exécution du mandat n'est pas suspendue. Si le mandat est presque rempli et qu'aucun nouveau mandat sensible n'est attribué à l'entreprise, le service spécialisé PSE ne répétera pas la procédure pour des raisons d'économie. Si des indices concrets donnent à penser que des changements importants survenus dans l'entreprise ont fait apparaître de nouveaux risques pour la sécurité, la procédure est répétée.

Art. 70 Voies de droit

Lors de la PSE, les organes de l'entreprise disposent des mêmes droits que dans le cadre des CSP (cf. art. 45). Les décisions du service spécialisé PSE peuvent faire l'objet d'un recours auprès du Tribunal administratif fédéral. Cette norme prévoit implicitement que l'exception prévue par l'art. 32, al. 1, let. a, LTAF (le recours est, en principe, irrecevable contre les décisions concernant la sûreté intérieure ou extérieure du pays) ne s'applique pas. Toutefois, si la décision du service spécialisé PSE se fonde sur des informations relevant des services de renseignement qui ne doivent être divulguées ni à l'entreprise ni au public, les règles de procédure correspondantes sont applicables (art. 27 et 28 PA).

Section 7 Traitement des données personnelles

Art. 71 Système d'information sur la procédure de sécurité relative aux entreprises

La base juridique du système en place de longue date (art. 150 ss LSIA) doit, pour des raisons de systématique, être reprise dans la LSI. Étant donné que le système peut contenir des données sensibles et des profils de la personnalité, sa base légale doit figurer dans une loi au sens formel (art. 17, al. 2, LPD).

Art. 72 *Consultation et communication des données*

Les adjudicateurs ont accès aux données qui les concernent ainsi qu'à la liste de toutes les entreprises au bénéfice d'une DSE. Cet accès leur permet de savoir rapidement si une entreprise bénéficie ou non d'une DSE. Le Conseil fédéral pourra, dans les dispositions d'exécution, habiliter certaines entreprises à ouvrir elles-mêmes des CSP dans leur propre domaine. Ces entreprises doivent donc avoir accès à certaines données du système d'information. Par ailleurs, le système actuel permet déjà aux préposés à la sécurité de certaines entreprises d'accéder aux décisions relatives aux contrôles et aux degrés de contrôle CSP des membres du personnel de leur entreprise.

Art. 73 *Conservation, archivage et destruction des données*

Cette disposition est analogue à celle proposée pour le CSP (cf. art. 48).

Section 8 Dispositions édictées par le Conseil fédéral

Art. 74

Le commentaire de l'art. 49 pour les CSP vaut également pour la PSE.

Chapitre 5 Infrastructures critiques

Les art. 75 à 81 règlent les tâches et les compétences de la Confédération visant à soutenir les exploitants d' infrastructures critiques dans le domaine de la sécurité de l'information. La participation des exploitants d' infrastructures critiques au partenariat public-privé avec la Confédération est facultative. Pour de plus amples informations sur la SNPC, on se référera aux ch. 1.1.2 et 1.2.7.

Art. 75 Tâches de la Confédération

La société dans son ensemble a un intérêt au fonctionnement fiable des infrastructures critiques. Cet intérêt se reflète dans la première disposition du présent chapitre. En prêtant assistance aux exploitants d'infrastructures critiques, la Confédération veut s'assurer que les interruptions des systèmes et des réseaux restent rares, de courte durée, maîtrisables et peu dommageables. L'objectif est d'assurer les fonctionnalités techniques des infrastructures d'information, dont Internet, et de veiller à ce que les moyens informatiques ne soient pas utilisés par des tiers à l'insu et contre la volonté des ayants droit. Ce soutien comprend notamment les prestations énumérées à l'al. 2, mais il ne peut être invoqué pour lutter contre des abus liés au contenu tels les violations du droit d'auteur ou la diffamation.

L'al. 3 dispose que la Confédération gère d'une part un service national d'alerte chargé d'analyser continuellement les menaces en matière de sécurité de l'information et de préparer des informations concernant des dangers et des menaces identifiés au profit des exploitants d'infrastructures critiques afin de soutenir leurs processus en matière de sécurité de l'information et de gestion des risques. D'autre part, elle exploite un service d'assistance pour la prise de mesures préventives et réactives dans le domaine de la sécurité technique de l'information. Celui-ci effectue des analyses techniques, par ex. de logiciels malveillants, et peut fournir des recommandations concernant des mesures techniques concrètes de sécurité informatique afin de prévenir des dangers ou détecter des incidents. Les services chargés de tâches visées l'al. 3 sont par exemple autorisés à simuler des moyens informatiques vulnérables (*honeypots*) sur des réseaux afin d'améliorer leurs connaissances et à laisser fonctionner des moyens informatiques infectés sous surveillance pour découvrir le comportement des logiciels malveillants et des auteurs d'attaques.

Aux termes de l'al. 4, le Conseil fédéral veille à garantir à cet effet un échange sécurisé d'informations entre la Confédération et les exploitants d'infrastructures critiques ainsi qu'entre les exploitants eux-mêmes. Cet alinéa ne fonde aucune compétence autonome de traitement des données, mais il constitue la base légale permettant de mettre en place une plate-forme sûre d'échange d'informations. Souvent, les dangers, les menaces et la vulnérabilité ne concernent pas un objectif unique, mais plusieurs organisations actives dans un secteur spécifique, voire tous les exploitants d'infrastructures critiques dans l'ensemble des secteurs. Cependant, le recours aux prestations visées à l'art. 75 ainsi que la participation au partenariat public-privé sont totalement volontaires. Le principe de la propre responsabilité des exploitants d'infrastructures critiques est donc implicitement confirmé. Un échange permanent d'informations doit instaurer la transparence et la confiance; il profite non seulement aux exploitants d'infrastructures critiques, qui peuvent acquérir un savoir-faire, mais également aux autorités fédérales en leur qualité de propriétaires et d'exploitants d'infrastructures critiques. Elles peuvent ainsi obtenir des informations importantes afin d'évaluer leurs propres risques et prévenir des dangers.

Les services compétents se limitent aujourd'hui à MELANI, exploitée conjointement par l'UPIC et le SRC. Compte tenu de l'autonomie du Conseil fédéral en matière d'organisation, ces services ne sont pas mentionnés dans la loi, mais seront précisés au niveau de l'ordonnance (al. 5). Ils auront une pratique homogène dans leurs rapports avec les exploitants d'infrastructures critiques. En revanche, le Conseil fédéral pourra décider de l'organisation interne des services et de leur rattachement.

Art. 76 Traitement des données personnelles

Pour exécuter les tâches visées à l'art. 75, les services compétents de la Confédération doivent traiter des informations relatives aux menaces et aux dangers, de même que des indicateurs concernant des incidents dans le domaine de la sécurité de l'information et pouvoir les échanger avec les exploitants d'infrastructures critiques. Ces informations contiennent principalement des ressources d'adressage au sens de l'art. 3, let. f, LTC (par ex. des adresses IP, des adresses de messagerie et des noms de domaine). Ces ressources d'adressage se réfèrent à des personnes précises ou identifiables ou à des appareils ou des raccordements de télécommunication pouvant être attribués à une personne précise ou identifiable. Les clients finaux obtiennent généralement des ressources d'adressage de leurs fournisseurs de télécommunications ou d'autres fournisseurs, que l'on peut identifier à leur tour en fonction de la ressource d'adressage, généralement par la consultation de répertoires publics. Par conséquent, les ressources d'adressage peuvent être considérées comme des données personnelles et nécessitent une base légale pour être traitées (art. 4, al. 3, et 17, al. 1, LPD). La qualification des ressources d'adressage est contestée dans la doctrine et dans la pratique et peut être très hétérogène, notamment du fait que les ressources d'adressage étrangères font l'objet de procédures administratives et d'obligations de figurer dans un répertoire qui peuvent fortement diverger. C'est pourquoi le caractère de données personnelles des ressources d'adressage est interprété délibérément de manière très large dans la LSI, de façon à garantir la légalité du traitement des données et offrir une sécurité juridique au service chargé de leur traitement.

L'al. 1 prévoit donc que les services au sens de l'art. 75, al. 5, sont autorisés à traiter des données personnelles. Le traitement des données personnelles évoqué dans le présent chapitre ne peut être comparé aux mesures secrètes de surveillance des personnes et des conversations au sens du CPP et de la LSCPT. Les données dont il est question sont typiquement des commandes programmatiques informatiques sous la forme de codes informatiques (malveillants) et de ressources d'adressage apparues à la faveur d'un incident (par ex. utilisation abusive d'un service informatique ou contamination d'un moyen informatique par un logiciel malveillant) et communiqués à MELANI. L'échange de données de cette nature doit permettre de déterminer si des systèmes sensibles d'exploitants d'infrastructures critiques sont entrés en contact avec ces ressources d'adressage (comparaison avec les données de connexion des réseaux internes des exploitants d'infrastructures critiques), pour obtenir des *indices* (et non des preuves) d'une violation de la sécurité de l'information. Ces indices doivent ensuite être traqués dans les systèmes internes pour découvrir d'éventuelles contaminations du réseau interne par des logiciels malveillants.

Conformément à l'art. 17, al. 2, LPD, l'al. 2 autorise les services compétents à traiter des ressources d'adressage et les données personnelles liées, qui peuvent être jugées sensibles.

– Let. a: les attaques visant des moyens et des systèmes informatiques sont la plupart du temps menées pour des raisons financières. Il est néanmoins fréquent que leurs auteurs ne cherchent pas en priorité à s'enrichir, mais qu'ils planifient ou mènent une attaque pour des motifs religieux, philosophiques ou politiques: c'est le cas par exemple des «hacktivistes» qui interrompent des services informatiques, causent des préjudices financiers ou publient des données confidentielles des victimes de l'attaque pour attirer l'attention du public sur leurs revendications politiques. L'intention sous-jacente à une attaque pouvant être importante pour l'appréciation d'une menace et du risque qu'elle présente, MELANI doit pouvoir traiter les informations concernant les intentions si cela se révèle nécessaire à l'appréciation de menaces et de dangers concrets.

– Let. b: les attaques visant des moyens et infrastructures informatiques sont généralement poursuivies pénalement. Lorsque des données personnelles sont liées à une poursuite pénale, elles sont réputées sensibles en vertu de l'art. 3, let. c, ch. 4, LPD et ne peuvent être traitées par les organes de la Confédération que si base légale au sens formel le prévoit. Toutefois, étant donné qu'une plainte pénale ne peut écarter à elle seule le danger, du moins pas à court terme, l'information des exploitants d'infrastructures critiques à propos de ces vecteurs d'attaques est essentielle pour leur permettre de protéger leurs systèmes et d'identifier le cas échéant les attaques qui sont déjà survenues. Même sans communiquer le fait qu'une procédure concernant une ressource d'adressage a été introduite ou qu'une sanction a été prononcée, le destinataire de l'information peut, sur la base des données indiquant qu'une ressource d'adressage a été utilisée dans des buts criminels, conclure qu'une procédure correspondante est en cours. La présente disposition permet d'éviter que cet échange ne puisse plus avoir lieu dès qu'une plainte

pénale est déposée en lien avec un élément d'adressage ou qu'une procédure administrative est ouverte.

L'al. 3 autorise un traitement des données à l'insu de la personne concernée. Le système d'attribution des ressources d'adressage est souvent à plusieurs niveaux. En ce qui concerne les noms de domaines par exemple, de nombreuses personnes impliquées peuvent être identifiées par la consultation de répertoires publics (par le biais de requêtes dites WHOIS): services d'enregistrement, registraires, registrants, contacts techniques, contacts administratifs. Lorsque le domaine est actif, il est relié à une adresse IP et à d'autres personnes identifiables (également par la consultation de répertoires publics). Il serait disproportionné d'informer toutes les personnes physiques et morales identifiables de tout traitement d'un nom de domaine, mais souvent, certaines d'entre elles sont contactées de manière ciblée pour leur permettre de prendre des mesures préventives, éviter d'autres abus ou rétablir l'état conforme. En revanche, l'identification de l'utilisateur (final) en tant que personne concernée est souvent impossible ou possible uniquement moyennant une charge de travail considérable, en particulier lorsque les ressources d'adressage sont enregistrées à l'étranger. Elle n'est toutefois pas nécessaire à la prévention des dangers par des mesures de protection passives. Si l'identification n'a pas lieu, le traitement des données peut s'effectuer sans que les personnes concernées s'en aperçoivent ou en soient informées.

