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

Rapport explicatif

---

du 26 mars 2014

Condensé

L'information est la monnaie d'échange de la société de l'information. Il incombe aux autorités fédérales de veiller à la sécurité des informations qu'elles traitent ou dont elles confient le traitement à des organisations qui lui sont subordonnées, sur mandat et pour le compte de la Suisse. Elles doivent pour ce faire disposer d'instruments modernes. En raison du développement de la société de l'information, les informations sont exposées à des dangers et à des menaces plus complexes et plus dynamiques. Plusieurs attaques contre des systèmes informatiques de la Confédération ont montré que la protection des informations présentait des lacunes qui, notamment sur le plan organisationnel, sont également dues à des bases légales obsolètes ou incohérentes.

Se fondant sur des normes internationalement reconnues, le présent projet de loi crée des bases légales formelles uniformes pour la gestion de la sécurité de l'information dans le domaine de compétence de la Confédération. Il vise à adapter la protection des informations et la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC) aux exigences d'une société de l'information moderne et en réseau, et à remédier aux lacunes et faiblesse du droit en vigueur.

Points essentiels du projet

Sécurité de l'information

La notion de «sécurité de l'information» englobe toutes les exigences et mesures visant à protéger la confidentialité, la disponibilité, l'intégrité et la traçabilité des informations, indépendamment du fait qu'elles soient traitées sous forme électronique, oralement ou sur support papier.

Au sein de la Confédération, les bases légales actuelles qui permettent de définir de telles exigences et appliquer de telles mesures sont très sectorielles, guère harmonisées et souvent lacunaires. Il en va de même des compétences organisationnelles. Ainsi, la Confédération dispose aujourd'hui, aux niveaux tant juridique qu'organisationnel, d'organisations parallèles en matière de protection des données, de protection des informations (protection des informations classifiées), de sécurité informatique, de sécurité des personnes, de sécurité physique et de gestion des risques. La pratique a montré que cette orientation sectorielle n'était pas efficace. Le projet réunit par conséquent les mesures les plus importantes de protection des informations en une seule réglementation homogène. Il prévoit par ailleurs une structure unique permettant de piloter et de contrôler l'ensemble de la sécurité de l'information.

Champ d'application institutionnel

Les échanges d'informations électroniques entre les autorités et entre ces dernières et les particuliers (y compris les milieux économiques) se sont multipliés. Le besoin de protection d'une information ne dépend toutefois pas du service ou de la personne qui la traite. De plus, les infrastructures et systèmes TIC sont de plus en plus interconnectés, ce qui aggrave le risque de voir les attaques et les menaces contre une autorité déployer leurs effets dans les domaines de compétence d'autres autorités impliquées. Il est donc nécessaire de définir un niveau de sécurité uniforme et transversal, d'une part pour garantir la confiance mutuelle entre les autorités fédérales lors du traitement des informations, et d'autre part pour réduire les risques encourus par toutes les autorités concernées.

Le champ d'application primaire du projet s'étend ainsi à toutes les autorités fédérales (l'Assemblée fédérale, les tribunaux fédéraux, le Conseil fédéral, le Ministère public de la Confédération et son autorité de surveillance, la Banque nationale suisse) de même qu'à leurs organisations subordonnées (les Services du Parlement, les administrations des tribunaux fédéraux, l'administration fédérale et l'armée). Dans la mesure où les cantons ou des tiers sont chargés de traiter des informations de la Confédération ou ont accès à des moyens TIC de cette dernière, les prescriptions fédérales doivent également leur être applicables.

Gestion des risques

La complexité et la dynamique des menaces exigent des autorités fédérales qu'elles mettent davantage l'accent sur l'évaluation systématique du besoin de protection des informations et l'appréciation des risques y afférents. Il faut pour cela une gestion efficace des risques en matière de sécurité de l'information et un contrôle régulier de la mise en œuvre des mesures destinées à minimiser les risques, dispositifs qui font aujourd'hui largement défaut. Par conséquent, le projet propose également un processus de maintien durable et économique de la sécurité de l'information.

Classification des informations

En raison des attentes de plus en plus fortes des citoyennes et citoyens quant à la transparence des autorités fédérales, le projet définit clairement les critères de classification des informations de la Confédération et rehausse les valeurs seuils de classification. Le principe de la transparence de l'administration fédérale n'est d'aucune manière remis en cause par les dispositions relatives à la classification.

Sécurité dans l'engagement des TIC

Le projet tient compte du constat que la garantie de la sécurité de l'information dans l'engagement des moyens TIC a considérablement gagné en importance depuis quelques années. C'est pourquoi il définit un mécanisme d'évaluation de la criticité des moyens TIC, qu'il lie à la mise en œuvre conséquente de mesures de sécurité. L'accent principal devra porter sur la sécurité des systèmes et moyens TIC les plus critiques. Le projet renforce le rôle stratégique et opérationnel des autorités dans l'application des mesures et en en matière d'audits.

Contrôles de sécurité relatifs aux personnes (CSP)

Les CSP sont avant tout une mesure de sécurité de l'information: ils seront par conséquent régis par la nouvelle loi sur la sécurité de l'information et non plus par la LMSI. Simultanément, certaines lacunes de la législation en vigueur seront comblées, et le champ d'application de CSP sera restreint: les motifs de contrôle seront adaptés aux exigences actuelles de la sécurité de l'information et les degrés de contrôle ramenés de trois à deux. La récolte des données sera adaptée pour les deux degrés de contrôle. A l'avenir, il devrait y avoir moins de contrôles, mais ils seront davantage adaptés aux risques actuels.

Procédure de sécurité relative aux entreprises (PSE)

La PSE s'applique aux entreprises qui, dans le cadre d'un marché public de la Confédération, doivent se voir confier l'exercice d'une activité sensible. Elle vise d'une part à vérifier la fiabilité d'une entreprise et d'autre part à contrôler, faire respecter et garantir la sécurité de l'information durant l'accomplissement du mandat. Le champ d'application de l'actuelle procédure de maintien du secret est limité au domaine militaire. Le projet introduit une PSE unifiée. Parallèlement, il habilite les autorités à établir une déclaration de sécurité pour les entreprises suisses qui soumissionnent pour des mandats étrangers ou internationaux et ont besoin pour ce faire d'une déclaration de sécurité nationale. La compétitivité de ces entreprises s'en trouvera renforcée.

Soutien aux infrastructures critiques (IC)

Dans sa Stratégie nationale de protection de la Suisse contre les cyberrisques du 27 juin 2012 (SNPC; FF 2013 517), le Conseil fédéral a établi le principe du soutien de la Confédération aux exploitants d'IC en matière de sécurité de l'information. Dans le cadre de la collaboration entre les exploitants d'IC et la Confédération, les services concernés doivent pouvoir échanger des données personnelles (ressources d'adressage dans le domaine des télécommunications) éventuellement liées à des poursuites et sanctions administratives ou pénales. Le projet crée à cet égard les bases légales formelles nécessaires au traitement de données de cette nature.

Exécution

L'exécution de la présente loi doit d'une part intervenir de la façon la plus homogène possible, et d'autre part respecter l'indépendance et l'autonomie des diverses autorités de la Confédération.

L'avant-projet prend en compte ces exigences en soi contradictoires en prévoyant:

- *une réglementation d'exécution selon le principe du « opting out »: chaque autorité exécute la loi dans son domaine de compétences et édicte les ordonnances y afférentes. La législation d'exécution du Conseil fédéral s'appliquera toutefois par analogie aux autres autorités de la Confédération dans la mesure où elles n'auront pas édicté leur propre réglementation;*
- *des exigences et mesures standards: le Conseil fédéral est habilité à définir des exigences et mesures standards conformes à l'avancée des connaissances et de la technologie, qui vaudront recommandations pour les autres autorités fédérales;*
- *la création d'un organe de coordination transversal spécialisé (au niveau des autorités): cet organe de coordination (la Conférence des préposés à la sécurité de l'information) aura pour vocation principale l'exécution uniforme de la loi au niveau transversal sur la base des risques. Il sera également associé à la définition des exigences et mesures standards.*

La solution proposée préservera l'indépendance des autorités de la Confédération dans l'exécution de la loi. Ces dernières n'étant pas liées par les dispositions d'exécution du Conseil fédéral, la loi elle-même doit définir les exigences et mesures minimales contraignantes pour toutes les autorités. La loi comporte par conséquent nombre de dispositions qui, sous l'angle de la hiérarchie normative, relèveraient matériellement du niveau de l'ordonnance. Le projet ménage également une autonomie d'exécution suffisante aux cantons et à certaines organisations soumises à la loi et à la législation d'exécution du Conseil fédéral. Enfin, il crée la base légale formelle, aujourd'hui absente, habilitant le Conseil fédéral à conclure des accords internationaux en matière de sécurité de l'information.

Organisation de la sécurité de l'information

Le projet adapte l'organisation spécialisée de la sécurité de l'information à la nouvelle réalité complexe et changeante, et ce à deux niveaux organisationnels:

- *organisation interne:*
  - *gestion de la sécurité de l'information: en la matière, les autorités de la Confédération doivent s'inspirer des normes internationales reconnues et éprouvées (par ex. les normes DIN ISO/IEC 27001 et 27002);*
  - *préposés à la sécurité de l'information: les autorités de la Confédération désignent chacune un préposé ou une préposée à la sécurité de l'information et une suppléance à qui elles confient le pilotage de l'ensemble de la sécurité de l'information;*
- *organisation transversale:*
  - *service spécialisé de la Confédération en matière de sécurité de l'information: certains organes existants seront réunis en un nouveau service spécialisé, pour résoudre au plan systémique des problèmes de compétences avérés et améliorer le niveau des connaissances interdisciplinaires. Le service spécialisé, qui a vocation de soutien et de conseil, ne sera pas habilité à donner des instructions dans le cadre transversal en raison de l'indépendance des diverses autorités de la Confédération. La législation d'exécution du Conseil fédéral réglera le rattachement et les tâches détaillées de cet organe;*
  - *conférence des préposés à la sécurité de l'information: cet organe sert avant tout à l'exécution homogène de la loi au niveau transversal. En cas de nécessité, il pourra recourir à des experts des cantons et des milieux scientifiques et économiques;*
  - *services spécialisés CSP: pour garantir l'indépendance des contrôles de sécurité relatifs aux personnes, le Conseil fédéral instituera au minimum deux services spécialisés, comme c'est déjà le cas aujourd'hui;*
  - *service spécialisé PSE: pour mener les procédures de contrôle relatives aux entreprises, le Conseil fédéral devra instituer un service spécialisé.*

<u>Conséquences</u>

La loi entraînera une amélioration notable de la gestion de la sécurité de l'information de la Confédération. Elle réduira les risques y afférents, qui pour tout ou partie sont aussi de nature financière. La pratique a montré qu'une gestion efficiente de la sécurité de l'information peut même permettre des économies à moyen terme. Mais pour la Confédération, la loi aura également des conséquences directes sur le plan des finances et des ressources humaines. Les besoins supplémentaires ne peuvent encore être estimés avec précision, mais ils seront exposés dans le message. Les sources de coûts principales sont:

- *l'organisation, le pilotage et le contrôle de la sécurité de l'information;*
- *le renforcement des contrôles et des audits;*
- *les contrôles de sécurité relatifs aux personnes;*
- *les procédures de sécurité relatives aux entreprises;*
- *la création et les tâches du service spécialisé de la Confédération en matière de sécurité de l'information.*

On notera que la loi elle-même ne définit pratiquement aucune mesure de détail et qu'elle n'est par conséquent pas directement applicable: les diverses autorités fédérales devront, dans leurs domaines de compétence, édicter leurs propres dispositions d'exécution. Seront dès lors déterminants pour l'évaluation des coûts d'exécution le niveau de sécurité qu'elles définiront, de même que les mesures y afférentes sur les plans organisationnel et technique, et sur ceux du personnel et des constructions: ces mesures seront décidées aux niveaux des ordonnances, des directives ou des projets, après une analyse approfondie du rapport coût/utilité.

Pour les cantons, les conséquences seront minimes, et le projet ne touche guère la société et l'économie.

Table des matières

Actes normatifs cités par leur abréviation

CP	Code pénal suisse du 21 décembre 1937; RS **311.0**
CPM	Code pénal militaire du 13 juin 1927; RS **321.0**
CPP	Code de procédure pénale suisse du 5 octobre 2007; RS **312.0**
Cst.	Constitution fédérale de la Confédération suisse du 18 avril 1999; RS **101**
ISA CH-EU	Accord du 28 avril 2008 entre la Confédération suisse et l'Union européenne sur les procédures de sécurité pour l'échange d'informations classifiées, RS **0.514.126.81**
LAAM	Loi fédérale du 3 février 1995 sur l'armée et l'administration militaire; RS **510.10**
LApEl	Loi fédérale 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**
LBN	Loi fédérale du 3 octobre 2003 sur la Banque nationale suisse; RS **951.11**
LENu	Loi du 21 mars 2003 sur l'énergie nucléaire; RS **732.1**
LF concernant la protection des ouvrages militaires	Loi fédérale du 23 juin 1950 concernant la protection des ouvrages militaires; RS **510.518**
LFC	Loi du 7 octobre 2005 sur les finances de la Confédération; RS **611.0**
LFRC	Loi fédérale du 3 octobre 2008 sur le renseignement civil; RS **121**
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 l'Assemblée fédérale; 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**
LPTh	Loi fédérale du 15 décembre 2000 sur les médicaments et les dispositifs médicaux; loi sur les produits thérapeutiques; RS **812.21**
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**
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**
O concernant la sauvegarde du secret	Ordonnance du DDPS du 29 août 1990 concernant la procédure à suivre lors de la passation de contrats dont le contenu est classifié du point de vue militaire; RS **510.413**
OCSP	Ordonnance du 4 mars 2011 sur les contrôles de sécurité relatifs aux personnes; RS **120.4**
OCSPN	Ordonnance du 9 juin 2006 sur les contrôles de sécurité relatifs aux personnes dans le domaine des installations nucléaires; RS **732.143.3**
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 de la Confédération; RS **510.411**
PA	Loi fédérale du 20 décembre 1968 sur la procédure administrative; RS **172.021**
PPM	Procédure pénale militaire du 23 mars 1979; RS **322.1**

1 Partie générale

1.1 Contexte

1.1.1 Evolution de la Suisse vers une société de l'information

Depuis quelques décennies, le monde connaît un changement sociétal fondamental provoqué par le développement des technologies de l'information et de la communication (TIC). 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 qu'auparavant. En regard de l'histoire, notre façon de vivre a radicalement changé en très peu de temps.

Le recours aux TIC offre à la Suisse de multiples chances dans son évolution vers une société de l'information. Les nouvelles possibilités et liaisons techniques présentent toutefois des risques que l'on ne peut ignorer. En tant que monnaie d'échange de la société de l'information, l'information peut avoir une valeur considérable. La perte, le vol, la divulgation et l'usage abusif d'informations, ou encore le dérangement des moyens de traitement de l'information, peuvent mettre gravement en péril des intérêts publics majeurs ou des droits de tiers, occasionner des préjudices financiers substantiels, voire entraver l'accomplissement de tâches légales critiques de la Confédération. Si des incidents graves ou répétés donnaient à penser que la Confédération ne protège pas les informations qu'elle détient avec tout le soin voulu, la confiance du peuple en ses autorités pourrait s'en trouver durablement ébranlée, de même que celle des partenaires étrangers de la Suisse.

1.1.1.1 Stratégie pour une société de l'information en Suisse

Le Conseil fédéral est conscient de l'importance capitale des TIC pour la place économique suisse et l'espace de vie de notre pays. En 1998 déjà, il a approuvé une stratégie pour une société de l'information en Suisse, révisée en 2006 et 2012 (FF 2012 3505). Il entend exploiter les chances qu'offre le recours aux TIC, et préconise pour cette raison que les TIC doivent être engagées dans le but de renforcer la prospérité commune, le développement durable, la cohésion interne et la diversité culturelle du pays. La stratégie circonscrit les champs d'intervention dans lesquels le potentiel d'innovation des TIC peut avoir des répercussions significatives et définit les priorités de l'action de la Confédération en la matière.

Ce faisant, le Conseil fédéral poursuit deux objectifs stratégiques principaux:

- les TIC contribuent à rendre l'espace économique suisse innovant et compétitif sur le plan international;
- les TIC profitent à tous et rendent l'espace de vie suisse attrayant.

En rapport avec ce changement sociétal, le Conseil fédéral a commandité de nombreux projets (par ex. dans le domaine de la cyberadministration, de la cyberjustice, de la cybersanté, de la gestion électronique des affaires [GEVER], etc.). De plus, il a confié au DFJP plusieurs mandats visant à assurer les bases légales de la société de l'information en Suisse. De ces projets est issu un réseautage de plus en plus complexe et dynamique d'échange d'informations des citoyens avec les autorités d'une part, et des autorités entre elles d'autre part.

1.1.1.2 Principe de la transparence dans l'administration fédérale

Dans son message du 12 février 2003 relatif à la LTrans (FF 2003 1807), le Conseil fédéral admettait 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 citoyennes et citoyens. La loi sur la transparence a été adoptée le 17 décembre 2004: elle autorise toute personne à consulter des documents officiels sans devoir faire 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'Etat traite ses informations sur mandat et au nom du peuple suisse. Ce dernier est habilité en tout temps à exercer son contrôle. Des exceptions existent, mais elles sont exhaustivement énumérées 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, il est en conséquence nécessaire que le document concerné soit effectivement protégé en fonction de ce besoin.

1.1.1.3 Données publiques en libre accès (*Open Government Data*; OGD)

L'OGD est une notion étroitement liée au principe de la transparence, qui vise l'accessibilité et la réutilisation de données produites dans le cadre des activités de l'administration. La publication et la réutilisation libre de données des autorités peuvent offrir des avantages économiques, politiques et internes à l'administration.

Dans son rapport du 13 septembre 2013 en réponse au postulat Wasserfallen 11.3884 du 29 septembre 2011 («Le libre accès aux données publiques comme priorité stratégique de la cyberadministration»), le Conseil fédéral estime que l'appréciation des chances et des risques de l'OGD montre un potentiel intéressant pour une conduite transparente et efficace de l'administration et la création d'une plus-value économique. Il a chargé l'Unité de pilotage informatique de la Confédération (UPIC), en collaboration avec les Archives fédérales suisses (AFS), de diriger et coordonner le développement de l'OGD et de formuler une stratégie nationale en la matière.

1.1.2 Risques de la société de l'information

Le Conseil fédéral veut limiter les risques de voir le changement sociétal désavantager la population et l'économie, ou mettre en péril les droits individuels. Certains risques ne concernent pas en priorité les effets du changement (par ex. la «fracture numérique»), mais les informations elles-mêmes et les réseaux d'information et de communication. Souvent, la valeur réelle des informations n'apparaît malheureusement qu'à la faveur d'un incident source d'effets négatifs. Tant pour les pouvoirs publics que pour les entreprises et les particuliers, la perte, le vol, la diffusion non autorisée ou l'utilisation abusive d'informations peut avoir des conséquences extrêmement déplaisantes.

Tout aussi vulnérables sont les infrastructures d'information et de communication, de même que les moyens TIC pris individuellement, dont les autorités et les entreprises se servent dans leurs processus d'affaires. Ainsi, la défaillance d'un système informatique peut avoir des conséquences financières considérables selon la place qu'il occupe dans les processus d'affaires (criticité). Lorsqu'une telle défaillance touche l'exploitant d'une infrastructure fournissant des services indispensables au fonctionnement de la société, de l'économie ou de la Confédération (infrastructure critiques, IC), les effets peuvent être catastrophiques et, dans le pire des cas, entraîner mort d'homme.

1.1.2.1 Menaces sur les informations et les moyens TIC

Chaque jour, les médias relatent des cas d'espionnage, d'attaques ou de défaillances touchant des services TIC, 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 du 27 juin 2012 (SNPC; FF 2013 517, cf. ch. 1.1.2.2). Pour une appréhension réaliste la menace, il faut tenir compte de trois éléments:

Les menaces doivent être prises au sérieux. Les spécialistes ont souvent tendance à dramatiser les risques et leurs effets potentiels. A l'inverse, on ne saurait non plus les sous-estimer. Les organisations criminelles investissent souvent énormément d'argent et de savoir-faire pour dérober des données informatiques de clients (notamment les données des banques et des cartes de crédit) ou pour faire chanter des particuliers. Leurs moyens restent toutefois très modestes en regard des ressources financières et humaines engagées par certains acteurs étatiques dans l'espionnage politique, diplomatique, scientifique et économique. Certains Etats accordent la priorité à des activités ciblées d'espionnage économique et industriel en vue de favoriser l'industrialisation et le développement de leur 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 des TIC. 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. Mais les dérangements ou interruptions de l'activité en raison de défaillances techniques, de fausses manipulations ou d'événements naturels, par exemple une panne d'électricité ou un incendie, sont nettement plus fréquents et peuvent avoir des conséquences tout aussi graves.

Enfin, la surveillance à grande échelle du trafic sur Internet, notamment par le détournement et la perversion de services et applications TIC très répandus ne saurait être passée sous silence, pas plus que la corruption systématique des normes de cryptage. Les révélations les plus récentes à propos de tels agissements prouvent que les hypothèses quant à l'intégrité d'Internet et des services de base sont erronées, notamment en ce qui concerne la sécurité du traitement des informations.

On assiste à une véritable «course aux armements informatiques». La plupart des pays développés sont conscients de leur dépendance à l'égard de l'infrastructure d'information et de communication, de même que

des dangers qu'ils encourent, et ils prennent des mesures de protection. Mais de loin pas tous les Etats se contentent de stratégies purement *défensives*: nombreux sont ceux qui se dotent de capacités *offensives* de nature militaire ou dans le domaine du renseignement. En Suisse également, des voix s'élèvent en faveur du renforcement de telles capacités offensives. Contrairement à la course classique aux armements, la participation ne se limite pas aux acteurs étatiques ou financés par l'Etat. Les solutions n'étant pas toujours particulièrement complexes et coûteuses et n'exigeant pas nécessairement des installations d'envergure, nombre d'informaticiens, de mathématiciens et d'autres spécialistes en technologie travaillent inlassablement au développement de nouveaux 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. Il est donc compréhensible que l'attention et l'action se focalisent sur la protection contre ces nouveaux risques. Pour autant, on ne saurait réduire la protection de l'information et des moyens TIC à la seule prévention des cyber-attaques: des menaces significatives ont en effet 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 sont aujourd'hui encore échangées oralement entre des personnes ou traitées sur support papier. Les risques qui y sont liés ne sauraient par conséquent être ignorés du point de vue de la sécurité de l'information.

1.1.2.2 Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)

En collaboration avec les autorités, les milieux économiques et les exploitants d'infrastructures critiques (IC), le Conseil fédéral veut minimiser les risques de cette nature auxquels ils sont quotidiennement exposés. La SNPC identifie les cyberrisques en tant qu'émanations des processus et responsabilités en place, raison pour laquelle ils doivent être pris en compte 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 domaine informatique;
- le renforcement de la capacité de résistance des infrastructures critiques;
- la réduction efficace des risques liés à l'informatique, notamment de la cybercriminalité, du cyberespionnage et du cybersabotage.

Il entend approfondir la collaboration entre les autorités et les milieux économiques dans le domaine informatique et renforcer les bases existantes. Il s'appuie pour ce faire sur les structures actuelles et renonce à un organe national central de pilotage et de coordination dont d'autres pays se sont dotés. La SNPC expose les champs d'action et les mesures qui doivent permettre de réduire les cyberrisques au plan national. A cette fin, l'actuelle Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), qui assumait déjà cette tâche sous forme de partenariats public-privé, a été renforcée. De plus, le Conseil fédéral a donné mandat aux départements de mettre en œuvre diverses mesures à leur niveau et dans le dialogue avec les autorités cantonales et les milieux économiques. Ces mesures vont de l'analyse des risques encourus par les infrastructures TIC critiques à une défense plus soutenue des intérêts suisses sur la scène internationale. Un organe de coordination a été créé au DFF pour assurer la coordination de la mise en œuvre de la SNPC.

Pour ce qui est de la stratégie nationale pour la protection des infrastructures critiques, cf. ch. 3.5.3.

1.1.2.3 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, le dérangement ou la destruction peuvent mettre en péril l'accomplissement de tâches fédérales légales critiques et entraîner de ce fait des préjudices considérables pour la société, l'économie ou l'Etat. Dans l'accomplissement de ses tâches légales, la Confédération traite quotidiennement des volumes importants d'informations, parmi lesquelles se trouvent des informations particulièrement sensibles pour la sécurité intérieure et extérieure, les relations internationales ou les intérêts économiques de la Suisse, et qui nécessitent pour cela d'être protégées par classification.

Les informations classifiées ne sont toutefois pas les seules informations qui nécessitent une protection élevée. Certes, l'espionnage se focalisait par le passé essentiellement sur la recherche de renseignements militaires ou d'informations de politique extérieure. De nos jours, il vise de plus en plus souvent l'économie.

Dans un contexte de forte concurrence au niveau mondial, quiconque réussit à se procurer le savoir de ses concurrents (résultats de recherche et développement, savoir-faire, etc.) obtient du même coup un avantage décisif. Par conséquent, les activités d'espionnage se multiplient depuis quelques années dans les secteurs économique et industriel, notamment dans les domaines de haute technologie. A cet égard, l'administration fédérale constitue un centre névralgique très sensible: elle réglemente l'économie privée, vérifie certains produits et en autorise la diffusion, contrôle certaines entreprises, acquiert elle-même des biens et services de valeur, etc. Ce faisant, l'administration fédérale est 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, à juste titre, de ces autorités qu'elles protègent leurs informations avec toute la diligence voulue.

La Confédération traite également un volume important de données personnelles qui, en vertu de la législation sur la protection des données, doivent être traitées de façon régulière, conformément au but recherché et dans le respect du principe de proportionnalité. Elles doivent être protégées par des mesures tant organisationnelles que techniques. En cas d'utilisation abusive, les personnes dont les données sont traitées peuvent être gravement lésées dans leurs droits individuels. Certaines données personnelles sont aussi recherchées que les informations technologiques de l'industrie. Leur valeur financière ne doit pas être sous-estimée: il existe un marché florissant pour l'acquisition et la diffusion de données personnelles.

Si des incidents graves ou répétés devaient se produire, la confiance en nos autorités fédérales pourrait s'en trouver fortement ébranlée. Cela pourrait même conduire à ce que des informations importantes ne soient pas transmises à la Confédération aussi longtemps que cette dernière n'apporte pas la preuve qu'elle les protège de manière fiable.

Ces risques pour la Confédération ne sont pas des hypothèses abstraites ou invraisemblables. Ainsi, en octobre 2009, un programme malveillant voué à l'espionnage a été découvert au DFAE: il s'est introduit dans le réseau par un courriel et n'a été découvert que très tard. Auparavant, l'entreprise RUAG et la société Mowag, toutes deux proches de la Confédération, ont été victimes d'attaques similaires. On ne doit pas non plus oublier les menaces que peuvent représenter les membres du personnel de la Confédération: un grave cas de vol de données a été découvert en mai 2012 au Service de renseignement de la Confédération (SRC). Un collaborateur de ce service a copié sur des supports amovibles de grandes quantités d'informations sensibles auxquelles il avait accès grâce à ses autorisations et les a 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 portables ou de smartphones, la perte de supports d'informations classifiées, la divulgation non autorisée, généralement pour des motifs politiques, d'informations protégées, les perturbations d'activité en raison de la défaillance d'un serveur, de surcharges du réseau ou d'une mauvaise configuration d'un logiciel, etc. Etant donné que la plupart de ces incidents ne sont pas systématiquement consignés ou ne sont pas au moins communiqués aux services spécialisés pour examen, il est difficile d'estimer le préjudice global subi par la Confédération.

1.1.3 Mandats du Conseil fédéral

Le Conseil fédéral a attribué nombre de mandats en rapport avec la sécurité de l'information, dont il a fallu tenir compte dans le cadre de la préparation du projet: ne seront commentés ci-après que ceux qui ont sensiblement influé sur le projet de loi.

1.1.3.1 Adoption de l'ordonnance concernant la protection des informations et mandat d'étude du Conseil fédéral

Au milieu de l'année 2007, le Conseil fédéral a adopté la nouvelle ordonnance concernant la protection des informations (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. Pour la première fois, les prescriptions qu'elle contient quant à la classification et au traitement des informations ont permis d'instaurer un niveau de protection uniforme dans l'ensemble de l'administration fédérale. Le troisième échelon de classification INTERNE introduit par l'ordonnance a, en outre, permis de traiter plus aisément une grande partie des informations classifiées. Pour la même raison, elle a également permis de simplifier la coopération internationale, notamment avec l'UE.

L'OPrI a été conçue comme un acte normatif transitoire et sa durée de validité est par conséquent 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 le coût de la mise en œuvre de l'ordonnance, et de lui présenter des propositions visant la création de bases légales formelles.

1.1.3.2 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 décidé les 16 décembre 2009 et 4 juin 2010 de mesures visant à améliorer la sécurité de l'information dans l'administration fédérale, en définissant 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. De plus, il a proposé au Contrôle fédéral des finances (CDF) d'examiner l'état d'avancement de la mise en application de ces mesures. Le premier rapport d'audit du CDF a été porté à la connaissance des membres du Conseil fédéral le 2 décembre 2011[1].

1.1.3.3 Mandat du Conseil fédéral visant la création de bases légales formelles pour la protection des informations ou pour la sécurité de l'information

Le rapport demandé par le Conseil fédéral parallèlement à l'adoption de l'OPrI, qui devait rendre compte de l'exécution et de l'efficacité de l'ordonnance en question, a montré que le délai transitoire (fin 2009) qu'elle prévoyait pour les adaptations techniques permettant de garantir la protection des informations n'avait généralement pas été respecté. Des lacunes importantes ont été constatées, notamment en ce qui concerne la protection électronique d'informations classifiées.

Le 12 mai 2010, après avoir pris connaissance du rapport du DDPS et suite à l'attaque contre le DFAE évoquée ci-dessus, le Conseil fédéral a chargé le DDPS d'élaborer des bases légales formelles pour la protection des informations de la Confédération. La nouvelle réglementation devait notamment:

- élargir le champ d'application de la réglementation de la protection des informations à toutes les personnes chargées par la Confédération de traiter des informations protégées;
- créer des bases légales formelles uniformes pour des procédures de protection du secret auprès des entreprises 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.

De plus, le Conseil fédéral a chargé le DDPS, dans le cadre de l'élaboration du projet, d'examiner si et dans quelle mesure les bases légales formelles devaient être étendues à d'autres problèmes matériels dans le domaine de la protection des informations, et si les compétences et responsabilités en matière de sécurité de l'information satisfaisaient aux exigences actuelles.

1.1.3.4 Décision du Conseil fédéral relative à la recommandation 12 de la Commission de gestion du Conseil des Etats (CdG-E) en rapport avec la crise libyenne

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 du 3 décembre 2010, 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 recommandait 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*»[2].

Le Conseil fédéral a pris par la suite des mesures destinées à pallier les lacunes identifiées sur les plans organisationnel et technique[3].

---

1 www.efk.admin.ch/images/stories/efk_dokumente/publikationen/querschnittspruefungen/QP%20%2816%29/11387BE_Publikation.pdf

2 Rapport de la Commission de gestion du Conseil des Etats du 3 décembre 2010 sur la gestion par les autorités fédérales de la crise diplomatique entre la Suisse et la Libye, FF **2011** 3901**,** p. 3990.

3 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 : avis du Conseil fédéral du 20 avril 2011, FF **2011** 4059, pp. 4079s.

1.1.3.5 Compléments au mandat du Conseil fédéral

Le 14 janvier 2011, le chef du DDPS a institué un groupe d'experts interdépartemental dirigé par Markus Müller, docteur en droit et professeur ordinaire de droit public et de droit administratif à l'Université de Berne. Il l'a chargé d'élaborer une esquisse d'acte normatif et, sur la base de ce dernier, un avant-projet de loi à soumettre en consultation. Le groupe d'experts a proposé son esquisse d'acte normatif au chef du DDPS le 29 juin 2011, et ce dernier a informé les membres du Conseil fédéral des résultats des travaux du groupe d'experts. Par décision du 30 novembre 2011, le Conseil fédéral a élargi le futur domaine réglementaire de la protection des informations au sens strict à la sécurité de l'information. Il a par ailleurs chargé le DDPS de coordonner les travaux législatifs avec les mandats relatifs à l'élaboration d'une stratégie de cyber-défense et à la stratégie pour une société de l'information en Suisse.

L'extension du domaine réglementaire et la coordination exigée avec les projets cités a nécessité un élargissement du groupe d'experts qui regroupait nouvellement des représentants de la ChF, du DFAE, du DFJP (SG, OFJ, fedpol), du DDPS (SG, Etat-major de l'armée), du DFF (SG, UPIC, OFIT), du DETEC (OFCOM), du PFPDT, des Services du Parlement, des tribunaux fédéraux et des cantons (CSI). Le SRC a participé ponctuellement aux travaux.