Par contre, si l'on soupçonne (cf. al. 4) qu'une ressource d'adressage (suisse) ou un appareil utilisant la ressource d'adressage en question est employé abusivement par des personnes non autorisées, l'utilisateur légitime de la ressource d'adressage doit pouvoir être identifié et informé. L'identification et l'information ne relèvent toutefois pas nécessairement des autorités compétentes. S'il est question, par exemple, d'adresses IP dynamiques, il est possible d'informer le fournisseur de services de télécommunication concerné afin qu'il puisse transmettre les informations correspondantes aux clients visés. Ces derniers pourront donc prendre des mesures afin d'empêcher de nouvelles utilisations abusives, signaler une infraction et, éventuellement, déposer une plainte pénale.

Par conséquent, le présent article doit être considéré comme une loi spéciale dérogeant aux art. 4, al. 4, et 18*a* LPD.

Art. 77 Coopération sur le plan national

L'art. 77 habilite les services compétents à communiquer dans l'accomplissement de leurs tâches les types de données énumérés aux exploitants d'infrastructures critiques afin que ces derniers puissent se protéger. Ils peuvent par ailleurs communiquer des données aux exploitants d'infrastructures critiques afin que ces derniers puissent limiter les conséquences d'une utilisation abusive de leurs systèmes, pour eux-mêmes et pour leurs clients.

L'al. 3 confère aux exploitants d'infrastructures critiques et aux fournisseurs et exploitants de services informatiques et de communication le droit de communiquer sur une base volontaire aux services visés à l'art. 75 des informations liées à des dangers et des incidents en matière de sécurité de l'information. Dans le but de prévenir des dangers et d'éviter des préjudices, ils peuvent fournir des indications

sur les services qu'ils fournissent, leurs activités d'intermédiaire et d'autres opérations. Cette disposition permet le traitement en toute légalité des données personnelles concernées et d'autres informations. La disposition peut s'appliquer lorsque l'on constate auprès d'un hébergeur la présence d'un serveur de commande (*command and control server*) grâce auquel un réseau est piloté par des ordinateurs personnels (réseau de machines zombies ou *bot-net*) infectés par des logiciels malveillants. Dans ce cas, l'hébergeur pourrait livrer à MELANI des fichiers journaux contenant les adresses IP des ordinateurs personnels infectés. MELANI remettrait alors ces fichiers aux fournisseurs de services de télécommunication qui pourraient ainsi alerter leurs clients. De plus, l'hébergeur pourrait transmettre les données de configuration et les modèles de communication du serveur de commande qui permettront d'identifier d'autres réseaux de machines zombies. Les règles en vigueur d'administration des preuves s'appliquent aux enquêtes policières et aux procédures judiciaires. Les autorités de poursuite pénale ne peuvent exiger aucune donnée de MELANI et doivent requérir l'administration des preuves auprès du détenteur initial. Lorsque le fournisseur de données consent expressément à leur transmission, MELANI peut les communiquer de son propre chef aux autorités de poursuite pénale concernées.

Art. 78 Coopération internationale

La protection des infrastructures critiques contre les dangers menaçant la sécurité de l'information est une tâche qu'aucune entreprise ni aucun État n'est en mesure d'assumer seul. La dimension mondiale d'Internet fait que les incidents ne sont généralement pas de portée locale ou nationale, mais qu'ils touchent des exploitants d'infrastructures critiques dans plusieurs pays. De nombreux États ont donc des intérêts communs et coopèrent déjà sur une base volontaire en matière d'identification et de gestion des incidents. Il n'existe aucune obligation de livrer certaines données: la loi ne change rien à cet égard. L'art. 78 ne confère qu'explicitement à MELANI la compétence de coopérer sur le plan international et d'échanger les données afférentes. Même si des données sont régulièrement échangées dans ce cadre, MELANI pourra renoncer dans chaque cas particulier à une communication si elle juge que cette dernière est incompatible avec l'art. 6 LPD ou qu'elle ne respecte pas le principe de la proportionnalité. Les services étrangers doivent garantir que les données obtenues serviront exclusivement aux fins évoquées dans la disposition. En matière de protection des infrastructures critiques, le *Traffic Light Protocol* s'est imposé dans le contexte international: l'échange d'informations peut être assorti de prescriptions précisant à qui les informations doivent ou peuvent être transmises (par ex. au seul secteur de l'énergie).

L'échange d'informations entre autorités porte en premier lieu sur des ressources d'adressage. On retiendra à cet égard que MELANI ne communique à ses partenaires étrangers que dans de très rares cas des ressources d'adressage se rapportant à des personnes, des entreprises ou des moyens informatiques situés en Suisse. Les menaces et dangers émanant de Suisse sont en effet combattus en Suisse dans le cadre de la coopération sur le plan national. Cependant, l'échange d'informations porte également sur d'autres informations importantes pour la sécurité de l'information des infrastructures critiques (par ex. la description et l'appréciation de menaces,

des instructions de détection et de contrôle des incidents, des analyses d'incidents et des recommandations de sécurité, des analyses concernant les lacunes de sécurité et la vulnérabilité). La coopération internationale visant la protection et la prévention des dangers, l'al. 3 précise que les dispositions régissant l'assistance administrative et l'entraide judiciaire s'appliquent aux procédures juridiques. Il précise ainsi que la présente loi ne peut servir à contourner les conditions qui y sont prévues.

Art. 79 Système d'information pour le soutien aux infrastructures critiques

Pour garantir la haute sécurité et la traçabilité du traitement des données, la mise en place d'un système d'information spécifique est indiquée. Cependant, l'échange d'informations peut aussi passer par d'autres canaux, par exemple des courriels chiffrés ou des rencontres interpersonnelles. L'énumération des renseignements que contient le système d'information atteste qu'il ne s'agit pas nécessairement de données personnelles et que les ressources d'adressage ne sont pas liées par principe à des personnes. Néanmoins, des recommandations techniques visant à identifier des incidents peuvent contenir des ressources d'adressage qui, par la consultation de répertoires publics, permettent d'identifier les personnes liées à ces ressources. Bien que ces personnes ne soient souvent pas les utilisateurs finaux des ressources d'adressage, elles peuvent être identifiées grâce à elles: ces ressources doivent donc être considérées comme des données personnelles.

Art. 80 Conservation et archivage des données

Les données personnelles ne peuvent être conservées qu'aussi longtemps qu'elles sont nécessaires à l'identification des incidents et à la prévention des dangers. La définition d'une durée maximale de conservation de cinq ans pose une limite temporelle. Dans la plupart des cas, les données traitées ont un cycle de vie très limité et peuvent être détruites peu de temps après leur traitement. Par contre, certaines indications concernant les vecteurs d'attaque peuvent rester utiles de longues années. L'opportunité d'un traitement durable des données peut être vérifiée par des experts indépendants lors des contrôles prévus à l'art. 81, let. d.

Art. 81 *Dispositions édictées par le Conseil fédéral*

Le Conseil fédéral réglera par voie d'ordonnance la répartition des tâches et la collaboration entre les services visés à l'art. 75, al. 5. La LRens attribue des compétences au SRC en matière de protection des infrastructures critiques. Le Conseil fédéral réglera les modalités de la répartition des tâches, de la collaboration et de l'échange d'informations. Afin de garantir la transparence et la sécurité du droit, le Conseil fédéral réglera le traitement des données, leur échange entre les services en question, leur transmission aux exploitants d'infrastructures critiques et aux services étrangers et internationaux, de même que la sécurité des données dans un tel contexte. Il veillera également au contrôle périodique externe de la légalité du traitement des données. Le Conseil fédéral pourra choisir librement l'instance de contrôle dans la mesure où cette dernière dispose de l'indépendance nécessaire vis-à-vis de MELANI.

Chapitre 6 Organisation et exécution

Section 1 Organisation

Art. 82 Préposés à la sécurité de l'information

Pour le rôle des préposés à la sécurité de l'information, on se référera au ch. 1.2.9. La LSI touche à l'autonomie d'organisation des autorités en raison du besoin prépondérant d'une gestion globale de la mise en œuvre de la loi. Elle exige que les autorités ainsi que les départements et la ChF désignent pour leur domaine de compétence un préposé à la sécurité de l'information et un suppléant adéquat. Puisqu'une gestion intégrale et efficace de la sécurité de l'information exige des connaissances politiques, juridiques, organisationnelles et techniques et que les préposés à la sécurité de l'information doivent en outre accomplir de nombreuses tâches, la mise en œuvre requiert que deux personnes au minimum par autorité assument les tâches en question. Il n'est toutefois pas exigé que les deux personnes soient engagées à plein temps à cette fin.

Le Conseil fédéral lui-même devra également désigner un préposé à la sécurité de l'information. En revanche, l'autorité de surveillance du Ministère public de la Confédération n'y est pas tenue en raison de ses ressources limitées en personnel. Les tribunaux fédéraux ne sont pas énumérés de manière détaillée, car il serait disproportionné d'exiger de tribunaux disposant de peu de personnel qu'ils mettent en place de tels services. La loi autorise donc les tribunaux fédéraux à désigner par exemple un seul service et une seule suppléance pour l'ensemble des tribunaux ou de choisir une autre approche garantissant l'autonomie des autorités. Les offices fédéraux et l'administration fédérale décentralisée ne sont pas non plus légalement tenus de désigner des préposés. Afin de remplir son devoir d'organisation, le Conseil fédéral décidera par voie d'ordonnance comment il convient d'organiser et de gérer la sécurité de l'information à ce niveau.

L'al. 2 décrit en termes généraux les tâches et les compétences des préposés à la sécurité de l'information.

- La let. a souligne que la compétence décisionnelle et la responsabilité des décisions en matière de sécurité de l'information demeurent de la responsabilité de la hiérarchie, c'est-à-dire des autorités compétentes et de leurs services subordonnés. Les préposés à la sécurité de l'information sont toutefois appelés à conseiller et à assister les responsables hiérarchiques dans leur domaine de spécialisation.
- La let. b dispose que les préposés à la sécurité de l'information doivent gérer, sur mandat de leur autorité ou organisation, la sécurité de l'information et les risques correspondants sur le plan technique.
- La let. c prévoit que les préposés à la sécurité de l'information ont une obligation générale de vérifier le respect des prescriptions de la présente loi, de faire rapport à ce sujet et de proposer à leur autorité les mesures qui s'imposent. Ils sont encore chargés d'établir la liste des fonctions liées à des tâches sensibles. Les audits et les contrôles sont toujours des points délicats. Ils doivent en principe être ordonnés par les responsables hiérarchiques. Les

préposés à la sécurité de l'information devront soumettre annuellement à cet effet un programme d'audit à leur autorité ou organisation, qui précisera les priorités en matière d'audits et les ressources éventuellement nécessaires.

– La let. d dispose que les préposés à la sécurité de l'information peuvent signaler les incidents au service spécialisé de la Confédération pour la sécurité de l'information et à la Conférence des préposés à la sécurité de l'information ainsi qu'aux services assumant les tâches relatives à la sécurité de l'information au sein des infrastructures critiques. Pour sauvegarder l'autonomie des autorités, on renonce donc à une *obligation* d'annoncer les incidents au niveau transversal. S'il le juge nécessaire, le Conseil fédéral pourra prévoir au niveau de l'ordonnance une obligation d'annoncer les incidents pour l'administration fédérale et l'armée.

Les préposés à la sécurité de l'information doivent être indépendants dans leur statut et dans l'accomplissement de leurs tâches et ne peuvent être exposés à des conflits d'intérêts matériels. Dans la pratique, l'absence de séparation des fonctions génère des problèmes récurrents dans l'application des prescriptions de sécurité. Par exemple, la plupart des délégués à la sécurité informatique sont aujourd'hui subordonnés aux directions de l'informatique. Les responsables informatiques ont dès lors souvent d'autres priorités que la sécurité et, en raison de l'urgence ou des coûts, on néglige régulièrement d'appliquer dans les projets les mesures de sécurité qui s'imposent. Les préposés à la sécurité de l'information ne devraient pas non plus être directement chargés de l'exploitation de moyens informatiques ou diriger des projets qui ne concernent pas en priorité la sécurité de l'information, car ce sont justement ces cumuls de tâches qui génèrent régulièrement des conflits entre les exigences différentes de l'exploitation et une évaluation aussi objective que possible des risques. La présente réglementation donne également suite à la recommandation 7 du rapport de la DélCdG sur la sécurité informatique au sein du SRC (cf. ch. 1.1.4).