1.1.3.6 Mandat du Conseil fédéral visant l'harmonisation et la restriction des contrôles de sécurité relatifs aux personnes

Le 1er février 2012, le Conseil fédéral a chargé le DDPS d'examiner les moyens d'harmoniser et de restreindre les fonctions concernées par les CSP, d'étudier les degrés de contrôle y afférents et d'identifier d'autres mesures d'optimisation avec impact sur les ressources. Après avoir pris connaissance du rapport établi par le GTI CSP institué pour l'occasion, le Conseil fédéral a notamment, le 29 novembre 2013, chargé le GTI LSI de tenir compte dans ses travaux des recommandations du rapport et de les intégrer de façon appropriée au projet de loi (cf. ch. 1.2.4).

1.1.3.7 Mandat complémentaire et élargissement à un groupe de travail interdépartemental (GTI LSI)

Après que l'on eut été informé d'un incident au SRC, le Conseil fédéral a confié le 24 octobre 2012 un mandat complémentaire au groupe d'experts demandant un rapport sur les menaces et les lacunes en matière de sécurité de l'information au sein de l'administration fédérale et des propositions de mesures urgentes. Le groupe d'experts a encore été complété, devenant un groupe de travail interdépartemental (GTI) en accueillant des représentants du DFI et du DEFR.

Le GTI LSI a remis son rapport au DDPS le 29 janvier 2013, y compris ses recommandations. Le Conseil fédéral a décidé le 15 mars 2013 d'une formation à l'intention de l'ensemble des cadres dirigeants de l'administration fédérale, et confié la responsabilité de cette tâche à l'Office fédéral du personnel (OFPER).

1.2 Points essentiels de la nouvelle réglementation proposée

Les besoins en matière de réglementation et les solutions proposées au sujet des points essentiels de la nouvelle législation sont commentés ci-après. Les dispositions concernant la nouvelle organisation de la sécurité de l'information seront commentées séparément (cf. ch. 1.3).

Deux remarques liminaires s'imposent:

- le besoin de réglementer ressort des lacunes et faiblesses matérielles et juridiques en matière de sécurité de l'information. La focalisation sur les lacunes pourrait donner l'impression que l'ensemble des prescriptions, processus et mesures antérieurs n'était pas pertinent: ce n'est pas le cas;
- les rapports détaillés sur les lacunes et les faiblesses en matière de sécurité de l'information sont généralement classifiés: de ce fait, il n'est pas possible d'entrer dans tous les détails des lacunes et faiblesses dans le cadre du présent rapport.

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. Le traitement électronique d'informations de toute sorte présente aujourd'hui d'importantes lacunes en matière de sécurité.

1.2.1.1 Lacunes techniques

Dans un rapport sur l'exécution, l'efficacité et la rentabilité de l'ordonnance concernant la protection des informations de la Confédération (cf. ch. 1.1.3.3), le DDPS a montré au Conseil fédéral que les ambitions de l'ordonnance, plutôt modestes en comparaison internationale en matière de traitement électronique des in-

formations classifiées, ne pouvaient généralement être respectées du fait que des solutions et services de sécurité nécessaires font aujourd'hui défaut, ou qu'ils ne sont pas utilisés ou offerts pour diverses raisons, notamment financières. Il en résulte une situation un peu absurde, dans laquelle des membres du personnel de la Confédération qui, dans le privé, n'utiliseraient jamais les services bancaires en ligne si ceux-ci ne répondaient pas aux exigences actuelles de sécurité technique, n'hésitent parfois pas à conserver ou à transmettre dans leur environnement de travail des informations classifiées CONFIDENTIEL voire SECRET sans prendre la peine de les crypter.

Ce constat ne concerne pas seulement des informations classifiées, qui ne représentent aujourd'hui qu'une petite fraction de toutes les informations de la Confédération dignes de protection. Des lacunes semblables existent en matière de protection des données personnelles, du secret professionnel, des secrets d'affaires et de fabrication et d'autres informations dont la confidentialité, la disponibilité, l'intégrité ou la traçabilité doivent être protégées. En cas de besoin élevé de protection des informations, des mesures techniques de sécurité particulières doivent être prises. Toutefois, ces mesures de sécurité particulières requièrent la mise en place préalable d'une protection de base forte, sans laquelle les mesures techniques particulières pourront plus facilement être contournées. Or, des contrôles de l'OFIT montrent que les mesures minimales de la protection de base sont souvent appliquées de façon lacunaire.

Dans ce contexte de lacunes importantes en matière de protection électronique des informations, il faut toutefois 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 des ressources financières et humaines insuffisantes.

1.2.1.2 Lacunes organisationnelles

Eu égard aux défis techniques, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) avait déjà préconisé 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»[4].

Cette affirmation est capitale pour la compréhension de la nouvelle réglementation proposée. La seule sécurité technique des TIC ne suffit plus: une protection plus efficace des informations requiert des mesures organisationnelles. A la Confédération, les lacunes dans ce domaine concernent en particulier la gestion de la sécurité de l'information et les bases légales.

Dans le secteur privé, on prend conscience du fait que la sécurité est une affaire de dirigeants et qu'elle est économiquement rentable au plus tard après qu'un dommage ait eu lieu et que l'on se soit efforcé de limiter les dégâts. 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 TIC, 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 aussi dans le domaine de la protection des informations de la Confédération. Par exemple, la sécurité des TIC est souvent considérée comme une affaire purement technique et non pas comme une tâche de direction. Ainsi, la ligne ne prête généralement qu'une attention minime à son 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 de 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 la rentabilité des mesures (analyse coût/utilité). Enfin, en cas d'incident ou de violation des prescriptions, les responsables ne sont que rarement sommés de rendre des comptes.

Les conditions cadres juridiques présentent aussi des lacunes. Au niveau de la Confédération, les bases légales de la protection des informations sont très sectorielles, peu harmonisées et souvent lacunaires. C'est ainsi que la Confédération exploite aujourd'hui, 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 contrôles de sécurité relatifs aux personnes

4 MELANI, Rapport semestriel 2008/I, http://www.melani.admin.ch/dokumentation/00123/00124/01065/index.html?lang=fr

(cf. ch. 1.2.4) et les procédures de sécurité relatives aux entreprises (cf. ch. 1.2.5) sont principalement applicables aux personnes et entreprises traitant des informations classifiées de la Confédération, mais non aux personnes gérant ou exploitant des moyens TIC critiques.

De plus, les bases légales ne sont pas toujours adaptées aux besoins concrets du traitement électronique des données. Quelques exemples:

- les secrets d'affaires et de fabrication sont principalement protégés par une obligation de garder le secret (secret de fonction) imposée aux personnes qui doivent les traiter. Dans une société de l'information, le maintien du secret de fonction exige toutefois davantage qu'une simple obligation personnelle. Lorsque des secrets d'affaires ou de fabrication sont saisis par voie électronique, des moyens techniques et organisationnels doivent les protéger en fonction de leur besoin de protection effectif. Des prescriptions sur la manière de concevoir, de mettre en œuvre et de vérifier cette protection font généralement défaut;
- en revanche, pour ce qui est de la protection des données personnelles, la réglementation est particulièrement dense. En ce qui concerne les autorités fédérales, l'accent est mis davantage sur l'existence des bases légales nécessaires au traitement régulier des données, conformément au but recherché et dans le respect du principe de proportionnalité, que sur le traitement concret de ces informations par le personnel de la Confédération (notamment quant à leur transmission, leur conservation, leur destruction, leur cryptage, etc.);
- enfin, les prescriptions concernant la protection des informations classifiées recèlent de nombreuses contradictions quant aux exigences informatiques, notamment pour ce qui de la réglementation des compétences et de certaines procédures.

Des informations peuvent avoir un besoin de 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 sécurité. Pour ce faire, la ligne doit mieux assumer ses tâches; par ailleurs, les bases légales doivent impérativement s'aligner sur les besoins du traitement électronique.

1.2.1.3 Vers une sécurité intégrale des informations

Le Conseil fédéral est conscient de l'interdépendance croissante de la protection organisationnelle des informations et de la sécurité informatique technique, de même que des lacunes organisationnelles évoquées plus haut. Dans le sens d'une mesure urgente, il a ordonné une formation des cadres de l'administration fédérale en matière de sécurité de l'information (cf. ch. 1.1.3.7). Lors d'une discussion du 30 novembre 2011, il a de plus déclaré que la limitation du champ d'application matériel du présent projet de loi à la seule protection des informations classifiées ne saurait répondre au besoin de réglementation identifié. Il a par conséquent chargé le DDPS de réorienter les travaux législatifs: le but visé est dès lors une *sécurité de l'information intégrale*, tenant compte des exigences tant organisationnelles que techniques de sécurité; de plus, la nouvelle réglementation doit, sur le plan de l'organisation, s'inspirer de *normes internationales reconnues*.

Cette réorientation vers une sécurité intégrale de l'information correspond à ce qui a déjà cours en tant que standard dans le secteur privé et dans de nombreuses administrations publiques dans le monde. Elle est formalisée par quelques normes internationales, notamment les normes ISO/IEC 27001/27002. 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 sécurité de l'information et sur les mesures organisationnelles qui s'imposent à cette fin. Toutefois, les normes contiennent également de *bonnes pratiques* de sécurité applicables et éprouvées quant à la technique, au personnel ou aux constructions.

Le présent projet crée des bases légales formelles uniformes pour la gestion de la sécurité de l'information de la Confédération. Quant à sa structure et à son contenu, il se fonde pour l'essentiel sur les normes évoquées et prévoit 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 réunis, pilotés, mis en œuvre, analysés et améliorés en un tout. Par conséquent, le projet regroupe en une seule réglementation les mesures organisationnelles les plus importantes pour protéger *toutes* les informations et pour assurer la sécurité dans l'engagement des TIC. Par rapport aux structures juridiques et organisationnelles actuelles de la Confédération, très sectorielles, la sécurité de l'information prend une orientation intégrale.

1.2.2 Champ d'application

1.2.2.1 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. La loi vaut

pour des informations de toute nature (par ex. non seulement pour les informations textuelles, mais également graphiques), quelle que soit leur forme, c'est-à-dire outre les informations électroniques, celles portées par des supports physiques (documents papier). Il s'agit principalement d'informations que les autorités produisent elles-mêmes, mais sont également concernées celles que ces autorités obtiennent de tiers et dont le traitement régulier relève de leur compétence. De plus, sont incluses dans le champ d'application les données que les autorités fédérales confient pour traitement à des tiers. Une limitation aux seules informations sensibles serait peu judicieuse: déterminer si une information est sensible ou digne de protection présuppose des critères et des mécanismes d'appréciation qui doivent *nécessairement s'appliquer à toutes les informations*.

Le projet couvre tous les moyens TIC 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 dont ils servent au traitement ou des processus d'affaires qu'ils étayent. Toutefois, la pratique considérant les moyens TIC comme des *objets de protection*, la LSI les mentionne expressément.

1.2.2.2 Champ d'application institutionnel

Par maints aspects, le présent acte est une loi d'organisation, qui doit être appliquée, dans leur domaine de compétence respectif, par toutes les autorités fédérales et toutes les organisations qui leur sont subordonnées: c'est en effet la seule façon d'assurer une sécurité efficace de l'information. D'autres organisations de droit public ou de droit privé doivent également tomber sous le coup de la loi dans la mesure où elles exercent une activité sensible pour le compte de la Confédération: cela correspond au mandat du Conseil fédéral d'étendre 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 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. Parmi ces dernières, on trouve également des informations classifiées ou d'autres informations dignes de protection. Les autorités fédérales ne se sont toutefois pas dotées d'un système de classification unique. Les mesures prises par les diverses autorités pour protéger ces informations sont de plus très hétérogènes et guère harmonisées. Par conséquent, il est par exemple souvent arrivé que des informations classifiées de l'administration fédérale remises à d'autres autorités fédérales soient traitées d'une manière contrevenant à d'importantes prescriptions de sécurité du Conseil fédéral. 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.

De plus, la mise en réseau des systèmes informatiques des autorités fédérales se poursuit sans discontinuer. L'un des objectifs du Conseil fédéral est de favoriser et de renforcer l'échange électronique d'informations et les services électroniques (cyberadministration). 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 participantes. Il est donc indispensable que toutes les autorités fédérales concernées appliquent les mêmes critères et méthodes d'évaluation des risques, et qu'elles harmonisent leurs mesures de sécurité dans l'utilisation des TIC, sur les plans organisationnel, technique et physique comme dans le domaine du personnel.

Le champ d'application institutionnel ne doit toutefois pas limiter l'indépendance constitutionnelle des autorités concernées, raison pour laquelle elles exécuteront la loi en toute autonomie. On renonce à un organe de pilotage transversal habilité à donner des instructions. L'exécution en toute autonomie présente un inconvénient: toutes les exigences minimales de la sécurité de l'information devant être satisfaites par toutes les autorités de la Confédération doivent nécessairement figurer dans la loi: dès lors, le projet comporte de nombreuses dispositions qui, si l'on se tenait à la hiérarchie normative, relèveraient davantage du niveau de l'ordonnance.

1.2.3 Mesures générales de sécurité de l'information

1.2.3.1 Gestion de la sécurité de l'information

La sécurité de l'information est de la responsabilité des dirigeants: la direction de l'autorité concernée en porte la responsabilité et ne peut la déléguer. Le projet précise donc certaines obligations spécifiques, qui imposent par exemple aux plus hautes autorités:

- d'édicter les dispositions portant exécution de la loi (cf. art. 87);

- d'organiser, de mettre en œuvre et de contrôler la sécurité de l'information en fonction de l'avancement des connaissances et de la technologie (par ex. conformément à la norme ISO 27001), ce qui implique la définition claire des tâches, des compétences et des responsabilités (cf. art 5, al. 1, let. a, et al. 2);
- de déterminer leurs objectifs quant à la sécurité de l'information et le niveau de sécurité à atteindre (cf. art. 5, al. 3, let. a);
- de fixer les principes pour le traitement des risques (cf. art. 5, al. 3, let. b);
- de déterminer les conséquences en cas de violation des prescriptions (cf. art. 5, al. 3, let. c);
- d'ordonner la vérification périodique de la mise en œuvre et de l'efficacité des mesures (cf. art. 11);
- d'établir une liste des fonctions soumises à un contrôle de sécurité relatif aux personnes (art. 33).

Enfin, le projet renforce le rôle opérationnel de la ligne dans le recours aux TIC (cf. art. 23 à 26).

1.2.3.2 Gestion des risques

Les dangers et menaces pour les informations et les moyens TIC sont devenus plus complexes avec l'évolution vers une société de l'information. 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 des mesures de réduction des risques. Ces deux éléments font aujourd'hui largement défaut, raison pour laquelle on a lancé un processus visant une sécurité durable et rationnelle des informations.

Pour les autorités fédérales, la gestion des risques est une tâche aussi bien politique qu'économique. Le projet appelle les autorités concernées à définir le niveau qu'ils veulent atteindre en matière de sécurité de l'information (objectifs quant à la sécurité de l'information). Ce niveau est déterminant pour la conception des mesures de sécurité et pour l'évaluation de leur efficacité. Dans leur approche des risques, les autorités concernées doivent par ailleurs définir qui est habilité à assumer tel risque et ce qu'il advient lorsque les risques résiduels sont trop importants.

La gestion des risques évoquée est spécifique au domaine de la sécurité de l'information. Elle doit toutefois être intégrée au processus général de gestion des risques de toutes les autorités concernées, car les risques liés à la sécurité de l'information font évidemment partie de l'ensemble des risques d'affaires.

Le besoin de protection des informations (quant à leur confidentialité, leur intégrité, leur disponibilité et leur traçabilité) est évalué dans le cadre de la gestion des risques. Les dangers que recèlent des personnes, la technique ou des événements naturels sont analysés, tout comme les faiblesses correspondantes. L'évaluation des risques doit être aussi objective et systématique que possible. La ligne doit décider des mesures visant à assurer le niveau de sécurité déterminant. Enfin, les risques identifiés doivent être placés sous surveillance.

La continuité opérationnelle («*business continuity management*», ou BCM) est intimement liée à la gestion des risques. Elle doit garantir que les autorités soient en mesure d'assumer leurs tâches essentielles même en situation extraordinaire. En raison de la dépendance grandissante de l'accomplissement des tâches vis-à-vis des TIC, les risques en matière de sécurité de l'information sont susceptibles de mettre en péril des tâches légales critiques de la Confédération (cf. également art. 6, al. 3, LOGA). Par conséquent, les autorités fédérales sont appelées à élaborer des planifications préventives et à mener les exercices y afférents dans la perspective d'incidents en matière de sécurité de l'information risquant d'empêcher l'accomplissement de tâches indispensables.

1.2.3.3 Contrôles et audits

Chaque mesure ordonnée en matière de sécurité de l'information doit pouvoir être contrôlable et doit être contrôlée. Seuls des contrôles 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. Le contrôle constitue aujourd'hui l'un des points faibles majeurs en matière de sécurité de l'information de la Confédération: il ne s'exerce que ponctuellement, voire uniquement à la suite d'un incident. En l'absence presque totale de contrôles, le savoir-faire et les ressources nécessaires font largement défaut. Il faut dès lors s'attendre à ce que les autorités et organisations concernées ne puissent éviter d'engager des ressources supplémentaires pour assumer cette tâche.

Les instruments et mécanismes de contrôle doivent impérativement être renforcés dans tous les domaines de la sécurité de l'information. C'est pourquoi le projet prévoit une obligation de contrôle générale (art. 11). Lorsque des contrôles, des audits ou des examens ciblés sont nécessaires, ils sont expressément exigés (en ce qui concerne les TIC, cf. ch. 1.2.3.5). Au quotidien, la responsabilité des contrôles et des audits incombe par

principe à la ligne. Le contrôle de l'application des mesures ordonnées est du ressort de la direction. Le projet renforce par ailleurs les instruments dont dispose la ligne en matière de contrôles et d'audits. Ainsi, les préposés à la sécurité de l'information doivent pouvoir, sur mandat de leur autorité, procéder à des contrôles. Pour ce qui est des audits plus complexes ou des contrôles indépendants, les autorités doivent pouvoir les confier au service spécialisé de la Confédération en matière de sécurité de l'information prévu par le projet ou au CDF.

1.2.3.4 Classification des informations

La classification des informations est une mesure de protection appliquée de longue date pour protéger les informations propre à une organisation, dont la prise de connaissance par des personnes non autorisées peut nuire aux buts de l'organisation ou causer un préjudice à cette dernière. La classification n'est aujourd'hui réglée par l'OPrI que pour l'administration fédérale et l'armée. L'un des objectifs du présent projet est la mise sur pied d'un système de classification transversal, c'est-à-dire valable pour toutes les autorités fédérales, fondé sur des critères uniformes. Il est aussi tenu compte des attentes de la population quant à la transparence de l'action des autorités fédérales. La classification doit donc être conçue comme une exception fondée. Les valeurs seuils de la classification sont par ailleurs en partie relevées par rapport à la situation actuelle.

Le système à trois échelons assure une protection des informations adaptée au risque: les charges et coûts des mesures de sécurité augmentent en fonction du risque pour les intérêts publics méritant protection. L'échelon INTERNE permet de traiter simplement et à moindre coût des informations certes dignes de protection, mais qui ne sauraient justifier les charges occasionnées par le traitement des informations classifiées CONFIDENTIEL. L'une des raisons principales pour le système à trois échelons est d'assurer la compatibilité avec les systèmes de classification usuels au plan international, notamment avec le système de l'Union européenne, et partant, de garantir un niveau de sécurité uniforme. La plupart des Etats utilisent un système à quatre échelons (pour l'UE par ex. RESTRICTED, CONFIDENTIAL, SECRET et TOP SECRET).

1.2.3.5 Sécurité dans l'engagement des TIC

Actuellement, les dispositions régissant la sécurité en matière de TIC se retrouvent soit au niveau de l'ordonnance, soit, dans la plupart des cas, au niveau des directives. Depuis quelques années, la sécurité relative aux moyens TIC 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. Certains incidents, survenus dans le monde et en Suisse, ont montré la vulnérabilité des moyens TIC et ses conséquences potentielles. On ne peut se dispenser aujourd'hui d'inscrire au niveau formel de la loi certaines valeurs de référence en matière de sécurité des TIC, notamment dans la perspective de la mise en réseau croissante des moyens TIC des autorités et de la multiplication des échanges électroniques d'informations: des solutions et processus applicables à toutes les autorités s'imposent donc. En raison de la rapidité des évolutions technologiques, la plupart des mesures concrètes de sécurité devront encore être définies et consignées au niveau de l'ordonnance, voire à celui des directives.

Les rapports évoquant en détail des lacunes et des faiblesses dans le domaine des TIC sont généralement classifiés. Le premier rapport de révision du CDF après la décision du Conseil fédéral du 16 décembre 2009 relative à des mesures de renforcement de la sécurité de l'information au sein de l'administration fédérale donne une bonne vue d'ensemble des actions à entreprendre dans l'utilisation des TIC, malgré le champ d'étude restreint de l'audit (cf. ch. 1.1.3.2).

La sécurité de l'information dans l'engagement des TIC est souvent considérée comme une affaire technique, ce qui n'est vrai que dans une faible mesure: la majorité des mesures de sécurité en relation avec les TIC sont en effet de nature organisationnelle. Les autorités et organisations décidant de l'engagement de TIC (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'interventions.

La réglementation proposée se fonde sur des processus et des procédures en place, qu'il convient d'adapter aux besoins identifiés. Au-delà du renforcement de la gestion des risques (cf. ch. 1.2.3.2), il s'agit essentiellement:

- *de répartir clairement les compétences et responsabilités entre les bénéficiaires de prestations TIC et les fournisseurs de ces mêmes prestations.* La responsabilité principale en matière de sécurité dans l'engagement des TIC incombe aux bénéficiaires de prestations. Ils sont compétents pour l'exécution de la procédure de sécurité. En revanche, les fournisseurs de prestations sont tenus de garantir la sécurité lors de

l'exploitation des moyens TIC. 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;

- *d'évaluer la criticité des moyens TIC utilisés en rapport avec les informations qu'ils sont appelés à traiter et avec l'accomplissement des tâches de l'autorité ou de l'organisation concernée (détermination de la catégorie de sécurité).* La détermination de la catégorie de sécurité d'un moyen TIC sert d'une part à faire prendre conscience aux autorités de la criticité de leurs informations et moyens TIC et leur permettre par la suite de mettre l'accent sur leurs valeurs critiques lorsqu'elles décideront des mesures de sécurité. D'autre part, des exigences et mesures minimales standard de sécurité devront être définies pour chaque catégorie et appliquées avant la mise en exploitation du moyen TIC;
- *de renforcer le rôle opérationnel de la direction de l'autorité ou organisation concernée*. La direction de l'autorité ou de l'organisation doit être associée à la procédure de sécurité. Elle doit être informée précocement des risques et être en mesure de prendre les mesures en conséquence. C'est pourquoi le projet prévoit que tous les moyens TIC qui seront utilisés doivent être autorisés à l'exploitation par l'autorité ou l'organisation *sous l'angle de la sécurité*. Pour autant que, en raison de la criticité d'un moyen TIC, un concept de sécurité de l'information s'impose, ce dernier doit être approuvé par l'autorité ou l'organisation;
- *de renforcer les contrôles et les examens*. Abstraction faite des contrôles généraux (art. 11), le projet prévoit trois autres types de contrôles en matière de TIC:
  - *contrôle de conformité*. Pour chaque moyen TIC qui sera engagé, il faut s'assurer que la procédure de sécurité a été menée conformément au droit et que les mesures de sécurité prévues ont bien été appliquées. Il s'agit donc ici d'un contrôle de qualité;
  - *examen du concept de sécurité de l'information*. Les préposés à la sécurité de l'information examineront tous les concepts de sécurité de l'information avant qu'ils ne soient soumis à la direction pour approbation;
  - *contrôle d'efficacité pour les moyens TIC les plus critiques*. Avant toute autorisation de mise en service d'un moyen TIC de la catégorie de sécurité la plus élevée («protection très élevée»), il convient d'examiner l'efficacité réelle des mesures prises. Seuls des auditeurs qualifiés et certifiés entrent en ligne de compte pour de tels audits. Le contrôle d'efficacité est la seule mesure susceptible de renseigner sur l'état réel de la sécurité de l'information.

1.2.3.6 Mesures concernant le personnel

Les membres du personnel et les tiers chargés de traiter des informations de la Confédération sont responsables du respect des prescriptions régissant l'utilisation des informations et des moyens TIC. Pour ce faire, une formation appropriée s'impose. À cet égard, le besoin est considérable.

Un autre élément important de la sécurité de l'information est la délivrance restrictive d'autorisations. Selon ce principe, les autorités et organisations concernées veillent à ne délivrer que les autorisations de traiter des informations, d'utiliser des moyens TIC et d'accéder aux locaux dont les personnes concernées ont effectivement besoin pour l'accomplissement de leurs tâches. De plus, les autorisations doivent être revues périodiquement. Cette règle, qui vise en particulier à réduire le risque d'une malveillance interne, n'est pas appliquée partout.

Le projet définit par conséquent ces deux principes (formation et délivrance restrictive d'autorisations) comme exigences minimales vis-à-vis du personnel. Les autorités et organisations concernées devront édicter des prescriptions détaillées dans le cadre de l'exécution.

1.2.3.7 Protection physique d'informations et de moyens TIC

On oublie trop souvent l'importance que revêtent les contrôles à l'entrée et d'autres mesures physiques de protection pour la sécurité de l'information. Le projet fixe à cet égard les exigences minimales.

Il crée également une base légale permettant d'établir des zones dites « de sécurité ». Il s'agit de locaux et de 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 TIC des catégories de sécurité «protection élevée» ou «protection très élevée». Ces zones de sécurité sont usuelles dans le contexte international, mais peu répandues au sein de la Confédération. La délimitation de zones de sécurité n'est pas une mesure obligatoire et fait l'objet d'une disposition potestative. Leur mise en place nécessite une base légale formelle parce ces zones peuvent être liées à des mesures qui constituent une intervention relativement lourde dans les droits individuels (par ex. le recours à des méthodes d'identification biométriques ou la surveillance vidéo permanente). Un contrôle de sécurité relatif aux personnes peut également être une condition de l'accès à des

zones de sécurité. Dans la pratique, ces zones concernent principalement des locaux abritant des serveurs ou encore des lieux de commandement ou des chambres-fortes.

1.2.4 Contrôles de sécurité relatifs aux personnes

L'une des menaces les plus critiques et les plus graves se présente lorsque des personnes qui ont accès à des informations classifiées aux échelons supérieurs ou qui gèrent ou exploitent des moyens TIC particulièrement critiques se rendent coupables de trahison ou de sabotage, ou tentent de déstabiliser les institutions de l'Etat. Les fonctions sensibles ne doivent par conséquent être confiées qu'à des personnes présentant toutes les garanties qu'elles n'abuseront pas de la confiance placée en elles. Ce n'est pas le cas lorsque des indices donnent à penser que la personne pourrait être victime de chantage ou de corruption. L'expérience montre que souvent, ces deux risques sont liés à des facteurs conjoncturels qui peuvent être, par exemple des difficultés personnelles ou financières. Un contrôle de sécurité relatif aux personnes (CSP) peut attirer l'attention des supérieurs hiérarchiques sur des risques en rapport avec les antécédents ou l'environnement de la personne contrôlée (cf. également le message du 7 mars 1994 concernant la LMSI ainsi que l'initiative populaire «S. o. S. - pour une Suisse sans police fouineuse», FF 1994 **II** 1123).

Le CSP est une mesure de prévention destinée à protéger des malveillances internes. Elle vise à *identifier* le risque d'une atteinte volontaire ou par négligence à d'importants intérêts publics lorsque une personne donnée exerce une activité sensible. L'autorité ou l'organisation compétente pour la décision d'engagement de la personne concernée porte seule la responsabilité de décider si elle prend un risque accru, si elle veut assortir l'engagement de charges supplémentaires pour réduire le risque ou si, pour éviter ou supprimer le risque, elle entend renoncer à l'engagement ou licencier. Même une évaluation positive du risque de sécurité par les services compétents en matière de contrôles de sécurité relatifs aux personnes (services spécialisés CSP) 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 revêtir une fonction clé.

1.2.4.1 Transfert de la réglementation de la LMSI à la loi sur la sécurité de l'information

Les bases légales formelles du contrôle de sécurité relatif aux personnes se trouvent actuellement dans deux lois, dont la LMSI pour la Confédération. La LENu quant à elle prévoit à son art. 24 des contrôles de fiabilité pour le personnel des exploitants de centrales nucléaires. Le Conseil fédéral a institué deux services spécialisés CSP: l'un est rattaché au DDPS et est compétent pour la majorité des contrôles. Le second est administrativement rattaché à la ChF et contrôle les cadres supérieurs de l'administration, de même que le personnel de l'autre service spécialisé CSP.

La future loi sur le service de renseignement 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 *exclusivement* à la protection des informations (cf. art. 19, al. 1, LMSI), il est judicieux de transférer ces dispositions dans la présente loi. L'opportunité d'élaborer une loi séparée pour les CSP (et pour les procédures de sécurité relatives aux entreprises; cf. ch. 1.2.5) a également été examinée, mais cette variante a été rejetée parce qu'elle ne répondait pas à l'objectif de regrouper dans un même acte toutes les mesures de sécurité de l'information.

1.2.4.2 Suppression de lacunes juridiques

Le transfert dans le présent projet des bases légales formelles du contrôle de sécurité relatif aux personnes permettra de combler certaines lacunes du droit en vigueur. Le CSP représente une intervention marquée dans les droits individuels de la personne qui doit être contrôlée. Le principe constitutionnel de la légalité exige pour de telles interventions une base légale formelle et détaillée. La réglementation proposée est à cet égard bien plus précise que la LMSI. Elle répond également aux attentes du Parlement quant à une définition légale formelle des critères d'évaluation du risque (cf. art. 42).

Bien que la réglementation de la LMSI relative aux CSP réponde exclusivement aux besoins de protection des informations, les motifs justifiant un CSP ont été étendus *contra legem* dans l'OCSP. On propose dès lors d'énumérer exhaustivement dans la future loi sur la sécurité de l'information les motifs de contrôle et de limiter ces derniers aux besoins directs de la sécurité de l'information. Ces motifs, définis de façon restrictive, sont réunis sous l'expression générique «*activité sensible*», par laquelle il faut entendre:

- le traitement d'informations des échelons CONFIDENTIEL ou SECRET ainsi que la manipulation de matériel classifié à ces échelons;

- l'administration, l'exploitation, la maintenance ou la vérification de moyens TIC des catégories de sécurité «protection élevée» ou «protection très élevée»;
- l'accès aux zones de sécurité, en particulier les zones de protection 2 ou 3 d'une installation au sens de la législation sur la protection des ouvrages militaires.

Certains motifs de contrôle sont ainsi biffés sans remplacement. Il s'agit notamment de l'accès régulier à des données personnelles 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.

Dans la mesure où, pour des raisons de sécurité, un contrôle est nécessaire pour d'autres activités que celles de la présente loi, les motifs devront figurer dans la législation spéciale. Pour que l'on puisse distinguer clairement les CSP au sens de la loi sur la sécurité de l'information des contrôles prévus par d'autres actes, une autre terminologie devrait être utilisée pour les seconds: «*contrôles de fiabilité*». C'est pourquoi l'annexe au présent projet propose une modification de la LPers et de la LAAM. Ainsi, des personnes qui représentent régulièrement la Suisse à l'étranger, ou qui ont des compétences décisionnelles ou des tâches de surveillance dans d'importants dossiers financiers, pourront faire l'objet d'un contrôle de fiabilité.

Les opinions divergeaient quant à la question de savoir si, pour inscrire une fonction dans la liste des employés à contrôler, le critère de l'exercice unique d'une activité sensible suffisait ou s'il convenait de s'en tenir au principe de la *régularité* prévu par le système en vigueur (cf. art. 19, al. 1, LMSI). Le critère de la régularité repose, entre autres, sur l'appréciation du Service de renseignement de la Confédération qui, en matière de protection de l'Etat, juge le risque particulièrement élevé lorsque des collaboratrices et 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 ou 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 découlerait alors non seulement de la régularité de l'accès, mais encore du contenu de l'information. D'autre part, la notion de «*régularité*» n'est guère univoque et a déjà mené, sous le droit en vigueur, à des interprétations divergentes.

Les conditions matérielles de l'inscription d'une fonction dans la liste, et partant d'un contrôle de sécurité relatif aux personnes, diffèrent quelque peu entre le projet et le système actuel. Du point de vue légal formel, il convient de renoncer au critère de la régularité, notamment en ce qui concerne le traitement d'informations classifiées. 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 TIC des catégories de sécurité «protection élevée» ou «protection très élevée», ou *doit* pouvoir accéder à des zones de sécurité. Lorsqu'une telle activité est *indispensable* à l'accomplissement des tâches liées à la fonction, alors - mais alors seulement - la fonction doit figurer dans la liste des fonctions à contrôler. Ce principe correspond à ceux de la délivrance restrictive d'autorisations (art. 29) et du «*need to know*» (besoin de savoir), qui s'appliquent au traitement d'informations classifiées (art. 15, al. 1).

En outre, la réglementation en vigueur a été notamment modifiée sur les points suivants:

- *nature juridique de la déclaration à établir:* l'art. 22 OCSP dispose qu'à l'issue du CSP, les services spécialisés CSP rendent une décision au sens de l'art. 5 PA. L'évaluation du risque pour la sécurité par les services spécialisés CSP ne correspond toutefois pas à la définition légale d'une décision, car du *point de vue juridique*, elle n'a aucune influence directe sur les droits et obligations de la personne concernée, ni sur son statut. Le service appelé à confier l'activité sensible n'est en effet pas lié par la décision du service spécialisé CSP compétent (cf. art. 46) et la personne contrôlée n'a aucun droit à être engagée, ni à se voir confier une fonction donnée ou un mandat. Les évaluations des services spécialisés CSP sont donc, sous l'angle juridique, des actes matériels au sens de l'art. 25*a* PA (en ce qui concerne les voies de recours, cf. art. 51);
- *déclaration de sécurité assortie de réserves au lieu de conditions:* en présence d'un risque conditionnel pour la sécurité, que l'on peut suffisamment réduire par certaines mesures ou conditions, les services spécialisés CSP établissent une déclaration assorties de réserves (et non plus de conditions). Elles ne décident pas elles-mêmes des conditions, se bornant à les recommander. La nouvelle formulation montre d'une part que les services spécialisés CSP émettent des réserves quant à la déclaration de sécurité. D'autre part,

elle précise que les réserves n'ont qu'un caractère de recommandation pour l'autorité ou l'organisation appelée à confier l'activité ou la fonction sensible: il incombe à ses dernières de définir des conditions en conséquence;

- *suppression de l'interdiction de recueillir des données sur l'exercice des droits constitutionnels (art. 20, al. 1, LMSI):* bien que le sens et le but de cette disposition soient clairs et appropriés, cette interdiction n'est pas applicable. Toute personne dispose par exemple du droit constitutionnel de se marier. Lors de la récolte des données, on se procure évidemment des informations sur l'état-civil, ce qui serait en soi interdit en vertu de la disposition citée de la LMSI. La réglementation en vigueur veut simplement éviter qu'une personne soit exclue du point de vue de la sécurité pour ses opinions politiques. C'est pourquoi le projet prévoit que dorénavant, le risque pour la sécurité devra toujours être motivé par des faits concrets liés à la personne contrôlée. Des positions d'extrême-gauche ou d'extrême-droite, et d'autres opinions politiques ou visions du monde ne peuvent dès lors justifier l'hypothèse d'un risque pour la sécurité aussi longtemps que la personne concernée n'aura pas commis d'acte répréhensible *à cet égard* (cf. art. 42);
- *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 encore par le droit suisse que les informations classifiées SECRET. Pour accéder à ces dernières, un CSP élargi au sens de l'art. 11 OCSP est requis. Mais la Confédération ne connaît pas d'échelon de classification «TRÈS SECRET», pour lequel un contrôle au sens de l'art. 12 OCSP serait nécessaire. Dans le sens d'une adaptation du droit en vigueur au système de classification de la LSI et d'une simplification des modalités de contrôle, la présente loi ramène 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 (cf. art. 39).

La contestation a également porté sur le système actuel d'établissement d'une liste de fonctions par une norme de droit, qui 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 de fonctions. Pour des raisons de sécurité également, elles posent problème: les listes donnent en effet une image complète de toutes les fonctions des autorités comportant des activités sensibles. Leur publication permet 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 concernées, de sorte que l'on évite une multiplication sauvage des contrôles. Avant d'adopter les dispositions d'exécution, le Conseil fédéral pourra encore déterminer si la publication sans limites des listes est adéquate.

Dans le cadre de la révision, on s'est de plus demandé si les services spécialisés CSP devaient automatiquement être informées de toute nouvelle mention au casier judiciaire ou dans une autre banque de données pertinente pour le CSP au sujet de la personne contrôlée. Techniquement, cette information automatique serait parfaitement réalisable, après adaptation des bases légales. Elle pourrait améliorer notablement la sécurité dans la mesure où l'on pourrait très rapidement prendre conscience de nouveaux risques pour la sécurité. Mais pour autant, une annonce automatique aux services spécialisés CSP ne signifierait pas que cette dernière doive informer l'autorité requérante ou le service chargé de confier l'activité sensible pour qu'un nouveau contrôle ait lieu. Le rôle du CSP changerait en effet fondamentalement en ce qu'il imposerait en quelque sorte une surveillance permanente de la personne contrôlée. Pour cette raison, on a renoncé à régler l'information automatique des services spécialisés CSP.

1.2.4.3 Restriction et harmonisation des CSP

Lors de l'établissement de la première liste de personnes à contrôler en vertu de l'ordonnance du 15 avril 1992 concernant les contrôles de sécurité dans l'administration fédérale, le Conseil fédéral a décidé pour des considérations politiques de n'y faire figurer qu'un nombre restreint de fonctions. Il a retenu un ordre de grandeur de quelque 1'200 fonctions (cf. le message LMSI). Toutefois, depuis l'entrée en vigueur de la LMSI en 1998, le nombre de personnes contrôlées n'a cessé d'augmenter, et en 2012, plus de 75'000 contrôles ont eu lieu, dont 60'000 CSP de conscrits et de militaires, ce chiffre incluant le nouveau contrôle 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.

Le projet de loi prévoit plusieurs mesures qui devraient globalement réduire le nombre des CSP à mener:

- les activités requérant un contrôle seront mieux définies que dans la LMSI. Les motifs de contrôle seront réduits aux stricts besoins de la sécurité de l'information;
- le passage à deux degrés de contrôle au lieu de trois devrait également avoir pour conséquence que le contrôle élargi ne s'appliquera plus qu'aux personnes traitant effectivement des informations classifiées SECRET ou exerçant des activités d'une sensibilité correspondante. En 2012, plus de 28'000 contrôles élargis ont été menés, ce qui voudrait dire que plus de 28'000 personnes ont accès à des informations classifiées SECRET, un chiffre totalement invraisemblable. Le nombre des CSP de ce degré devrait par conséquent nettement diminuer;
- les tâches de contrôle des préposés à la sécurité de l'information (cf. art. 84) incluent également la vérification de la légalité de l'inscription d'une fonction dans la liste des fonctions à contrôler.

Le relèvement des valeurs seuils applicables aux CSP qu'entraîneront les mesures évoquées aura pour conséquence que certains besoins de sécurité ne seront plus couverts par les CSP. Pour éviter un vide en matière de sécurité, il faudra mettre à la disposition des employeurs d'autres moyens plus proportionnés pour répondre à leurs besoins légitimes de sécurité: ils devront ainsi être autorisés à exiger des candidates et candidats et des membres de leur personnel des extraits du casier judiciaire et du registre des poursuites pour autant que la préservation de leurs intérêts d'employeur l'exige. Une révision de la LPers est proposée à cette fin (cf. art. 20*a* LPers).

1.2.5 Procédure de sécurité relative aux entreprises

La procédure de sécurité relative aux entreprises (PSE; 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 à des tiers (ci-après «entreprises») non soumis à une surveillance directe. Dans de nombreux domaines matériels, les autorités confient à l'économie privée des mandats liés à des activités sensibles. Pour préserver les intérêts publics au sens de l'art. 1, al. 2, même hors du strict champ d'application de la loi, les mandataires en question feront l'objet d'une PSE. La procédure vise d'une part à vérifier si l'entreprise susceptible de bénéficier du mandat est digne de confiance, et d'autre part à permettre le contrôle et l'application des mesures nécessaires à la sauvegarde de 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 mandant.

La PSE est adéquate et usuelle dans le contexte international (cf. par ex. l'art. 11 de la décision du Conseil du 31 mars 2011 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'UE[5] ou la section VII des Règlements de l'Agence spatiale européenne du 15 décembre 2011[6]). Elle est appliquée en Suisse depuis la fin des années 1970 aux mandats de la Confédération à contenu militaire classifié, sur la base de l'O sur la sauvegarde du secret. Le champ d'application matériel restreint de cette dernière ne permet actuellement d'y recourir que pour les mandats militaires classifiés. Le Conseil fédéral déplore depuis longtemps déjà l'absence d'une PSE uniforme, c'est-à-dire également applicable aux mandats du 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'Etats tiers, ou la participation à certains projets scientifiques. La compétitivité de l'économie suisse s'en trouve ainsi préjudiciée.

Esquissée à grands traits, la procédure se présente de la manière suivante: le mandant (adjudicateur) propose au service chargé de la procédure de sécurité auprès des entreprises (service spécialisé PSE) d'ouvrir une PSE. Après l'ouverture de la procédure, le service spécialisé PSE, en accord avec l'adjudicateur, définit tout d'abord les exigences de sécurité, puis il 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 Etats ou sous leur influence, et le cas échéant si cette dépendance ou cette influence est compatible avec la sécurité de l'information de la Confédération. L'adjudicateur attribue par la suite le mandat à une entreprise qualifiée du point de vue de la sécurité. Le service spécialisé PSE définit alors dans un concept de sécurité la façon dont l'adjudicataire doit satisfaire aux exigences de la 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'adjudicataire. Puis, lorsque les déclarations de sécurité 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.)

5 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32011D0292:FR:HTML
6 http://esamultimedia.esa.int/docs/eso/esa-reg-004f.pdf

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 habilitée à inspecter l'entreprise à l'improviste et à prendre d'autres mesures. Le Conseil fédéral réglera les détails de la PSE au niveau de l'ordonnance.

Pour partie, la réglementation proposée est en relation étroite avec le CSP, mais elle s'en distingue sur des aspects importants de la procédure:

- en principe, il s'agit dans les deux cas de vérifier la fiabilité de l'entreprise. Selon le résultat de l'évaluation, une DSE est établie, qui confirme que l'entreprise est digne de confiance et qui lui permet en tant que mandataire d'exercer des activités sensibles de la Confédération (ou d'autorités étrangères). Il ne s'agit toutefois pas seulement d'examiner l'entreprise, mais encore de définir les mesures de sécurité liées au mandat qu'il convient d'appliquer au sein de l'entreprise;
- contrairement au CSP, la procédure applicable aux entreprises ne se termine pas simplement par une DSE: le respect des mesures imposées peut en effet être vérifié en tout temps.

1.2.6 Sécurité de l'information pour les infrastructures critiques (IC)

Par décision du 30 novembre 2011, le Conseil fédéral a chargé le DDPS d'intégrer si nécessaire à la présente loi les besoins légaux formels de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC). Dans la SNPC, le Conseil fédéral a retenu le principe de la réglementation décentralisée des IC (cf. ch. 1.1.2.2). L'examen des besoins réglementaires légaux formels pour assurer l'exécution décentralisée de la SNPC incombe ainsi aux départements qui, dans l'accomplissement de leurs tâches, disposent de compétences réglementaires vis-à-vis d'exploitants d'IC (par ex. le DETEC pour les secteurs des infrastructures de communication et d'approvisionnement en énergie). Si l'on identifie un besoin sectoriel d'agir au plan légal formel, la législation spéciale concernée doit être adaptée.

Mais il existe aussi certaines tâches supra-sectorielles qui, notamment pour des raisons d'efficacité et de coût, ne peuvent être assumées de manière décentralisée. Il s'agit en premier lieu du soutien aux diverses IC par l'échange d'informations quant aux 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'IC souhaitent expressément disposer d'un interlocuteur unique auprès de la Confédération (sous la forme de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI). De plus, on a pu constater que le partenariat public-privé mis en place dans le cadre de MELANI est très performant, notamment en raison de son accès aux informations du Service de renseignement de la Confédération. Outre les informations fournies par MELANI, on apprécie particulièrement que les fournisseurs de renseignements échangés sur des incidents restent maîtres de leurs informations, que la collaboration repose sur une base volontaire et que l'on ait pour principe de favoriser la sécurité de l'information et la gestion des risques par des informations, éventuellement des recommandations, plutôt que par des directives contraignantes.

Cette tâche supra-sectorielle de la Confédération au profit des IC doit être prévue dans la présente loi transversale, dans la mesure où une base légale formelle s'impose. Ainsi, le projet énumère les tâches essentielles de MELANI. Dans l'accomplissement de ces tâches, MELANI doit régulièrement traiter des données personnelles, y compris (quoique rarement) des données personnelles sensibles. Le projet de loi crée les bases légales formelles pour ce faire.

1.2.7 Exécution

1.2.7.1 Exécution par les autorités de la Confédération

La réglementation de l'exécution de la présente loi doit relever le défi d'une application uniforme des dispositions et du respect généralisé des prescriptions. Si une exécution uniforme devait se révéler impossible (notamment en ce qui concerne le traitement des informations classifiées ou l'engagement des moyens TIC), cela se traduirait immanquablement par des lacunes de sécurité dans l'échange d'informations entre les autorités. L'autonomie des autorités concernées (Parlement, Conseil fédéral, tribunaux fédéraux, Ministère public de la Confédération, Banque nationale) en matière d'organisation et d'exécution doit 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 transversales d'une seule autorité (par exemple le Conseil fédéral).

L'avant-projet prend en compte ces exigences en soi contradictoires en prévoyant:

- *une réglementation d'exécution selon le principe du « opting out »:* chaque autorité exécute la loi dans son domaine de compétence et édicte les ordonnances y afférentes. Les dispositions d'exécution du Con-

seil fédéral s'appliqueront toutefois par analogie aux autres autorités de la Confédération dans la mesure où elles n'auront pas édicté leur propre réglementation;

- *des exigences et mesures standards:* le Conseil fédéral doit être habilité à définir des exigences et mesures de sécurité standards conformes à l'avancée des connaissances et de la technologie, qui vaudront recommandations pour les autres autorités fédérales. Elles ne touchent pas des problèmes organisationnels de fond, mais des processus, moyens et prestations subordonnés (par ex. détermination des besoins de protection des informations, méthodes d'évaluation des risques, cryptage, exigences quant aux supports d'informations, 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 doit pouvoir déléguer la définition de ces exigences et mesures à des organes spécialisés;
- *la création d'un organe de coordination transversal spécialisé (au niveau des autorités):* les préposés à la sécurité de l'information, chargés de piloter la mise en œuvre de la loi, auront de par leur statut des connaissances approfondies de la situation et des problèmes en matière de sécurité de l'information dans leurs domaines de compétence, notamment à propos de l'applicabilité et de l'efficacité des prescriptions et des 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 aura pour vocation principale l'exécution uniforme de la loi au niveau transversal sur la base des risques. Elle devra également être associée à la définition des exigences et mesures de sécurité standard.

La solution proposée préservera l'indépendance des autorités de la Confédération dans l'exécution. Cette dernière se fera de manière décentralisée. Le niveau de sécurité uniforme recherché sera atteint par une doctrine unique, par l'élaboration de mesures standards et par un soutien et un conseil professionnels assurés par des organes spécialisés. Pour ce qui est des inconvénients de la solution sous l'angle de la technique législative, on se référera au ch. 1.2.2.2).

1.2.7.2 Exécution par l'administration fédérale et par d'autres organisations concernées

Le projet de loi règle surtout le cadre transversal (au niveau des autorités). L'exécution par l'administration fédérale et d'autres organisations chargées de tâches administratives au sens de l'art. 2, al. 4, LOGA ressortit à la compétence du Conseil fédéral. Sous réserve du respect des exigences matérielles et organisationnelles de la loi, son autonomie en matière d'exécution n'est guère restreinte. Le projet prévoit néanmoins deux limitations de cette autonomie:

- à l'instar de toutes les autres autorités de la Confédération, le Conseil fédéral doit, dans son domaine de compétence, organiser, mettre en œuvre et contrôler la sécurité de l'information en fonction de l'avancée des connaissances et de la technologie (cf. art. 5, al. 1);
- le Conseil fédéral, les départements et la Chancellerie fédérale doivent désigner, dans leurs domaines de compétence, un préposé à la sécurité de l'information et une suppléance (cf. ch. 1.3.2 et art. 84).

Le projet ne contient pas d'autres prescriptions quant à l'exécution par l'administration fédérale ou au droit subordonné correspondant. La loi laisse ici une grande marge d'action au Conseil fédéral. Par exemple, ce dernier peut concéder une plus grande autonomie d'exécution aux organisations décentralisées ou à des organisations au sens de l'art. 2, al. 4, LOGA. A cet égard, il pourra aussi décider s'il entend s'en tenir à l'exécution majoritairement décentralisée d'aujourd'hui ou s'il veut centraliser certaines compétences et responsabilités.

1.2.8 Renonciation à réglementer certains domaines

L'examen des possibilités et de l'opportunité d'introduire une réglementation légale dans les domaines ci-après a montré qu'une réglementation par la loi sur la sécurité de l'information dépasserait à divers titres le cadre matériel qui est le sien et ne serait guère acceptée. On renonce par conséquent à présenter les propositions de réglementation correspondantes.

1.2.8.1 Dispositions pénales

On a certes pu constater que les dispositions du CP et du CPM relatives à la protection du secret de fonction et à celle des informations de la Confédération et des cantons classifiées ou dignes de protection étaient peu cohérentes et méritaient d'être révisées de plusieurs points de vue. Il s'agit toutefois d'une matière fondamentale du droit pénal, qu'une loi d'organisation ne peut réviser à titre accessoire: il convient donc d'envisager une révision autonome du CP. Le Conseil fédéral attribuera en temps voulu un mandat à ce propos.

1.2.8.2 Limitations de l'accès à des informations classifiées en raison de la nationalité

Les premiers avant-projets du groupe d'experts prévoyaient de réserver, en principe, l'accès aux informations de la Confédération classifiées SECRET aux seuls citoyens et citoyennes suisses. Les personnes possédant la nationalité d'un Etat avec lequel la Suisse a conclu un accord de protection des informations auraient toutefois exceptionnellement pu y avoir accès. Il faut renoncer à limiter, sur mandat du Conseil fédéral, l'accès de ressortissants étrangers à des informations de la Confédération classifiées SECRET.

1.2.8.3 Restitution d'informations protégées de la Confédération tombées en mains de particuliers

On a examiné si, pour une mise en œuvre rapide de la protection de l'information, les supports d'informations contenant des informations protégées tombés en mains de tiers sans l'assentiment de l'autorité compétente devaient pouvoir être mis en sûreté par une décision directe de l'autorité concernée. De la sorte, les autorités fédérales concernées auraient pu décider la restitution ou la destruction des supports d'informations en question, dans le cadre du droit de la procédure administrative (c'est-à-dire sans procédure civile ou pénale préalable). Comme il faut s'attendre à ce qu'une disposition de cette nature génère de nombreux conflits, notamment sous l'angle de la liberté de la presse, et rencontre une forte opposition politique, on a renoncé à une réglementation en ce sens.

1.2.8.4 Mise en péril de la sécurité par la diffusion d'informations par des particuliers

Outre les faits constitutifs d'infraction au sens strict, les autorités ne disposent actuellement d'aucune base légale explicite qui leur permette d'empêcher la diffusion par des particuliers d'informations susceptibles de mettre gravement en danger la collectivité et l'Etat. On songe à cet égard plus particulièrement aux plans d'assemblage de certaines armes, à des données de laboratoire, à des plans d'infrastructures, etc. On a donc étudié la possibilité de conférer une compétence aux services fédéraux concernés leur permettant, dans le cas d'espèce, d'interdire de telles publications dans le cadre de la procédure administrative, ou d'imposer aux détenteurs de ces informations des mesures de sécurité au sens de la loi (classification des informations, contrôle de sécurité relatif aux personnes ou procédure de sécurité relative aux entreprises). Une réglementation de cette nature constituerait toutefois une atteinte considérable aux droits fondamentaux des tiers concernés et susciterait certainement une farouche opposition politique.

1.2.8.5 Intégration de réglementations en vigueur dans le domaine de la protection des objets

En soi, personne ne conteste que la sécurité de l'information (y compris la protection des moyens TIC) et les contrôles de sécurité relatifs aux personnes sont étroitement liés à la protection des objets, c'est-à-dire à la protection des bâtiments et installations de la Confédération. Cette matière est actuellement couverte par diverses dispositions légales, de diverses façons et sous diverses formes (cf. dans le domaine militaire la loi sur la protection des ouvrages, dans le domaine civil les art. 22 à 24 LMSI, 62 ss LOGA, 69 LParl et 25*a* LTF). L'analyse a montré qu'une certaine harmonisation de ces dispositions ou la création d'une base légale homogène serait certes souhaitable, mais la portée matérielle et organisationnelle d'une telle réglementation dépasserait le cadre du présent projet. Le projet contient toutefois deux dispositions sur la protection physique d'informations et de moyens TIC. Ainsi, les compétences actuelles en matière de protection des objets ne sont pas remises en question.

1.3 Organisation de la sécurité informatique de la Confédération

Par sa décision du 12 mai 2010, le Conseil fédéral a chargé le DDPS d'examiner lors de l'élaboration du projet si et dans quelle mesure les compétences et les responsabilités en matière de sécurité de l'information répondaient aux exigences actuelles. De plus, il s'agissait notamment de s'interroger sur l'opportunité de réunir les divers organes interdépartementaux œuvrant dans ce domaine. Ce mandat ne concerne 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 (des autorités).

1.3.1 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 sécurité de l'information 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 classifiées, protection des données, sécurité informatique, protection des objets et gestion des risques). On trouvera ci-après une analyse détaillée des trois domaines explicitement mentionnés par le Conseil fédéral (protection des informations, protection des données et sécurité informatique) sous l'angle des compétences et des responsabilités.

1.3.1.1 Organisation de la protection des informations

Au sein de l'administration fédérale, la protection des informations est pour l'essentiel réglée dans l'ordonnance concernant la protection des informations (OPrI). Des règles supplémentaires figurent dans les accords internationaux dits de protection des informations (cf. également le commentaire de l'art. 90). 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).

- *Conférence des secrétaires généraux (CSG):* en vertu des art. 8 et 18 OPrI, la CSG a la compétence d'édicter des prescriptions de détail (catalogue de classification et directives de traitement) dans le domaine de la protection des informations. 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 lors de l'engagement de moyens TIC.
- *Préposés à la protection des informations:* aux termes de l'art. 19 OPrI, tous les départements et la Chancellerie fédérale doivent désigner un ou une préposé(e) à la protection des informations. Ces personnes veillent à la mise en œuvre de la protection des informations dans leur domaine de compétences. Bien que l'OPrI ne l'impose pas, tous les départements ont désigné des «conseillers en protection des informations» au niveau des unités administratives;
- *Comité de coordination pour la protection des informations au sein de la Confédération (KOAISchB):* la coordination interdépartementale est assurée par le KOAISchB (art. 20 OPrI). Cet organe veille à une application homogène de la protection des informations au niveau de la Confédération, élabore les prescriptions à l'intention de la CSG et fait rapport tous les deux ans à cette dernière. Il coordonne ses activités avec le Comité pour la sécurité informatique (C-SI) de l'UPIC.
- *Organe de coordination pour la protection des informations au sein de la Confédération (KISchB):* en vertu de l'art. 20*a* OPrI, le KOAISchB et les préposés à la protection des informations bénéficient du soutien du KISchB, rattaché administrativement à la protection des informations et des objets (PIO) au sein du DDPS. L'organe de coordination élabore les moyens didactiques nécessaires et joue le rôle d'interlocuteur pour les contacts avec des services nationaux, étrangers et internationaux œuvrant dans le domaine de la protection des informations. Il peut également mener les inspections de sécurité prévues par des conventions de droit international public, et d'autres contrôles en accord avec les départements et la Chancellerie fédérale.

1.3.1.2 Organisation de la protection des données

Les bases légales du traitement des données personnelles sont fournies par les lois spéciales y afférentes. En revanche, l'organisation de la protection des données au sein de la Confédération est réglée dans son principe 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 intervient de manière décentralisée, mais elle est toutefois coordonnée de façon centrale par le Préposé à la protection des données et à la transparence (PFPDT) et par le groupe Protection des données, un organe informel non habilité à donner des instructions.

- *Préposé fédéral à la protection des données et à la transparence (PFPDT):* la LPD a institué la fonction du PFPDT dans le but de conseiller et de surveiller les particuliers et les organes de la Confédération quant au respect des dispositions régissant la protection des données. Le PFPDT surveille le respect de la LPD et des autres dispositions fédérales par les organes de la Confédération. Il relève sur le plan administratif de la ChF.
- *Conseillers à la protection des données:* aux termes de l'art. 23 OLPD, la Chancellerie fédérale et les départements doivent chacun désigner au moins un conseiller à la protection des données. Ces conseillers assistent les organes responsables et les utilisateurs, promeuvent l'information et la formation des collaboratrices et collaborateurs, et participent à l'exécution des dispositions relatives à la protection des données. La communication entre les organes fédéraux et le PFPDT passe par les conseillers. La plupart des unités administratives ont également désigné, à leur niveau, un conseiller à la protection des données.
- *Groupe Protection des données:* la législation sur la protection des données ne prévoit aucun organe chargé de la coordination supradépartementale de la protection des données au sein de la Confédération. C'est la raison pour laquelle un groupe informel Protection des données a été créé, présidé par le conseiller à la protection des données de la Chancellerie fédérale. En font partie tous les conseillers à la protection des données des départements, une représentation du PFPDT et une autre des services du Parlement. En particulier, le groupe s'assure d'une exécution uniforme et coordonnée des dispositions de la protec-

tion des données au sein de la Confédération, soumet au PFPDT des problèmes liés à la pratique et veille à l'organisation de sessions de formation.

1.3.1.3 Organisation spécialisée de la sécurité informatique

Pour l'essentiel, l'organisation de la sécurité informatique est réglée dans l'ordonnance sur l'informatique dans l'administration fédérale (OIAF), mais de nombreux autres actes normatifs ont une incidence sur les compétences et les responsabilités en la matière (OPrI, accords internationaux de protection des informations, OLPD, O-GEVER, etc.). La sécurité informatique est exécutée de manière décentralisée. Les départements et la Chancellerie fédérale 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) et accompagnée par un organe consultatif (C-SI).

- *Conseil fédéral:* le Conseil fédéral joue un rôle stratégique en matière de sécurité des TIC. Une part substantielle des tâches qu'il exerce dans ce domaine se fonde sur sa responsabilité dans le domaine général des TIC au sens de l'art. 14 OIAF: il définit la stratégie de la Confédération en matière de TIC, surveille la mise en œuvre de la stratégie de la Confédération en matière de TIC et prend des mesures si nécessaire, définit les services standard TIC, édicte des instructions sur la sécurité en matière de TIC et autorise les dérogations à ses directives.
- *UPIC:* dans les domaines de la sécurité des TIC, l'UPIC statue en vertu de l'art. 17 OIAF sur les propositions des départements, de la Chancellerie fédérale et des unités administratives concernant des 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 de mesures de sécurité spécifiques aux TIC. Elle peut enquêter en qualité d'expert et sur mandat d'un département ou de la Chancellerie fédérale, sur des événements supposés ou avérés en rapport avec la sécurité. Elle désigne le délégué à la sécurité informatique de la Confédération. Elle dirige la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) en collaboration avec le service de renseignement de la Confédération. Enfin, elle préside l'organe consultatif qu'est le Comité de la sécurité informatique.
- *Délégués à la sécurité informatique:* en vue de l'exécution décentralisée, les départements et la Chancellerie fédérale désignent chacun un délégué à la sécurité informatique (art. 19, al. 1, OIAF). Les délégués coordonnent tous les aspects de la sécurité informatique au sein de leur département et avec les organes supradépartementaux. Les unités administratives sont également tenues de désigner des délégués à la sécurité informatique, chargés de coordonner tous les aspects de la sécurité informatique au sein de leur unité et avec les organes départementaux.
- *Comité de la sécurité informatique (C-SI):* le C-SI est l'organe consultatif de l'UPIC pour toutes les questions de sécurité relatives aux TIC (art. 19 OIAF). Il contribue également à la coordination supradépartementale. Il regroupe les délégués à la sécurité informatique des départements et de la Chancellerie fédérale. Le Contrôle fédéral des finances (CDF), le PFPDT et les Services du Parlement peuvent chacun y nommer un représentant avec voix consultative.
- *Conseil informatique de la Confédération (CI):* le Conseil informatique de la Confédération (CI) est l'organe consultatif de l'UPIC pour les affaires relatives aux TIC (y compris leur sécurité) nécessitant l'accord des départements et de la Chancellerie fédérale, notamment pour l'édiction de prescriptions et l'approbation de dérogations à leur application. Il regroupe le délégué au pilotage des TIC et un représentant nommément désigné de chaque département et de la Chancellerie fédérale. Un représentant de l'Administration fédérale des finances (AFF), du PFPDT, des fournisseurs de prestations internes et des Services du Parlement peut y participer avec voix consultative.
- *Contrôle fédéral des finances (CDF):* depuis le 1er janvier 2012, le CDF assure la révision de l'informatique au sein de l'administration fédérale (art. 28 OIAF).

Outre cette organisation de base, de nombreux autres organes ou services se préoccupent également de la sécurité informatique au sein de la Confédération. On ne citera ci-après que ceux assumant des compétences et des responsabilités spécifiques importantes pour la sécurité des TIC des autorités fédérales, en faisant abstraction de ceux relevant des domaines du renseignement, du droit pénal ou d'autres secteurs.

- *Protection des informations et des objets (PIO):* la PIO, rattachée au Groupement Défense, est compétente pour les prescriptions de sécurité du DDPS et de l'armée en matière de TIC et vérifie leur application. A cet égard, elle assume, pour l'armée et en partie le DDPS, des tâches très semblables à celles de l'UPIC.

- *Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI):* MELANI a été définitivement instituée par le Conseil fédéral en 2004 et chargée de la protection des infrastructures d'information critiques en Suisse. La coopération, dirigée par l'UPIC (art. 17, al. 1, let. i, OIAF), entre le DFF, le DDPS et les milieux économiques privés aux fins de la protection des infrastructures d'information critiques se fonde sur le modèle du partenariat public-privé. Il s'agit d'une collaboration étroite entre l'administration et des entreprises privées des divers secteurs économiques, qui œuvrent dans le contexte de la sécurité des systèmes informatiques et d'Internet, de même que dans le domaine de la protection des infrastructures critiques suisses.
- *Etat-major pour la sûreté de l'information (SONIA):* SONIA se réunit lors de crises déclenchées par des dérangements dans l'infrastructure d'information et de communication. Il regroupe des décideurs de l'administration, des cantons et de l'économie (infrastructures critiques) et est dirigé par le délégué au pilotage informatique de la Confédération. MELANI assure la permanence de SONIA.
- *Computer Security Incident Response Team (CSIRT):* cet organe, abrité par le DFF/OFIT, veille à la sécurité du réseau civil de la Confédération par le biais de la surveillance, de la prévention et de l'intervention. Il travaille en étroite collaboration avec d'autres partenaires de la Confédération tels MELANI ou fedpol. Ses tâches principales sont les suivantes: observer les menaces actuelles et analyser les fichiers journaux; élaborer des recommandations visant à minimiser les risques, à circonscrire rapidement les dommages consécutifs à des incidents en matière de sécurité des TIC et à protéger les données confiées à l'OFIT (protection opérationnelle des infrastructures TIC centrales de la Confédération).
- *Computer Emergency Response Team (MilCERT):* le MilCERT est l'homologue du CSIRT pour la sécurité des réseaux du DDPS et de l'armée. Au sein de la Base d'Aide au Commandement (BAC), il est intégré au Centre des opérations électroniques (COE) et peut enquêter en tant qu'unité indépendante sur des incidents relatifs à la sécurité survenant au sein du DDPS et de l'armée.
- *Sécurité de l'information et cryptologie (SI crypt):* le domaine SI crypt est également rattaché à la BAC/COE. Ses cryptologues s'assurent de la sécurité des communications de l'armée, du DDPS et d'autres unités de l'administration fédérale en évaluant et en développant eux-mêmes des procédures et des systèmes de cryptage. Ses activités s'étendent de l'évaluation de systèmes cryptologiques de base à l'analyse de fonctions cryptologiques spécifiques, ce qui nécessite des connaissances approfondies de la recherche actuelle en matière de cryptologie.
- *Armasuisse, Sciences et technologies (S+T):* le domaine Informatique et cyberespace de la S+T procède à des analyses de risques, à des vérifications de sécurité et à des audits en matière de sécurité organisationnelle et technique de l'information. Les services S+T sont de plus en plus souvent sollicités par les services civils de l'administration fédérale, notamment pour vérifier l'efficacité des concepts de sécurité et les répercussions réelles des mesures de sécurité, et pour procéder à des tests techniques de vérification et de pénétration. Dans ce domaine, S+T assure également un suivi des développements technologiques et de l'évolution de la menace.

1.3.1.4 Comparaison des compétences et des responsabilités

Les trois organisations spécialisées précitées, qui assument toutes des tâches partielles en matière de sécurité de l'information, n'ont qu'un cahier des charges limité. Dans les trois domaines concernés, les départements et la Chancellerie fédérale sont responsables de l'application des prescriptions. De plus, tous les domaines présentent fondamentalement la même structure organisationnelle:

- un organe chargé d'édicter les prescriptions;
- des préposés au niveau des départements/de la Chancellerie fédérale et des unités administratives, et
- un organe supradépartemental de coordination.

Dans leur domaine de spécialisation, les détenteurs des diverses fonctions assument fondamentalement les mêmes tâches. Les seules exceptions significatives sont les organes chargés d'édicter les prescriptions, dont les pouvoirs divergent pour partie sensiblement.

Le tableau ci-dessous donne un aperçu de cette situation. Il inclut les deux autres domaines connexes à la sécurité de l'information, à savoir la sécurité des objets et la gestion des risques.