Le rattachement exact de la fonction est laissé à l'appréciation des autorités ou des départements et de la ChF. La pratique montre toutefois que l'efficacité des préposés à la sécurité de l'information est optimale s'ils sont relativement proches de la direction de l'autorité concernée, car ils sont alors mieux à même d'obtenir une vue d'ensemble des processus d'affaires et d'évaluer les besoins. En outre, il serait souhaitable de placer les préposés à la sécurité de l'information de telle sorte qu'ils puissent assurer une coordination étroite avec les gestionnaires des risques, les conseillers à la protection des données, les préposés à la sécurité (protection des objets) et, le cas échéant, les conseillers à la transparence.

Art. 83 Conférence des préposés à la sécurité de l'information

Pour le rôle de la conférence, on se référera au ch. 1.2.9. Outre les autorités soumises à la loi, les départements, la ChF et les cantons doivent y être représentés. On s'assure ainsi que l'exécution de la loi sera aussi homogène que possible au sein de l'administration fédérale et dans le cadre de la collaboration avec les cantons. Le PFPDT y siégera également, afin que la coordination avec la protection des données soit systématique et intervienne déjà au moment de la définition des exigences. La

conférence veillera en particulier à l'évaluation de l'applicabilité, de l'efficacité et de l'économicité des mesures standard proposées (art. 86), seule manière de trouver des solutions qui soient uniformes et acceptées. Le nouveau service spécialisé de la Confédération pour la sécurité de l'information associera la conférence à toutes les questions importantes en relation avec la sécurité de l'information (concernant par ex. la stratégie en matière de sécurité de l'information). La conférence doit également contribuer à l'identification des risques et des tendances ainsi qu'à la définition des mesures préventives qui s'imposent. Elle pourra aussi consulter des experts indépendants pour l'assister dans ses investigations et l'aider à se forger une opinion.

Art. 84 Service spécialisé de la Confédération pour la sécurité de l'information

Pour le rôle du service spécialisé de la Confédération pour la sécurité de l'information, on se référera au ch. 1.2.9. Au niveau transversal, le service spécialisé n'est pas habilité à donner des instructions et ne dispose d'aucune compétence d'exécution, car de tels pouvoirs seraient contraires à l'autonomie d'exécution des autorités soumises à la loi.

- Let. a: les autorités nommées dans la loi peuvent solliciter les compétences techniques du service spécialisé pour toutes les questions relatives à l'exécution (y compris les CSP). Le service spécialisé est ainsi le «centre de compétences» en matière de sécurité de l'information.
- Let. b: lorsque de nouveaux dangers et menaces apparaissent ou que l'on découvre de nouvelles lacunes et points faibles, tous les participants doivent être informés sans délai. S'il s'agit de menaces opérationnelles dans le domaine technique, MELANI se charge de cette tâche pour le compte de ses clients.
- Let. c: les audits et les contrôles incombent en principe aux autorités et organisations. Toutefois, notamment pour ce qui est des audits techniques d'infrastructures critiques, des connaissances approfondies que toutes les autorités soumises à la loi ne doivent pas obligatoirement acquérir sont nécessaires: la constitution d'une équipe d'experts est plus économique. Le service spécialisé ne peut cependant mener ces contrôles que sur mandat d'une autorité. Après consultation de la conférence, le service spécialisé établira ou adaptera chaque année un programme de contrôle stratégique, qu'il soumettra aux autorités compétentes pour approbation. Le programme précisera les priorités en matière d'audit et les ressources éventuellement nécessaires.
- Let. d: les différentes autorités soumises à la loi recourent en permanence à de nouvelles technologies. Les risques liés à ces nouveaux moyens (matériels et logiciels) sont souvent peu connus. Pour les technologies particulièrement importantes ou qui peuvent avoir un champ d'application relativement vaste, les autorités doivent pouvoir solliciter du service spécialisé une analyse de risque, dont la conférence examinera les résultats.

- Let. e: cette disposition est une mesure opérationnelle visant à standardiser les processus, les moyens, les installations, les objets et les prestations. Par exemple, dans le domaine informatique, les fournisseurs de prestations ont intérêt à savoir si les solutions techniques qu'ils développent répondent aux exigences de la Confédération. Si c'est le cas, ils peuvent les réutiliser beaucoup plus facilement pour d'autres projets et moyens informatiques. Il en va de même pour des objets ou des prestations destinés à la protection physique. Même si les exigences de sécurité sont remplies, la responsabilité reste toutefois assumée par l'autorité ou l'organisation qui engage de tels moyens. Cette compétence est aussi requise dans le contexte international: le service spécialisé devra assumer le rôle d'autorité nationale d'accréditation (cf. ch. 5.2), ce qui est habituel sur le plan international mais qui fait défaut en Suisse. Le service spécialisé sera donc habilité à certifier officiellement que le moyen engagé satisfait par exemple aux exigences de l'UE.
- Let. f: la responsabilité des projets transversaux est attribuée à une autorité ou organisation donnée. Les intérêts et besoins des diverses autorités et organisations en matière de sécurité étant souvent hétérogènes, il faut s'assurer que les exigences de sécurité de l'information soient coordonnées avec professionnalisme. Le service spécialisé assumera cette tâche pour les projets transversaux importants fortement liés à la sécurité de l'information.
- Let. g: les connaissances techniques adéquates devant être réunies au sein du futur service spécialisé, la let. g prévoit que ce dernier sera l'interlocuteur pour la Confédération des services suisses, étrangers et internationaux en matière de sécurité de l'information. Il assumera également les rôles requis dans le cadre des relations entre autorités au niveau international (cf. ch. 5.2). D'autres autorités ou organisations pourront toutefois maintenir des contacts spécialisés dans ce domaine (par ex. le DFAE, le SRC ou l'OFCOM).
- Let. h: le Conseil fédéral doit être informé régulièrement de l'état de la sécurité de l'information de manière à pouvoir en évaluer l'efficacité et l'économicité et informer en conséquence les organes de surveillance de l'Assemblée fédérale (cf. art. 89, al. 2).

Al. 2 et 3: le Conseil fédéral désignera également un préposé à la sécurité de l'information. Pour éviter d'éventuels conflits de compétences, la personne en question dirigera simultanément le service spécialisé. De plus, le Conseil fédéral définira les tâches que le service spécialisé sera appelé à assumer, seul ou en collaboration avec d'autres services de la Confédération. Il décidera également de sa subordination. Enfin, il précisera s'il entend lui confier d'autres tâches ou pouvoirs d'exécution vis-à-vis de l'administration fédérale et de l'armée.

Section 2 Exécution

Art. 85 *Dispositions d'exécution*

Pour l'exécution, on se référera également au ch. 1.2.8. Les autorités soumises à la loi ne seront pas liées par les dispositions d'exécution du Conseil fédéral. En contrepartie, elles devront édicter elles-mêmes, dans leur domaine de compétence, les dispositions d'exécution requises. La 2e phrase de l'al. 1 règle le rapport avec l'art. 15, al. 2, LOGA. L'al. 2 attribue clairement, en relation avec l'art. 70 LParl, la compétence d'exécution pour l'Assemblée fédérale. L'al. 3 institue le principe de subsidiarité. Les dispositions d'exécution seront préparées en collaboration avec la Conférence des préposés à la sécurité de l'information. De plus, le Conseil fédéral consultera les autres autorités et les cantons avant d'édicter ses dispositions d'exécution.

Art. 86 Exigences et mesures standard

L'un des buts principaux de la présente loi est d'atteindre un niveau de sécurité aussi homogène que possible entre les différentes autorités, le Conseil fédéral est chargé de fixer des exigences et des mesures standard en fonction des connaissances scientifiques et techniques les plus récentes. La disposition ne vise pas des exigences et des mesures organisationnelles de base, qui seront définies au niveau de l'ordonnance, mais principalement des exigences de nature secondaire ou technique, par exemple:

- norme pour l'évaluation du besoin de protection des informations sous l'angle des quatre critères mentionnés à l'art. 6, al. 2;
- méthode standard pour l'évaluation des risques;
- normes pour les mesures à prendre aux niveaux de l'organisation, du personnel, de la technique et des constructions (art. 8);
- normes pour des processus et des moyens particuliers destinés à protéger des informations classifiées (art. 11 à 15);
- normes pour la protection de base, l'élaboration de plan de sécurité de l'information et la sécurité des moyens informatiques des catégories «protection élevée» et «protection très élevée» (art. 16 à 19).

De nombreux États ou organisations internationales ont déjà défini des normes dans leur domaine. Les autorités fédérales ne seront dès lors pas obligées de réinventer la roue. Il importe à cet égard que la Suisse participe à ces processus de normalisation.

Le Conseil fédéral pourra, si nécessaire, déléguer l'élaboration et l'adoption des normes à des services subordonnés pour ne pas devoir ordonner des mesures opérationnelles techniques. Les mesures de sécurité relevant principalement de la compétence décisionnelle des responsables hiérarchiques, déléguer cette tâche à la Conférence des secrétaires généraux (art. 53 LOGA) pourrait se révéler une solution particulièrement appropriée. On pourrait songer également à une délégation au service spécialisé de la Confédération pour la sécurité de l'information, ou encore à fedpol dans le domaine de la protection des objets. Les fournisseurs de prestations

de la Confédération devraient aussi pouvoir élaborer des normes techniques de sécurité et, le cas échéant, en faire examiner l'adéquation pour la Confédération par le service spécialisé dans un souci de standardisation (cf. art. 84, al. 1, let. e). Une telle délégation par le Conseil fédéral ne doit toutefois pas être trop absolue. Certaines mesures techniques peuvent avoir d'importantes conséquences financières qui ne devraient pas être décidées par des services subordonnés. S'il délègue ses compétences, le Conseil fédéral doit donc aussi s'assurer de prendre lui-même les décisions concernant les mesures globales les plus coûteuses.

Les normes ne sont pas obligatoires pour les autres autorités soumises à la loi car elles sont élaborées par le Conseil fédéral. Toutefois, étant donné que la conférence participera de façon décisive à l'élaboration des normes, le caractère de recommandations qu'elles présentent ne devrait pas empêcher, dans la pratique, leur reprise par les autres autorités et les cantons.

Art. 87 Cantons

Pour la collaboration entre la Confédération et les cantons, on se référera au ch. 1.2.2. En vertu de l'art. 3, les cantons sont tenus de garantir un niveau de sécurité équivalent lorsqu'ils traitent des informations classifiées de la Confédération ou recourent à ses moyens informatiques. Ils doivent par conséquent garantir que leurs mesures permettent réellement d'atteindre le niveau de sécurité requis. Les contrôles se limitent à la sécurité du traitement des informations classifiées et à l'accès à des moyens informatiques de la Confédération, et les cantons en sont responsables. Ils doivent néanmoins informer le service spécialisé de la Confédération pour la sécurité de l'information des résultats des contrôles. Par ailleurs, il faut s'assurer que l'échange d'informations entre la Confédération et les cantons soit systématique et efficace et que la mise en œuvre des mesures prévues par la présente loi soit coordonnée. On n'attend pas des cantons qu'ils se réorganisent ou qu'ils créent de nouvelles structures. Ils seront par ailleurs directement associés à l'élaboration des dispositions d'exécution de la loi et des normes au sens de l'art. 86.

Bien que les cantons soient compétents pour la sécurité de l'information dans leur propre domaine, la Confédération dispose d'instruments et de capacités spécifiques auxquels les cantons peuvent recourir pour répondre à leurs propres besoins. Du point de vue économique, l'acquisition par les cantons de ces instruments et capacités ne serait guère judicieuse, notamment pour ce qui a trait au CSP. Les employés cantonaux chargés de tâches sensibles de la Confédération sont soumis au CSP en vertu de l'art. 30, al. 1, let. b. Les coûts afférents sont actuellement pris en charge par la Confédération. La PSE et les capacités d'audit du service spécialisé de la Confédération pour la sécurité de l'information suscitent également l'intérêt des cantons. Le Conseil fédéral doit dès lors être habilité à déterminer, en collaboration avec les cantons, les ressources de la Confédération auxquelles les cantons peuvent recourir et dans quelle mesure ils peuvent le faire. Pour autant que les cantons recourent aux prestations de la Confédération pour répondre à leurs propres besoins, ils indemniseront la Confédération de manière à couvrir les coûts.

Art. 88 Traités internationaux

Les traités internationaux en matière de sécurité de l'information contiennent principalement des règles techniques relatives à la reconnaissance mutuelle de prescriptions et de processus nationaux (par ex. à propos des CSP ou des PSE), des listes de concordance concernant le traitement des informations classifiées, des normes de sécurité dans le domaine informatique ou de la sécurité des communications, et des réglementations sur l'exécution de contrôles mutuels. De plus, des traités peuvent se révéler nécessaires pour la protection des informations que d'autres États ou des organisations internationales mettent à la disposition de la Confédération; dans de tels cas, on peut être amené à déroger sur certains points à des prescriptions légales (par ex. pour les conditions imposant une classification, autorisant l'accès ou le traitement d'informations classifiées ou régissant la délivrance de déclarations de sécurité). Le fournisseur des informations peut ainsi exiger des autorités fédérales destinataires un accord imposant un degré de protection plus ou moins sévère de ses informations. Pour des raisons d'économie administrative, le Conseil fédéral sera habilité à conclure directement des traités internationaux en matière de sécurité de l'information.