	Prescriptions	Dép. / ChF	Unité administrative	Coordination
Protection des informations	CSG	Préposés à la protection des informations	Préposés ou conseillers à la protection des informations	KOAISchB/KISchB
Protection des données	PFPDT	Conseillers à la protection des données	Conseillers à la protection des données	Groupe Protection des données
Sécurité TIC	CF / UPIC	Délégués à la sécurité informatique	Délégués à la sécurité informatique	UPIC-Sec / C-SI
Sécurité des objets	fedpol / SFS	Préposés à la sécurité	Préposés à la sécurité	Comité de coordination de la sécurité
Gestion des risques	CF / CSG	Gestionnaires des risques	Responsables de la gestion des risques	Organe de coordination AFF

1.3.1.5 Lacunes organisationnelles

L'organisation actuelle présente de nombreuses lacunes et de nombreux points faibles:

- *Les compétences des divers domaines ne sont pas toujours clairement définies et les intersections entre les secteurs spécialisés de la sécurité de l'information ne bénéficient pas d'une attention suffisante.*

  Le manque de clarté en matière de compétences se constate à tous les niveaux. Lorsque des données personnelles sensibles ou des informations classifiées à partir du niveau CONFIDENTIEL doivent être traitées de manière électronique, l'élaboration d'un concept de sécurité de l'information et de protection des données est requis. S'agit-il d'une question de protection des données, de protection des informations ou de sécurité en matière de TIC, et qui est compétent pour l'évaluation correcte du besoin de protection des informations et le contrôle de l'application des mesures prévues? La protection des câbles d'un réseau informatique relève-t-elle de la sécurité informatique ou de la protection des objets? La destruction des documents concerne-t-elle la protection des informations, la protection des données ou la sécurité physique, et qui définit les exigences correspondantes ? Qui est compétent pour leur mise en œuvre? Une clé USB est-elle un support d'informations au sens de l'OPrI ou un moyen TIC au sens de l'OIAF?

  Les problèmes évoqués peuvent également avoir des répercussions directes au plan international. En raison du manque de clarté en matière de compétences et de responsabilités au sein de l'administration fédérale, il n'a par exemple jamais été possible de trouver une solution au problème de la transmission électronique d'informations classifiées avec l'UE. Ainsi, même les informations du plus faible échelon de classification de l'UE sont-elles aujourd'hui encore échangées exclusivement sur support papier. Des problèmes semblables se posent dans la coopération avec l'Agence spatiale européenne (ASE): dans ce cas, la question de savoir qui est compétent pour la sécurité des communications (COMSEC[7]) n'a pas encore trouvé de réponse. Or, cette question a une importance considérable pour le succès de la participation d'institutions et entreprises suisses aux activités de l'ASE. On attend encore une solution.

  Les domaines spécialisés sont également tenus de prendre des mesures de sensibilisation et de formation. Malgré leurs contenus semblables, les mesures de sensibilisation et de formation des divers services ne sont souvent pas coordonnées.

- *Trop d'acteurs ne disposent que de connaissances spécialisées insuffisantes ou de trop peu de ressources en personnel. Pour partie, les ressources existantes sont mal utilisées, et la masse critique n'est atteinte nulle part.*

  Les cahiers des charges des préposés des divers domaines évoqués contiennent généralement d'autres tâches que celles liées à la sécurité de l'information. Ils ne peuvent réserver qu'une faible part de leur temps de travail aux tâches de sécurité de l'information, qui constituent alors une sorte d'activité accessoire. Ils ne disposent dès lors souvent pas ou plus des connaissances spécialisées requises, ce qui a un effet direct important sur la sécurité. Dans les domaines de la protection des informations et de la protection des données, les tâches sont assumées principalement par des juristes qui ne sont généralement que peu familiarisés avec les besoins de la sécurité informatique. Ils tendent, par conséquent, à aborder les problèmes sous le seul angle juridique et ne sont souvent pas en mesure d'accompagner ou de surveiller la mise en œuvre des exigences de sécurité dans des projets TIC. La situation est inverse en ce qui concerne

[7] On entend par *COMSEC* la sécurité des communications au sens de l'application de mesures de sécurité destinées à empêcher des tiers non autorisés à se procurer des informations de valeur en accédant aux télécommunications et en les exploitant, ou encore pour garantir l'authenticité, la confidentialité et l'intégrité des télécommunications.

les spécialistes de la sécurité informatique: leurs connaissances en matière de protection des informations et de protection des données sont souvent lacunaires.

Ce constat vaut également pour les services spécialisés: presque tous sont sous-dotés en personnel au regard des tâches confiées. Là encore, la masse critique n'est jamais atteinte. De plus, pour partie, leurs connaissances spécialisées dans les autres domaines sont insuffisantes. Par ailleurs, et notamment dans le domaine de la sécurité informatique, on trouve de nombreux services chargés de tâches complémentaires à celles des autres services. Ces tâches et services ne sont toutefois pas coordonnés, voire ne sont pas sollicités du tout (par ex. les services des cryptologues du DDPS).

Les spécialistes de la sécurité de l'information, que ce soit dans le domaine technique ou dans celui de la gestion, sont à l'heure actuelle plus demandés que jamais. La Confédération dispose de tels spécialistes, mais nombre d'entre eux n'assument pas à plein temps leurs tâches liées à la sécurité de l'information. On doit dès lors se demander si ces ressources rares sont vraiment engagées à bon escient.

- *Les pouvoirs des divers acteurs sont souvent insuffisants.*

  Un constat particulièrement inquiétant est que la mise en œuvre des mesures décidées en matière de sécurité de l'information n'est que très rarement vérifiée. En règle générale, ni les services spécialisés ni les préposés ne sont habilités à mener des contrôles. Or, sans contrôle, il est impossible de déterminer l'efficacité des mesures ou l'existence de lacunes et de points faibles.

- *La conscience du besoin en sécurité est lacunaire.*

  Les départements et la Chancellerie fédérale accordent une importance très variable aux thèmes de la sécurité de l'information. Pourtant, l'engagement des cadres, et notamment de la direction, est essentiel pour la sensibilisation des collaboratrices et collaborateurs.

1.3.1.6 Appréciation de la situation et conséquences

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 et dynamisé les menaces qui pèsent sur l'information et les moyens TIC. Il est nécessaire d'affronter ces dangers de manière intégrale et coordonnée, 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 aspects suivants sont importants pour améliorer l'organisation:

- la responsabilité de la mise en œuvre des prescriptions doit rester auprès de la ligne, et cette dernière doit être conseillée et assistée de manière plus compétente à tous les niveaux;
- la future organisation de la sécurité de l'information devra davantage se concentrer sur la détection précoce et la gestion des risques. La condition *sine qua non* en est non seulement une gestion systématique des risques dans le domaine de la sécurité de l'information, qui fait aujourd'hui largement défaut, mais également un meilleur contrôle de l'application des mesures destinées à réduire les risques;
- les divers organes spécialisés doivent être regroupés dans la mesure du possible, afin de pouvoir exploiter les synergies et les économies d'échelle. Cela doit également permettre de régler les problèmes de compétences sur le plan systémique et de renforcer le savoir interdisciplinaire. Un regroupement complet est toutefois impossible: il faut donc d'une part définir plus clairement les compétences et les responsabilités respectives, et d'autre part renforcer la coordination et l'échange de connaissances;
- pour ce qui est des divers préposés, leurs compétences peuvent être renforcées par une professionnalisation plus marquée. Le professionnalisme pourrait être amélioré si l'on concentrait les diverses tâches de gestion de la sécurité de l'information auprès d'un petit nombre de personnes;
- la séparation et l'attribution des fonctions méritent une attention particulière. Les préposés ne devraient pas être rattachés à un domaine spécialisé dont ils doivent évaluer les risques de manière objective et en toute indépendance. Ils ne devraient pas non plus assumer des tâches susceptibles de générer des conflits d'intérêts.

Les considérations qui précèdent répondent sur le fond à la question de l'opportunité de fusionner les trois comités existants. Il est toutefois évident que le regroupement préconisé n'empêchera nullement de traiter les divers thèmes (classification, protection des données ou sécurité technique) de manière spécifique. Il con-

viendra simplement de les aborder au sein d'un seul organe consolidé, dont l'agenda répondra aux besoins réels.

1.3.2 Nouvelle organisation au niveau de la Confédération

Le projet tient compte des résultats de l'étude commanditée par le Conseil fédéral au sujet de l'organisation actuelle de la sécurité de l'information. La solution proposée jette les bases d'une clarification et d'une simplification des compétences et des responsabilités en la matière. Elle met également l'accent sur l'acquisition des qualifications nécessaires par les services chargés de la mise en œuvre grâce à un appui et aux conseils d'experts et à un échange plus soutenu d'informations entre ces services. En conséquence, le projet prévoit un seul rôle de préposé (préposé à la sécurité de l'information), un seul organe de coordination et un service spécialisé de la Confédération en matière de sécurité de l'information, qui tous assumeront des tâches transversales dans le domaine de la sécurité de l'information. La nouvelle réglementation proposée permettra, au sein de l'administration fédérale, de regrouper intégralement les structures d'exécution actuelles de la protection des informations et de la sécurité informatique.

1.3.2.1 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 de la loi. 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, sur mandat de leur autorité (ou des départements et de la Chancellerie fédérale), piloteront l'organisation spécialisée de la sécurité de l'information et vérifieront l'application des mesures prises. Ils devront aussi mettre un accent principal sur la gestion des risques et la coordination avec d'autres domaines. Pour assumer leurs tâches de façon efficace et proportionnée aux risques, 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 Chancellerie fédérale, 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 au niveau de l'ordonnance si un regroupement des fonctions est utile et nécessaire au niveau des unités administratives.

1.3.2.2 Conférence des préposés à la sécurité de l'information

L'un des objectifs déclarés de la présente loi est d'atteindre un niveau de sécurité uniforme au sein des diverses autorités et organisations de la Confédération. En raison de l'indépendance constitutionnelle des autorités fédérales, un niveau uniforme ne peut être atteint qu'à la condition de développer une doctrine commune, malgré des besoins pour partie hétéroclites. En raison de leur statut, les préposés à la sécurité de l'information (cf. art. 84) 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 prévue se préoccupera principalement de la coordination transversale de l'exécution. Elle jouera de ce fait un rôle non négligeable dans le développement d'une doctrine uniforme et dans les nécessaires échanges d'expériences. Les préposés à la sécurité de l'information des départements et de la Chancellerie fédérale, de même qu'un représentant du PFPDT seront également associés à la conférence. La conférence pourra également recourir à des experts des cantons, des milieux scientifiques et du monde de l'économie pour des questions stratégiques en matière de sécurité de l'information.

La conférence remplacera les actuels Comité de coordination pour la protection des informations au sein de la Confédération (KOAISchB) et Comité de la sécurité informatique (OIAF), les aspects techniques restant du ressort d'organes spécialisés subordonnés.

1.3.2.3 Service spécialisé de la Confédération en matière de sécurité de l'information

L'organisation de la sécurité de l'information doit être pilotée et contrôlée comme un tout. Les tâches prévues par la présente loi et qui existent déjà aujourd'hui sont assumées par divers organes spécialisés, raison pour laquelle elles sont conçues et accomplies de manière sectorielle et guère harmonisée. Une simple coordination renforcée ne suffira pas à garantir une approche intégrale de la sécurité de l'information. Dans le projet, le service spécialisé est conçu avant tout comme un centre de compétences pour les tâches transversales au niveau des autorités fédérales. Il ne sera par conséquent pas habilité à donner des instructions: il

agira en principe toujours sur proposition ou sur mandat d'une autorité concernée, 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 être chargé d'évaluer les risques liés à l'introduction de nouvelles technologies, ou de 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 concernées). S'il s'avère que les processus, moyens et services en question répondent aux exigences standards de la Confédération, ils pourront être standardisés, puis utilisés plus simplement par d'autres autorités ou organisations de la Confédération. Par ailleurs, le service spécialisé pourra aussi être appelé à mener des contrôles de sécurité et des audits. Enfin, dans le cadre des relations internationales, il sera l'interlocuteur privilégié pour des contacts avec les services étrangers et internationaux œuvrant dans le domaine de la sécurité de l'information: cette fonction est importante dans la perspective de la mise en œuvre d'accords internationaux de droit public (cf. art. 90 et ch. 4.2).

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. Au sein de l'administration, et en matière de sécurité de l'information, de nombreux services 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 PIO pour le compte de l'administration fédérale. Les tâches des unités administratives seront par conséquent redéfinies au niveau de l'ordonnance, et certaines compétences devront être revues.

A cet égard, le Conseil fédéral devra évidemment se prononcer sur le problème épineux du rattachement administratif du service spécialisé. Pour préserver l'autonomie du Conseil fédéral en matière d'organisation, cette question ne doit pas être tranchée au niveau légal formel. Une proposition ne sera présentée au Conseil fédéral que lorsque l'on saura avec précision quelles tâches et compétences seront confiées au service spécialisé, et que l'on disposera d'une programme détaillé de mise en œuvre des prescriptions légales au sein de l'administration fédérale et des organisations concernées de droit public et de droit privé.

1.3.3 Nouvelle réglementation pour l'administration fédérale et d'autres organisations concernées.

Dans le cadre transversal, le service spécialisé de la Confédération en matière de sécurité de l'information n'aura *de par sa conception aucun pouvoir exécutoire légal*. En revanche, pour l'administration fédérale et les organisations concernées de droit public et de droit privé soumises aux dispositions d'exécution du Conseil fédéral, ce dernier pourra attribuer d'autres compétences au service spécialisé et définir de manière différenciée ses relations avec la ligne et les préposés à la sécurité de l'information. Bien que la hiérarchie reste en principe responsable de l'application des prescriptions, une forte majorité des participants aux travaux s'est prononcée en faveur d'un renforcement des compétences exécutoires du service spécialisé, notamment en matière de contrôles.

A cet égard, certains services ont souhaité que l'on définisse à ce stade déjà des options quant à l'organisation de l'exécution au sein de l'administration fédérale, assorties d'une évaluation de leurs avantages et inconvénients, et qu'on les soumette à décision. Il s'agirait d'opposer un modèle d'organisation totalement décentralisée avec simple fonction de coordination pour le service spécialisé, et un autre, plus centralisé, habilitant ce dernier à donner des instructions aux préposés à la sécurité de l'information des départements. Bien que la nécessité d'élaborer et d'évaluer de tels modèles de mise en œuvre ne fasse aucun doute, ces problèmes ne pourront recevoir de réponse sérieuse que plus tard: avant que l'on puisse décider en détail de l'exécution au sein de l'administration fédérale, il faudra faire toute la clarté sur les principes supérieurs du présent projet, son contenu matériel et les rapports transversaux.

2 Commentaires des dispositions

2.1 Loi fédérale sur la sécurité de l'information

Titre

Concernant le titre de l'acte, deux précisions sont importantes:

- 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 ou utilisent des moyens et installations relevant des technologies de l'information et de la communication (moyens

TIC) de la Confédération. 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 TIC. Elle n'est pas réduite à la sécurité informatique. Elle englobe en effet toutes les procédures de traitement, documents papier et déclarations orales comprises, et pas uniquement le traitement des informations au moyen de l'infrastructure électronique de la Confédération. Cette notion couvre également la réalisation des exigences de sécurité de la législation sur la protection des données ou d'autres lois imposant une protection de l'information.

Préambule

Cf. ch. 4.1

2.1.1 Dispositions générales

Art. 1

La présente disposition définit le but de l'acte normatif sous une forme générale.

L'al. 1 dispose que la loi porte non seulement sur les informations en tant que telles, mais également sur les TIC. La notion d'*information* n'est pas définie par la loi sur la sécurité de l'information (LSI) car l'acte renonce à donner de définitions légales et la notion admise dans la LSI correspond à l'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. Sa notion de *moyens TIC* englobe toutes les installations, appareils, systèmes et applications servant au traitement électronique (incl. enregistrement et communication) de l'information. Pour la mention expresse des TIC dans l'article consacré au but, cf. ch. 1.2.2.1.

Al. 2 : la sécurité n'est pas une fin en soi. La protection de l'information sert certains intérêts publics ou des intérêts de la Confédération en tant qu'institution. Dans ce contexte, ce sont les intérêts de la Confédération et de la Suisse qui sont prioritairement protégés et non ceux des particuliers. 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 les buts et le champ d'application de cette dernière diffèrent de ceux du présent projet (pour tout lien entre la LSI et la LTrans, cf. art. 3, al. 1).

La présente loi protège les intérêts ci-après:

- Let. a : la protection, par la prise de mesures de la sécurité de l'information, de la capacité des autorités fédérales à décider et à agir est l'un des intérêts essentiels 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. également art. 7, al. 1, let. a et b, LTrans, et ch. 2.2.2.1.1-2 du message relatif à la LTrans).
- Let. b : dans le cadre de la défense de cet intérêt, ce sont en priorité les informations émanant de la police, des douanes, des services de renseignement et de l'armée, de même que de ceux chargés de l'approvisionnement du pays qui sont protégées, ainsi que les moyens engagés par les autorités fédérales pour assurer la sécurité intérieure et extérieure du pays. De telles informations présentent souvent un haut besoin en confidentialité dans la mesure où leur utilisation abusive peut avoir des conséquences existentielles sur l'Etat, la population, certains individus ou groupes de personnes. Pour la même raison, les moyens TIC de la Confédération engagés pour appuyer les tâches critiques liées à la sécurité doivent aussi être disponibles et fonctionnels en permanence en temps de crise (cf. également art. 7, al. 1, let. d, LTrans, et ch. 2.2.2.1.3 du message relatif à la LTrans).
- Let. c : les relations avec l'étranger, tout comme les questions de sécurité, comptent parmi les domaines sensibles des activités de l'Etat. A ce niveau, le souci principal est de préserver la confidentialité des informations. L'acquisition d'informations sur la situation et les processus 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 parties adverses ou du public les stratégies en cause et les intentions correspondantes. Il en va de même pour les processus diplomatiques dans les

rapports entre Etats. Pour terminer, il faut mentionner que la Suisse peut être tenue, sur la base d'obligations contractuelles internationales ou de pratiques étatiques reconnues, de ne pas publier certains documents émanant de l'étranger (cf. également art. 7, al. 1, let. d, LTrans, et ch. 2.2.2.1.4 du message relatif à la LTrans).

- Let. d : la communication non autorisée ou la falsification de certaines informations et, dans ce domaine, le dérangement des systèmes d'information des autorités fédérales peuvent porter un préjudice considérable aux intérêts économiques et financiers de la Suisse ou à sa politique monétaire. Vu l'âpreté actuelle de la concurrence internationale, ces intérêts économiques gagnent en importance (cf. également art. 7, al. 1, let. f, LTrans, et ch. 2.2.2.1.6 du message relatif à la LTrans).
- Let. e : cette lettre concerne le domaine de la *compliance*, c'est-à-dire celui de l'accomplissement des obligations légales et contractuelles des autorités fédérales quant à la protection des informations qui ne relèvent pas des let. a à d. Dans l'accomplissement de leurs tâches légales, les autorités fédérales traitent notamment 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, LPTh, 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. S'il devait, toutefois, être établi que les autorités fédérales ne respectent pas leur devoir de protection de ces informations, la perception quant à leur fiabilité en pâtirait sérieusement. La let. e sert donc d'intérêt-cadre à toutes les informations que les autorités fédérales traitent et doivent protéger, sans que cette protection s'assure par la classification des informations concernées. Elle protège ainsi l'intérêt des autorités fédérales à préserver leur haut niveau de fiabilité (cf. également art. 7, al. 1, let. e, g et h, LTrans, et ch. 2.2.2.1.5 et 2.2.2.1.7-8 du message relatif à la LTrans).

Art. 2

L'art. 2 porte sur le champ d'application institutionnel ou relevant de l'organisation administrative.

L'al. 1 énumère les autorités obligées d'appliquer la présente loi dans leur domaine de compétence. Les autorités concernées 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), 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 leurs activités en tant qu'autorités, ces institutions ne reçoivent pas directement d'instructions de la part d'une autre autorité. Néanmoins, en raison du flux d'informations entre elles, elles sont tenues d'appliquer la présente loi dans leur propre domaine administratif de compétence. Dans la mesure où la loi contient des délégations législatives, elle se réfère toujours à ces autorités en les appelant "*les autorités concernées*". Les raisons pour lesquelles les autorités fédérales, dans leur ensemble, ont dû être énumérées dans la loi sont énoncées sous ch. 1.2.2.2.

Il va de soi que la loi doit tenir compte, dans certaines dispositions, du statut constitutionnel et des particularités des diverses institutions et autorités. Ainsi, elle contient, par exemple, des exceptions à l'obligation de subir un contrôle de sécurité (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. 19, 33, al. 4, 35, 36 et 84, al. 1). Au niveau de la loi, il n'est pas possible de définir toute l'organisation d'exécution des diverses autorités ni l'ensemble des compétences de leurs organes ou services ; la législation d'exécution des diverses autorités y pourvoira.

L'al. 2 prend en considération le fait que les autorités mentionnées sous l'al. 1 ne doivent assumer, que dans une moindre mesure, leurs propres tâches d'exécution et que les organisations qui leur sont subordonnées, dans le domaine de leurs tâches légales, doivent être elles-mêmes directement obligées 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 concernées ne doivent pas assumer elles-mêmes des tâches d'exécution mineures ; quant aux organisations énumérées, elles ne peuvent pas endosser de compétences législatives ou décisionnelles qui dépassent le cadre du droit administratif auquel elles sont soumises. La notion d'*organisations concernées* est introduite dans les articles qui suivent, à titre de désignation abrégée, pour simplifier la structure rédactionnelle de la loi. En l'occurrence, il s'agit plus particulièrement des services du Parlement, des administrations des tribunaux fédéraux, des départements, de la Chancellerie fédérale, de l'administration fédérale et des unités décentralisées, ainsi que de l'armée.

- La let. d prévoit, en principe, la soumission à la présente loi des organisations de droit public ou privé qui assument des tâches administratives de la Confédération au sens de l'art. 2, al. 4, LOGA, et qui sont soumises, à ce titre, à la surveillance de la Confédération (cf. à ce sujet art. 8, al. 4 et 5, LOGA). Il s'agit plus spécialement d'organisations habilitées par la loi à prendre des décisions formelles à l'encontre des particuliers. En l'occurrence, la condition pour que ces organisations soient soumises à la loi est qu'elles exercent des activités sensibles (cf. al. 3) dans le cadre de l'accomplissement de leurs tâches administratives. Cette soumission ne les concerne que pour ces tâches administratives. Il est impossible de préciser exhaustivement et durablement dans le présent acte le nom des diverses organisations subordonnées. Le Conseil fédéral doit donc déterminer, par voie d'ordonnance, qui doit être soumis à la présente loi et dans quelle mesure (cf. art. 87, al. 4).
- Let. e : la Confédération et les cantons tablent sur une collaboration très étroite pour accomplir leurs tâches respectives. Ils s'échangent de très nombreuses informations, dont certaines sont des informations classifiées de la Confédération. De surcroît, les infrastructures TIC et les systèmes de la Confédération et des cantons sont de plus en plus interconnectés. Cela va de pair avec un risque plus élevé de voir les attaques et les menaces perpétrées dans le domaine de compétence d'une autorité s'étendre aux domaines de compétence d'autres intervenants. Les cantons sont responsables de la sécurité de leurs propres informations. Toutefois, lorsqu'ils accomplissent des tâches de droit fédéral sous la surveillance directe de la Confédération, les directives de cette dernière s'appliquent en principe aussi pour eux. La présente loi prévoit une soumission des cantons selon des critères établis en fonction des risques : ainsi, dans le cadre de l'exécution de leurs tâches, ils doivent être soumis à la loi uniquement lorsqu'ils effectuent des activités sensibles sur mandat de la Confédération et sous sa surveillance directe (cf. al. 3).

  La présente loi ne s'applique pas aux autorités et services cantonaux qui appliquent la législation fédérale de manière autonome. La LSI ne règle pas spécialement l'interconnexion des réseaux informatiques cantonaux et fédéraux. A ce niveau, les autorités fédérales et les cantons doivent s'accorder sur la prise de mesures de sécurité qui soient adaptées à la situation et qui garantissent matériellement le niveau de protection exigé par la loi pour les autorités fédérales. Concernant l'exécution par les cantons, cf. art. 89.

L'al. 3 décrit la notion centrale d'*activité sensible* pour l'application de la présente loi. L'exercice d'une activité sensible n'est pas seulement une condition permettant de soumettre à la loi les cantons et des organisations de droit public ou privé accomplissant des tâches administratives, mais aussi d'assujettir à des contrôles de sécurité relatifs aux personnes (CSP) ou à des procédures de sécurité relatives aux entreprises (PSE) des tiers devant être investis de mandats de la Confédération. L'activité sensible est définie dans le contexte de la sécurité de l'information. Pour ce qui concerne son contenu matériel, le traitement d'informations figure au premier plan, comme dans la LMSI. Quant à sa définition, des équivalences ont été établies entre la réglementation sur la protection des informations classifiées et celle sur la sécurité lors de l'engagement de moyens TIC.

- Let. a : l'adoption de l'échelon de classification CONFIDENTIEL comme point de départ pour la définition d'une activité sensible 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*. Dans le cadre du traitement d'informations classifiées, la notion de sensibilité ne s'applique pas au seul *accès* à ces informations, mais aussi à leur *traitement* effectif et justifié. En d'autres termes, en prenant comme exemple le personnel de nettoyage, celui-ci n'exerce généralement pas une activité sensible au sens de la présente loi, bien que la probabilité qu'il puisse parfois, pendant ses travaux, accéder à des informations classifiées soit grande dès lors que certains collaborateurs ne respectent pas toujours les prescriptions de sécurité.

  La lettre mentionne aussi l'utilisation du matériel classifié. Il s'agit, en l'occurrence, de divers appareils et objets devant être protégés pour éviter que des personnes non autorisées connaissent leur existence ou leurs propriétés, ou que leurs caractéristiques mêmes puissent transmettre des informations classifiées du fait que le matériel contient ou *est* lui-même l'information sensible. Sont principalement concernés les biens d'armement, des systèmes d'armes et des systèmes intégrés de communication. Il arrive souvent qu'un Etat tiers qui en a autorisé la livraison à la Suisse exige que ces appareils ou objets soient classifiées. Jusqu'à présent, la Suisse n'appliquait le système des échelons de classification que dans le domaine militaire ; le domaine civil (par ex. la police et le Corps des gardes-frontière), quant à lui, ne disposait pas d'une base correspondante ; elle existe désormais implicitement dans la présente disposition.
- Let. b : elle relève les activités impliquant des droits d'accès étendus aux moyens TIC des deux catégories de sécurité supérieures ou à des activités particulières relatives à ces moyens TIC dont l'exercice permettrait à des personnes de nuire considérablement aux intérêts au sens de l'art. 1, al. 2, par exemple en volant des données ou en commettant des actes de sabotage. La simple utilisation de ces moyens n'est donc

pas considérée comme sensible (seul le contenu des informations à traiter détermine si l'utilisateur exerce une activité sensible ou non). La let. b concerne avant tout certains administrateurs ou responsables d'application.

- Let. c : pour terminer, est considéré comme sensible l'accès aux zones de sécurité réglées par l'art. 31, car les dommages que peuvent occasionner l'espionnage ou le sabotage dans ces zones peuvent être considérables en raison des informations sensibles et des moyens TIC qu'elles contiennent.

L'al. 3 s'écarte de la réglementation en vigueur de l'art. 19, al. 1, LMSI. Ainsi, la présente loi ne qualifie plus d'activité sensible l'accès régulier à des données personnelles sensibles dont la révélation pourrait porter gravement atteinte aux droits individuels des personnes concernées. En outre, le traitement de secrets d'affaires ou de fabrication n'est pas considéré comme sensible selon la LSI. A signaler néanmoins qu'en matière de données personnelles et de secrets d'affaires ou de fabrication, certains besoins de protection sont couverts par les dispositions relatives à l'engagement de moyens TIC. Une autre modification importante par rapport à la réglementation actuelle tient au fait que la *régularité* de l'exercice des activités mentionnées n'est pas un élément constitutif du caractère sensible de ces activités. Le traitement ponctuel d'informations classifiées CONFIDENTIEL est déjà considéré comme sensible par la LSI. Cette modification est nécessaire en rapport avec le contrôle de sécurité dont les tiers devant exécuter des mandats de la Confédération doivent faire l'objet. Ces catégories de personnes n'effectuant pas en permanence leurs activités sous le contrôle des autorités ou organisations concernées, elles doivent être soumises à des conditions spéciales dans le cadre de leur assujettissement au CSP.

Pour les conditions en lien avec les contrôles de sécurité relatifs aux personnes, cf. ch. 1.2.4.

Art. 3

Al. 1 : de par la réserve émise pour les dispositions de la LTrans, il est clairement établi que le domaine d'application de la loi sur la transparence n'est, en aucune façon, restreint par la réglementation sur la sécurité de l'information. Les informations qui ont été classifiées conformément à la LSI ne sont pas concernées par la réserve de l'art. 4 LTrans (dispositions spéciales déclarant certaines informations secrètes). Ainsi, les dispositions de la LTrans relatives à l'accès à des documents officiels s'appliquent également pleinement aux informations classifiées selon la LSI.

L'appréciation des documents dans le cadre de la procédure prévue par la LTrans est indépendante des dispositions de la LSI. En cas de demande d'accès à des documents officiels, l'autorité compétente examine donc, indépendamment de toute mention éventuelle de classification, s'il y a lieu d'autoriser, de restreindre, de différer ou de refuser l'accès. La classification d'informations peut toutefois, lors de l'examen de documents selon la LTrans, être jugée comme un indicateur de non-divulgation du document correspondant. La décision de classification implique en effet une évaluation du besoin de protection de l'information concernée au regard d'une éventuelle atteinte portée aux intérêts publics au sens de l'art. 1, al. 2, LSI, qui, dans le fond, devrait correspondre matériellement à une évaluation de la restriction, du report ou du refus du droit d'accès selon l'art. 7, al. 1, LTrans. Le contenu des dispositions sur la classification est structuré de telle sorte qu'il ne puisse pas contredire celui du catalogue des exceptions visé à l'art. 7 LTrans.

En outre, il convient de souligner que le champ d'application de la LSI doit, en principe, être plus large que celui de la LTrans du fait que la LSI doit s'appliquer à l'ensemble des autorités fédérales. Par ailleurs, la LSI ne se concentre pas uniquement sur la protection de la confidentialité, mais protège aussi la disponibilité, l'intégrité et la traçabilité des informations.

L'al. 2 règle les liens entre le nouvel acte normatif et les nombreuses lois fédérales fixant les exigences en matière de protection de la confidentialité, de la disponibilité, de l'intégrité et de la traçabilité des informations, ou en matière de protection de la disponibilité et de l'intégrité des moyens TIC (cf. art. 4, al. 2, let. a à d). Les dispositions de la LSI doivent s'appliquer, à titre complémentaire, à de telles lois. Cela signifie que la LSI donne un cadre uniforme à l'évaluation du besoin de sécurité lié à ces informations et à la mise en œuvre des exigences de sécurité fixées par les lois spéciales pour ces informations.

L'exemple de la LSP permet de clarifier ce principe. La LPD fixe les exigences concernant le traitement légitime et la protection des données personnelles. Il va de soi que le traitement de ces données dans le cadre des tâches assignées aux autorités fédérales devra répondre aux exigences de la loi sur la protection des données. Comme la LPD ne contient que peu de prescriptions détaillées sur les mesures pratiques de protection personnelles, techniques et physiques, celles de la présente loi devront s'appliquer, à titre de droit complémentaire, au traitement des données personnelles. Enfin, si des données personnelles sont jugées importantes, par exemple pour le maintien de la sécurité publique, elles seront traitées conformément aux prescriptions de la présente loi et, le cas échéant, classifiées.

Al. 3: le Conseil fédéral a fixé le principe de la régulation décentralisée des infrastructures critiques (IC) dans la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC). Dans la mesure où une intervention s'impose sur le plan formel de la loi, la législation spéciale en vigueur doit être adaptée (cf. ch. 1.1.2.2 et 1.2.6). La LSI permet toutefois à la Confédération de disposer, dans le domaine de la sécurité de l'information, d'instruments particuliers, tout spécialement le CSP, que certains régulateurs et exploitants d'IC aimeraient pouvoir utiliser. Les dispositions sur la classification ou sur la sécurité lors de l'engagement de TIC suscitent, en partie aussi, de l'intérêt. Certaines IC recourent, aujourd'hui déjà, à ces instruments. Tel est, par exemple, le cas des centrales nucléaires pour lesquelles la Confédération prescrit certaines mesures concernant la protection des informations (cf. art. 5 et 24 LENu). Dans le domaine de la surveillance de l'espace aérien également (Skyguide), certains membres du personnel font l'objet, au préalable à leur engagement, d'un CSP. Désormais, certains employés de la société nationale du réseau de transport qui gèrent le réseau d'alimentation en électricité à l'échelle de la Suisse (Swissgrid) devront aussi être assujettis à un contrôle de fiabilité. Cet article rappelle ainsi que la législation spéciale peut soumettre (même partiellement) certaines IC aux dispositions de la LSI.

Pour les modifications de la législation spéciale dans ce domaine, cf. également ch. 2.9 et 2.10.

2.1.2 Mesures générales de la sécurité de l'information

Art. 4

L'art. 4 reprend le contenu matériel de la sécurité de l'information ainsi que les principes majeurs selon lesquels elle doit être concrétisée. En détaillant les objectifs de protection, il complète aussi l'article portant sur le but de la présente loi (art. 1), .

L'al. 1 dispose que les autorités et organisations concernées déterminent le besoin de protection des informations dont ils sont responsables. Ce besoin est établi en fonction du préjudice potentiel porté aux intérêts visés à l'art. 1, al. 2, et défini en regard des critères détaillés de l'al. 2. Le besoin spécifique de protection à raison de la matière est très souvent déterminé par d'autres lois (cf. également art. 1, al. 2, let. e, et art. 3, al. 2).

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 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 aussi 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 dans la notion d'*intégrité* dans la présente loi), l'imputabilité ou l'incontestabilité (découlant des critères *intégrité* et *traçabilité* visés dans la présente loi).

- let. a : le principe de la confidentialité doit s'entendre comme celui selon lequel seules les personnes autorisées ont 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. Lorsque les informations doivent être rendues publiques, la notion de cercle tombe au profit de celle d'universalité.
- Let. b : la disponibilité des informations n'est pas absolue, mais la capacité de décision et d'action des autorités et des organisations exige que ces dernières puissent consulter à temps les informations nécessaires à l'accomplissement de leurs tâches légales. Les exigences quant à la disponibilité sont d'autant plus élevées que les informations doivent être disponibles en permanence pour l'accomplissement des tâches importantes. Cela s'applique en particulier lorsque ces informations doivent être traitées électroniquement.
- Let. c : la préservation de l'intégrité et de l'exactitude des informations est une tâche partielle importante de la protection des informations; elle est également d'importance – en regard de la fiabilité des autorités - lorsque les informations sont destinées au public. Elle est aussi décisive pour le bon fonctionnement des moyens TIC.
- Let. d : la transparence dans le 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.

Les autorités et organisations concernées doivent donc évaluer le besoin de protection des informations et déterminer l'objectif et l'ampleur de cette protection (exigences de sécurité). Ainsi, le maintien de la confidentialité n'est nécessaire que si cette confidentialité doit être garantie pour une raison légale (par ex. LPD, secrets d'affaires ou de fabrication de tiers, ou encore art. 14 LSI). Il s'agit toutefois de noter aussi que cer-

taines informations peuvent justifier des exigences accrues quant à la 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 plus particulièrement les informations et les moyens TIC qui soutiennent ses processus critiques des autorités. Le besoin de protection ressort donc aussi de l'importance de l'accomplissement de la tâche légale où les informations sont utilisées ou servent à l'étayer.

Al. 3 : la protection de la disponibilité et de l'intégrité des moyens TIC complète notablement les quatre critères évoqués permettant une protection intégrale des informations. Bien qu'émanant en principe déjà de l'al. 2, let. b et c, l'exigence d'une protection adéquate face aux abus et aux dérangements est, une fois encore, expressément mentionnée, car l'appui TIC aux processus d'affaires ne cesse de gagner en importance. Désormais, son bon fonctionnement est une condition *sine qua non* de l'accomplissement efficient des tâches des autorités fédérales.

Al. 4 : la sécurité de l'information doit être axée sur les risques, efficace et économiquement rationnelle. Une appréciation aussi objective que possible des risques est déterminante pour l'application adéquate des mesures de sécurité (cf. art. 6 et 7). 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 compétentes doivent donc veiller à ce que leurs mesures soient appropriées et efficientes. Les échelons hiérarchiques sont ainsi tenus, dans leur suivi des mesures de protection, d'évaluer le rapport coût/utilité de la sécurité.

Dans ce contexte, le principe de simplicité d'emploi pour les utilisateurs est également au programme. Les personnes traitant les informations ou utilisant des moyens TIC doivent souvent respecter certaines prescriptions comportementales pour maintenir la sécurité de l'information (par ex. obligation de fermer à clé la porte du bureau ou de crypter un message électronique). Mais force est 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 vont pas être respectées ou seront intentionnellement contournées.

Art. 5

La sécurité est l'affaire du chef. L'art. 5 décrit le contenu des responsabilités majeures au plus haut niveau dans le domaine de la sécurité de l'information. Il ne s'adresse donc qu'aux autorités concernées (art. 2, al. 1) qui seules supportent ces responsabilités.

L'al. 1 exige des autorités concernées qu'elles organisent la sécurité de l'information dans leur domaine de compétence.

- Let. a : la sécurité de l'information doit être organisée, mise en œuvre et contrôlée en fonction de l'état d'avancement des connaissances et de la technologie. Plusieurs standard non contraignants formulent ce qui est communément appelé de *bonnes pratiques* dans la gestion de la sécurité de l'information (par ex. norme DIN ISO/IEC 27'001 et 27'002). Ces derniers sont particulièrement importants parce qu'ils ont été testés pratiquement et qu'ils répondent aux exigences d'une approche intégrale. De plus, ils définissent des exigences quant à l'application de mesures de sécurité pouvant répondre adéquatement aux besoins des autorités et organisations.

  Les autorités de moins grande ampleur (par ex. Tribunal fédéral des brevets, Tribunal militaire de cassation et autorité de surveillance du Ministère public de la Confédération) ne pourront naturellement pas, à elles seules, constituer une telle organisation. Cependant, 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.

- Let. b : la mise en œuvre de la sécurité de l'information concerne de nombreux domaines spécialisés, par exemple celui des finances (effets de l'organisation et des mesures sur les finances), les services du personnel (tâches relevant du domaine du personnel), les domaines du droit et de la *compliance* (bases juridiques de la sécurité de l'information), l'informatique (influence de la sécurité de l'information sur l'engagement des TIC et concrétisation des exigences au niveau des systèmes TIC) et le domaine de la gestion des risques et du controlling (sécurité de l'information comme élément constitutif de la gestion des risques). Pour assurer une sécurité efficace de l'information, il est donc nécessaire que ces domaines spécialisés évoqués comprennent les besoins liées à la sécurité de l'information, qu'ils participent aux processus de décision y relatifs et qu'ils coordonnent entre eux la mise en œuvre des mesures prises.

Al. 2 : pour la sécurité au sens général, il est important que les tâches et les compétences soient clairement réglées. Cela concerne en particulier la sécurité de l'information dans la mesure où de nombreux domaines spécialisés fixent des exigences pour un traitement sûr des informations ou vont assumer une partie des res-

ponsabilités dans l'application de la présente loi. Un manque de clarté dans l'attribution de ces compétences peut aboutir au fait que des risques importants peuvent ne pas être identifiés, que personne ne se sente responsable de l'application de certaines mesures de sécurité et que personne n'assume consciemment le risque.

L'al. 3 charge les autorités de fixer, pour leur propre domaine de compétence, certains principes devant permettre de faire connaître les intentions de l'autorité concernée à propos de la sécurité de l'information.

- Let. a : les objectifs des autorités concernées quant à la sécurité de l'information déterminent le niveau de sécurité qui doit être atteint (niveau exigé de sécurité de l'information). Ces objectifs impliquent une analyse coût-utilité (quelle sécurité les autorités veulent-elles et à quel prix) et doivent être déterminants pour l'attribution des ressources nécessaires. Exemple: les secrets d'affaires des tiers qui doivent être traités par les autorités ou les organisations de la Confédération doivent être protégés de toute divulgation non autorisée. Si ces informations doivent être protégées contre les services de renseignement les plus actifs et les mieux fournis du monde, alors les mesures de sécurité nécessaires pour atteindre ce niveau de sécurité seront sensiblement plus coûteuses que celles prises lorsque les autorités acceptent le risque relativement élevé de voir ces services de renseignement étrangers acquérir ces informations. Ces objectifs quant à la sécurité de l'information sont également déterminants pour l'évaluation de l'efficacité des mesures de sécurité (cf. art. 24, al. 2).
- Let. b : chaque autorité concernée doit, en particulier, régler la façon dont les organisations subordonnées doivent aborder les risques, déterminer les risques qui peuvent sans autres être supportés et ceux qui doivent être rapportés aux autorités elles-mêmes. 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. C'est en particulier le cas des risques liés aux informations classifiées SECRET (art. 14, al. 3) ou aux moyens TIC de la catégorie de sécurité "protection très élevée" (art. 21, al. 3). Les risques stratégiques devraient être communiqués aux autorités concernées avant qu'un incident n'ait lieu.
- Let. c : 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 TIC mis à leur disposition négligemment ou en enfreignant les consignes de sécurité. Très souvent, de tels manquements sont *a priori* excusés et n'entraînent dès lors aucune investigation. Ils peuvent néanmoins avoir d'importantes répercussions. Ils ne devraient donc pas être considérés comme des infractions bénignes. Les autorités concernées doivent ainsi appliquer les consignes de manière conséquente et indiquer, en les expliquant, les suites de leur violation.

Al. 4: les autorités concernées doivent veiller à informer régulièrement, et en fonction des niveaux de responsabilité, les cadres et le personnel à propos des affaires en lien avec la sécurité de l'information. Il s'agit, par exemple, de communiquer les modifications apportées à la réglementation relative à l'organisation et aux compétences, ou d'informer les cadres et les spécialistes des causes et des conséquences d'un incident. Une information régulière est donc nécessaire car elle permet aux cadres et au personnel de comprendre l'attitude des organes de direction vis-à-vis de la sécurité de l'information et de pouvoir réagir face aux changements. Elle leur permet aussi de tirer les enseignements des incidents survenus dans leur domaine de compétence. Les cadres et le personnel doivent donc aussi être instruits en conséquence.

Art. 6

L'art. 6 impose aux autorités et aux organisations l'instauration d'un système de gestion des risques dans le domaine de la sécurité de l'information (concernant la gestion des risques, cf. ch. 1.2.3.2).

L'al. 1 dispose que les autorités et organisations concernées doivent identifier, évaluer, juger et vérifier les risques, et ce tant dans leur propre domaine de compétence que dans le cadre de leur collaboration avec les tiers. Idéalement, ces autorités et organisations devraient toutes recourir aux mêmes méthodes. Dans ce domaine, le Conseil fédéral fixera des exigences et des mesures standard (art. 88), en étant conscient que les critères établis pour l'acceptation du risque - qui sont déterminants pour l'évaluation des risques - sont déterminés par les diverses autorités en fonction de leur besoin propre en matière de sécurité de l'information (cf. également art. 5, al. 3, let. a et b).

L'évaluation des risques implique des connaissances approfondies des tâches légales et des processus critiques d'affaires qui en découlent, une méthode d'appréciation des menaces et des dangers appliquée régulièrement aux valeurs à protéger, l'analyse des points faibles, ainsi que l'estimation de la probabilité de survenance d'un évènement et de l'étendue potentielle du dommage lié à cet évènement. Dans le domaine de la sécurité de l'information, la gestion des risques doit être un processus permanent. C'est tout particulièrement vrai pour le domaine de l'informatique dans la mesure où des logiciels malveillants sont développés au quo-

tidien. Les applications informatiques et les logiciels de sécurité doivent donc faire l'objet de mises à jour rapides.

Selon l'al. 2, les mesures nécessaires de prévention ou de réduction des risques doivent être prises. Bien entendu, des risques peuvent également être pris en compte ou supportés (cf. al. 3). Ils ne devraient cependant pas être ignorés. Les risques peuvent être évités dans la mesure où il est possible de 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 économiquement pas justifiable ou interdire le traitement d'informations classifiées SECRET par des moyens TIC en réseau). Les mesures à prendre sont subdivisées en diverses catégories (cf. ci-après) qui se recoupent parfois:

- *Mesures organisationnelles*. Par exemple, l'édiction de bases juridiques, la fixation de la politique et de l'organisation de la sécurité, l'attribution de responsabilités et de compétences claires, la classification des informations, la séparation des fonctions sensibles, la réglementation et les contrôles des accès pour les personnes, les contrôles d'ordre général, la réglementation des accès aux systèmes, la création de concepts de sécurité pour les moyens TIC critiques, l'organisation du traitement des incidents.
- *Mesures relatives aux personnes*. Par exemple, la formation et la sensibilisation, l'obligation contractuelle de respecter la sécurité de l'information, la réalisation de CSP, les entretiens personnels menés régulièrement avec les personnes-clés en vue de favoriser leur prise de conscience face à certains dangers, la formulation et l'application de sanctions.
- *Mesures techniques*. Par exemple, le cryptage des informations, la redondance des services importants, la protection contre les logiciels malveillants, l'authentification forte, la protection des accès aux réseaux.
- *Mesures relatives aux constructions*. Par exemple, la mise en place d'un périmètre de sécurité, l'utilisation de systèmes de fermeture de sécurité, l'établissement de zones et de locaux de sécurité, le recours à des installations de surveillance.

L'al. 3 dispose que les risques subsistant après l'application des mesures de sécurité prévues (appelés risques résiduels) ou les risques ne devant pas être minimisés soient clairement annoncés. Les décideurs doivent être pleinement avisés de ces risques et de leurs conséquences potentielles afin de pouvoir peser les intérêts correspondants (sécurité et coûts). Les risques résiduels doivent être clairement acceptés et supportés.

L'al. 4 précise que la gestion des risques dans le domaine de la sécurité de l'information doit impérativement être intégrée à tous les niveaux dans le processus général de gestion des risques de la Confédération. Même si le processus de gestion présentement exigé a un caractère spécifique et doit donc être géré et exploité par des spécialistes, la sécurité de l'information reste une préoccupation relevant de la gestion des risques d'affaire usuels. Les autorités concernées doivent donc régler la collaboration entre l'organisation spécialisée chargée de la gestion générale des risques et celle chargée de la sécurité de l'information.

Art. 7

L'al. 1 exige que les autorités et les organisations fixent leurs exigences et mesures de sécurité en s'inspirant des exigences et mesures standard au sens de l'art. 88. Les autorités et organisations qui ne sont pas subordonnées au Conseil fédéral ne sont pas tenues de suivre ces standards. Etant donné qu'un des objectifs importants de cette loi est d'obtenir, autant que possible, de toutes les autorités l'application des normes de sécurité équivalentes, le Conseil fédéral est tenu de fixer des exigences et des mesures standard en fonction de l'état d'avancement des connaissances et de la technologie. Pour répondre au principe d'efficience économique, la loi cherche à éviter que chaque autorité ou organisation réinvente la roue lorsque, pour un problème similaire, une autre autorité ou organisation a déjà développé ou trouvé une solution efficace.

Al. 2 : les mesures de sécurité doivent être prises en fonction de l'état d'avancement des connaissances et de la technologie. La sécurité de l'information est un domaine relativement nouveau qui évolue rapidement. Même si les principes d'organisation en matière de sécurité de l'information ont atteint un certain stade de stabilité et de maturité du fait qu'ils correspondent aux principes généraux d'organisation appliqués dans le domaine de la gestion des risques, de meilleures mesures organisationnelles, plus efficaces et plus économiques, sont régulièrement développées. *En fonction de l'état d'avancement des connaissances* signifie donc, dans le contexte du présent alinéa, que les autorités et organisations concernées doivent adopter des solutions et des approches de nature organisationnelle qui ont fait leurs preuves (*best practices*).

L'évolution est très rapide dans le domaine technique de la sécurité de l'information, en particulier au niveau des moyens TIC, mais également dans celui de la sensorique (par ex. détecteurs de feu, de chaleur ou de mouvements), ou dans les techniques de verrouillage (par ex. systèmes de verrouillage des portes). Il est très important que les mesures de sécurité ne soient pas issues de technologies surannées, mais montrent leur efficacité face aux menaces actuelles.

Art. 8

Au sens de la présente loi, les tiers sont les autorités, organisations et personnes de droit public ou privé qui ne sont pas des autorités ou organisations concernées au sens de l'art. 2 et qui agissent donc, en principe, indépendamment de ces autorités et organisations. Les autorités fédérales, quant à elles, ont souvent besoin de l'appui des acteurs de l'économie privée ou d'autres organes pour accomplir leurs tâches. 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.

Ce mode de collaboration avec des tiers ainsi que les mesures de sécurité à respecter sont généralement réglés contractuellement. En principe, les tiers ne devraient être habilités à accéder aux informations ou aux moyens TIC que lorsque les mesures nécessaires ont été mises en œuvre. La LSI contraint également les autorités et organisations concernées à contrôler l'application effective de telles mesures. Lorsque le mandat implique l'exercice d'une activité sensible, ces autorités et organisations doivent requérir l'ouverture d'un contrôle de sécurité relatif aux personnes (cf. art. 32 ss) ou, le cas échéant, demander d'ouverture d'une procédure de sécurité relative aux entreprises (cf. art. 56 ss).

Art. 9

A l'avenir également, des incidents surviendront dans le domaine de la sécurité de l'information. Il est dès lors nécessaire d'adopter une procédure efficace et uniforme pour faire face à ces incidents. Les autorités et organisations concernées doivent, dans un premier temps, prendre les mesures nécessaires pour être capables, avant toute autre chose, d'identifier ces incidents suffisamment tôt (par ex. contrôles réguliers, capteurs, installations d'alarme, surveillance des réseaux, analyses régulières des log-files, etc.). Elles doivent également fixer une procédure dictant le comportement à adopter lorsque des événements ou des points faibles sont identifiés et attribuer des compétences claires pour le traitement des cas. Le personnel impliqué, qu'il soit interne ou externe à l'autorité ou organisation concernée, doit aussi savoir comment réagir face à de tels événements pour pouvoir limiter leurs effets le plus possible.

Pour tirer des enseignements à partir des incidents, les autorités et organisations concernées doivent veiller à ce que leurs causes soient identifiées et examinées. Cela doit permettre d'améliorer continuellement l'identification et le traitement des incidents de sécurité.

Art. 10

Les autorités doivent exploiter un "business continuity management" (BCM) dans le domaine de la sécurité de l'information. Exploiter un BCM signifie prendre les dispositions nécessaires pour que les autorités puissent assurer à temps l'accomplissement de leurs tâches essentielles, même en situation extraordinaire (cf. également art. 6, al. 3, LOGA). L'accomplissement des tâches des autorités fédérales dépendant toujours plus de l'engagement fiable des moyens TIC, les risques et les planifications préventives dans le domaine de la sécurité de l'information doivent impérativement être pris en compte dans le cadre du BCM général des autorités. La loi n'exige l'établissement de pareilles planifications préventives que pour les tâches indispensables des autorités concernées, mais pas pour celles des organisations concernées. En d'autres termes, le Conseil fédéral doit veiller à ce que les tâches de l'administration fédérale et celles de l'armée *qu'il juge* critiques *d'un point de vue stratégique* soient identifiées. La loi ne l'exigeant pas à proprement parler, les départements et unités administratives sont libres, dans le domaine de la sécurité de l'information, d'établir ou non des planifications préventives pour leurs tâches critiques qui ne sont pas visées par le Conseil fédéral.

Art. 11

Concernant les contrôles et les audits, cf. ch. 1.2.3.3.

L'al. 1 exige des autorités et organisations concernées qu'elles contrôlent régulièrement que les dispositions et prescriptions de la LSI soient respectées. En principe, ces contrôles incombent aux supérieurs hiérarchiques. Cependant, les préposés à la sécurité de l'information effectueront aussi, sur mandat de leur autorité, des contrôles et des audits conformément à l'art. 84, al. 2, let. c.

L'al. 2 ne s'adresse qu'aux autorités concernées. Un examen périodique par un organe indépendant est nécessaire car il doit avant tout se focaliser sur l'efficacité de l'organisation de la sécurité de l'information. Cette organisation inclut naturellement les tâches des personnes responsables des contrôles ordinaires. La décision concernant la périodicité des contrôles d'efficacité aussi bien que celle portant sur le choix des organes chargés de les réaliser appartient à l'autorité concernée. Les autorités peuvent, par exemple, mandater un service interne de révision ou une entreprise ou un organe externe. Elles peuvent aussi recourir au service spécialisé de la Confédération en matière de sécurité de l'information (cf. art. 86, al. 1, let. c). En outre, le Conseil fédéral peut demander au CDF de mener de telles investigations.

Art. 12

L'al. 1 dispose que la classification d'informations est impérative lorsque les critères de classification visés à l'art. 14 sont remplis. A l'heure actuelle, chaque autorité concernée est, en principe, libre d'établir (le cas échéant) son propre système de classification, ses propres motifs de classification et ses propres prescriptions de traitement. Certains incidents qui se sont produits au cours de ces dernières années ont montré qu'une différence dans le traitement des informations classifiées peut accroître le sentiment de méfiance entre autorités et/ou organisations. Une réglementation uniforme des échelons de classification et des motifs de classification s'avère donc nécessaire.

L'al. 2 confirme, au niveau de la loi, que la classification d'informations doit être l'exception et non la règle, eu égard notamment au principe de la transparence et aux charges occasionnées par la classification.

L'al. 3 précise que la classification doit, dans la mesure du possible, être limitée dans le temps. Souvent, les informations dignes de protection deviennent anodines avec le temps ou après un événement précis (par ex. publication d'un rapport ou levée d'une mesure spécifique). La classification de ces informations (par ex. après être devenues désuètes) ne se justifie alors plus. Elle n'entraînerait que des dépenses inutiles ou provoquerait des problèmes après l'archivage des informations. Par ailleurs, les informations devant demeurer classifiées durant une longue période requièrent des mesures de sécurité techniques différentes de celles applicables aux informations dont le besoin en protection est plus limité dans le temps.

Dès lors qu'une classification dans le temps ne peut être établie à l'avance, l'obligation que renferme l'al. 4 - la nécessité de contrôler périodiquement la classification - garantit que les informations ne resteront pas inutilement classifiées.

Art. 13

Al. 1 : les autorités concernées doivent déterminer qui a la compétence de procéder à la classification. Actuellement, au sein de l'administration fédérale, cette compétence revient à l'auteur d'un document car il est celui qui peut le mieux estimer le besoin de protection des informations et les risques éventuels. La réglementation du Conseil fédéral ne doit toutefois pas être contraignante pour les autres autorités fédérales. Ainsi, ces dernières doivent pouvoir aussi décider que la classification soit, par exemple, le fait de l'organe directionnel de l'autorité, d'un service central jugé compétent ou simplement par les supérieurs hiérarchiques. La notion d'*auteur de la classification* est particulièrement importante pour la décision concernant le cercle des destinataires autorisés, la déclassification, l'archivage et la destruction d'informations classifiées ; elle l'est cependant aussi pour les éventuelles mesures préalables de protection qui doivent être prises lorsqu'un danger menace des informations classifiées (cf. art. 18).

L'al. 2 établit le caractère contraignant de la classification. 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 voie de service, 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.

Art. 14

Concernant les objectifs de la réglementation de la classification, cf. ch. 1.2.3.4.

L'art. 14 règle les conditions matérielles de la classification des informations et fixe les échelons correspondants pour toutes les autorités et organisations concernées. Le texte proposé se limite à des critères de classification assez généraux et prend directement en compte les intérêts publics à protéger décrits à l'art. 1, al. 2, let. a à d. La référence à ces intérêts est limitée : la protection des intérêts publics selon 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. Ainsi, les données personnelles au sens de la LPD ou les secrets d'affaires, de fabrication ou professionnels ne sont en principe pas classifiées, 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 pour les 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, voire doivent, être classifiées. Ainsi, le traitement de données personnelles sensibles dans un système d'information implique la classification du concept de sécurité de l'information y relatif.

En ce qui concerne les échelons de classification à proprement parler, il est déterminé par la *gravité du préjudice* que la prise de connaissance des informations par des personnes non autorisées peut porter aux intérêts au sens de l'art. 1, al. 2, let. a à d. L'attribution à un échelon de classification dépend du fait que la prise de connaissance par des personnes non autorisées peut :

- *nuire à ces intérêts:* échelon de classification INTERNE ;
- *nuire considérablement à ces intérêts:* échelon de classification CONFIDENTIEL ;
- *nuire gravement à ces intérêts:* échelon de classification SECRET.

Ces qualifications sont des notions juridiques indéterminées qui doivent 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 au sens de 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 prise de connaissance des informations par des personnes non autorisées et le préjudice potentiel pour les intérêts à protéger. Il convient donc de tenir compte de la probabilité du dommage. La classification d'une information correspond dès lors au résultat d'une évaluation du risque et doit ainsi faire état du *besoin effectif de protection* de l'information classifiée.

Lors de l'appréciation du besoin de protection des informations de *nature politique*, il est impératif de faire tout particulièrement preuve de retenue. De fait, la protection de la libre formation de l'opinion et de la volonté des autorités et organisations concernées est prise en compte dans 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, concepts 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 quand aucun intérêt public *majeur* n'est en jeu.

La proposition et ses trois échelons de classification répondent formellement à la réglementation en vigueur de l'OPrl. Comme susmentionné, les valeurs seuils pour la classification dans les divers échelons ont toutefois été rehaussées (concernant le lien avec le principe de la transparence, cf. art. 3, al. 1).

Al. 1: la classification INTERNE est exigée lorsque la divulgation d'une information peut nuire aux intérêts publics au sens de l'art. 1, al. 2, let. a à d. L'échelon INTERNE représente la limite entre une information devant être classifiée et celle qui ne le doit pas. Même si le préjudice exigé pour la classification peut sembler "simple" à la lecture de la disposition, il est nécessaire que la classification soit justifiée par les indications d'un *dommage potentiel qualifié*. Ainsi, le dommage potentiel pouvant résulter de la prise de connaissance de l'information par des personnes non autorisées ne peut pas être simplement négligeable : le préjudice pouvant être porté aux intérêts au sens de l'art. 1, al. 2, let. a à d, doit être bien plus sensible.

Lorsqu'il s'agit d'informations touchant 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 TIC ou de simples plans d'engagement établis pour les forces de sécurité peuvent généralement être classifiés INTERNE. Cependant, il est aussi concevable, par exemple, que la divulgation du calendrier de mise en œuvre d'une mesure concrète puisse avantager indûment certaines personnes. Même si la mesure en soi ne s'en trouvait pas remise en cause pour autant, son application, fût-elle conforme à la loi - et par la force des choses la capacité de décision et d'action de l'autorité fédérale concernée - pourrait s'en trouver pour le moins entravée. En pareil cas, une classification INTERNE, limitée dans le temps, du calendrier en question se justifierait.

Les classifications forfaitaires INTERNE sont, en principe, contraires aux prescriptions. La pratique (hypothétique) d'une unité de l'administration fédérale consistant à classifier d'emblée INTERNE chaque note de discussion et procès-verbal de séance sans tenir compte du besoin réel de protection des informations ne respecterait ni l'esprit de la LTrans ni celui de la réglementation de l'al. 1. Par contre, la classification de procès-verbaux de séances se justifierait, par exemple dans le domaine de la fedpol, *lorsque leur contenu a une portée opérationnelle*. Reste que les informations émanant des travaux des commissions parlementaires *peuvent* généralement être classifiées INTERNE. Cette mesure permet aux parlementaires concernés de savoir clairement quelles informations issues des travaux parlementaires ne vont être destinées qu'à un cercle restreint de personnes afin de protéger la libre formation de l'opinion et de la volonté du Parlement.

Al. 2 : la classification CONFIDENTIEL est exigée lorsque la prise de connaissance d'une information par des personnes non autorisées peut *nuire considérablement* aux intérêts au sens de l'art. 1, al. 2, let. a à d. Par rapport à la réglementation en vigueur selon laquelle seul un "dommage" non qualifié est exigé (art. 6 OPrl), la réglementation proposée se traduit par une élévation des exigences en termes de classification.

La concrétisation détaillée de la notion de *préjudice considérable* doit encore être considérée sous l'angle de la politique de gestion des risques. La formulation utilisée introduit néanmoins une notion de *dommage important* pour la Confédération, par exemple :

- la libre formation de l'opinion et de la volonté des autorités concernées se trouve provisoirement injustement entravée ;
- une organisation concernée est temporairement dans l'incapacité d'agir ;
- l'accomplissement de certaines tâches par une autorité ou organisation est sensiblement entravé sur le long terme ;
- certaines ressources de l'armée ou des organes de sécurité de la Confédération ne peuvent temporairement pas être engagées ;
- la position de la Suisse dans le cadre de 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 classification SECRET (échelon de classification le plus élevé) est exigée lorsque la prise de connaissance d'informations par des personnes non autorisées peut *nuire gravement* aux intérêts au sens de l'art. 1, al. 2, let. a à d. Comme pour les échelons de classification INTERNE et CONFIDENTIEL, la notion clé de *préjudice grave* doit encore être concrétisée. La formulation utilisée introduit néanmoins une notion de *dommage particulièrement grave* pour la Confédération, par exemple :

- une des autorités concernées est temporairement dans l'incapacité de prendre des décisions ou d'agir, voire très sérieusement entravée sur le long terme ;
- une des organisations concernées est momentanément empêchée d'accomplir ses tâches essentielles, voire sérieusement entravée sur le long terme ;
- des ressources très 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 sabotées ;
- la Confédération subit de graves préjudices financiers.

Art. 15

L'al. 1 décrit les conditions d'accès à des informations classifiées, laquelle est, à son tour, une condition permettant de traiter les informations concernées. Le principe du "*besoin d'en connaître*" vaut pour chaque information classifiée. Il n'existe donc pas de droit général à accéder à toutes les informations classifiées. Cela concerne tout autant les organes de vérification, de contrôle et de surveillance qui, bien que disposant d'un droit général à l'information dans les cas d'espèce, doivent, pour chaque information classifiée, justifier que les informations visées sont effectivement nécessaires à l'accomplissement de leurs tâches. En cas de droit d'accès convenu contractuellement, les accords correspondants doivent prévoir l'accès aux informations classifiées et régler leur traitement. La "garantie" d'un traitement correct des informations classifiées implique que les personnes devant 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 CONDFIDENTIEL ou SECRET, la conduite d'un CSP (cf. art. 33 ss) peut aussi constituer une condition supplémentaire.

Al. 2 : la plupart des pays et des organisations internationales avec lesquels la Suisse a conclu un accord sur l'échange d'informations classifiées exigent que leurs informations soient traitées exclusivement par des personnes ayant leur propre nationalité ou la nationalité suisse (clause d'exclusion des Etats tiers). De telles informations ne peuvent en principe pas être rendues accessibles à des personnes d'une autre nationalité. Demeure réservé un accord préalable avec l'auteur de ces informations.

Art. 16

Al. 1 : les informations classifiées doivent être traitées de telle sorte qu'elles soient protégées de toute prise de connaissance non autorisée. Cette protection doit être garantie pendant tout le temps où les informations concernées méritent d'être protégées, ce qui empêche leur archivage tant qu'elles sont encore classifiées.

Selon l'al. 2, les informations classifiées doivent contenir une indication sur l'auteur de la classification. Cette indication est non seulement importante pour la déclassification, l'archivage et la destruction de ces informations, mais aussi pour la prise éventuelle de mesure provisoires de protection lorsque les informations sont menacées (cf. art. 18).

Al. 3 : lorsque la Suisse conclut un accord d'échange d'informations classifiées avec un pays ou une organisation internationale spécifique, le traitement des informations tombant dans le champ d'application de l'accord est réglé par les dispositions particulières de ce dernier. Si aucun accord de ce genre n'existe, le traitement des informations classifiées provenant de l'étranger s'articule autour des dispositions de la LSI et de ses dispositions d'exécution.

Art. 17

L'art. 17, al. 1, prévoit une réserve au droit de procédure de l'Assemblée fédérale et à celui des tribunaux et des ministères publics. Pour la communication d'informations classifiées (par ex. dans le cadre de leur utilisation comme bases de décision ou de moyens de preuve), c'est le droit de procédure concerné qui doit s'appliquer. Les lois de procédure de la Confédération contiennent elles-mêmes 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 jusqu'à quel point les témoins peuvent refuser de s'exprimer compte tenu des obligations légales de maintien du secret (cf. par ex. les 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 les art. 70, 170, 173, al. 2, 194, al. 2, CPP, de même que les art. 45, 48, al. 2, 77, CPM ; cf. encore l'art. 58 de l'ordonnance du 24 octobre 1979 concernant la justice pénale militaire, RS 322.2).

Selon l'al. 2, l'occasion peut néanmoins être donnée, avant une décision relative à la divulgation de certaines informations classifiées, à l'auteur de la classification de s'exprimer sur les motifs de la classification et d'être entendu sur les conséquences possibles d'une telle divulgation. L'autorité ou le tribunal compétent décide alors de la suite de la procédure en fonction de son appréciation de la situation.

Art. 18

Les obligations formulées ici correspondent, dans leur teneur, aux art. 15 et 16, OPrl, actuellement en vigueur. En l'absence d'informations sur l'auteur de la classification, l'annonce doit être faite auprès de l'autorité de surveillance compétente qui décide alors de la suite de la procédure.

Art. 19

L'al. 1 exige d'emblée des autorités concernées (mais pas des organisations) qu'elles déterminent une procédure pour la mise en œuvre et l'amélioration constantes de la sécurité de l'information lors de l'engagement de moyens TIC. La procédure doit fixer les tâches, les compétences et les responsabilités relevant de la sécurité des organes qui planifient l'engagement des moyens TIC, le décident et qui développent, exploitent, gèrent, modifient, entretiennent, contrôlent et, pour finir, mettent hors service ces moyens. La procédure inclut en particulier les dispositions matérielles des art. 20 à 26.

Les autorités fédérales recourent déjà à ce genre de procédure. Cependant, ces procédures doivent être systématisées, et dans la mesure où cela s'impose, complétées. Les principales étapes de la procédure doivent être uniformisées. En outre, le déroulement correct de la procédure n'est souvent pas contrôlé ou alors seulement partiellement. L'efficacité des mesures appliquées, elle, n'est que très rarement vérifiée.