Pour minimiser les risques en matière de sécurité de l'information, un renforcement de la mise en réseau et de la collaboration à l'échelon international s'impose. La mise en œuvre de la SNPC requiert donc que l'échange d'expériences, de travaux de recherche et de développement, d'informations concernant des incidents, ainsi que d'activités liées à la formation et à des exercices soit intensifié (cf. également ch. 1.1.2). Le Conseil fédéral doit aussi être autorisé à conclure des traités internationaux portant sur l'échange d'informations en matière de menaces, de vulnérabilités et d'incidents liés notamment à des infrastructures critiques. Il pourra aussi régler des questions secondaires concernant l'organisation et la technique (par ex. la collaboration avec d'autres CERT gouvernementaux; cf. art. 78).

Art. 89 Évaluation

Une évaluation devra avoir lieu cinq ans après l'entrée en vigueur de la loi. Le compte rendu du service spécialisé de la Confédération (cf. art. 84, al. 1, let. h) fera office de rapport annuel. L'Assemblée fédérale désignera la commission qui traitera les rapports du Conseil fédéral.

Chapitre 7 Dispositions finales

Art. 90 Modification d'autres actes

Cf. ch. 2.3.

Art. 91 Dispositions transitoires

Le passage au nouveau droit doit être conçu de la manière la plus économique possible et en fixant des priorités. Il serait disproportionné d'exiger que la classification de toutes les informations soit vérifiée dans un délai donné. Ce principe vaut

également pour le domaine informatique: une adaptation immédiate de tous les systèmes aux nouvelles prescriptions serait certes souhaitable sous l'angle de la sécurité, mais les moyens financiers et les charges de personnel qu'elle exigerait seraient totalement disproportionnés. La loi prévoit dès lors que l'on procède dans un premier temps à l'attribution des catégories de sécurité aux moyens informatiques. La mesure devra être appliquée dans un délai de deux ans de manière à identifier rapidement les moyens informatiques les plus critiques. La mise à niveau des moyens informatiques occasionne souvent de lourdes charges et s'avère bien plus onéreuse que lorsque la sécurité est assurée dès le départ. Si les coûts de mise à niveau d'un système se révèlent disproportionnés par rapport à la sécurité de l'information visée, les risques doivent être identifiés et assumés en toute transparence. Quatre années supplémentaires devraient suffire à adapter si nécessaire les systèmes eux-mêmes ou les plans de sécurité de l'informationet de protection des données existants, les systèmes les plus critiques étant prioritaires. La condition sine qua non de ces adaptations est la définition préalable des standards au sens de l'art. 86.

La réglementation transitoire des CSP et PSE sert la transparence vis-à-vis des personnes et des entreprises au bénéfice d'une déclaration, mais également au passage ordonné au nouveau droit en fonction des risques. La durée de validité des déclarations de sécurité est déjà de cinq ans. En ce qui concerne les CSP, la situation est un peu plus compliquée car les déclarations ne portent pas de date d'échéance formelle (le contrôle est simplement «répété» après un certain temps). La réglementation proposée offre une continuité tant aux services requérants qu'aux services spécialisés CSP. Elle ménage par ailleurs au Conseil fédéral une marge de manœuvre suffisante pour faire contrôler en priorité les fonctions les plus critiques.

2.2 Coordination avec d'autres actes

Le présent projet de loi doit être coordonné avec les projets de loi ci-après.

Loi sur le renseignement

Si la LRens entre en vigueur avant la présente loi, l'art. 51, al. 4, LRens devra être modifié conformément au présent projet.

Si la LRens entre en vigueur après la présente loi, la modification de l'art. 51, al. 4, LRens prévue dans le présent projet n'entrera en vigueur qu'à la même date.

Quel que soit l'ordre dans lequel la LRens et la présente loi entrent en vigueur, à l'entrée en vigueur du second de ces actes ou à leur entrée en vigueur simultanée, l'art. 367, al. 2, let. i, 2^{bis}, let. b, et 4, CP aura la teneur suivante:

Art. 367, al. 2, let. i, 2^{bis}, let. b, et 4

2 Les données personnelles relatives aux jugements visés à l'art. 366, al. 1, 2 et 3, let. a et b, peuvent être consultées en ligne par les autorités suivantes:

i. les services spécialisés chargés des contrôles de sécurité relatifs à des personnes (services spécialisés CSP) visés à l'art. 32, al. 2, LSI[29];

2bis Les données personnelles relatives aux jugements visés à l'art. 366, al. 3, let. c, peuvent aussi être consultées en ligne par les autorités suivantes:

b. les services spécialisés CSP visés à l'art. 32, al. 2, LSI;

4 Les données personnelles relatives aux enquêtes pénales en cours ne peuvent être traitées que par les autorités visées à l'al. 2, let. a à e, i, j, l et m.

Loi sur le casier judiciaire

Si la loi sur le casier judiciaire (LCJ) entre en vigueur avant la présente loi, les modifications des art. 365, al. 2, let. d, et 367, al. 2, let. i, 2bis, let. b, et 4, CP prévues par le présent projet seront caduques. L'art. 46, al. 6, let. a, LSI, l'art. 46, let. e, LCJ et l'art. 51, let. f, LCJ devront alors être modifiés comme suit:

Art. 46, al. 6, let. a, LSI

6 Les données visées à l'al. 4 peuvent être collectées automatiquement et systématiquement en ligne dans les systèmes d'information suivants:

a. casier judiciaire informatique au sens de la loi du 17 juin 2016 sur le casier judiciaire[30];

Art. 46, let. e, LCJ

Les autorités raccordées suivantes peuvent consulter en ligne toutes les données figurant sur l'extrait 2 destiné aux autorités (art. 38), lorsqu'elles leur sont nécessaires pour accomplir les tâches mentionnées ci-après:

e. les services spécialisés qui mènent les contrôles de sécurité relatifs aux personnes au sens de l'art. 32, al. 2, de la loi du … sur la sécurité de l'information (LSI)[31]:	1. pour évaluer le risque dans le cadre de contrôles de sécurité relatifs aux personnes au sens de la LSI, 2. pour évaluer le potentiel d'abus ou de dangerosité au sens de la loi du 3 février 1995 sur l'armée[32], 3. pour évaluer le risque dans le cadre d'autres contrôles prévus dans la législation spéciale;

Art. 51, let. f, LCJ

Abrogée

29 RS …; FF **2017** 2765 2907
30 RS …; FF **2016** 4703
31 RS …; FF **2017** 2765 2907
32 RS **510.10**

Si la LCJ entre en vigueur après la présente loi, l'art. 46, al. 6, let. a, LSI et les art. 46, let. e, et 51, let. f, LCJ seront modifiés comme ci-dessus. En revanche, la modification de l'art. 20*a* LPers prévue par la LCJ sera caduque; en d'autres termes, la modification de l'art. 20*a* LPers prévue par le présent projet restera en vigueur.

Loi sur l'énergie

Si la loi sur l'énergie entre en vigueur avant la présente loi, l'art. 20*a* LApEl aura, à l'entrée en vigueur de la présente loi, la teneur prévue par le présent projet.

Si la loi sur l'énergie entre en vigueur après la présente loi, la modification de l'art. 20*a* LApEl prévue par la loi sur l'énergie sera caduque; en d'autres termes, la modification de l'art. 20*a* LApEl prévue par le présent projet restera en vigueur.

2.3 Modification d'autres actes

Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure

Art. 2, al. 4, let. c, et art. 19 à 21

Pour l'essentiel, le CSP sera réglé dans la LSI. Les dispositions correspondantes de la LMSI doivent donc être abrogées.

Art. 24a, al. 7, 1re phrase

Pour évaluer le risque pour la sécurité lors d'un CSP dans le cadre de la LSI, vérifier la loyauté au sens de la législation spéciale et apprécier le potentiel de violence au sens de l'art. 113 LAAM, les services spécialisés CSP doivent avoir accès à la banque de données de fedpol sur le hooliganisme.

Loi fédérale sur le renseignement

Art. 51, al. 4, let. d

Les services spécialisés CSP peuvent solliciter des données auprès du SRC (art. 35, al. 1, let. c). L'INDEX SRC sert à établir si le SRC traite des données relatives à une personne donnée, une organisation, un objet ou un événement. Les données relatives à toutes les personnes recensées dans les systèmes IASA SRC et IASA-GEX SRC (cf. art. 49 et 50 LRens) peuvent être consultées en ligne. Concrètement, les données d'identification les plus importantes sont saisies, pour les personnes par exemple le nom, la date de naissance, la nationalité, etc. L'INDEX SRC permet ainsi la coordination des activités de renseignement de la Confédération et des cantons, mais également la coordination entre les activités de renseignement et les activités de police de sécurité et de police judiciaire. Les services spécialisés CSP n'ont pas directement accès aux informations au-delà des données d'identification. Lorsqu'une personne figure dans l'INDEX SRC, le service spécialisé CSP compétent doit solli-

citer du SRC la livraison des données nécessaires (cf. art. 46, al. 6, LSI, et 49 ss LRens).

Loi sur le personnel de la Confédération

Art. 20a Extrait du casier judiciaire et du registre des poursuites

L'augmentation de la valeur seuil pour l'exécution du CSP doit permettre d'appliquer les mesures en question uniquement pour des activités qui sont réellement sensibles pour la sécurité. Le danger subsiste néanmoins que la valeur seuil des CSP soit abaissée dans la pratique ou que les exigences relatives à la nécessité d'un CSP soit réduites si les autorités et organisations soumises à la LSI ne disposent pas d'autres instruments afin de contrôler la loyauté des candidats à un poste et des membres de leur personnel. Le nouvel art. 20*a* LPers fournit à l'employeur des moyens correspondants. La production d'extraits du casier judiciaire et du registre des poursuites ne devrait toutefois pas constituer la norme, mais être demandée uniquement dans la mesure nécessaire à la défense des intérêts de l'employeur. Le Conseil fédéral édictera des dispositions d'exécution à ce sujet.

Art. 20b Contrôle de loyauté

Les CSP au sens de la LSI ne peuvent être menés qu'en vue de l'identification de risques substantiels pour la sécurité de l'information. Il subsiste néanmoins d'autres activités des autorités fédérales qui sont sans rapport direct avec la sécurité de l'information mais qui peuvent fortement mettre en péril les intérêts de la Confédération. La loyauté des personnes exerçant ces activités doit pouvoir être contrôlée. L'introduction d'une nouvelle disposition concernant le contrôle de loyauté à l'art. 20*b* LPers doit permettre de couvrir un besoin identifié de contrôler certains employés de la Confédération.

- Il s'agit en premier lieu du personnel diplomatique et consulaire du DFAE, mais le contrôle pourra aussi concerner le personnel d'autres départements qui assume des fonctions similaires (par ex. auprès du SECO).
- Le contrôle peut s'appliquer aux directeurs d'offices, mais également à des membres du personnel disposant de compétences décisionnelles dans le cadre de l'adjudication de marchés publics importants ou des personnes assumant des tâches particulièrement sensibles liées aux finances, par exemple.

La disposition ne s'applique pas à tous les employeurs énumérés à l'art. 3 LPers. Ainsi, l'Autorité de surveillance du Ministère public de la Confédération n'en fait pas partie dès lors qu'aucun de ses employés ne remplit les critères de l'art. 20*b*, al. 1, LPers. Concernant les unités administratives décentralisées et les autres tribunaux fédéraux, le Conseil fédéral décidera par voie d'ordonnance, après consultation de l'organe concerné, dans quelle mesure le personnel doit pouvoir être contrôlé (cf. compétence du Conseil fédéral mentionnée à l'art. 3, al. 2 et 3, LPers). De plus, le contrôle ne doit être ordonné qu'en cas de besoin avéré, c'est-à-dire lorsque le dommage potentiel est considérable. La présente disposition ne saurait servir à déroger à la réduction du nombre des CSP voulue par le Conseil fédéral. Il n'est pas

judicieux de prévoir une procédure spécifique ou d'autres services spécialisés pour le contrôle de loyauté, car les points à élucider sont en principe les mêmes que ceux relevant de la sécurité de l'information. Le contrôle en question doit dès lors se fonder sur la LSI. En reprenant la procédure, on tiendra compte notamment du principe du consentement de la personne concernée s'agissant de l'exécution du contrôle, des règles régissant la collecte des données, des listes de fonctions, des degrés de contrôle et des dispositions relatives aux conséquences de l'évaluation. Les listes de fonctions nécessaires devront être dressées et mises à jour par le service spécialisé de la Confédération pour la sécurité de l'information – en collaboration avec l'OFPER pour l'administration fédérale et avec les services compétents des autres autorités fédérales.

Code de procédure civile

Pour la modification de l'art. 166, al. 1, let. c, du code de procédure civile, on se référera au commentaire de l'art. 320, ch. 1, CP.

Loi fédérale de procédure civile fédérale

Pour la modification de l'art. 42, al. 3, de la loi fédérale de procédure civile fédérale, on se référera au commentaire de l'art. 320, ch. 1, CP.

Code pénal

Art. 320

De nos jours, l'e*xternalisation* en matière de technologies de l'information et de la communication est, dans beaucoup de secteurs, non seulement usuelle, mais encore inévitable, dans la mesure où le savoir-faire spécialisé des producteurs de logiciels et de matériel informatique est souvent indispensable. La Confédération et les cantons font eux aussi appel au soutien de nombreux prestataires de services externes en matière de technologies de l'information et de la communication (cf. art. 10*a* LPD). Les banques de données, en particulier, renferment souvent une quantité difficilement quantifiable d'informations protégées par un secret. Même en appliquant le principe selon lequel le moins de données personnelles possibles sont traitées (principe dit d'utilisation économe ou de minimisation des données), ainsi que d'autres mesures techniques ou organisationnelles (anonymisation des données, contrôle des collaborateurs, etc.), les personnes chargées de tâches techniques ont (souvent de manière inévitable) *accès à des informations protégées par le secret de fonction*.

Les auxiliaires externes du domaine des technologies de l'information et de la communication qui fournissent des prestations à l'administration (par ex. la maintenance de banques de données) ne sont pas soumis à l'obligation de l'*art. 320 CP* de garder secrètes les informations dont ils prennent connaissance dans l'exercice de

leur activité. Ces collaborateurs externes à l'administration *ne constituent en principe pas des fonctionnaire* au sens de l'art. 110, ch. 3, CP[33] et n'entrent ainsi pas dans le cercle des auteurs de l'*art. 320, ch. 1, CP* (infraction propre)[34]. Un recours au droit pénal n'est envisageable que si les auxiliaires externes participent à l'infraction propre du fonctionnaire en tant que complices ou instigateurs ou s'ils transmettent des informations protégées et commettent simultanément une autre infraction, comme un acte exécuté sans droit pour un État étranger (art. 271 CP) ou un service de renseignements politiques ou économiques (art. 272 ou 273 CP). Ainsi, contrairement à la protection du secret professionnel (art. 321 CP) qui s'étend également aux auxiliaires du détenteur du secret, le secret de fonction contient une *lacune dans sa protection et dans la punissabilité de sa transgression*, dans la mesure où seule une activité d'auxiliaire externe à l'administration entre en ligne de compte.

Aux termes de l'*art. 320, ch. 2, CP*, la révélation de secrets de fonction[35] n'est pas punissable si elle est faite avec le *consentement* écrit de l'autorité supérieure. Dans la mesure où l'art. 320 CP comprend des *secrets* qui ne sont pas exclusivement *de nature publique*, mais également *de nature privée*[36] (par ex. des données relatives à la santé contenues dans un dossier médical ou des secrets de fabrication ou d'affaires recueillis dans le cadre d'un appel public d'offres), l'autorité compétente pour délivrer l'autorisation doit examiner avec soin, lors de la pesée des intérêts, quels intérêts sont touchés par la divulgation. La divulgation est autorisée ou refusée selon la nature et le poids de l'intérêt au maintien du secret dans le cas concret[37]. Au cas où l'intérêt au maintien du secret n'est pas au moins partiellement de nature publique, mais exclusivement de nature privée, il est en principe exclu que le consentement de l'autorité supérieure au sens de l'art. 320, ch. 2, CP justifie la divulgation[38]. À cela s'ajoute que, dans le domaine des technologies de l'information et de la communication, il est pratiquement impossible de recueillir les autorisations nécessaires (nombre indéterminé de détenteurs ou de maîtres de secrets), lorsque,

33 Weber Rolf H., «Outsourcing von Informatik-Dienstleistungen in der Verwaltung» in: *Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht*, 100. Jahrgang (1999), p. 97 ss, ch. 2.2.1; cf. également (a contrario) ATF 135 IV 198, consid. 3.3.

34 Oberholzer Niklaus in: Niggli/Wiprächtiger (éd.), *Basler Kommentar Strafrecht I*, Bâle 2013, n. 13 ss ad art. 110, al. 3; pour un vaste exposé de la casuistique, v. Trechsel Stefan/Vest Hans in: Trechsel/Pieth (éd.), *Schweizerisches Strafgesetzbuch Praxiskommentar*, Zurich/St-Gall 2013, n. 13 ad art. 110, al. 3.

35 Le fait de rendre possible la prise de connaissance d'un secret suffit; cf. Oberholzer Niklaus *op. cit.*, n. 10 ad art. 320.

36 Oberholzer Niklaus, *op. cit.*, n. 3 et 8 ad art. 320

37 Trechsel Stefan/Vest Hans in: Trechsel/Pieth (éd.), *Schweizerisches Strafgesetzbuch Praxiskommentar*, Zurich/St-Gall 2013, n. 11 ad art. 320; à propos du consentement structurellement identique de l'autorité supérieure en matière de secret professionnel, v. Stratenwerth Günter/Bommer Felix, *Schweizerisches Strafrecht Besonderer Teil II*, Berne 2013, § 61, n. 23; à propos du pendant procédural de la norme pénale matérielle, v. l'art. 170, al. 3, CPP, ainsi que Donatsch Andreas in: Donatsch/Hansjakob/Lieber (éd.), *Kommentar zur Schweizerischen Strafprozessordnung*, Zurich 2014, n. 14 ad art. 170; à propos de la pesée des intérêts en matière de droit d'accès à des documents officiels, v. art. 7 (en particulier l'al. 3) LTrans.

38 À propos de la portée du consentement, v. Stratenwerth Günter, *Schweizerisches Strafrecht Allgemeiner Teil I*, Berne 2011, § 10, n. 5 et 13 et Stratenwerth Günter/Bommer Felix, *op. cit.*, § 61, n. 10 s.

par exemple, une banque de données tombe en panne et requiert l'intervention immédiate du support technique externe. Or, en l'absence d'autorisation valable, les collaborateurs internes de l'administration se rendent punissables s'ils permettent à des prestataires de services externes d'accéder à des secrets de fonction. En l'état actuel du droit, les collaborateurs internes de l'administration s'exposent donc à une *sanction*.

Le Conseil fédéral est d'avis que le législateur devrait résoudre rapidement ces problèmes. Il renonce cependant à étendre dans la loi la portée du *consentement* de l'autorité supérieure à la divulgation de secrets de nature purement privée. Cela ne changerait en effet rien au fait que, comme dans le droit en vigueur, l'obligation pour les prestataires de services externes de garder secrètes les informations couvertes par le secret de fonction ne pourrait être garantie, de manière indirecte, que par la voie contractuelle (peines conventionnelles). De plus, la situation juridique des particuliers s'en trouverait plutôt affaiblie. De même, l'extension de la *définition légale* de la notion de fonctionnaire de l'art. 110, ch. 3, CP, n'est pas appropriée, car elle déploierait des conséquences sur toutes les infractions aux devoirs de fonction. Les auxiliaires externes à l'administration qui ne correspondent pas à la notion matérielle de fonctionnaire n'exercent cependant aucune fonction de service public et ne s'identifient pas, vus de l'extérieur, comme des représentants de l'administration publique. Ils ne doivent dès lors pas pouvoir être tenus de répondre de manière générale de toutes les infractions aux devoirs de fonction.

Le Conseil fédéral juge préférable d'*étendre le cercle des auteurs de l'art. 320, ch. 1, CP,* aux auxiliaires et de *renforcer* ainsi *la protection des secrets de fonction*. La réglementation en vigueur en matière de secret professionnel (art. 321 CP) justifie d'autant plus le fait de soumettre les auxiliaires à l'obligation pénale de respecter le secret de fonction[39]. Cela règle du même coup la question du risque de punissabilité des collaborateurs internes de l'administration, lorsqu'ils rendent des secrets de fonction accessibles à des auxiliaires externes sans disposer d'une autorisation, mais pour les besoins du service.

Au cas où un auxiliaire externe doit être libéré du secret de fonction au sens de l'art. 320, ch. 2, CP, c'est l'autorité supérieure du mandant interne à l'administration qui doit donner son consentement par écrit. La situation est ainsi comparable à celle des auxiliaires de détenteurs de secrets professionnels au sens de l'art. 321 CP. Seule l'autorité administrative supérieure est en mesure de procéder de manière appropriée, en tenant compte des éléments décisifs, à la pesée des intérêts nécessaire à l'autorisation de divulguer un secret.

Les explications qui précèdent s'appliquent par analogie à la violation du secret de service au sens de l'*art. 77 CPM*. La révision implique d'étendre de manière correspondante le cercle des personnes pouvant se prévaloir du *droit de refuser de témoigner fondé sur le secret de fonction* au sens de l'art. 170 CPP, de l'art. 77 PPM, de

39 À propos des auxiliaires de détenteurs de secrets professionnels, v. Oberholzer Niklaus, *op. cit.*, n. 10 ad art. 321.

l'art. 166 du code de procédure civile[40] et de l'art. 42 de la loi fédérale de procédure civile fédérale[41] (en raison du renvoi de l'art. 16, al. 1, PA).

Art. 365, al. 2, let. d

Puisque le CSP est réglé dans la LSI et non plus dans la LMSI, les dispositions concernant les services bénéficiant d'un droit d'accès et le but de la collecte des données doivent être adaptées en conséquence.

Art. 367, al. 2, let. i, 2bis, let. b, et 4

Pour les al. 2 et 2bis, on se référera au commentaire de l'art. 365, al. 2, let. d. Selon la pratique en vigueur, les services spécialisés CSP ont également accès aux données relatives à des procédures pénales en cours, bien qu'ils ne figurent pas parmi les autorités visées à l'art. 367, al. 4, CP. Comme mentionné dans le message relatif à la loi sur le casier judiciaire[42], il s'agit d'un oubli auquel il convient de remédier. L'art. 20, al. 2, let. d, LMSI autorise déjà ces services spécialisés à demander des renseignements relatifs à des procédures pénales en cours aux organes de poursuite pénale compétents, mais ils ne peuvent le faire que s'ils sont au courant des procédures pénales pendantes. Pour obtenir cette information, ils doivent consulter VOSTRA. L'art. 367, al. 4, CP doit être modifié en conséquence (en y ajoutant le renvoi à la let. i).

Code de procédure pénale

Pour la modification de l'art. 170, al. 1, CPP, on se référera au commentaire de l'art. 320, ch. 1, CP.

Code pénal militaire

Pour la modification de l'art. 77 CPM, on se référera au commentaire de l'art. 320, ch. 1, CP.

Procédure pénale militaire

Pour la modification de l'art. 77, al. 2, PPM, on se référera à la modification de l'art. 320, ch. 1, CP.

40 RS **272**
41 RS **273**
42 FF **2014** 5525, pp. 5623 s.

Loi fédérale sur les systèmes d'information de police de la Confédération

Art. 15, al. 4, let. f, et 17, al. 4, let. l

Les services spécialisés CSP ont désormais accès à l'index national de police (cf. art. 46, al. 6, LSI). L'accès à RIPOL (art. 15 LSIP) peut être abrogé.

Loi sur l'armée

Art. 14 Contrôle de loyauté

Conformément à l'art. 20*b* LPers proposé, la LSI prévoit que le Conseil fédéral peut soumettre à un contrôle de loyauté deux domaines de tâches dans le cadre des dispositions d'exécution de la LAAM:

- la let. a vise principalement les militaires qui, dans le cadre d'engagements réguliers à l'étranger, représentent la Suisse ou assument des tâches dans le domaine de la diplomatie militaire;
- la let. b ne concerne que les militaires qui pourraient porter une atteinte considérable aux intérêts financiers de la Confédération dans le cadre de leur obligation de servir.

La présente disposition ne saurait servir à déroger à la réduction du nombre des CSP voulue par le Conseil fédéral. Dans la pratique, elle ne devrait être appliquée qu'à titre exceptionnel.