Selon l'al. 2, la compétence de conduire la procédure de sécurité incombe à l'autorité ou organisation qui mandate l'engagement des moyens TIC (bénéficiaire de prestations). Le bénéficiaire de prestations est effet responsable des processus d'affaires et de la mise en œuvre des exigences de sécurité. Il doit donc communiquer clairement ses exigences à ce niveau au service chargé de l'exploitation des moyens TIC en question (fournisseur de prestations).

L'al. 3 fixe le principe selon lequel la procédure de sécurité (ou, pour le moins, les étapes concernées de la procédure) doit être répétée lorsque les risques changent. La sécurité de l'information est dans une situation constante de changement dynamique. Les autorités concernées doivent donc fixer un contrôle périodique, ou en fonction des risques, de l'état de sécurité du moyen TIC engagé et le renouvellement de la procédure.

Art. 20

L'analyse du besoin de protection selon l'al. 1 est la première étape de la procédure de sécurité. Un service qui procède au développement, à l'acquisition ou à la modification d'un moyen TIC, ou confie l'une de ces tâches à des tiers, envisage d'engager ce moyen TIC à certaines fins et pour une durée déterminée. Cette première étape en lien avec la mise en œuvre de la sécurité de l'information consiste à définir, lors de la dé-

termination du but de l'engagement des moyens TIC, les processus d'affaires qui doivent être appuyés par les moyens TIC concernés et à identifier les informations que ces derniers serviront à traiter. Lors de cette phase - soit la phase de planification -, le bénéficiaire de prestations doit évaluer le besoin de protection des informations conformément à l'art. 4, al. 1, ainsi que les effets potentiels d'un dérangement ou d'un usage abusif des moyens TIC concernés sur les intérêts visés à l'art. 1, al. 2. Lors de l'évaluation du besoin de protection, il convient également de tenir compte du fait que les moyens TIC s'insèrent et sont exploités, dans la plupart des cas, dans un environnement technique et/ou logique (appelé architecture) donné. L'identification en temps opportun des interrelations et des interdépendances contribue également à l'application des mesures de sécurité là où elles sont le plus efficace.

A l'heure actuelle, soit on néglige parfois d'évaluer le besoin de protection, soit on ne le fait que lorsque les moyens TIC sont déjà en service. L'application *a posteriori* de mesures de sécurité est généralement bien plus complexe et peut engendrer des coûts sensiblement plus élevés.

L'analyse du besoin de protection fait ressortir les exigences liées à la protection de la confidentialité, de la disponibilité, de l'intégrité et de la traçabilité des informations, ainsi que celles liées à la disponibilité et à l'intégrité des moyens TIC. Cette analyse est aussi déterminante pour la détermination de la catégorie de sécurité afférente aux moyens TIC au sens de l'art. 21.

L'al. 2 règle le cas d'une autorité ou organisation qui entend recourir à de nouvelles technologies (matériels informatiques et logiciels), et donc pas uniquement à de nouveaux moyens TIC. En pareille situation, l'autorité ou organisation concernée doit évaluer les risques liés à l'engagement de cette nouvelle technologie avant de l'engager. L'alinéa précise également que l'autorité ou organisation doit communiquer leur évaluation des risques au service spécialisé de la Confédération en matière de sécurité de l'information. L'information donnée à ce service doit garantir que l'appréciation du risque relatif à ces nouvelles technologies n'est conduite qu'une fois et que les autorités et organisations concernées peuvent en tirer profit. La communication de l'évaluation des risques doit aussi servir à contrôler la conformité des nouvelles technologies aux bases existantes, et même stratégiques.

Les autorités concernées ont la possibilité, en vertu de l'art. 86, al. 1, let. d, de charger le service spécialisé de la Confédération de l'évaluation des risques.

Art. 21

L'art. 21 systématise et unifie, pour les autorités et organisations concernées, les catégories de sécurité relatives aux moyens TIC. Les dispositions en vigueur de l'administration fédérale ne prévoient que deux catégorie de besoin de protection : un besoin général et un besoin élevé. Le nouveau modèle à trois niveaux s'inspire du standard de l'office fédéral allemand chargé de la sécurité informatique (BSI).

Les catégories de sécurité sont avant tout une mesure visant à identifier, sous l'angle des intérêts publics au sens de l'art. 1, al. 2, la criticité d'un moyen TIC déterminé. L'attribution à une catégorie de sécurité permet aussi de savoir quelles exigences de sécurité sont applicables et comment les mesures de sécurité doivent être définies (cf. art. 22 à 24). Pour chaque catégorie de sécurité, le Conseil fédéral doit fixer des exigences et des mesures standard en rapport avec la protection de la confidentialité, de l'intégrité, de la disponibilité et de la traçabilité (cf. art. 88). La standardisation des exigences et des mesures de sécurité est absolument indispensable pour assurer un échange aussi sûr qu'efficace entre autorités. Ses avantages sont significatifs : des exigences claires en matière de sécurité sont d'emblée imposées aux organes de développement et d'acquisition de moyens TIC ; elles leur permettront de savoir immédiatement quelles exigences de sécurité doivent être remplies, ce qui leur simplifiera la tâche lors de la mise en place des mesures de sécurité techniques. Il sera également possible de calculer et de planifier plus simplement et avec une plus grande transparence les coûts liés à la sécurité (les coûts de la sécurité sont les coûts des projets).

Al. 1 : la catégorie de sécurité "protection de base" s'applique aux moyens TIC ne devant pas satisfaire à des exigences de sécurité particulièrement élevées (cf. également art. 22). Les données personnelles, les informations classifiées INTERNE et d'autres informations devant être protégées quant à leur confidentialité, mais ne nécessitant pas une protection particulièrement élevée, peuvent être traitées avec les moyens de cette catégorie.

Al. 2 : pour les moyens TIC de la catégorie de sécurité "protection élevée", des exigences et des mesures de sécurité particulières sont applicables en sus des exigences liées à la protection de base, par exemple l'obligation d'établir un concept de sécurité de l'information et l'assujettissement à un CSP des personnes exploitant, gérant, entretenant ou contrôlant de tels moyens.

- Let. a : les moyens TIC sont classés dans cette catégorie lorsque les informations qu'ils doivent servir à traiter présentent un besoin de protection élevé en termes de confidentialité, d'intégrité, de disponibilité et

de traçabilité. Les diverses exigences sont évaluées en fonction d'un préjudice considérable pouvant menacer les intérêts au sens de l'art. 1, al. 2, qui peut apparaître en cas de violation de l'un des quatre critères de protection susmentionnés. En ce qui concerne les informations classifiées CONFIDENTIEL, le préjudice potentiel est déjà sous-entendu dans la définition de l'échelon de classification ("peut nuire considérablement"). Les moyens TIC devant traiter les informations classifiées CONFIDENTIEL appartiennent donc à la catégorie "protection élevée". Cela vaut aussi pour les moyens TIC engagés pour traiter des données personnelles ou des secrets d'affaires ou de fabrication dans la mesure où l'atteinte à la confidentialité de ces informations peut provoquer un dommage considérable pour la Confédération.

- Let. b : moyen TIC peut aussi être classé dans cette catégorie dans la mesure où une panne peut déranger un processus d'affaires dont l'interruption peut nuire considérablement à la capacité d'agir d'une autorité. La let. b est, de fait, déjà incluse dans la let. a, car les TIC servent uniquement au traitement d'informations et ne visent aucun but qui leur soit propre. Reste que la présente loi reprend le dérangement et l'usage abusif de la capacité de fonctionnement des moyens TIC comme motifs de catégorisation, cette disposition étant ainsi sensiblement plus compréhensible pour de nombreux non-spécialistes.

Al. 3 : les moyens TIC appartiennent à la catégorie de sécurité "protection élevée" lorsque les informations qu'ils doivent servir à traiter ont un très haut besoin de protection en termes de confidentialité, de disponibilité, d'intégrité ou de traçabilité. La structure de cette disposition est identique à celle de l'al. 2; dans ce cas toutefois, le préjudice potentiel requis doit être *grave*. Il s'agit, par exemple, dans ce cas, de moyens TIC devant servir au traitement d'informations classifiées SECRET ou ceux dont le dérangement peut nuire gravement aux intérêts au sens de l'art. 1, al. 2.

Art. 22

Al. 1 : la pratique a montré qu'avec un certain nombre d'exigences et de mesures de sécurité prédéfinies, il est possible de réduire le risque dans une proportion supportable pour une majorité de moyens TIC. L'ensemble de 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 effectuer d'analyses du risque détaillées et coûteuses pour les moyens TIC concernés par cette catégorie. Les autorités concernées doivent définir le niveau minimum de sécurité qu'elles veulent obtenir pour tous leurs moyens TIC. La détermination d'une protection de base n'est dès lors pas une opération technique dont la décision incombe à des experts. C'est une tâche de conduite qui suppose de mettre sur la balance les objectifs de sécurité et les coûts engendrés. Selon l'efficacité de la protection de base, les mesures à appliquer, notamment en termes d'organisation et de personnel, ainsi que les mesures techniques et physiques, peuvent en effet être plus ou moins chères.

L'al. 2 fixe le principe selon lequel tous les moyens TIC, indépendamment de la catégorie de sécurité qui leur est attribuée, doivent remplir les exigences de la protection de base. La protection de base est donc aussi définie comme une fondation sur la base de laquelle les moyens TIC des catégories de sécurité "protection élevée" et "protection très élevée" doivent reposés. Les mesures applicables à la protection de base doivent donc être relativement souples et modulables: si certaines mesures ne sont pas applicables pour un moyen TIC en particulier, d'autres mesures permettant une protection équivalente doivent être prises.

Art. 23

Al. 1 : pour les moyens TIC concernés par les catégories "protection élevée" et "protection très élevée", les exigences et les mesures de sécurité de la protection de base sont insuffisantes. Pour de tels moyens, il est nécessaire de procéder, dans un premier temps, à une analyse du risque quant au moyen TIC concerné. Le point d'orgue de cette analyse réside dans la protection des critères soumis à des exigences élevées de protection. Lorsqu'un moyen TIC atteint la catégorie "protection élevée" en raison d'exigences élevées en ce qui concerne sa disponibilité 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, un concept de sécurité de l'information doit être établi. La responsabilité en incombe au bénéficiaire de prestations ; une collaboration étroite avec le fournisseur de prestations est néanmoins nécessaire. En principe, l'application des mesures techniques relève du domaine de compétence des services qui exploitent les moyens TIC et qui, dès lors, détiennent le savoir-faire sur le plan technique.

L'al. 2 détermine les responsables de l'examen et de l'approbation du concept de sécurité de l'information. Afin d'assurer que ce concept soit contrôlé par un personnel spécialisé, la loi exige que cet examen soit effectué par le préposé à la sécurité de l'information compétent (art. 84). Sa tâche est de vérifier que le concept de sécurité réponde bien aux exigences formelles et techniques, ainsi qu'à celles de l'autorité ou de l'organisation concernée, de sorte à ce que le concept décrive la situation effective dans laquelle se trouve la sécurité

de l'information et présenter un relevé exhaustif des risques résiduels devant être supportés. Idéalement, la préposée à la sécurité de l'information devrait accompagner l'établissement du concept afin de déceler à temps les éventuels problèmes et de les résoudre promptement. Ensuite, l'autorité ou l'organisation concernée doit, elle-même, approuver le concept de sécurité. Cette approbation intervient dès la phase de planification et de conceptualisation, c'est-à-dire avant que le projet TIC n'entre dans sa phase de réalisation, afin de garantir que la direction puisse assumer suffisamment tôt ses responsabilités quant à la sécurité de l'information. La direction ne devrait pas devoir décider uniquement lorsque le moyen TIC est sur le point d'être mis en service (cf. art. 25) et lorsque des moyens financiers considérables ont déjà été engagés.

Al. 3 : le concept de sécurité de l'information n'est pas un document qui doit simplement être établi à une seule occasion - par exemple lors de la planification de l'engagement d'un moyen TIC - pour être ensuite laissé tel quel. Souvent, les mesures prévues ne correspondent pas à celles effectivement prises. C'est pourquoi le concept doit être constamment mis à jour pour qu'il puisse refléter l'état actuel de la sécurité. Il doit également être adapté en cas de modification des risques.

Art. 24

L'al. 1 exige, pour chaque moyen TIC devant être autorisé en vue de sa mise en service, la preuve que la procédure de sécurité s'est déroulée conformément aux prescriptions et que les mesures de la protection de base et, le cas échéant, celles définies dans le cadre du concept de sécurité de l'information ont été appliquées. Les autorités concernées devront décider qui doit effectuer le contrôle de conformité.

Al. 2 : pour les moyens TIC relevant de la catégorie de sécurité "protection très élevée", la loi exige en outre que l'efficacité réelle des mesures prises soit contrôlée. Lors de ce contrôle, le moyen TIC concerné est soumis à de vraies attaques afin d'identifier d'éventuelles lacunes dans la sécurité et des faiblesses exploitables (par ex. par des *tests de pénétration*). Le but étant, bien sûr, de combler lesdites lacunes avant la mise en service du moyen TIC concerné. Le contrôle d'efficacité n'est exigé que pour les moyens TIC les plus critiques, ceux de la catégorie "protection très élevée", car ils engendrent un coût non négligeable (entre 0,5 et 2% de l'investissement total pour le moyen TIC concerné).

Art. 25

Al. 1 : l'organe de direction de l'autorité ou de l'organisation bénéficiaire des prestations est responsable de la sécurité de l'information. Il lui est donc demandé qu'il autorise lui-même l'engagement de ses moyens TIC du point de vue de la sécurité.

Al. 2 : en délivrant l'autorisation de mise en service relative à la sécurité, l'autorité ou l'organisation signifie qu'elle connaît les risques résiduels identifiés et qu'elle est également prête à les assumer. Si elle estime que ces risques sont encore trop élevés, elle peut refuser de délivrer l'autorisation et exiger l'application de mesures complémentaires visant à les réduire.

Art. 26

Pour que la gestion des risques soit efficace, il est nécessaire d'avoir une vue d'ensemble sur tous les moyens TIC engagés. Les autorités et organisations concernées doivent donc inventorier les moyens TIC qu'elles engagent. La responsabilité de chacun de ces moyens doit pouvoir être imputée à une personne ou à un organe spécifique.

Pour chaque moyen TIC répertorié, l'inventaire doit contenir, entre autres, la catégorie de sécurité, le nom des personnes ou organes compétents, les documents relatifs à la sécurité, ainsi que toutes les informations du système qui sont indispensables à sa remise en service suite à un dérangement ou à une panne.

Art. 27

Les autorités, organisations ou tiers qui exploitent des moyens TIC sur mandat des autorités ou organisations concernées portent la responsabilité du maintien de la sécurité de l'information durant l'exploitation de ces moyens. Les fournisseurs internes de prestations tombent tous dans le domaine d'application de la présente loi et doivent donc aussi appliquer les art. 19 à 26 dans le cadre de leurs activités. Par contre, les fournisseurs externes de prestations sont considérés comme des tiers au sens de l'art. 8 et doivent être tenus contractuellement à respecter les mesures dictées par la présente loi. Les autorités et organisations compétentes qui mandatent l'exploitation de moyens TIC doivent fixer au fournisseur leurs exigences de sécurité en rapport avec les moyens TIC concernés.

Dans le cadre de l'exploitation, le fournisseur de prestations assure, dans le contexte de la sécurité de l'information, les capacités et activités suivantes :

- la gestion du réseau, comme les rôles et les responsabilités, la structure du réseau, les audits de sécurité ;

- la gestion du trafic, comme la configuration des éléments du réseau, la réglementation des accès du management, le cryptage et l'authentification, les pare-feu, les accès externes, les accès via les technologies sans fil ;
- l'exploitation du réseau, comme le descriptif détaillé des prestations et le respect des SLA, le monitoring (surveillance du réseau incluse), la gestion de la mise en service, du changement et du cycle de vie, la gestion des incidents et de la sécurité, la gestion des capacités et des ressources, la gestion des accidents et de la remise sur pied ;

  l'établissement de rapports d'audit à l'intention du bénéficiaire de prestations.

Art. 28

Les personnes devant traiter des informations ou utiliser des moyens TIC de la Confédération doivent remplir certaines exigences. Il est de la responsabilité de l'employeur ou du mandant de veiller à ce que respectivement leur personnel ou leurs mandataires remplissent ces exigences.

- Let. a : lors du choix des employés ou des mandataires, les critères de sélection doivent tenir compte du degré de confidentialité des informations ou de la criticité des moyens TIC que ces personnes devront traiter ou utiliser. Les employeurs et les mandants sont responsables du choix de leur personnel et de leurs mandataires. L'assujettissement d'une personne à un CSP ne la délie pas cette responsabilité.
- Let. b : les autorités et organisations concernées doivent suffisamment instruire les membres de leur personnel. Dans le domaine de la sécurité de l'information, une formation unique ne suffit pas. Le personnel et les mandataires doivent régulièrement être instruits et sensibilisés à cette problématique. Une attention particulière doit être accordée à la formation des cadres.
- Let. c : lorsque le personnel ou les mandataires doivent traiter des informations soumises à de fortes exigences en termes de préservation de la confidentialité, ils sont tenus au maintien du secret. Le personnel de la Confédération qui est soumis à la LPers doit, en vertu de l'art. 22 de cette même loi, préserver le secret de fonction. Concernant les tiers chargés d'exécuter des mandats pour la Confédération, l'obligation du maintien du secret doit être stipulée contractuellement, de même qu'une énumération claire des conséquences que peuvent entraîner une violation de cette obligation.

Art. 29

Quiconque travaille ou exerce un mandat pour la Confédération doit, selon les circonstances, avoir accès à des informations, des moyens TIC ou des locaux pour effectuer ses tâches. L'al. 1 pose un principe central pour la sécurité de l'information. 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 sensiblement réduit lorsqu'une personne ne peut pas traiter, sans motif, des informations d'un autre domaine.

L'al. 2 exige une gestion constante de ces autorisations. 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 du mandant. 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 au niveau interne.

L'al. 3 exige un processus adapté au contrôle régulier des autorisations.

Art. 30

Les mesures physiques de protection servent à réduire les risques engendrés par des menaces physiques. Les actions répréhensibles commises par l'homme comptent, par exemple, parmi ces menaces, comme l'espionnage, le vol, le vandalisme ou le sabotage. Tombent également dans cette catégorie les dommages provoqués par des éléments comme la chaleur, le feu, l'eau, la poussière, les vibrations, etc. L'évaluation des mesures destinées à la protection physique, appelée *protection des objets*, relève de la compétence de fedpol, qui agit en collaboration avec l'OFCL. Pour certains domaines du DDPS et de l'armée toutefois, c'est la PIO, en collaboration avec armasuisse et l'OFCL, qui est compétente.

L'al. 1 fixe le principe de base selon lequel les autorités et organisations concernées doivent assurer la protection physique de leurs informations et moyens TIC dans leurs locaux. L'objectif est, en particulier, d'empêcher tout accès non autorisé aux informations et moyens TIC, par exemple par des contrôles d'accès, des caméras vidéo, des systèmes de verrouillage, des locaux et des conteneurs sécurisés, des appareils de

destruction de documents et de supports de données, des mesures de protection visuelle, etc. Pour prévenir les dommages causés par les éléments, il est par exemple préconisé d'installer des installations d'alarme incendie, d'extinction automatique ou des paratonnerres.

L'al. 2 règle le cas des informations et des moyens TIC accessibles au public. Il s'agit, pour une part, d'informations et de moyens TIC qui sont emmenés hors de leur endroit habituel (bureau) et qui - en dehors du périmètre de sécurité usuel - doivent recevoir une protection adéquate. Il s'agit aussi 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, comme les zones de livraison et de chargement.

Art. 31

La LSI utilise la notion de *zone de sécurité* pour qualifier les locaux et les domaines dans lesquels des informations classifiées CONFIDENTIEL ou SECRET sont souvent traitées ou des moyens TIC des catégories de sécurité "protection élevée" ou "protection très élevée" sont exploités et qui, de ce fait, nécessitent une protection particulière. La délimitation de ces zones ou locaux en zones de sécurité constitue une mesure physique en faveur de la sécurité de l'information ; cette mesure est déjà appliquée pour partie 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. Les dispositions d'exécution du Conseil fédéral définiront vraisemblablement deux sortes de zones de sécurité en tenant compte, pour chacune d'elles, de la criticité des informations ou des moyens TIC. Les mesures à prendre dans ces deux sortes de zones devront être conçues en fonction du risque. Le Conseil fédéral et les organes fédéraux compétents en matière de protection des objets (fedpol, OFCL, PIO, armasuisse) fixeront, en collaboration avec le service spécialisé de la Confédération en matière de sécurité de l'information, des mesures techniques standard pour les zones de sécurité (cf. art. 88).

L'al. 1 fixe, en premier lieu, les conditions permettant de désigner une zone de sécurité selon la LSI : les zones concernées sont celles destinées au traitement très fréquent d'informations classifiées CONFIDENTIEL ou SECRET ou à l'exploitation de moyens TIC appartenant aux catégories de sécurité "protection élevée" ou " protection très élevée". Contrairement à la législation d'autres pays ou organisations internationales (cf. également al. 5), les autorités et organisations concernées au sens de la LSI ne sont pas tenues de désigner de tels emplacements comme zones de sécurité. C'est leur appréciation du risque qui décide du besoin effectif de la désignation.

L'al. 2 dispose que seules les personnes identifiées et autorisées peuvent accéder à une zone de sécurité. L'autorisation d'accès doit donc être nécessaire à l'accomplissement d'une tâche précise. Cela exige un contrôle approprié des accès et un protocole des entrées.

L'al. 3 règle les pouvoirs particuliers de l'autorité ou organisation établissant une zone de sécurité:

- Let. a : pour le contrôle d'accès, l'autorité ou l'organisation peut recourir à des méthodes d'identification biométrique (par ex. empreintes digitales ou lecteur oculaire). Ces méthodes sont sensiblement plus fiables que l'identification par une pièce de légitimation. Elles sont déjà appliquées dans certains domaines.
- Let. b : l'introduction de certains objets dans une zone de sécurité peut être limitée. Les appareils de prises de vues ou de sons (incl. smartphones ou notebooks avec fonctions correspondantes) exigent généralement une autorisation spéciale.
- Let. c : les domaines des zones de sécurité considérés comme 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 en permanence par des appareils vidéo.
- Let. d : 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 de personnes afin d'éviter que des personnes amènent sans autorisation des appareils (cf. let. b) ou repartent avec des informations (par ex. avec une clé mémoire USB).
- Let. e: pour la mise en œuvre efficace des dispositions relatives à la sécurité de l'information, il est également nécessaire de pouvoir également contrôler les bureaux dans une zone de sécurité. Lors de ces contrôles, le respect de ce que l'on appelle la "clean desk policy" (*la politique du bureau bien rangé)* est aussi mis à l'épreuve (aucune information sensible ne doit traîner sur le bureau ou ailleurs, le PC 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 même en l'absence de la personne concernée, par exemple de nuit.

Selon l'al. 4, l'autorité ou l'organisation peut avoir la possibilité d'exploiter, si nécessaire et dans certaines zones de sécurité seulement, une installation perturbatrice au sens de l'art. 34, al. 1ter, de la loi du 30 avril 1997 sur les télécommunications (LTC; RS 784.10). Le besoin effectif d'une telle installation ainsi que les conditions de son exploitation sont établis à l'aune de la LTC.

A l'art. 5, les dispositions relatives aux zones de sécurité selon les conventions de droit international public (art. 90) et les dispositions correspondantes relatives à la protection des ouvrages militaires sont réservées. Dans les deux cas, l'instauration d'une zone de sécurité ou de protection ne constitue pas une option, mais une obligation (cf. par ex. ISA CH-UE).

2.1.3 Contrôles de sécurité relatif aux personnes

Art. 32

Le contrôle de sécurité relatif aux personnes (CSP) est une mesure préventive de protection contre les infractions venant de l'intérieur. Il doit permettre d'identifier le risque de voir les intérêts au sens de l'art. 1, al. 2, menacés par une personne donnée dans l'exercice d'une activité sensible. Le CSP consiste donc à estimer l'éventualité qu'une personne donnée puisse menacer, intentionnellement ou par négligence, les intérêts visés à l'art. 1, al. 2. C'est pourquoi des données pertinentes sur le parcours de cette personne sont récoltées. Sur la base de ces données, le risque pour la sécurité est évalué par des spécialistes spécialement formés à cette tâche (*profileurs de risques)*. Il va de soi qu'une telle évaluation ne peut être absolument fiable dans tous les cas.

Après avoir pris connaissance de cette évaluation, l'autorité ou l'organisation concernée décide seule si elle entend assumer un éventuel risque élevé, le réduire en posant certaines conditions ou l'éviter en n'engageant pas la personne concernée ou en la licenciant.

Pour comprendre la réglementation proposée, deux points important sont à relever.

- L'évaluation du risque pour la sécurité par les services spécialisés responsables du CSP (services spécialisés CSP) constitue une recommandation. La décision d'éventuellement engager ou mandater une personne dépend uniquement de l'autorité qui engage ou qui mandate. Le risque n'est donc jamais assumé par le service spécialisé CSP responsable de l'évaluation. Cela vaut autant pour une déclaration de risque (un risque pour la sécurité existe) que pour une déclaration de sécurité (aucun risque pour la sécurité n'a été identifié). Les supérieurs hiérarchiques ne sont pas non plus déchargés de leur obligation d'identifier, voire d'écarter, des risques potentiels élevés auxquels une personne au bénéfice d'une déclaration de sécurité peut être liée.
- Le CSP doit être engagée en fonction des risques réels. La présente loi fixe des conditions claires à la réalisation du contrôle. Cela ne signifie pas que les fonctions qui avaient fait l'objet d'un CSP selon la LMSI soient aujourd'hui moins importantes ou ne puissent pas être exposées à un risque élevé. Pour ces fonctions et toutes celles qui ne sont pas contrôlées, la responsabilité de l'évaluation du risque pour la sécurité est uniquement et seulement assumée par les organes hiérarchiques. L'introduction proposée d'un nouvel l'art. 20*a* LPers mettra, à l'avenir, des moyens adéquats (extraits du casier judiciaire, du registre des poursuites et des faillites) à la disposition des employeurs au sens de l'art. 3 LPers.

Art. 33

L'art. 33 règle, en relation avec l'art. 34, al. 1, l'assujettissement du personnel des autorités et organisations concernées au CSP. Les autorités concernées (c'est-à-dire hormis les organisations au sens de l'art. 2, al. 2) doivent édicter, pour leur domaine de compétence, une liste des fonctions dont l'accomplissement des tâches implique *nécessairement* l'exercice d'une activité sensible et qui doivent, dès lors, être contrôlées. Concernant les conditions matérielles permettant l'inscription d'une fonction sur cette liste, le système actuel de la LMSI n'est toutefois pas repris purement et simplement. Comme le mentionne le ch. 1.2.4., le critère de la *régularité* est mis à part, en particulier dans le cadre du traitement d'informations classifiées. La question décisive pour l'assujettissement du personnel fédéral au CSP est de savoir si la personne titulaire d'une fonction *doit* exercer une activité sensible pour accomplir sa tâche. Si l'exercice d'une telle activité est *effectivement nécessaire*, alors - et alors seulement - la fonction *doit* être reportée sur la liste de celles 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. Pour accomplir ses tâches, elle doit traiter des informations classifiées et, parfois, accéder à des ouvrages militaires. Sa fonction doit figurer sur la liste.

- Un collaborateur de l'Administration fédérale des finances doit, à titre exceptionnel, évaluer les effets d'une demande classifiée CONFIDENTIEL formulée par le DFJP à l'intention du Conseil fédéral. En situation normale, d'autres collaborateurs sont responsables du traitement de pareilles affaires, mais ils sont soit en vacances, soit en arrêt maladie. Cette tâche n'entre en principe 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 y relatives ne doivent donc pas être reprises dans la liste, à moins qu'à la fonction particulière ne soient attribués les 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 *de iure* pas pertinent. Même si le cahier des charges d'une fonction donnée ne prévoit que 5% du temps de travail pour accomplir des tâches sensibles, cette fonction doit être inscrite sur la liste, et cela même lorsque la personne titulaire de cette fonction n'a, peut-être, pas dû accomplir de pareilles tâches pendant un temps relativement longtemps. L'*éventualité* de l'exercice d'une activité sensible liée à cette fonction ne justifie par contre en aucun cas le report d'une fonction sur la liste.

Cette approche restrictive implique que les autorités et organisations concernées ont un aperçu net des processus d'affaires et des domaines d'activité, tant internes que transversaux, liés nécessairement à l'exercice d'activités sensibles. Prendre du recul dans ce domaine et garder une vue d'ensemble constitue, en parallèle, 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 (ou cahiers des charges) des différentes fonctions doivent décrire précisément les tâches dont l'exécution nécessite l'exercice d'une activité sensible. En outre, les autorités et organisations concernées sont tenues, indépendamment de tout assujettissement à un CSP, de prendre les mesures d'organisation et relatives aux personnes qui s'imposent afin de réduire à son 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 concernées. Ainsi, les listes des fonctions devront donc figurer dans des ordonnances ou des règlements. Concernant l'administration fédérale, il s'agit, en principe, de maintenir le système selon lequel le Conseil fédéral désigne ces fonctions dans les annexes de l'OCSP (cf. ch. 1.2.4). Toutefois, en raison de la réglementation sur les compétences au sens de la LOGA, il pourra, s'il le désire, continuer d'habiliter les départements et la Chancellerie fédérale à établir leurs propres listes détaillées.

Art. 34

Al. 1: l'art. 34 précise qui doit faire l'objet d'un CSP.

- Let. a : pour le personnel des autorités et organisations concernées, seules les personnes dont la fonction figure sur les listes visées à l'art. 33 font l'objet d'un CSP. La liste a donc un caractère impératif. Les exceptions sont réglées aux al. 3 et 4.
- Let. b : les tiers font l'objet d'un CS lorsqu'ils exercent une activité sensible dans le cadre d'un mandat.
- Let. c : dans le contexte international, les conditions relatives au CSP sont réglées par les conventions de droit international public correspondantes. En principe, la règle de l'al. 2 s'applique.

Al. 2 : le principe de l'al. 1, let. b, s'applique aussi aux personnes devant exercer une activité sensible sur mandat d'une autorité étrangère ou internationale.

L'al. 3 règle le cas d'une fonction remplissant les critères visés à l'art. 33, mais qui n'est pas encore répertoriée dans la liste correspondante. Dans ce cas, le contrôle peut être réalisé avec l'accord exprès de l'autorité concernée. Une modification rapide de la liste s'impose alors.

Al. 4 : les membres des autorités élus par le peuple ou les magistrats nommés par l'Assemblée fédérale ne font l'objet d'un CSP, même s'ils exercent souvent une activité sensible.

Art. 35

Concernant les degrés de contrôle, la LMSI ne donne pas de règles précises. Le principe de légalité exige cependant, en raison de l'atteinte profonde dans les droits fondamentaux des personnes assujetties à un CSP, que les modalités les plus importantes de cette atteinte soient définies au niveau de la loi au sens formel. Etant donné que les degrés de contrôle déterminent l'ampleur de l'atteinte, ils doivent être réglés dans la LSI.

Le texte proposé prévoit désormais (cf. ch. 1.2.4) les deux degrés de contrôle ci-après:

- Let. a : le contrôle de sécurité de base s'applique aux activités sensibles dont l'exercice inadéquat ou contraire aux prescriptions peut nuire considérablement aux intérêts visés à l'art. 1, al. 2. Vu le potentiel de dangerosité mentionné, il s'agit donc implicitement : (a) du traitement d'informations classifiées CONFIDENTIEL ; (b) de l'administration, de l'exploitation, du contrôle ou de la maintenance des moyens TIC 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 pouvoir accéder aux zones de protection 2 d'un ouvrage militaire.
- Let. b : 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 TIC relevant de la catégorie de sécurité "protection très élevée" ; (c) de l'accès à des zones de sécurité où les activités visées au let. (a) et (b) sont exercées. Un CSP élargi est également nécessaire pour pouvoir accéder aux zones de protection 3 d'un ouvrage militaire.

C'est aux autorités concernées qu'il incombe de déterminer les degrés de contrôle pour les fonctions et mandats correspondants.

Art. 36

Les services spécialisés CSP ne peuvent, en aucun cas, entamer et mener un CSP de leur propre chef ; ils doivent toujours être mandatés à cet effet. D'une part, on ne saurait confier à la plus haute autorité le soin d'ouvrir directement toutes les procédures de contrôle, mais d'autre part, on ne peut pas non plus autoriser n'importe quel organe à confier des mandats de cette nature. L'art. 36 prévoit dès lors que les autorités concernées désignent, dans leur domaine de compétence, les services habilités à ouvrir une procédure de contrôle et à attribuer aux services spécialisés CSP le mandat y afférent. Il s'agit là d'une compétence formelle. A cet égard, on précisera que le service chargé de l'ouverture de la procédure (service requérant) n'est souvent pas celui qui, en vertu de l'art. 44, décide, après le contrôle, de confier l'activité sensible (instance de décision).

Le Conseil fédéral peut aussi, s'il l'estime utile, habiliter certains tiers à ouvrir un CSP. Cela concerne en particulier les entreprises exerçant souvent des activités sensibles au profit de la Confédération et qui sont au bénéfice d'une déclaration de sécurité pour les entreprises au sens de l'art. 68. Tel peut aussi être le cas pour les cantons ou les organisations au sens de l'art. 2, al. 2, let. e.