Art. 113, al. 6

La modification est purement formelle: l'al. 6 renvoie désormais à la présente loi plutôt qu'à la LMSI.

Art. 150, al. 4

La compétence de conclure avec des États étrangers des traités visant au maintien du secret militaire figurera désormais à l'art. 88 LSI.

Loi fédérale sur les systèmes d'information de l'armée

Art. 14, al. 1, let. n

L'introduction du contrôle de loyauté au sens de l'art. 14 LAAM exige la création d'une base légale pour le traitement des résultats dans le SIPA. Seuls les résultats du contrôle, sa date et la décision pourront être traités dans le SIPA.

Art. 17, al. 1, let. a

Cette modification est purement formelle: le sigle LAAM étant désormais introduit à l'art. 14, il peut être directement réutilisé dans le présent article.

Chapitre 5, sections 1 et 2 (art. 144 à 155)

Les systèmes d'information sur le CSP et la PSE seront réglés dans la LSI.

Loi sur l'énergie nucléaire

Art. 5, al. 3 et 3bis

L'art. 5, al. 3, LENu prévoit déjà que les mesures de sûreté doivent, autant que possible, être classifiées. La modification vise à garantir que la classification de ces mesures et le traitement des informations classifiées soient conformes à la LSI.

Loi sur l'approvisionnement en électricité

Art. 20a

Dans son message du 4 septembre 2013 relatif au premier paquet de mesures de la Stratégie énergétique 2050 (Révision du droit de l'énergie) et à l'initiative populaire fédérale «Pour la sortie programmée de l'énergie nucléaire (Initiative ‹Sortir du nucléaire›)»[43], le Conseil fédéral avait proposé d'introduire le contrôle de sécurité relatif aux personnes pour certains membres du personnel de la société nationale du réseau de transport. La présente modification a pour seul but d'adapter cette proposition à la terminologie et à la systématique de la LSI.

Loi sur la Banque nationale

Art. 16, titre et al. 5

En raison de ses tâches de politique monétaire, la Banque nationale est considérée comme une autorité soumise à la LSI.

3 Conséquences

3.1 Conséquences pour la Confédération

La Confédération investit annuellement plus de 800 millions de francs au total dans son informatique. En raison de l'évolution vers une société de l'information, les menaces pesant sur les informations et les moyens informatiques sont devenues plus complexes et plus dynamiques. Les dommages qui peuvent résulter de la défaillance ou de la perturbation de moyens informatiques ou encore du vol ou de l'utilisation abusive d'informations sont par conséquent plus importants. La sécurité de l'information a pour objectif de réduire, aussi efficacement et économiquement que possible, la probabilité, et le cas échéant l'ampleur, de tels dommages qui peuvent également être d'ordre financier. La loi et ses dispositions d'exécution permettront

43 FF **2013** 6771

une amélioration durable de la sécurité de l'information au sein de la Confédération. La LSI règle principalement la gestion de la sécurité de l'information, et elle en améliorera l'efficience. L'expérience atteste qu'une gestion efficiente de la sécurité de l'information favorise souvent une sécurité plus efficace, économique et durable que ne le feraient de simples investissements dans des mesures techniques. La pratique montre par ailleurs qu'une optimisation de la gestion, notamment lorsqu'elle se fonde sur une gestion efficace des risques, peut conduire à moyen terme à des économies.

Le projet prévoit en outre plusieurs mesures organisationnelles qui apporteront non seulement une meilleure protection de l'information par rapport à la situation actuelle, mais conduiront également à des économies si elles sont mises en œuvre de manière systématique. L'augmentation des valeurs seuils relatives à la classification doit par exemple permettre de réduire le nombre d'informations classifiées et, par conséquent, les charges correspondantes. S'agissant des CSP, les critères pour leur exécution seront plus sévères, tandis que le nombre des activités pour lesquelles un CSP sera nécessaire (et admissible) diminuera. Le nombre des CSP menés devrait donc baisser de manière significative. En outre, la standardisation, l'amélioration de l'échange d'informations entre les autorités fédérales et le soutien de ces dernières par le service spécialisé de la Confédération pour la sécurité de l'information éviteront de réinventer la roue pour chaque projet. Enfin, la nouvelle réglementation facilitera la collaboration internationale dans le domaine de la sécurité et améliorera la protection des données au sein de la Confédération.

Il s'agit dès lors de pondérer systématiquement les répercussions sur les finances et le personnel, d'une part, et l'atténuation des risques évoqués de même que les réductions de charges, d'autre part.

3.1.1 Conséquences financières

Les conséquences financières de la loi dépendent presque exclusivement du niveau de sécurité que les autorités veulent atteindre (art. 7, al. 2), et ne pourront être évaluées que lors de l'élaboration de la législation d'exécution. La loi elle-même n'a qu'une influence minime sur ces coûts.

Les coûts de la réorganisation conformément aux connaissances scientifiques et techniques actuelles (art. 7, al. 1) varient fortement en fonction du modèle d'organisation. Les autorités décideront du modèle après une analyse coût-utilité dans le cadre de l'exécution. Une solution minimale par laquelle on se pencherait sur les processus en vue d'y déceler les lacunes les plus importantes et de les harmoniser entre les divers autorités et organisations serait en principe finançable avec les ressources existantes. Une solution maximale par laquelle l'ensemble des autorités et organisations soumises à la loi se conformeraient pour leur système de gestion de la sécurité de l'information à la norme DIN ISO/IEC 27001 entraînerait selon les experts des coûts de projet (charges de conseil) de l'ordre de 8 à 12 millions de francs. Entre ces deux extrêmes, d'autres solutions sont envisageables pour la mise en œuvre, qui entraîneraient des charges de conseil plus ou moins élevées en fonction de leur portée et des besoins de sécurité. La gestion et l'exploitation de

l'organisation relèvent des préposés à la sécurité de l'information. Les coûts d'audit éventuels devront être planifiés et inscrits au budget ordinaire.

En fonction du modèle d'organisation (cf. ch. 3.1.2), les contrôles de l'efficacité (art. 18, al. 3) pourraient entraîner des coûts annuels de l'ordre de 1,5 à 1,8 million de francs au titre des auditeurs externes. L'expérience montre que les coûts d'audit se situent généralement entre 0,5 et 2 % de l'investissement total dans le système contrôlé.

Par décision du 12 décembre 2013, le Parlement a libéré un crédit d'engagement pour le programme GIA Confédération (art. 24 à 27). Les ressources sont inscrites au budget et dans le plan financier de la Confédération.

Le coût annuel attendu de la collecte de données auprès d'établissements financiers et de banques dans le cadre du CSP élargi (art. 35, al. 2, let. c en relation avec l'art. 37, al. 2) est de quelque 10 000 à 20 000 francs.

3.1.2 Conséquences pour le personnel

Globalement, les organes spécialisés de la sécurité de l'information pourraient nécessiter de 13,5 à 14,5 postes supplémentaires. Le Conseil fédéral décidera de l'engagement de personnel supplémentaire lorsqu'il édictera la législation d'exécution. Toutefois, à moyen terme, ces postes devraient être en majorité compensés par une réduction correspondante des effectifs dans le domaine des CSP. En ce qui concerne les préposés à la sécurité de l'information, il est encore impossible d'estimer correctement les besoins supplémentaires en personnel car ils dépendent de la réglementation de l'organisation interne (option centralisée ou décentralisée). On peut néanmoins s'attendre à des besoins supplémentaires de deux à sept postes, qui pourront être plus ou moins compensés sur le plan interne en fonction du modèle d'organisation choisi. Les conséquences estimées pour le personnel sont détaillées ci-après.

Services spécialisés CSP

Les services spécialisés CSP mènent entre 75 000 et 80 000 contrôles par an. Il s'agit de contrôles non seulement au titre de la LMSI mais aussi de la LENu (500 contrôles), ainsi que d'évaluations du potentiel de violence de militaires au sens de l'art. 113 LAAM (40 500 contrôles). Le Conseil fédéral affecte actuellement à ces activités 61 postes, soit 27 postes à durée indéterminée et 30 à durée déterminée (jusqu'à fin 2017) auprès du DDPS et quatre postes à durée indéterminée auprès de la ChF. La plupart des postes à durée déterminée auprès du DDPS (16 postes) ont été autorisés à la fin de 2012 pour réduire le nombre de cas à risques en suspens et 10 nouveaux postes à durée déterminée de deux ans ont été autorisés à la fin de 2015 par le DDPS. Malgré ces renforts, on constate déjà que les ressources du service spécialisé CSP du DDPS ne suffisent pas à mener tous les contrôles nécessaires. Le coût total des CSP (charges de personnel, coûts d'administration et coût des systèmes d'information) s'est élevé à 12,5 millions de francs en 2015. S'ajoutent à ce montant, selon les indications des départements et de la ChF, des charges administratives correspondant à dix postes à temps plein pour l'ouverture des CSP et

l'établissement et la tenue à jour des listes de fonctions. Le Conseil fédéral vise une réduction sensible du nombre des CSP et, à moyen terme, des charges administratives et de personnel qui en découlent. Il voudrait supprimer à ce titre au moins douze postes. En revanche, le présent projet n'aura aucune incidence sur le nombre de CSP au titre de la LENu, de la LApEl et de l'art. 113 LAAM.

Service spécialisé PSE

À l'heure actuelle, quelque 550 entreprises ayant leur siège en Suisse bénéficient d'une DSE. Le DDPS consacre 2,2 postes aux PSE pour des mandats militaires classifiés (2 postes de spécialistes de la sécurité et 20 % de poste pour l'ouverture des CSP). L'extension des PSE au domaine civil et à d'autres autorités de la Confédération entraînera selon les prévisions une augmentation du nombre des entreprises de l'ordre de 30 % environ. Les adaptations de la procédure en vigueur nécessiteront une légère augmentation des effectifs. On s'attend au total à 1,5 poste supplémentaire pour les PSE. Sans ces ressources, il faudrait renoncer à l'uniformisation de la PSE.

MELANI

Les ressources affectées à MELANI ont été examinées dans le cadre le la planification de la mise en œuvre de la SNPC. Il n'existe aucun besoin supplémentaire en personnel.

Préposés à la sécurité de l'information

Le rôle des préposés à la sécurité de l'information englobe les attributions des préposés à la protection des informations et des délégués à la sécurité informatique. Les préposés à la sécurité de l'information reçoivent par ailleurs de nouvelles compétences dans le domaine des CSP et PSE et se voient confier d'autres tâches (par ex. le pilotage de la sécurité de l'information et la gestion des risques afférents, de même que l'organisation d'audits). Les dispositions d'exécution seront déterminantes pour l'estimation des ressources en personnel nécessaires. L'organisation spécialisée interne des départements (option centralisée ou décentralisée) influera également substantiellement sur les ressources. L'expérience montre que l'on peut s'attendre à des besoins supplémentaires de deux à huit postes, qui pourront être plus ou moins compensés sur le plan interne en fonction du modèle d'organisation retenu. Les autorités soumises à la loi décideront des ressources dans le cadre de la mise en œuvre.

Service spécialisé de la Confédération pour la sécurité de l'information

Selon les experts, le service spécialisé de la Confédération pour la sécurité de l'information aura besoin de 22 postes au total pour assumer *a minima* ses tâches au sens de l'art. 84 et élaborer les normes visées à l'art. 86. Ces postes se répartissent entre la direction du service spécialisé (1,2 poste, y compris la suppléance), le secrétariat (1,1 poste), la coordination des services spécialisés (1 poste), la formation et la sensibilisation (1 poste), la gestion des risques et des exigences (4 postes), les audits et les rapports (2 postes), les audits techniques (5 postes), la cryptologie (3,5 postes), le droit et la gestion des dossiers politiques (2 postes) et les relations internationales (1,2 poste). Ces postes seront pourvus et compensés par étapes (11 postes la pre-

mière année et 11 postes durant les deuxième et troisième années). Sur ces 22 postes, 7,2 seront compensés par des ressources que le DFF et le DDPS affectent déjà au pilotage interdépartemental de la sécurité informatique ou à la mise en œuvre coordonnée de l'OPrI. Entre 2 et 3 autres postes seront transférés par le DDPS au département compétent (avant tout dans le domaine juridique et dans celui des relations internationales). Globalement, 12 à 13 postes supplémentaires pourraient être nécessaires. Le Conseil fédéral s'efforcera, dans la mesure du possible, de compenser ces besoins éventuels en personnel soit à l'interne, soit par des gains d'efficacité.

Ces postes supplémentaires seront affectés essentiellement à trois tâches nouvelles ou élargies, présentées et justifiée ci-après.

– *Gestion des risques et des exigences:* il s'agit d'une part d'élaborer les normes, puis de les développer. Les exigences et mesures standardisées peuvent générer des économies dans le cadre des projets. Elles sont également importantes pour une exécution homogène. D'autre part, il convient de garantir l'appui aux autorités (et aux cantons) dans le pilotage de leur sécurité de l'information et la gestion des risques afférents. Sans ces quatre postes supplémentaires, il faudrait renoncer à la standardisation.

– *Audits techniques:* il s'agit ici d'une tâche nouvelle, incluant aussi bien le contrôle de l'aptitude (art. 84, al. 1, let. e) que le contrôle périodique de l'efficacité (art. 18, al. 3). Le contrôle de l'aptitude est nécessaire dans le contexte international (cf. ch. 5.2) et pour la standardisation opérationnelle auprès des fournisseurs de prestations (cf. commentaire de l'art. 84, al. 1, let. e). Le contrôle de l'efficacité est la seule mesure permettant de rendre compte du degré effectif de sécurité technique de l'information. Les bases légales en vigueur ne prévoient pas le degré de sécurité «protection très élevée» auquel ce contrôle est destiné. Les experts estiment toutefois que la Confédération exploite entre 10 et 20 systèmes nécessitant une protection très élevée. Ces systèmes sont généralement très complexes et les charges d'audit sont particulièrement lourdes. Les projections concernent 12 à 16 systèmes qui devront faire l'objet d'un audit tous les quatre ans, sur la base de l'état des connaissances. Pour ce faire, la Confédération a besoin soit de onze postes supplémentaires (un poste pour la direction du service d'audit, un autre pour l'administration et trois groupes de trois auditeurs chacun), soit de huit postes (direction du service, administration et deux groupes d'auditeurs) et d'un budget de 750 000 à 900 000 francs pour des experts extérieurs à l'administration, soit de cinq postes supplémentaires (direction du service, administration et un groupe d'auditeurs) avec un budget de 1,5 à 1,8 million de francs pour des experts extérieurs à l'administration, soit encore de deux postes supplémentaires (direction du service et administration uniquement) et d'un budget de 2,25 à 2,7 millions de francs pour des experts extérieurs à l'administration. Le Conseil fédéral propose de retenir la solution des cinq postes de manière à s'assurer que la Confédération dispose sur le plan interne des connaissances spécialisées nécessaires et que les autorités fédérales puissent décider régulièrement des charges d'audit, car les ressources correspondantes doivent faire l'objet d'une demande de crédit.

De plus, il n'est pas certain que la Confédération puisse trouver davantage d'experts.

Sans ces cinq postes supplémentaires, il faudrait soit se rabattre sur la solution à deux postes supplémentaires assortie du budget correspondant, soit renoncer à cette tâche. Dans le second cas, les exigences sur le plan international ne seraient pas satisfaites et la standardisation opérationnelle auprès des fournisseurs de prestations ne pourrait intervenir qu'au prix de coûts externes supplémentaires. De plus, on ne pourrait pas évaluer correctement la sécurité de l'information des moyens informatiques les plus critiques de la Confédération.

– *Cryptologie:* les mesures de cryptologie sont indispensables à la couverture des besoins de protection renforcée de la confidentialité et de l'intégrité des informations. L'engagement de la cryptologie suppose des exigences claires, mais implique aussi que le processus d'acquisition soit accompagné, que les programmes cryptologiques soient examinés par des spécialistes et que les composantes cryptologiques soient mises à jour périodiquement. Tant les exigences que les compétences évoquées font majoritairement défaut à la Confédération. En revanche, le DDPS affecte 7,5 postes à ces tâches (4,5 à la BAC et 3 auprès d'armasuisse), au profit du département et de l'armée. Les experts estiment que l'accomplissement de ces tâches au profit de tous les moyens informatiques nécessitant une protection très élevée et des moyens informatiques transversaux nécessiterait 3,5 postes supplémentaires. À défaut, on devrait renoncer à l'accompagnement et au contrôle des mesures cryptologiques hors du DDPS.

3.2 Conséquences pour les cantons et les communes, ainsi que pour les villes, les agglomérations et les régions de montagne

Les conséquences pour les cantons ne pourront être définitivement évaluées que lorsque les dispositions d'exécution seront édictées. Toutefois, le champ d'application de la LSI aux cantons reste limité et dépendra principalement des projets ou des applications. De plus, les cantons seront étroitement associés à l'élaboration des dispositions d'exécution et des normes, de sorte qu'ils seront en mesure d'apprécier à temps la rentabilité des mesures et de les influencer. Par ailleurs, la Confédération assumera encore les coûts des CSP menés auprès des employés cantonaux (environ 400 par an) chargés de tâches sensibles de la Confédération. Les cantons bénéficieront également de l'appui du service spécialisé de la Confédération pour la sécurité de l'information. En revanche, ils seront tenus de vérifier périodiquement l'efficacité des mesures de protection prises. Ils ne devraient néanmoins pas avoir besoin de mettre en place une nouvelle organisation et pourront recourir à cette fin aux structures de surveillance existantes. Dans le cadre des CSP, l'obtention d'extraits des registres cantonaux des poursuites et des faillites devrait être gratuite (à l'heure actuelle, la Confédération débourse à ce titre 250 000 francs par an). Cependant, étant donné que ces données seront dorénavant recueillies électronique-

ment par une interface dans le cadre du projet visant à développer une norme d'échange de données dans le domaine des poursuites[44], les cantons seront dispensés du coût de la collecte. Globalement, la nouvelle réglementation devrait entraîner une augmentation modérée des charges des cantons, qui sera partiellement compensée par les mesures de soutien effectives de la Confédération.

En principe, la loi n'a aucune conséquence pour les villes, les agglomérations et les régions de montagne.

3.3 Conséquences économiques

La loi ne s'applique qu'indirectement aux tiers, plus précisément lorsque ces derniers doivent traiter des informations ou utiliser ou gérer des moyens informatiques de la Confédération dans le cadre d'un contrat. Les entreprises qui soumissionnent pour des mandats civils de la Confédération comportant une activité sensible seront dorénavant soumises à la PSE. Ce changement ne devrait occasionner qu'un faible accroissement de la charge administrative. À l'inverse, la compétitivité des entreprises suisses s'en trouvera renforcée, car la loi crée la base légale de la délivrance d'une déclaration de sécurité des autorités aux particuliers qui soumissionnent pour des mandats classifiés étrangers ou internationaux et qui ont besoin à ce titre d'un certificat de sécurité.

Les tiers, dont les banques ou les instituts de crédit, qui seront appelés à collaborer dans le cadre d'un CSP ne devraient être indemnisés que si la charge qui leur est occasionnée est importante, par exemple lorsque leur contribution dépasse l'établissement d'extraits de comptes ou nécessite des recherches particulièrement intensives. Cette participation n'est prévue que pour le degré de contrôle le plus élevé, de sorte que son coût restera minime.

3.4 Conséquences sanitaires et sociales

La société est concernée à deux points de vue. D'une part, la protection et la sécurité des données seront améliorées. D'autre part, les principes de classification seront publiés et les critères de classification seront plus sévères, de sorte que l'on classifiera moins. Ces changements revêtent une importance particulière pour l'application du principe de la transparence, qui ne doit en aucun cas être remis en question par la loi.

3.5 Conséquences environnementales

La loi n'a aucune conséquence sur l'environnement.

44 Le projet peut être consulté à l'adresse suivante: www.ofj.admin.ch > État et citoyen > Informatique juridique > Projet e-LP.

3.6 Autres conséquences

Formellement, la loi ne transpose aucun engagement international direct. Sur le plan pratique, elle facilitera la coopération internationale en définissant clairement les compétences dans le contexte international (cf. ch. 5.2).

4 Relation avec le programme de la législature et les stratégies nationales du Conseil fédéral

4.1 Relation avec le programme de la législature

Le projet découle de la mesure «mettre à jour et mettre en œuvre la stratégie pour une société de l'information» en Suisse annoncée dans le message du 25 janvier 2012 sur le programme de la législature 2011 à 2015[45] et l'arrêté fédéral du 15 juin 2012 sur le programme de la législature 2011 à 2015[46].

4.2 Relation avec les stratégies nationales du Conseil fédéral

4.2.1 Stratégie pour une société de l'information en Suisse

Pour la stratégie, on se référera au ch. 1.1.1. La LSI est inscrite au catalogue des projets relatifs à la société de l'information 2011–2015 (état novembre 2013) dans le champ d'action «Sécurité et confiance». Elle fournira des bases claires aux exigences de sécurité pour les projets réalisés par la Confédération.

4.2.2 Stratégie nationale de protection de la Suisse contre les cyberrisques

Pour la SNPC, on se référera au ch. 1.1.2; pour les liens entre la SNPC et la LSI, au ch. 1.2.7 et pour le soutien aux exploitants d'infrastructures critiques, au commentaire des art. 75 à 81.

4.2.3 Stratégie nationale de protection des infrastructures critiques

La stratégie nationale de protection des infrastructures critiques du 27 juin 2012 (stratégie PIC)[47] vise à renforcer la capacité de résistance des infrastructures critiques de la Suisse. Elle propose diverses mesures dans deux domaines. L'auto-

45 FF **2012** 349, 414 et 468
46 FF **2012** 6667, 6669
47 FF **2012** 7173

protection sera renforcée par l'élaboration et l'application de programmes de protection intégrale par les organes compétents. Cette mesure permettra d'identifier et de limiter les risques spécifiques liés aux infrastructures critiques. Dans le domaine «transinfrastructures», la stratégie vise à améliorer la collaboration entre les acteurs (autorités, exploitants) des différents secteurs des infrastructures critiques tout en diminuant la vulnérabilité de la société, de l'économie et des pouvoirs publics en cas de défaillance grave. Des planifications seront élaborées à cette fin pour garantir la maîtrise des coûts lors de défaillances graves et pour apporter une aide subsidiaire aux exploitants lors de tels événements. Le Conseil fédéral souhaite assister les exploitants d'infrastructures critiques dans leurs efforts de protection. L'objectif à cet égard est d'atteindre la plus grande capacité de résistance possible en matière de sécurité de l'information. Par exemple, la mesure 7 de la stratégie PIC prévoit la création de bases légales formelles permettant de soumettre certaines catégories de personnel des exploitants d'infrastructures critiques à un contrôle de sécurité. La LSI soutient donc aussi la mise en œuvre de la stratégie PIC.

5 Aspects juridiques

5.1 Constitutionnalité

En vertu de l'art. 42 Cst., le législateur fédéral doit disposer pour ses réglementations d'une base constitutionnelle (explicite ou implicite). Le projet repose sur des bases constitutionnelles suffisantes. Formellement, la présente loi contient principalement des dispositions transversales d'organisation pour les autorités fédérales. Le droit de l'organisation de la Confédération ne figure certes pas sous une forme explicite au catalogue de la répartition des compétences législatives entre la Confédération et les cantons, mais l'art. 164, al. 1, let. g, Cst., qui énumère les compétences de l'Assemblée fédérale, inclut «l'organisation et […] la procédure des autorités fédérales» aux objets devant être réglés par une loi fédérale (voir par ex. le préambule de la LParl). De plus, la législation d'organisation en vigueur se réfère également à l'art. 173, al. 2, Cst., qui attribue à l'Assemblée fédérale tous les objets qui relèvent de la Confédération et qui ne ressortissent pas à la compétence d'une autre autorité fédérale (voir par ex. le préambule [avec note de bas de page 1] de la LOGA ou celui de la LTrans).

Sur le fond, la LSI sert en premier lieu à garantir la sécurité du pays sur le plan national et vis-à-vis de l'extérieur, ainsi qu'à protéger la capacité de décision et d'action des autorités. Les dispositions concernées se fondent sur l'art. 54, al. 1 et 2, Cst. (relations avec l'étranger et maintien de la sécurité extérieure), ainsi que sur l'art. 57, al. 1, Cst., qui dispose que «la Confédération et les cantons pourvoient à la sécurité du pays … dans les limites de leurs compétences respectives».

En revanche, les dispositions concernant la PSE ne correspondent pas aux objectifs mentionnés dans la mesure où elles concernent les entreprises qui ont besoin d'une déclaration de sécurité pour soumissionner pour des mandats classifiés d'autorités étrangères ou internationales. Cette réglementation est couverte par l'art. 101 Cst., sur lequel repose la sauvegarde des intérêts de l'économie suisse à l'étranger. Les dispositions relatives à la protection des infrastructures critiques peuvent se fonder

aussi bien sur les bases de la sécurité intérieure et extérieure que sur les compétences de la Confédération en matière d'approvisionnement du pays (art. 102 Cst.). En ce qui concerne l'armée, on peut renvoyer à l'art. 60 Cst., qui dispose que l'organisation de l'armée relève de la compétence de la Confédération.