Art. 37

En principe, la réalisation d'un CSP nécessite le consentement de la personne concernée (al. 1). Seules l'armée et la protection civile peuvent, selon l'al. 2, réaliser des CSP sans l'accord des personnes concernées. Cette exception s'impose sans quoi 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.

Art. 38

Le droit en vigueur (art. 19, al. 3, LMSI) exige que le CSP soit effectué avant l'attribution de la fonction ou du mandat. L'application de la réglementation en vigueur (en soi logique) ne peut toutefois être réalisée sans une augmentation importante des ressources en personnel des services spécialisés CSP. C'est pourquoi l'al. 1 revoit la règle applicable au personnel des autorités et organisations concernées : il exige dorénavant que, pour ce groupe de personnes, la procédure de contrôle soit *ouverte* avant l'attribution de la fonction. Les employeurs conservent naturellement le droit d'attendre la déclaration du service CSP avant d'engager 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 (art. 43, al. 1, let. b), d'une déclaration de risque (art. 43, al. 1, let. c) ou d'une déclaration de constatation (art. 43, al. 1, let. d) peut être un motif de dénonciation 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. 20a LPers).

L'al. 2 reprend les dispositions du droit en vigueur (art. 19, al. 3, LMSI) et résulte d'une enquête de la Commission de gestion du Conseil national à propos de la nomination du commandant de corps R. Nef au poste de chef de l'armée. La réglementation en question a été décidée par la modification de la LMSI du 23 décembre 2011 et est entrée en vigueur le 1er juillet 2012.

L'al. 3 précise quand le CSP doit être réalisé pour les tiers chargés d'exécuter un mandat sensible pour une des autorités ou organisations concernées. Dans ce cas, la réglementation actuelle s'applique encore : le CSP doit être terminé avant que la personne puisse être chargée d'exercer l'activité sensible concernée. La raison qui motive 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 lorsqu'il s'agit de 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.

Selon l'al. 4, le moment auquel des personnes doivent faire l'objet d'un CSP en vertu d'un accord international est déterminé en fonction des dispositions dudit accord. Même si l'accord ne le règle pas expressément, une déclaration de sécurité est toujours exigée avant que l'activité sensible puisse être exercée.

Art. 39

Cette disposition règle la collecte des données pour les deux degrés de contrôle. La collecte des données s'inspire largement de la législation en vigueur et de la pratique. En raison du passage de trois à deux degrés de contrôle, cette collecte est organisée de telle sorte que le contrôle de base soit renforcé, notamment par la possibilité d'obtenir des renseignements à partir du registre des poursuites et des faillites.

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. Cela s'avère particulièrement important lors d'un contrôle élargi car la réduction à deux degrés ne doit pas entraîner une augmentation massive des coûts relatifs aux CSP. Le Conseil fédéral, qui édictera les dispositions d'exécution pour ces contrôles, pourra aussi déterminer quelles données *devront* être collectées et à quel moment.

Al. 1 : pour le contrôle de base, les sources ci-après peuvent être consultées.

- Let. a à d : le casier judiciaire et les banques de données du SRC, des autorités de police et de sécurité de la Confédération et des cantons peuvent renseigner sur la fiabilité et sur les éventuels antécédents d'une personne. La LSIP habilite les services spécialisés CSP à consulter en ligne l'index national de police (cf. ch. 2.6). Ils peuvent dorénavant prendre connaissance, aisément et efficacement, des données des organes de police cantonaux qui y sont reliés. Il va de soi que les résultats éventuels doivent être pondérés en regard de l'activité envisagée pour la personne concernée et remis dans leur contexte.
- Let. e : les informations obtenues à partir des registres des poursuites et des faillites sont nécessaires pour pouvoir évaluer - dans l'éventualité d'un risque pour la sécurité qui pourrait, par exemple, résulter en cas de corruption - la situation financière de la personne concernée.
- La let. e introduit une nouveauté : les documents et résultats des contrôles de sécurité antérieurs peuvent aussi être utilisés.
- Let. g : cette lettre doit préciser explicitement que les services spécialisés CSP peuvent aussi accéder aux données que contiennent les sources publiques (par ex. à partir d'Internet en utilisant un moteur de recherche comme Google). De tels besoins peuvent se justifier par la fonction envisagée et des indices spécifiques au cas. Les informations émanant de réseaux sociaux non destinés au public et réservés à un cercle fermé de personnes ne peuvent toutefois pas être collectées.

Al. 2 : lors d'un CSP élargi, il est possible de consulter les sources ci-après, en plus de celles visées à l'al. 1.

- Let. a : 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 prestations fiscales.
- Let. b : 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.
- Let. c : lors du contrôle élargi, la situation financière de la personne concernée est analysée dans les détails. C'est pourquoi les données des établissements financiers et des banques avec lesquels la personne concernée entretient des rapports d'affaires peuvent être systématiquement collectées.
- Let. d : l'audition de la personne concernée sert à vérifier des faits qui ne ressortent pas ou pas clairement de la consultation des registres.

L'al. 3 règle la collecte des données à l'étranger. Les données qui doivent être collectées en Suisse selon les al. 1 et 2, peuvent aussi, au besoin, être collectées à l'étranger.

L'al. 4 exige que les services spécialisés CSP doivent, dans le cadre de l'évaluation du risque pour la sécurité, pouvoir acquérir suffisamment de données pertinentes sur une période suffisamment longue. Si ces conditions ne sont pas remplies, il n'est pas possible de juger si un risque pour la sécurité existe ou non. Le cas échéant, la personne concernée est interrogée à titre complémentaire, conformément à l'al. 5. Cela peut, par exemple, être le cas lorsque la personne, avant le contrôle, a séjourné longtemps dans un pays où il n'est pas

possible d'obtenir des données ou en tous les cas pas des données fiables. La notion de *données suffisantes sur une période suffisamment longue* est expressément floue. La formulation de l'art. 19, al. 3, OCSP, selon laquelle les services spécialisés CSP doivent, pour le moins, disposer de données couvrant la période de cinq ans précédant l'ouverture de la procédure du contrôle de sécurité de base et la période de dix ans précédant l'ouverture de celle du contrôle de sécurité élargi, a été partiellement critiquée comme étant disproportionnée et trop absolue. Deux solutions sont donc envisageables : soit le Conseil fédéral précise, dans le cadre de ses dispositions d'exécution relatives aux CSP, la notion de *un nombre suffisant de données sur une période suffisamment longue*, soit la définition de cette notion relève de l'appréciation des services spécialisés CSP.

L'al. 5 prévoit que les services spécialisés CSP peuvent auditionner les personnes concernées, indépendamment du degré de contrôle lorsque, dans le cadre de la récolte de données, ils découvrent des indices en rapport avec la sécurité. Une telle audition peut avoir lieu lorsque le service spécialisé CSP compétent n'a pas pu obtenir de données suffisantes sur une période suffisamment longue au sens de l'al. 4. Cette audition personnelle ne doit pas être confondue avec celle visée à l'al. 2, let. d. Cette dernière peut être réalisée sans la présence d'indices sur un risque pour la sécurité et n'est pas limitée dans son contexte. Pour faire la lumière sur des éléments particulièrement pertinents pour la sécurité ou pour obtenir un complément de données sur une plus longue période, services spécialisés CSP peuvent aussi interroger des tiers. De telles auditions ne peuvent être menées qu'avec l'assentiment de la personne contrôlée et celui des tiers concernés.

Al. 6 : il arrive que les données nécessaires à l'évaluation du risque concernent non seulement les personnes contrôlées, mais aussi des tiers. Cela peut, par exemple, être le cas pour des extraits de comptes bancaires d'une personne mariée. L'al. 6 prévoit alors que 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 représente à chaque fois l'obtention de l'assentiment des tiers pour traiter des données serait disproportionnellement élevée pour les services spécialisés CSP. Pour des raisons de transparence, les services spécialisés CSP doivent donc informer ces tiers sur le traitement des données. Si le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés, l'art. 18a, al. 4, let. b, LPD s'applique.

Art. 40

La participation des autorités à la procédure reste gratuite (al. 1). 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 le cadre de dispositions d'exécution.

Art. 41

Al. 1 : La procédure déjà engagée est suspendue lorsque la personne concernée revient sur son accord ou lorsqu'elle refuse de participer à la procédure, ou encore lorsque, pour une autre raison, elle n'entre plus en considération pour la fonction prévue ou pour l'exécution du mandat (par ex. en cas d'insolvabilité de l'entreprise pour laquelle la personne concernée aurait dû travailler).

L'al. 2 prévoit que tant la personne concernée que le service requérant doivent être informés de la suspension de la procédure. La personne concernée est, dès lors, réputée non contrôlée et ne peut exercer l'activité sensible en question ou la fonction envisagée.

L'al. 3 dispose que la suspension de la procédure entraîne la destruction de toutes les données et de tous les documents déjà récoltés par le service spécialisé CSP. La déclaration de suspension et le procès-verbal de destruction ne sont pas concernés. Toutefois, ni la déclaration de suspension ni le procès-verbal de destruction ne doivent contenir de données pouvant porter préjudice à la personne concernée. Les dispositions d'exécution du Conseil fédéral régleront la durée de conservation de ces deux documents.

Art. 42

Dans le passé, il a à plusieurs reprises été regretté que la réglementation de la LMSI ne précise pas explicitement ce qu'il faut entendre par « *risque pour la sécurité* ». Une nouvelle disposition s'impose donc à cet égard. Celle-ci reflète, par analogie, la jurisprudence y relative du Tribunal administratif fédéral et du Tribunal fédéral. Il va de soi qu'il n'existe pas de méthode purement quantitative lorsqu'il s'agit d'évaluer un risque en rapport avec les agissements ou omissions des humains. D'où le recours à une méthode qualitative qui repose sur la présence et l'interaction de facteurs de risque.

Al. 1: 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 dont l'élément déclencheur doit être évité. En l'occurrence, il s'agit d'un *préjudice considérable ou grave porté aux intérêts visés 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 de la présente loi, lorsque *la probabilité est élevée* de voir la personne concernée exercer l'activité sensible particulière de manière inadéquate ou contraire aux prescriptions, causant de ce fait, pour le moins, une atteinte considérable aux intérêts visés à l'art. 1, al. 2.

L'al. 2 précise clairement que les services spécialisés CSP doivent avant tout se concentrer sur la probabilité de survenance d'un incident. Par la force des choses, l'appréciation d'une telle probabilité restera toujours une prévision assortie d'incertitudes. 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 constatables autant que possible objectivement, 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 fiabilité 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 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 ce qui concerne la sécurité. Il est impossible de spécifier au niveau de la loi les indices et corrélations qui pourraient témoigner du manque de fiabilité d'une personne, de sa vulnérabilité au chantage ou de l'insuffisance de ses capacités de jugement et de décision : il conviendra de les mettre en lumière dans le cadre de chaque appréciation concrète.

L'al. 3 précise clairement qu'un risque pour la sécurité peut exister sans faute commise par la personne concernée. Le CSP est une mesure préventive de protection des intérêts publics supérieurs face à des actes commis intentionnellement ou par négligence de l'intérieur, qui se fonde sur une menace objective et non sur un comportement fautif, ce qui n'est pas le cas par exemple du 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'Etat ou les intérêts du pays priment les intérêts de la personne concernée. Il est également établi que 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 la couleur politique de cette personne, ne sont pas recevables.

Enfin, l'al. 4 doit assurer l'indépendance des services spécialisés CSP lors de l'évaluation du risque. Le CSP ne doit pas être détourné à des fins politiques.

Art. 43

L'al. 1 règle les diverses déclarations des services spécialisés CSP dans lesquelles figurent les résultats des appréciations.

- Let. a : lorsque le service spécialisé CSP compétent parvient à la conclusion que l'exercice de l'activité sensible par la personne concernée ne représente pas de risque pour la sécurité, il établit une déclaration de sécurité.
- Let. b : lorsque le service spécialisé CSP compétent constate qu'un certain risque pour la sécurité existe en cas d'exercice de l'activité sensible par la personne concernée, mais que celui-ci peut être atténué à certaines conditions, il établit une déclaration de sécurité assortie de réserves et émet, à l'intention de l'instance chargée de confier l'activité sensible (instance de décision), les recommandations de mesures qui s'imposent.
- Let. c : lorsque le service spécialisé CSP parvient à la conclusion que l'activité sensible exercée par la personne concernée représente un risque, il émet une déclaration de risque.
- Let. d : lorsque le risque relatif à une personne ne peut pas être évalué correctement par manque de données au sens de l'art. 39, al. 4, le service spécialisé CSP émet une déclaration de constatation.

L'al. 3 vise à offrir à la personne concernée l'assurance de pouvoir défendre équitablement ses intérêts à ce stade précoce de la procédure, nonobstant le fait qu'en rapport avec un acte matériel, le droit d'être entendu ne soit pas garanti d'office (cf. art. 51, al. 3). La disposition prévoit que la personne concernée doit avoir la possibilité d'exprimer son avis avant l'établissement des déclarations visées aux let. b à d. De fait, cela signifie que lorsque le projet de déclaration selon les 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. 44

En vertu de l'al. 1, la déclaration de sécurité doit être communiquée par écrit à la personne contrôlée et à l'instance de décision. Bien que la déclaration ne constitue pas une décision au sens de l'art. 5 PA (cf. art. 51, al. 3), la personne concernée doit avoir la possibilité de prendre connaissance des résultats de l'évaluation et, le cas échéant, de requérir une décision. Sur le fond, cet alinéa reprend le droit en vigueur (art. 21, al. 2 à 4, LMSI).

L'al. 2 dispose que, pour les personnes nommées par le Conseil fédéral, la déclaration doit être communiquée au département requérant.

L'al. 3 règle le cas où un CSP est mené alors que la personne concernée fait déjà l'objet d'un contrôle en rapport avec une autre activité au sens des let. a à c (par ex. selon l'art. 20*b* LPers). En ce cas, le service spécialisé CSP compétent doit pouvoir informer l'instance de décision concernée des résultats du contrôle principal. Les dispositions concernant le contrôle de fiabilité, au sens de l'art. 20*b* LPers et de l'art. 14 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.

L'al. 4 permet aux services spécialisés CSP d'informer l'organe compétent pour statuer sur la remise ou le retrait de l'arme militaire, au sens de l'art. 113 LAAM, des résultats du contrôle. Lorsque le service spécialisés CSP compétent constate, dans le cadre d'un contrôle, que la personne concernée - astreinte au service militaire - présente un potentiel élevé de violence, il doit en informer les instances militaires pour que celles-ci puissent trancher la question de la remise de l'arme personnelle.

Art. 45

L'art. 45 prévoit que si les services spécialisés CSP disposent d'indices attestant un éventuel risque pour la sécurité et s'il y a péril en la demeure, ils doivent en informer, à titre préventif, les instances compétentes au sens de l'art. 44, avant même l'achèvement de la procédure. Ces instances peuvent alors prendre les mesures de sécurité provisoires nécessaires. Cette disposition correspond à celle de l'art. 20 OCSP.

Art. 46

L'al. 1 précise que les déclarations des services spécialisés CSP n'ont qu'une valeur de recommandation pour l'instance de décision. Cela 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 organes de la ligne dans les décisions concernant le personnel, mais uniquement d'informer l'instance de décision du risque lié à l'attribution d'une activité sensible à une personne donnée.

Al. 2 : avant toute décision, l'instance de décision doit néanmoins prendre connaissance de la déclaration du service spécialisé CSP compétent, seule façon pour elle de prendre une décision en tenant compte du risque éventuel.

L'al. 3 habilite l'instance de décision de mettre des conditions à l'exercice de l'activité sensible par la personne concernée, notamment en se fondant sur les recommandations du service spécialisé CSP. Ces conditions constituent des mesures de sécurité visant à réduire le risque identifié et relevant généralement du droit du personnel. L'instance de décision peut, par exemple, exiger que, régulièrement, la personne rende compte de sa situation financière ou se soumette à des tests de dépistage de consommation de stupéfiants, etc. A cet égard, il est important de préciser que ces conditions s'appliquent exclusivement à l'exercice de l'activité sensible et non à l'accomplissement d'autres tâches. Lorsque, par exemple, l'instance de décision décide que la personne concernée ne peut exercer l'activité sensible en question, mais que rien n'empêche qu'elle accomplisse d'autres tâches non sensibles pour la sécurité, elle ne peut imposer aucune condition sur la base de cette disposition. Généralement, les conditions les mieux adaptées à la situation sont recommandées par le service spécialisé CSP compétent. L'instance de décision n'est toutefois pas liée par ces recommandations et peut fixer elle-même ses propres conditions. Lorsque, néanmoins, elle n'applique pas les recommandations, elle doit en informer le service spécialisé CSP compétent par écrit (cf. art. 47, let. b).

Art. 47

Le présent article statue sur le devoir d'information de l'instance de décision. Lorsque sa décision ne tient pas compte de l'appréciation du service CSP, elle doit en informer ce dernier. L'information peut prendre la forme d'une remarque dans le système d'information, adressée au service CSP, conformément aux art. 52 à 54. Il s'agit que le service CSP ait toujours un aperçu de la pratique des instances de décision et en tire des enseignements utiles pour l'appréciation du risque.

Art. 48

Lorsque la personne concernée est au bénéfice d'une déclaration de valeur au moins équivalente et encore d'actualité, un nouveau contrôle doit, pour des raisons d'économie de procédures, si possible être évité. L'art. 48 prévoit donc la possibilité de renoncer, dans un tel cas, à procéder à un contrôle. Dans la pratique, cette disposition ne pose généralement pas de problèmes lorsqu'une déclaration de sécurité est émise pour un degré de contrôle similaire ou ayant la même importance. Des problèmes peuvent cependant 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 dans le cadre du traitement d'informations classifiées SECRET, alors que ce risque peut être supportable lorsqu'il s'agit du traitement d'informations classifiées CONFIDENTIEL. Le Conseil fédéral devra concrétiser cette disposition potestative au niveau de l'ordonnance.

Art. 49

Les autorités étrangères ne concèdent l'accès aux informations et au matériel classifiés, de même qu'aux zones protégées et aux zones de sécurité, qu'aux seules personnes ayant subi un contrôle de sécurité. De même, le service spécialisé CSP compétent n'est habilitée à délivrer un certificat de sécurité à usage international qu'aux personnes qui ont obtenu une déclaration de sécurité.

Art. 50

L'al. 1 règle la répétition ordinaire du CSP. La loi renonce à prescrire des intervalles fixes pour ces répétitions. Elle se contente de fixer des lignes directrices. La raison en est que la répétition des contrôles devra, à l'avenir, dépendre du besoin réel de sécurité. Le Conseil fédéral devrait en régler les détails dans ses dispositions d'exécution. Bien entendu, il peut aussi laisser cette compétence aux autorités et organisations concernées dans la mesure où il ne prescrit rien lui-même.

L'al. 2 donne la possibilité au service requérant ainsi qu'à l'instance de décision de solliciter une répétition du CSP en dehors du cycle ordinaire de répétition. 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 présentant un lien potentiel avec l'activité sensible qu'elle exerce. Cette disposition correspond à la législation en vigueur au niveau de l'ordonnance (cf. art. 18, al. 2, OCSP).

Le Conseil fédéral, en vertu de sa compétence d'édicter des dispositions complémentaires (cf. art. 55), devra aussi décider s'il entend introduire d'autres répétitions anticipées. Un *contrôle complémentaire* pourrait, par exemple, s'avérer utile pour juger de l'efficacité des mesures ou conditions ordonnées dans le cadre des déclarations de sécurité assorties de réserves.

Art. 51

Les al. 1 et 2 règlent la consultation des documents du contrôle par la personne concernée et la rectification des données erronées. Malgré l'adaptation de sa formulation, la réglementation correspond à celle du droit en vigueur (cf. art. 21, al. 2, LMSI).

Al. 3 : selon le droit en vigueur, les déclarations des services spécialisés CSP sont édictées sous forme de décisions (cf. art. 20, al. 3 LMSI, et art. 22 OCSP). La qualification de « décision » est toutefois juridiquement fausse car ces déclarations ne sont que des recommandations (cf. art. 21, al. 4, LMSI, et art. 46, al. 1, LSI). Les droits des personnes ayant fait l'objet d'un CSP ne sont affectés que si l'instance de décision décide, en fin de compte, de ne pas confier la fonction ou le mandat en question. Juridiquement parlant, les déclarations correspondent plutôt au résultat d'une évaluation que les autorités et organisations mandatent souvent avant d'engager des personnes-clés (assessment). Dans ces cas, l'évaluation des assesseurs n'est pas non plus communiquée sous la forme d'une décision attaquable dans la mesure où l'employeur est libre de prendre la décision qu'il veut. Les déclarations des services spécialisés CSP représentent des actes matériels au sens de l'art. 25a PA. Dans la situation précédemment décrite, cela signifie que la personne concernée peut, dans un délai de 30 jours à compter de la remise de la déclaration, exiger du service CSP qu'il émette une décision attaquable. La suite de la procédure est réglée par la PA. La réglementation prévue aura, en outre, l'effet de diminuer la charge occasionnée par les CSP touchant les conscrits lors du recrutement militaire. Les services

CSP pourront communiquer simplement les résultats de l'évaluation aux conscrits et n'émettre de décision complète qu'en cas d'opposition.

Art. 52

La formulation de l'art. 52 correspond à celle du droit en vigueur (cf. art. 144 à 149 LSIA).

L'al. 1 dispose que les services spécialisés CSP doivent engager un système d'information pour réaliser et gérer les CSP.

Al. 2 : chaque service spécialisé CSP est responsable de gérer conformément au droit les données qu'il traite.

Al. 3 : parmi ces données peuvent également se trouver des données sensibles et des profils de la personnalité (art. 3, let. c et d, LPD).

L'al. 4 énumère les données traitées dans le système d'information.

Al. 5 : les données traitées en dehors du système d'information doivent être signalées dans ledit système. En l'occurrence, il s'agit en particulier de documents sur papier et d'enregistrements sonores effectués lors des auditions.

Art. 53

La formulation de l'art. 53 correspond à celle du droit en vigueur (cf. art. 144 à 149 LSIA).

Al. 1 : procédure d'accès en ligne

- Let. a : les services spécialisés CSP ont accès aux données dont ils sont responsables.
- Let. b : les services requérants ont uniquement accès aux données qu'ils ont eux-mêmes collecté lors de l'ouverture d'une procédure ainsi qu'aux résultats du CSP.
- La let. c détermine les données auxquelles les instances de décision ont accès.
- La let. d détermine les données auxquelles les préposés à la sécurité de l'information ont accès pour accomplir leurs tâches de contrôle.
- Let. e : les organisations de la Confédération et des cantons qui collectent des données ont uniquement accès à celles concernant l'identité de la personne assujettie au contrôle ou qui a été contrôlée. Elles ont principalement besoin de ces données pour savoir sur quelle personne elles doivent entreprendre des recherches et livrer des données.

Al. 2: interfaces

- La let. a détermine les données auxquelles l'autorité chargée de la procédure de sécurité relative aux entreprises (art. 56 ss) a accès.
- Let. b : pour que l'Etat-major de l'armée puisse continuer de traiter efficacement les demandes de visite à l'étranger impliquant l'accès à des informations classifiées, les données visées à l'art. 52, al. 4, let. a et d, doivent être transférées par une interface dans le système d'information sur les demandes de visite.
- La let. c, ch. 1 à 3, détermine les données auxquelles l'Etat-major de conduite de l'armée a accès pour contrôler l'accès aux zones de sécurité, accomplir ses tâches légales en rapport avec le système de gestion du personnel de l'armée et effectuer le recrutement des conscrits ainsi que du personnel prévu pour la promotion de la paix.

Al. 3: d'autres organisations de la Confédération (en particulier les fournisseurs de prestations TIC) ont besoin des résultats des CSP pour contrôler l'accès aux zones de sécurité.

Al. 4: les services CSP communiquent aux autorités et organisations concernées des listes et des statistiques lorsqu'elles en ont besoin dans l'accomplissement de leurs tâches de contrôle au sens de la présente loi. Ces listes ne sont donc fournies que pour répondre à ce besoin. La communication de ces listes s'effectue en dehors du système d'information visé à l'art. 52.

Art. 54

La formulation de l'art. 54 correspond à celle du droit en vigueur (cf. art. 144 à 149 LSIA, et OCSP).

L'al. 1 crée la base juridique nécessaire à l'enregistrement sonore des auditions.

Al. 2 : la durée de conservation des données ne doit pas dépasser dix ans. Si une personne a déjà subi plusieurs contrôles, les données remontant à plus de dix ans s'y rapportant doivent être détruites.

L'al. 3 règle la destruction des données d'une personne déjà contrôlée qui ne va pas occuper le poste considéré (cf. également art. 41).

Al. 5 : les données traitées en dehors du système d'information (cf. art. 52, al. 5) doivent être conservées et détruites conformément aux al. 2 et 3. Les remarques inscrites dans le système sont détruites lors de la destruction de ces données.

Al. 6 : les dossiers devant être archivés selon les prescriptions d'archivage ne doivent pas être détruits.

Art. 55

L'art. 55 dresse la liste des domaines pour lesquels le Conseil fédéral doit édicter des dispositions complémentaires (normes primaires). En l'occurrence, il ne s'agit pas simplement de dispositions d'exécution pour lesquelles le Conseil fédéral, sur la base de l'art. 182 Cst., est sans autres compétent.

- Let. a et b : en termes d'organisation, il est à noter qu'il existe actuellement deux services spécialisés CSP. L'un est à la Chancellerie fédérale et contrôle, à l'intention du Conseil fédéral, les cadres du plus haut échelon ainsi que le personnel de l'autre service spécialisé CSP. Ainsi, actuellement, il réalise exclusivement des CSP élargis accompagnés d'auditions. L'autre service spécialisé CSP est au DDPS, à l'Etat-major de l'armée, auprès de la Protection des informations et des objets, et réalise la grande majorité des CSP. La let. b donne le choix au Conseil fédéral de décider s'il entend maintenir ou non cette organisation.
- Let. c à d : le Conseil fédéral doit, en application de l'art. 16, al. 2, LPD, édicter des dispositions complémentaires sur la protection des données dans le cadre du CSP. Sont en particulier concernées l'organisation des compétences et les responsabilités pour la protection des données (incl. la sécurité des données) en lien avec le système d'information visé à l'art. 52, ainsi que le contrôle indépendant périodique du traitement des données.

2.1.4 Procédure de sécurité relative aux entreprises

Art. 56

Concernant le but de la PSE, cf. ch. 1.2.5.

Art. 57

Al. 1 : le sens donné par la présente loi à *entreprise* ne correspond pas, à proprement parler, 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 le contrôle : celui où une autorité ou organisation concernée envisage d'adjudiquer à une entreprise un mandat sensible, selon l'art. 56, 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 sensible émanant des autorités suisses doivent se faire contrôler par l'Etat dans lequel elles ont leur siège légal. Les compétences et les modalités de contrôle sont réglées par des conventions internationales au sens de l'art. 90. Dans de tels cas, les autorités étrangères de sécurité exigent la preuve que le soumissionnaire bénéficie d'une déclaration de sécurité au moyen du « formulaire d'information sur l'habilitation de sécurité des entreprises » (*Facility Security Information Sheet*) ou - si l'entreprise n'a pas encore été contrôlée - l'ouverture d'une procédure de contrôle.
- Inversement, l'al. 1, let. b, traite le cas des entreprises qui ont leur siège en Suisse et soumissionnent pour des mandats émanant de l'étranger, et qui 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'Etat où l'entreprise a son siège.

L'al. 2 dispose qu'une PSE ne peut en aucun cas avoir lieu sans l'assentiment de l'entreprise concernée. 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.

Al. 3 : dans le cas visé à l'al. 1, let. b, la Confédération n'est pas directement intéressée par l'ouverture de la procédure. Le Conseil fédéral réglera la question des coûts au niveau de l'ordonnance.

Art. 58

Al. 1 : la PSE n'est effectuée 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 interrompue. Ainsi, selon la let. d, cela 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 prescrit qu'après l'arrêt de la procédure, toutes les données et dossiers en rapport avec elle doivent être détruits.

Art. 59

L'al. 1 dispose tout d'abord que la PSE est le fait d'un service spécialisé (service spécialisé PSE). Ainsi, un seul service doit (comme aujourd'hui) s'occuper de cette procédure au sein de la Confédération. Le service spécialisé PSE n'agit que sur *demande* (et non sur mandat) des autorités ou organisations concernées. Ces dernières sont toutefois tenues de déposer une demande lorsqu'elles entendent confier un mandat sensible à une entreprise.

Al. 2 : les autorités concernées doivent déterminer, dans leur domaine de compétence, qui dépose la demande d'ouverture de la procédure. En fonction de leurs besoins au niveau organisationnel, il peut s'agir d'un service central ou de tout organe compétent pour attribuer des mandats sensibles à des entreprises du secteur privé.

L'al. 3 règle les compétences d'une autorité étrangère ou internationale mandat sensible attribué par une autorité étrangère ou internationale. Généralement, l'ouverture de la procédure est 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 détails de ces procédures doivent être réglés par voie d'ordonnance.

Art. 60

Al. 1 : après le dépôt de la demande d'ouverture d'une PSE, le service spécialisé PSE tout d'abord que les conditions sont réunies (par ex. l'attribution d'un mandat sensible) avant d'engager, le cas échéant, la PSE.

Al. 2 : 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 renoncer à la PSE pour des raisons d'économie administrative. Lorsque le mandat, placé par exemple sous le contrôle de l'autorité ou l'organisation émettrice du mandat (adjudicateur), est effectué dans les locaux de cette dernière 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. 61

Après l'ouverture de la procédure, le service spécialisé PSE prend contact avec l'adjudicateur pour discuter des détails du mandat. Il fixe, en accord avec ce dernier, les exigences de sécurité 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 exigences de sécurité sont également fixées pour cette phase-là. Cela se produit régulièrement lorsque la prise de connaissance d'informations classifiées est nécessaire en vue de l'établissement d'une offre.

Art. 62

La notion de qualification est prise dans le sens de la systématique du droit des marchés publics. Certes, le maintien de la sécurité de l'information n'est pas un critère formel de qualification au sens de l'art. 9 LMP ; le projet l'introduit cependant pour l'exécution de mandats sensibles au sens de la présente loi.

Al. 1: l'adjudicateur doit annoncer au service spécialisé PSE les entreprises en lice pour l'adjudication.

Al. 2 : le service spécialisé PSE examine si ces entreprises sont qualifiées, du point de vue de la sécurité de l'information, à exécuter le mandat sensible ou si son attribution aux entreprises contrôlées représenterait un risque pour la sécurité au sens de l'art. 64. Si un tel risque existe en lien avec un soumissionnaire, ce dernier n'est pas qualifié quant à la sécurité de l'information.

Al. 3 : le service spécialisé PSE ne doit pas être soumis à des directives pour l'évaluation de la qualification. En l'occurrence, il s'agit de pouvoir procéder à cette évaluation en dehors de toute considération des intérêts de politique économique (cf. également art. 42, al. 4, pour le CSP).

Art. 63

L'art. 63 crée la base légale formelle de la collecte des données permettant d'évaluer, sous l'angle de la sécurité, la qualification des entreprises, conformément à l'art. 62, al. 2.

L'al. 1 dresse la liste des données permettant au service spécialisé PSE d'évaluer la qualification. Les modalités des requêtes y afférentes et de la transmission d'informations doivent être réglées au niveau de l'ordonnance.

- Aux termes de la let. b, les données nécessaires sont surtout recueillies auprès de l'entreprise elle-même, avec son consentement (cf. également art.57).
- La let. b crée une base légale formelle pour les requêtes que le service spécialisé PSE adresse au Service de renseignement de la Confédération.
- La let. c permet au service spécialisé PSE de récolter si nécessaire, auprès du registre du commerce ou sur Internet, des données sur l'entreprise. Pareilles recherches peuvent livrer des renseignements importants sur la fiabilité de l'entreprise (cf. art. 39, al. 1, let. g, pour le CSP).

Al. 2 : cette possibilité est utilisée, par exemple, lorsque des entreprises étrangères soumettent leur candidature aux autorités fédérales pour l'obtention d'un mandat sensible.

Art. 64

Cette disposition constitue un pendant à l'art. 42 (évaluation, lors du CSP, du risque pour la sécurité). Les mécanismes d'évaluation du risque sont identiques quant à leur principe.

Selon l'al. 1, un risque pour la sécurité existe lorsque des indices concrets donnent à penser que l'entreprise, selon une probabilité élevée, exécuterait le mandat sensible de manière inadéquate ou contraire aux prescriptions.

L'al. 2 expose ensuite les trois raisons principales d'une probabilité élevée de voir le mandat exécuté de manière inadéquate ou contraire aux prescriptions:

- Let. a : cela peut, par exemple, être le cas lorsque des données saisies montrent que l'entreprise a commis des actes punissables qui ont un effet sur la sécurité de l'information.
- Let. b : cette disposition doit permettre d'empêcher la remise d'informations sensibles à une entreprises qui, en raison de ses rapports de propriété, de sa structure organisationnelle ou de ses relations d'affaires, pourrait, par exemple, être contrôlée par des services de renseignement étrangers ou des organisations à vocation criminelle.
- Let. c : lorsque l'entreprise est en raison individuelle ou que l'attribution du mandat rend indispensable la présence de certaines personnes (par ex. parce qu'elles sont des experts qui ne peuvent être remplacés, ou parce qu'elles gèrent l'entreprise et que le mandat ne pourrait être exécuté en leur absence), l'établissement d'une déclaration de risque dans le cadre d'un CSP pour ces personnes peut avoir pour conséquence que l'entreprise, dans son ensemble, soit considérée comme un risque pour la sécurité.