5.2 Compatibilité avec les obligations internationales

La Suisse a conclu avec divers États et organisations internationales des traités de protection des informations (cf. RS *0.514.xxx*), par lesquels la Suisse s'engage à respecter certaines normes visant à protéger les informations de ces États et organisations. Outre l'accord avec l'UE, la Suisse a également conclu des traités de protection des informations avec l'Agence spatiale européenne et l'OTAN, qui définissent des mécanismes de protection uniformes pour le traitement d'informations classifiées ou la reconnaissance mutuelle de certificats de sécurité. Ils précisent notamment les organismes chargés de la mise en œuvre des mesures de sécurité. Dans le domaine de la sécurité des communications, des interlocuteurs nationaux chargés d'élaborer des normes homogènes et de vérifier la conformité des systèmes sont exigés. Le service spécialisé de la Confédération pour la sécurité de l'information assumera ces tâches pour la Suisse.

Les obligations internationales de la Suisse en matière de sécurité de l'information sont compatibles avec la présente loi.

5.3 Forme de l'acte à adopter

Dans sa décision du 12 mai 2010 (cf. ch. 1.1.4), le Conseil fédéral était déjà parti de l'idée que les règles les plus importantes en matière de sécurité de l'information devaient être consignées dans une loi fédérale. D'une part, ce sont des dispositions d'organisation et de procédure destinées aux autorités fédérales (art. 164, al. 1, let. g, Cst.) qui, en raison de la nécessité d'une application uniforme, doivent déployer des effets transversaux; les cantons sont d'ailleurs également soumis à des obligations en matière de sécurité de l'information. D'autre part, les dispositions concernées sont susceptibles de porter gravement atteinte aux droits fondamentaux (art. 164, al. 1, let. b et c, Cst.), notamment dans le domaine des CSP et des PSE, ou nécessitent, pour des raisons de protection des données, d'être inscrites dans une loi au sens formel (art. 17, al. 2, LPD). Pour les inconvénients du champ d'application uniforme sous l'angle législatif, on se référera au ch. 1.3 (exécution).

5.4 Frein aux dépenses

Le projet n'est pas soumis au frein aux dépenses au sens de l'art. 159, al. 3, let. b, Cst., car il ne comporte aucune disposition relative aux subventions ou aux crédits d'engagement et plafonds de dépenses.

5.5 Conformité à la loi sur les subventions

Le projet ne prévoit ni aides financières ni indemnités au sens de la loi du 5 octobre 1990 sur les subventions[48].

5.6 Délégation de compétences législatives

Les lois fédérales peuvent déléguer des compétences législatives à moins que la Constitution ne l'exclue (art. 164, al. 2, Cst.). En raison du champ d'application qui s'étend à toutes les autorités de la Confédération, l'exécution de la loi ne peut suivre le schéma «ordinaire» qui attribue en principe la compétence d'édicter le droit d'exécution au seul Conseil fédéral. Pour préserver l'autonomie d'exécution des autorités, le projet prévoit qu'elles devront édicter elles-mêmes les dispositions d'exécution nécessaires (art. 85, al. 1). Cette délégation concerne l'ensemble de la loi, à moins que cette dernière n'attribue expressément la compétence législative au Conseil fédéral. Le projet délègue au Conseil fédéral les compétences législatives suivantes:

- art. 2, al. 3 et 4: il désigne les unités visées à l'art. 2, al. 4, LOGA chargées d'appliquer totalement ou partiellement la loi;
- art. 12, al. 3: il règle la déclassification des fonds d'archives;
- art. 32, al. 2: il met en place les services spécialisés CSP;
- art. 44, al. 2: il peut renoncer à la répétition du CSP pour certaines fonctions militaires et de la protection civile;
- art. 49: il édicte des dispositions complémentaires concernant la procédure de CSP et la protection des données;
- art. 74: il édicte des dispositions complémentaires concernant la PSE et la protection des données afférente et règle l'organisation du service spécialisé PSE;
- art. 75, al. 5: il désigne les services fédéraux compétents pour l'appui aux infrastructures critiques en matière de sécurité de l'information;
- art. 81: il édicte des dispositions complémentaires concernant la sécurité de l'information dans les infrastructures critiques et la protection des données afférentes;
- art. 84, al. 3: il règle l'organisation du service spécialisé de la Confédération pour la sécurité de l'information et peut lui confier d'autres tâches;
- art. 85, al. 1: il peut charger la ChF d'édicter les dispositions d'exécution pour les affaires du Conseil fédéral;
- art. 86: il définit des mesures standard conformément aux connaissances scientifiques et techniques les plus récentes et peut déléguer cette tâche;

48 RS **616.1**

- art. 87, al. 4: il définit les cas dans lesquels les cantons peuvent recourir aux ressources de la Confédération afin d'assurer leur propre sécurité de l'information et fixe les émoluments;
- art. 88: il est habilité à conclure en toute autonomie des traités internationaux;
- art. 14, al. 2, LAAM: il définit les fonctions soumises au contrôle;
- art. 20*a*, al. 2, LApEl: il désigne les groupes de personnes soumis au contrôle de loyauté.

5.7 Conformité à la législation sur la protection des données

L'accomplissement des tâches assignées par le présent projet exige le traitement de données personnelles dans les domaines suivants:

- art. 19, al. 2: le traitement de données personnelles dans le cadre de la surveillance des réseaux par les fournisseurs de prestations se fonde sur le droit en vigueur (art. 57*i* à 57*q* LOGA);
- art. 20, al. 2: une base légale au sens formel est créée conformément à l'art. 17, al. 2, LPD en vue de l'utilisation de données biométriques pour la vérification de l'identité des personnes devant accéder à des informations, des moyens informatiques ou des locaux de la Confédération;
- art. 24 à 27: une base légale au sens formel est créée conformément à l'art. 17, al. 2, LPD pour le recours à des systèmes d'information concernant le contrôle centralisé des données d'identification; étant donné que la responsabilité de la protection des données pourrait être partagée, les autorités soumises à la loi (et en premier lieu le Conseil fédéral) devront régler la responsabilité de la protection des données sur la base de l'art. 16, al. 2, LPD; le recours à ces systèmes améliorera la protection opérationnelle des données et leur sécurité;
- art. 28 à 49: les CSP impliquent le traitement de données sensibles (art. 3, let. c, LPD); en outre, le résultat du CSP correspond à un profil de la personnalité (art. 3, let. d, LPD); pour le traitement de ces données, la LSI crée une base légale au sens formel conformément à l'art. 17, al. 2, LPD; étant donné que le Conseil fédéral instituera au moins deux services spécialisés CSP, il devra encore régler les modalités de la responsabilité de la protection des données (art. 16, al. 2, LPD); globalement, sous l'angle de la protection des données, la nouvelle réglementation est nettement meilleure et plus proportionnée que le droit en vigueur (art. 19 à 21 LMSI et art. 144 à 149 LSIA); de plus, le Conseil fédéral souhaite abaisser le nombre des personnes soumises au CSP, ce qui réduira d'autant le traitement de données personnelles;
- art. 50 à 74: les PSE impliquent le traitement et la diffusion de données sensibles (art. 3, let. c, LPD); la LSI crée une base légale au sens formel conformément à l'art. 17, al. 2, LPD pour traiter ces données;

– art. 75 à 81: afin d'apporter son soutien aux infrastructures critiques dans le domaine de la sécurité de l'information, MELANI doit traiter régulièrement des données personnelles (ressources d'adressage) qui peuvent être dans certains cas des données sensibles; la LSI crée à cette fin une base légale au sens formel;
– modification d'autres actes: quelques dispositions d'autres actes règlent le traitement des données personnelles en relation avec le CSP au sens des art. 28 à 49; les commentaires afférents s'appliquent par analogie.

Au sens de la LSI, les données personnelles sont des informations dont la confidentialité, la disponibilité, l'intégrité et la traçabilité doit être protégée. Le projet crée au niveau transversal la base nécessaire à des processus, des mesures et des capacités homogènes visant la protection des informations, dans la mesure où la Confédération est compétente. Le PFPDT sera associé à l'exécution et notamment à l'élaboration de mesures standard. L'application complémentaire de la loi aux données personnelles améliorera donc aussi la mise en œuvre de la protection des données, en particulier la protection de la sécurité des données.

Liste des abréviations

BAC	Base d'aide au commandement
CdG-E	Commission de gestion du Conseil des États
CdG-N	Commission de gestion du Conseil national
CERT	Computer Emergency Response Team (centre de veille, d'alerte et de réponse aux attaques informatiques)
ChF	Chancellerie fédérale
CP	Code pénal; RS *311.0*
CPM	Code pénal militaire du 13 juin 1927; RS *321.0*
CPP	Code de procédure pénale; RS *312.0*
CSP	Contrôle(s) de sécurité relatif(s) aux personnes
Cst.	Constitution; RS *101*
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DélCdG	Délégation des Commissions de gestion
DEFR	Département fédéral de l'économie, de la formation et de la recherche
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFAE	Département fédéral des affaires étrangères
DFF	Département fédéral des finances
DFI	Département fédéral de l'intérieur
DFJP	Département fédéral de justice et police
DSE	Déclaration de sécurité relative aux entreprises
fedpol	Office fédéral de la police
GIA	Gestion des données d'identification et des accès
LAAM	Loi du 3 février 1995 sur l'armée; RS *510.10*
LApEl	Loi du 23 mars 2007 sur l'approvisionnement en électricité; RS *734.7*
LAr	Loi fédérale du 26 juin 1998 sur l'archivage; RS *152.1*
LAVS	Loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants; RS *831.10*
LBN	Loi fédérale du 3 octobre 2003 sur la Banque nationale; RS *951.11*
LENu	Loi du 21 mars 2003 sur l'énergie nucléaire; RS *732.1*

LFC	Loi du 7 octobre 2005 sur les finances de la Confédération; RS *611.0*
LMP	Loi fédérale du 16 décembre 1994 sur les marchés publics; RS *172.056.1*
LMSI	Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure; RS *120*
LOGA	Loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration; RS *172.010*
LParl	Loi du 13 décembre 2002 sur le Parlement; RS *171.10*
LPD	Loi fédérale du 19 juin 1992 sur la protection des données; RS *235.1*
LPers	Loi du 24 mars 2000 sur le personnel de la Confédération; RS *172.220.1*
LRCF	Loi fédérale du 14 mars 1958 sur la responsabilité de la Confédération, des membres de ses autorités et de ses fonctionnaires; RS *170.32*
LRens	Loi fédérale du 25 septembre 2015 sur le renseignement; FF *2015* 6597
LSI	Loi sur la sécurité de l'information (projet)
LSIA	Loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée; RS *510.91*
LSIP	Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération; RS *361*
LTAF	Loi du 17 juin 2005 sur le Tribunal administratif fédéral; RS *173.32*
LTC	Loi du 30 avril 1997 sur les télécommunications; RS *784.10*
LTF	Loi du 17 juin 2005 sur le Tribunal fédéral; RS *173.110*
LTrans	Loi fédérale du 17 décembre 2004 sur le principe de la transparence dans l'administration; RS *152.3*
MCF LTrans	Message du 13 février 2003 relatif à la LTrans (FF *2003* 1807)
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
OCSP	Ordonnance du 4 mars 2011 sur les contrôles de sécurité relatifs aux personnes; RS *120.4*
OFCOM	Office fédéral de la communication
OFIT	Office fédéral de l'informatique et de la télécommunication
OFJ	Office fédéral de la justice
OFPER	Office fédéral du personnel

OIAF	Ordonnance du 9 décembre 2011 sur l'informatique et la télécommunication dans l'administration fédérale; RS *172.010.58*
OLPD	Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données; RS *235.11*
OPrI	Ordonnance du 4 juillet 2007 concernant la protection des informations; RS *510.411*
PA	Loi fédérale du 20 décembre 1968 sur la procédure administrative; RS *172.021*
PFPDT	Préposé fédéral à la protection des données et à la transparence
PPM	Procédure pénale militaire du 23 mars 1979; RS *322.1*
PSE	Procédure de sécurité relative aux entreprises
SG	Secrétariat général
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques du 27 juin 2012 (FF *2013* 517)
SRC	Service de renseignement de la Confédération
UPIC	Unité de pilotage informatique de la Confédération