L'al. 3 dispose que le risque pour la sécurité soit fondé sur des faits concrets liés à l'entreprise, indépendamment de toute faute de l'entreprise elle-même ou de son personnel, par exemple lorsqu'elle est contrôlée par des personnes liées à un service de renseignement étranger ou à une organisation criminelle.

Art. 65

Al. 1 : 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 interjeter un recours auprès du Tribunal administratif fédéral (art. 76, al. 3). L'adjudicateur peut poursuivre la procédure de soumission ou les négociations contractuelles avec les entreprises ne présentant pas de risque pour la sécurité. Il n'est pas autorisé à recourir et n'est donc qu'informé de l'évaluation.

Al. 2 : lorsque le service spécialisé PSE décèle un risque pour la sécurité en relation avec une entreprise, l'adjudicateur ne peut conclure de contrats avec elle ou lui adjuger le mandat. Il exclut de la procédure d'adjudication l'entreprise jugée non qualifiée en regard de la sécurité. L'adjudicateur est ainsi lié à l'évaluation de l'autorité chargée de la procédure. La raison tient en ce qu'une entreprise, au sens de la présente loi, déclarée sûre reçoit de l'Etat ce que d'aucuns pourraient appeler 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.

Art. 66

Al. 1 : 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.

Al. 2 : pour que la sécurité de l'information au sein de l'entreprise appelée à exercer l'activité sensible soit assurée, des mesures adéquates doivent être prises au niveau de l'organisation et du personnel, de même que sur le plan technique et physique. Un concept de sécurité doit donc définir comment les exigences de sécurité de l'information, définies dès le lancement de la procédure par le service spécialisé PSE et l'adjudicateur, doivent être mises en œuvre (cf. art. 61).

Al. 3 : en règle générale, les entreprises ont déjà pris des mesures de sécurité dans les domaines les plus variés ; le service spécialisé PSE se contente alors de les vérifier, voire de les compléter le cas échéant. Toutes les mesures nécessaires qui ont déjà été prises et celles qui s'imposent en sus sont définies dans le concept au sens de l'al. 2. Le service spécialisé PSE collecte directement les données nécessaires auprès de l'entreprise.

Art. 67

Al. 1 : le personnel appelé à exercer une activité sensible est assujetti à un CSP. Il est contrôlé en application de l'art. 34, al. 1, let. b et, le cas échéant, let. c, ou de l'art. 34, al. 2. Le degré de contrôle est déterminé en fonction de l'art. 35.

Al. 2 : après le CSP, le service spécialisé PSE décide péremptoirement si l'activité sensible peut, ou non, être confiée à la personne concernée.

Art. 68

Al. 1 : dès que l'entreprise a pris les mesures de sécurité qui s'imposent et, ainsi, apporté la preuve que le concept de sécurité est mis en place, le service spécialisé PSE émet une déclaration de sécurité pour les entreprises (DSE). Cette déclaration est une décision selon l'art. 5 PA.

Al. 2 : lorsque l'entreprise n'applique pas le concept de sécurité - très rare en pratique -, elle ne répond pas aux exigences fixées pour la sécurité de l'information. Dans ce cas, le service spécialisé PSE refuse de lui remettre la déclaration de sécurité et décide de suspendre la procédure. Le service spécialisé PSE doit lui accorder un délai lui permettant de remplir ses obligations avant de prendre sa décision de refus.

Al. 3 : la notification de la DSE, ou son refus, constitue une décision - contrairement à la déclaration de sécurité émise dans le cadre d'un CSP - car elle a des effets juridiques immédiats sur les parties intéressées (cf. art. 69 ss). Si l'entreprise n'est pas d'accord avec la décision prise par le service spécialisé PSE, elle peut déposer un recours devant le Tribunal administratif fédéral (art. 76, al. 1). La décision est également notifiée à l'adjudicateur car celle-ci ne doit pas confier le mandat sensible à l'entreprise qui s'est vue refuser la déclaration de sécurité (art. 69). A ce moment précis de la procédure, l'adjudicateur aura probablement déjà versé des sommes considérables dans le projet. De ce fait (contrairement à l'art. 65, al. 1), il est également en droit de déposer un recours.

Al. 4 : la limitation à cinq ans de la validité de la DSE doit garantir une réévaluation à intervalles réguliers de la qualification au sens des art. 62 ss. De cette façon, il est possible de tenir compte des changements importants qui surviennent dans l'entreprise et qui influent sur la sécurité de l'information.

Art. 69

L'adjudicateur est lié à la décision du service spécialisé. Il ne peut pas confier de mandat sensible à l'entreprise qui s'est vue refuser la DSE (cf. art. 68, al. 3). 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. 38, al. 3, dans le domaine des CSP.

Art. 70

Al. 1 : les entreprises au bénéfice d'une DSE sont tenues de collaborer. Elles ont pour principale obligation d'appliquer régulièrement les mesures prévues par le concept de sécurité.

Selon l'al. 2, ces entreprises 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 informer le service spécialisé PSE et l'adjudicateur de tout incident relatif à la sécurité.

Art. 71

L'al. 1 habilite le service spécialisé PSE à contrôler, au sein de l'entreprise, le respect des mesures relatives au mandat prévues par le concept de sécurité. Il peut contrôler les domaines de l'entreprise où le mandat sensible est exécuté. Il peut aussi consulter les documents de l'entreprise relatifs au mandat. Le contrôle peut, de par sa nature, s'effectuer inopinément. Il ne peut se dérouler qu'en compagnie ou en présence d'un membre de l'entreprise, généralement le préposé à la sécurité.

Al. 2 : le service spécialisé PSE, face à des indices concrets donnant lieu de penser que la sécurité de l'information est menacée, peut prendre les mesures de sécurité qui s'imposent. 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 sûreté. Cela s'applique également aux cas où, suite à la faillite d'une entreprise, des documents ou moyens TIC doivent être retirés rapidement de la masse de la faillite.

Art. 72

Al. 1 : lors de l'attribution de nouveaux mandats sensibles, les entreprises au bénéfice d'une DSE sont réputées qualifiées au sens de l'art. 62 et leur qualification n'est donc pas réévaluée. Une procédure simplifiée est appliquée ; le Conseil fédéral la réglera au niveau de l'ordonnance.

Selon l'al. 2, il s'agit néanmoins de contrôler, face à des cas de cette nature, s'il faut adapter le concept de sécurité. Ce devrait, par exemple, être le cas si l'entreprise concernée, qui ne devait traiter jusque-là « que » des informations classifiées CONFIDENTIEL, était également chargée du traitement d'informations classifiées SECRET.

Art. 73

Les entreprises dont le siège est en Suisse et qui entendent soumissionner pour un mandat sensible à l'étranger doivent présenter aux autorités de l'endroit une attestation de sécurité officielle émise par les autorités suisses (cf. art. 57, al. 1, let. b, et art. 68, al. 1). Le service spécialisé PSE délivre donc une attestation correspondante à l'usage international aux entreprises bénéficiant d'une DSE valable.

Art. 74

Al. 1 : la DSE est révoquée lorsque l'entreprise ne remplit pas ses obligations au sens de l'art. 70 ou qu'une évaluation au sens de l'art. 62, menée dans le cadre de la répétition de la procédure, décèle un risque pour la sécurité.

La révocation doit, selon l'al. 2, être notifiée sous la forme d'une décision contre laquelle il est possible de recourir devant le Tribunal administratif fédéral, conformément à l'art. 76, al. 3. 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 parlant, à ce que la DSE ne soit pas révoquée.

Art. 75

La PSE est répétée lorsque le mandat sensible traité par l'entreprise est encore pendant alors que la durée de validité de la DSE est échue. 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 n'est attribué, le service spécialisé PSE, pour des raisons d'économie de procédure, ne répétera pas le contrôle. Si des indices concrets donnent à penser que de nouveaux risques pour la sécurité sont apparus suite à des changements importants survenus dans l'entreprise, la procédure est répétée.

Art. 76

L'al. 1 accorde aux organes de l'entreprise, lors de la PSE, différents droits (consultation, rectification, suppression, contestation) analogues à ceux énumérés à l'art. 51, al. 1 pour le CSP.

Selon l'al. 2, il est possible de recourir contre les décisions du le service spécialisé PSE auprès du Tribunal administratif fédéral. Cette norme dispose explicitement que la disposition de l'art. 32, al. 1, let. a, de la loi sur le Tribunal administratif fédéral (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 le service spécialisé PSE se fonde sur des informations relevant du SRC qui ne doivent être divulguées ni à l'entreprise ni au public, les dispositions correspondantes relatives à la procédure sont applicables (art. 27 et 28 PA).

Art. 77

Al. 1 : le service spécialisé PSE engage un système d'information pour réaliser et gérer la PSE. Ce système existe depuis des années et a récemment été entièrement reconçu. Sa base juridique actuelle (art. 150 ss LSIA) doit, pour des raisons de systématique, être reprise dans la présente loi.

Al. 2 : étant donné que le système peut contenir des données personnelles sensibles et des profils de la personnalité, il a besoin d'une base ancrée dans une loi formelle (art. 17, al. 2, LPD) que les art. 77 à 80 créent.

L'al. 3 établit la liste exhaustive de toutes les données enregistrées dans le système d'information.

L'al. 4 règle la responsabilité du traitement conforme au droit des données dans le système et la sécurité du système même.

Art. 78

L'art. 78 crée la base légale nécessaire pour rendre certaines données accessibles à des organes déterminés.

- Let. a : les adjudicateurs ont accès aux données qui les concernent ainsi qu'à la liste de toutes les entreprises au bénéfice d'une DSE. Cela leur permet de savoir rapidement si une entreprise bénéficie ou non d'une DSE.
- Let. b : le Conseil fédéral peut, de par son droit d'édicter des dispositions d'exécution, habiliter certaines entreprises à ouvrir elles-mêmes des CSP dans leur propre domaine. De ce fait, ces entreprises doivent 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 niveaux de contrôle CSP des membres du personnel de leur entreprise.

Art. 79

La disposition relative à la conservation et à la destruction des données correspond, *mutatis mutandis*, à celle proposée pour le CSP (cf. art. 54).

Art. 80

Le Conseil fédéral doit édicter les dispositions complémentaires qui s'imposent pour la PSE.

2.1.5 Sécurité de l'information pour les infrastructures critiques

A propos de la stratégie nationale de protection de la Suisse face aux cyberrisques, cf. les ch. 1.1.2.2 et 1.2.6.

Les art. 81 à 83 règlent les tâches de la Confédération visant à soutenir les exploitants des infrastructures critiques (IC) dans le domaine de la sécurité de l'information. Il n'est pas nécessaire d'être soumis à la loi selon la législation spéciale au sens de l'art. 3, al. 3 afin de participer au partenariat public-privé dans le cadre de MELANI et de bénéficier des prestations de la Confédération. La collaboration a lieu sur une base volontaire.

Art. 81

En vertu de l'al. 1, le soutien de la Confédération concerne notamment la détection précoce et l'appréciation des dangers et des menaces pesant sur des informations et des systèmes d'information dignes de protection, l'évaluation du risque correspondante, la détection des incidents, le rétablissement de la sécurité de l'information à la suite d'incidents et l'analyse a posteriori de ces incidents. Pour les exploitants d'IC, il s'agit de prestations importantes de la Confédération.

L'al. 2 dispose que la Confédération gère d'une part un service national d'alerte précoce 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'IC 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 (*governmental computer emergency response team*, GovCERT), qui effectue des analyses techniques – p. ex. de logiciels malveillants – et peut fournir des recommandations concernant des mesures techniques concrètes afin de prévenir des dangers ou de détecter des incidents. Les services chargés de tâches liées à l'al. 2 sont aussi autorisés à simuler des systèmes vulnérables (*honeypots*) sur des réseaux afin d'améliorer leurs connaissances.

Aux termes de l'al. 3, le Conseil fédéral veille à garantir à cet effet un échange sécurisé d'informations entre la Confédération et les exploitants d'IC ainsi qu'entre les exploitants eux-mêmes. Souvent, les dangers et les menaces ne concernent pas un objectif unique, mais plusieurs organisations actives dans un secteur spécifique, voire tous les exploitants d'IC dans l'ensemble des secteurs. Cependant, le recours aux prestations visées à l'art. 81 ainsi que la participation au partenariat public-privé sont totalement volontaires. Le principe de la propre responsabilité des exploitants d'IC est ainsi implicitement confirmé. Un échange permanent d'informations doit instaurer la transparence et la confiance; il profite non seulement aux exploitants d'IC, qui peuvent acquérir un savoir-faire, mais également aux autorités fédérales en leur qualité de propriétaires et d'exploitants d'IC. Ils peuvent obtenir des informations importantes afin d'évaluer leurs risques propres et prévenir des dangers.

Art. 82

Les informations au sujet de dangers et d'indicateurs relatifs à des incidents dans le domaine de la sécurité de l'information contiennent souvent des données concernant des ressources d'adressage dans le domaine des télécommunications (p. ex. adresses IP, adresses électroniques, noms de domaine). Ces ressources

d'adressage impliquent qu'elles se réfèrent (en théorie du moins) à des personnes précises ou identifiables, ou à des appareils ou des raccordements de télécommunication pouvant être attribués à une personne précise ou identifiable. En conséquence, les ressources d'adressage doivent potentiellement être considérées comme des données personnelles et nécessitent une base juridique pour être traitées, conformément à l'art. 4, al. 3, ainsi qu'à l'art. 17, al. 1, LPD.

L'al. 1 prévoit donc que les services compétents pour les tâches se rapportant à l'art. 81 sont autorisés à traiter des données personnelles. Néanmoins, l'identification de la personne concernée est souvent impossible ou possible uniquement moyennant un investissement considérable, en particulier lorsque les ressources d'adressage sont enregistrées à l'étranger. Elle n'est toutefois pas nécessaire à la prévention des dangers. Puisque l'identification n'a généralement pas lieu, le traitement des données peut s'effectuer sans que les personnes concernées s'en aperçoivent ni qu'elles puissent en être informées. Par conséquent, le présent article doit être considéré comme une *lex specialis* dérogeant à l'art. 4, al. 4, LPD. En revanche, si l'on soupçonne qu'une ressource d'adressage (suisse) ou un appareil utilisant la ressource d'adressage en question est employé abusivement par des personnes non autorisées et que cela constitue un danger, on peut, le cas échéant, identifier l'utilisateur légitime de la ressource d'adressage et l'informer de cette utilisation abusive. L'identification ne doit toutefois pas nécessairement être effectuée par les autorités compétentes. S'il est, par exemple, question 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 auront donc la possibilité de prendre des mesures afin d'empêcher de nouvelles utilisations abusives et de dénoncer une éventuelle infraction.

L'al. 2 octroie la compétence de traiter des données personnelles liées à des poursuites ou à des sanctions administratives ou pénales. En vertu de l'art. 3, let. c, ch. 4, LPD, ces données sont considérées comme sensibles, et les services étatiques ont besoin d'une base juridique formelle afin de traiter de telles données, conformément à l'art. 17, al. 2, LPD. L'échange d'informations concernant des infrastructures criminelles et des utilisations abusives de ressources d'adressage peut s'avérer nécessaire afin de prévenir des dangers ou de détecter des incidents. Même si l'on ne communique pas 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 compétence définie dans cet alinéa vise à empêcher que l'échange en question ne puisse plus avoir lieu dès l'instant où une enquête pénale ou une sanction administrative concernant une ressource d'adressage est introduite.

L'al. 3 permet aux exploitants de moyens TIC ainsi qu'aux fournisseurs de services TIC de transmettre volontairement aux services concernés au sens de l'art. 81 des informations liées à des dangers et à des incidents dans le domaine de la sécurité de l'information. Cette disposition les autorise à donner des indications concernant les prestations, les connexions et d'autres activités qu'ils fournissent afin de prévenir des dangers et, ainsi, d'éviter des dommages. Elle leur permet également de traiter légalement les données personnelles correspondantes. Puisqu'une telle transmission de données peut porter préjudice à la garantie des droits de la défense lors d'une éventuelle procédure, les données acquises de la sorte ne peuvent pas être utilisées dans un but judiciaire. Les différentes règles relatives à l'administration des preuves continuent de s'appliquer aux procédures judiciaires.

Art. 83

Le Conseil fédéral doit régler par voie d'ordonnance la répartition des tâches et la collaboration entre les services assumant les tâches visées à l'art. 81. Ces derniers doivent faire front commun vis-à-vis des exploitants d'IC. En revanche, le Conseil fédéral reste libre d'organiser ces services à l'interne comme il l'entend afin d'exécuter les tâches de la Confédération le plus efficacement possible. Des compétences du Service de renseignement de la Confédération en matière de protection des IC sont prévues dans la future loi fédérale sur le Service de renseignement de la Confédération. Le Conseil fédéral doit pouvoir fixer de manière détaillée la répartition des tâches et la collaboration correspondantes. En raison des particularités découlant du traitement d'informations issues du SRC, le Conseil fédéral doit régler de façon spécifique l'échange de telles informations entre les services fédéraux ainsi que leur transmission à des exploitants d'IC. Les services concernés ne doivent pas nécessairement appartenir au même département. Afin de garantir la transparence et la sécurité du droit, le Conseil fédéral règle le traitement des données ainsi que leur échange entre les services en question, de même que la sécurité des données adéquate dans un tel contexte.

2.1.6 Organisation et exécution

Art. 84

A propos du rôle des préposés à la sécurité de l'information, cf. le ch. 1.3.2.1.

L'al. 1 dispose que la loi intervient dans l'autonomie d'organisation des autorités en raison du besoin prépondérant d'une gestion intégrale de la mise en œuvre de la présente loi. Elle exige que les autorités concernées ainsi que les départements et la Chancellerie fédérale désignent pour leur domaine de compétence un préposé à la sécurité de l'information (international: *chief information security officer, CISO*) ainsi qu'une suppléance adéquate. Puisqu'une gestion intégrale 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 pratique requiert que deux personnes au minimum par autorité assument les tâches en question. Il n'est toutefois pas exigé que les deux personnes soient intégralement engagées à cette fin.

Le Conseil fédéral lui-même doit 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 relativement petits s'agissant du personnel (p. ex. le Tribunal fédéral des brevets et le Tribunal militaire de cassation) qu'ils disposent 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 un préposé à la sécurité de l'information. Afin de remplir son devoir d'organisation, le Conseil fédéral doit décider 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 restent auprès de la ligne, c'est-à-dire des autorités compétentes et de leurs services subordonnés. Les préposés à la sécurité de l'information ont toutefois appelés à conseiller et à assister la ligne sur le plan spécialisé.
- La let. b dispose que les préposés à la sécurité de l'information doivent gérer, sur mandat de leurs autorités ou de leur organisation, la sécurité de l'information ainsi que la gestion des risques correspondante 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.
- La let. d dispose que les préposés à la sécurité de l'information peuvent signaler les incidents au service spécialisé de la Confédération en matière de sécurité de l'information (art. 86) et à la Conférence des préposés à la sécurité de l'information (art. 85) ainsi qu'aux services assumant les tâches relatives à la sécurité de l'information au sein des IC. On renoncera donc à une *obligation* d'annoncer dans le cadre de l'ensemble des autorités. La communication de tels incidents est certes fortement recommandée, mais l'autonomie des autorités ne doit pas être entravée.

L'al. 3 dispose que 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 encore subordonnés aux directions de l'informatique. Les responsables des TIC 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 TIC ou diriger des projets qui ne concernent pas en priorité la sécurité, car ce sont justement ces cumuls de tâches qui génèrent régulièrement des conflits entre les exigences de l'exploitation et une évaluation aussi objective que possible du risque pour la sécurité.

Le rattachement exact de la fonction est laissé à l'appréciation des autorités ou des départements et de la Chancellerie fédérale. Les leçons tirées d'expériences pratiques montrent 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 au 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. 85

A propos de la conférence, cf. le ch. 1.3.2.2.

L'al. 1 désigne les membres permanents de la conférence. En particulier, les départements et la Chancellerie fédérale doivent être représentés.

L'al. 2 décrit les tâches de la conférence, qui visent toutes une coordination efficace de l'exécution. Le nouveau service spécialisé de la Confédération en matière de sécurité de l'information (cf. art. 86) devra consulter et associer la conférence pour toutes les questions importantes en relation avec la sécurité de l'information. A cet égard, les conseils de la conférence au service spécialisé sur des questions liées à la stratégie en matière de sécurité de l'information revêtent une importance cruciale. La conférence doit également contribuer à l'identification des risques et des tendances ainsi qu'à la définition des mesures de prévention qui s'imposent. Ce n'est qu'ainsi que l'on trouvera des solutions efficaces et acceptables. Il semble tout aussi important de transformer la coordination avec le PFPDT en un mandat explicite (let. d). La conférence peut aussi associer des représentants des cantons et des experts indépendants afin de l'assister dans ses investigations et pour se forger une opinion.

L'al. 3 dispose que la conférence définit elle-même son organisation et ses processus d'affaires. Elle prend également les décisions relatives à sa direction.

Art. 86

A propos du service spécialisé de la Confédération en matière de sécurité de l'information, cf. le ch. 1.3.2.3.

L'al. 1 comporte un catalogue des tâches et des compétences transversales du futur service spécialisé.

- La let. a exige du service spécialisé qu'il conseille les autorités concernées et leurs préposés à la sécurité de l'information. Ces derniers peuvent également solliciter un appui technique du service spécialisé, notamment dans l'analyse des incidents.
- La let. b prévoit que le service spécialisé doit pouvoir recommander des mesures de protection préventives en cas de mise en péril de la sécurité de l'information.
- Aux termes de la let. c, les autorités concernées ou les services qu'elles mandatent peuvent charger le service spécialisé de mener sur place certains contrôles et audits en matière de sécurité. Le service spécialisé n'est pas habilité à effectuer de tels audits de sa propre initiative. En ce qui concerne notamment les audits techniques de sécurité, il est nécessaire de posséder des connaissances approfondies dont toutes les autorités concernées ne devraient pas se doter: il est plus rentable de recourir à une équipe d'experts.
- La let. d dispose que les autorités et organisations concernées souhaitant recourir à de nouvelles technologies ont, conformément à l'art. 20, l'obligation d'effectuer une évaluation des risques. S'agissant de technologies particulièrement importantes ou qui peuvent avoir un large champ d'application, elles sont autorisées à mandater le service spécialisé afin qu'il prenne en charge cette analyse.
- La let. e autorise le service spécialisé à examiner, sur demande des autorités et organisations concernées, l'adéquation de certains processus, moyens, installations, objets et prestations avec les aspects liés à la sécurité. En l'occurrence, il est question de la standardisation au niveau sécuritaire de processus, de moyens, d'installations, d'objets et de prestations. Dans le domaine de la sécurité technique de l'information, les fournisseurs de prestations TIC ont par exemple un intérêt à savoir si les solutions techniques qu'ils développent remplissent les exigences de la Confédération. Si tel est le cas, il est alors significativement plus facile pour eux de recourir à ces solutions dans le cadre d'autres projets ou moyens TIC. Cela s'applique aussi notamment à des coffres-forts ou à des services. 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 de *national accreditation authority* (cf. ch. 4.2), qui fait actuellement défaut mais est nécessaire dans le contexte international.
- La let. f dispose que le service spécialisé doit gérer et coordonner, sur demande des autorités concernées, les aspects de sécurité de l'information dans le cadre de projets transversaux importants fortement liés à la sécurité de l'information.
- 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. 4.2). D'autres autorités ou organisations continueront toutefois d'être autorisées à maintenir des contacts spécialisés dans ce domaine.

- La let. h dispose que le service spécialisé devra rendre des comptes annuellement au Conseil fédéral.

En vertu de l'al. 3, le Conseil fédéral doit régler l'organisation du service spécialisé dans sa législation d'exécution. A cet effet, il devra déterminer les tâches que le service spécialisé assume lui-même ou en collaboration avec d'autres services fédéraux. Dans ce cadre, le Conseil fédéral devra aussi apporter une réponse à la question de son rattachement.

Art. 87

L'al. 1 dispose que l'autonomie des autorités concernées n'est pas remise en question. Elles ne sont pas soumises aux dispositions d'exécution du Conseil fédéral. En contrepartie, elles doivent édicter elles-mêmes pour leurs domaines les dispositions portant exécution de la présente loi. La disposition précise aussi que le Conseil fédéral peut déléguer à la Chancellerie fédérale le pouvoir d'édicter des dispositions d'exécution en lien avec ses affaires (cf. également art. 15, al. 2, LOGA).

Grâce à la réglementation de l'al. 2 et à l'art. 70 LParl, l'Assemblée fédérale a toutes les dispositions nécessaires lui permettant, ainsi qu'aux Services du Parlement, d'appliquer directement la LSI et ses dispositions d'exécution.

L'al. 3 établit un droit de retrait (*opting out*): Les dispositions d'exécution du Conseil fédéral s'appliquent par analogie aux autorités concernées dans la mesure où ces dernières n'édictent pas de dispositions au sens de l'al. 1 pour leur domaine de compétence. Il va de soi que le Conseil fédéral sollicite l'avis des autres autorités avant d'édicter ses dispositions d'exécution. Le Conseil fédéral est seul responsable d'édicter les dispositions d'exécution nécessaires concernant les CSP et les PSE en vertu du fait que les services en question font partie de l'administration fédérale, dont l'organisation incombe au Conseil fédéral.

En vertu de l'al. 4, avant que des organisations de droit public ou privé selon l'art. 2, al. 2, let. e puissent être soumises à la présente loi, il est nécessaire d'évaluer si elles exercent des activités sensibles de la Confédération. Le Conseil fédéral doit procéder à cette évaluation pour les organisations en question et définir ensuite le champ d'application détaillé par voie d'ordonnance. Cela peut être réalisé dans les dispositions d'exécution de la législation spéciale ou dans celles de la présente loi. En cas de nécessité, le Conseil fédéral peut autoriser les organisations en question à appliquer uniquement une partie de la loi (p. ex. les dispositions concernant la classification, l'engagement des TIC ou les CSP).

Art. 88

L'al. 1 dispose que le Conseil fédéral doit fixer des exigences et des mesures standard en fonction de l'état d'avancée des connaissances et de la technologie afin d'atteindre le niveau de sécurité uniforme escompté. Il ne s'agit pas d'exigences et de mesures organisationnelles de base, mais d'exigences de nature subordonnée, par exemple:

- norme pour l'évaluation du besoin de protection des informations sous l'angle des quatre critères mentionnés à l'art. 4, al. 2;
- méthode standard pour l'évaluation des risques au sens de l'art. 6, al. 1;
- normes pour les mesures à prendre aux niveaux de l'organisation, du personnel, de la technique et des constructions au sens de l'art. 6, al. 2;
- exigences standard pour des processus et des moyens particuliers destinés à protéger des informations classifiées au sens des art. 12 à 18;
- exigences et mesures standard pour la protection de base, l'élaboration de concepts de sécurité de l'information et la sécurité de moyens TIC des échelons «protection élevée» et «protection très élevée» au sens des art. 19 à 27; etc.

En vertu de l'al. 2, le Conseil fédéral peut, si nécessaire, déléguer l'élaboration et l'adoption des normes à des services subordonnés. Cela concerne en premier lieu le service spécialisé de la Confédération en matière de sécurité de l'information, mais aussi d'autres organes tels que fedpol dans le domaine de la protection des objets. Les fournisseurs de prestations TIC 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. 86, al. 1, let. e). Une telle délégation par le Conseil fédéral ne doit toutefois pas être intégrale. Certaines mesures techniques peuvent avoir d'importantes conséquences financières qui ne devraient pas nécessairement 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.

L'al. 3 prévoit que les standards ne sont pas obligatoires pour les autres autorités concernées.

Art. 89

L'art. 1 dispose que si la loi s'applique aux cantons ou à leurs autorités et services (cf. art. 2, al. 2, let. f), ceux-ci doivent appliquer les mesures de sécurité requises conformément à la présente loi. Cependant, les services fédéraux n'obtiennent pas le droit d'édicter directement des directives: les cantons sont, en principe, eux-mêmes responsables de l'exécution au sein de leur domaine de compétences.

En vertu de l'al. 2, le Conseil fédéral doit régler dans la législation d'exécution la vérification de la mise en œuvre des mesures ainsi que l'exécution de CSP pour les employés cantonaux. En particulier, il devra déterminer comment la mise en œuvre des prescriptions par les cantons sera contrôlée, le cas échéant, par les autorités fédérales. Il va de soi qu'il prendra en considération le statut constitutionnel des cantons et, plus particulièrement, leur autonomie d'organisation.

L'al. 3 impose à chaque canton de désigner pour de tels cas un service en tant qu'interlocuteur des autorités et organisations concernées compétentes. Cela permet de garantir l'échange systématique d'informations et la mise en œuvre coordonnée des mesures au sens de la présente loi.

Art. 90

Les conventions internationales de droit public en matière de sécurité de l'information contiennent principalement des règles techniques relatives à la reconnaissance mutuelle de prescriptions et de processus nationaux (p. ex. à propos des CSP ou des PSE), des listes de concordance concernant le traitement des informations classifiées et des réglementations sur l'exécution de contrôles mutuels. De plus, des conventions peuvent se révéler nécessaires pour la protection des informations que d'autres Etats 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 (p. ex. 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, le cas échéant, exiger des autorités fédérales destinataires un accord plus ou moins sévère sur le degré de protection de ses informations. Il conviendra donc d'inclure les réserves nécessaires dans les dispositions d'exécution et d'organisation attribuant les compétences de conclure des accords. Pour des raisons d'économie administrative, le Conseil fédéral sera habilité à conclure directement des conventions internationales sur la sécurité de l'information.

Un accroissement de la mise en réseau et de la collaboration à l'échelon international est nécessaire à la réduction des risques relatifs à la sécurité de l'information. 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 renforcé (voir aussi le ch. 1.1.2.2). C'est pourquoi le Conseil fédéral doit aussi être autorisé à conclure des conventions de droit international public portant sur l'échange d'informations en matière de menaces, de points faibles et d'incidents liés notamment à des IC. Il s'agit principalement de questions subordonnées concernant l'organisation et la technique (p. ex. la collaboration avec d'autres GovCERT; cf. art. 81).

Art. 91

L'application effective ainsi que l'opportunité, l'efficacité et le caractère économique de toute loi doivent être évalués périodiquement. L'al. 1 prévoit que le Conseil fédéral répond de cette tâche. L'Assemblée fédérale doit désigner la commission chargée de traiter les rapports du Conseil fédéral (al. 2).

Art. 92

La nouvelle réglementation requiert l'adaptation d'autres lois fédérales.

Art. 93

Pour des raisons d'économie de procédure, les déclarations de sécurité relatives aux personnes et aux entreprises fondées sur le droit en vigueur resteront valables sous le nouveau droit jusqu'à leur échéance. Le Conseil fédéral doit définir les délais transitoires pour l'adaptation des prescriptions liées au traitement d'informations classifiées et à la sécurité de l'information lors de l'engagement de moyens TIC.

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

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

Le CSP sera désormais régi pour l'essentiel par la LSI. Les dispositions correspondantes de la LMSI doivent par conséquent être abrogées.

2.3 Loi fédérale sur l'archivage

Art. 6, al. 2

La LAr règle uniformément l'archivage des documents de la Confédération. Sont notamment réputés documents « toutes les informations enregistrées sur quelque support que ce soit, qui ont été reçues ou produites dans le cadre de l'accomplissement de tâches publiques de la Confédération » (art. 3, al. 1, LAr). Les services de la Confédération sont tenus de proposer aux Archives fédérales pour archivage tous les documents « dont ils n'ont plus besoin en permanence » (art. 6 LAr). Les informations classifiées sont aujourd'hui également soumises à la législation sur l'archivage. Leur protection est assurée par des délais de protection au sens des art. 9 ss LAr.

Le nouvel al. 2 de l'art. 6 LAr règle le lien qui existe entre la LAr et la LSI. La présente disposition permet de délimiter clairement les domaines d'application des deux lois concernées. La LAr règle l'archivage, c'est pourquoi c'est elle qui règle ce lien et non pas la LSI. Selon l'art. 6, al. 2, LAr, les informations classifiées ne sont pas proposées pour l'archivage tant qu'elles sont dignes de protection au sens des dispositions de la LSI. Mais dès qu'elles peuvent être déclassifiées en application des dispositions de la législation sur la sécurité de l'information, elles doivent être proposées pour l'archivage. Dans ce contexte, la classification et la déclassification sont réglées en fonction des dispositions de la LSI. La plupart des informations classifiées n'ont un besoin de protection que pendant une période donnée et doivent pouvoir être archivées selon les règles usuelles fixées par la LAr. Il va de soi que l'on ne peut recourir à la classification pour se soustraire à l'obligation d'archiver.

2.4 Loi sur le personnel de la Confédération

Art. 20a

L'augmentation de la valeur seuil pour l'exécution du CSP au sens de la LSI doit désormais permettre d'appliquer les mesures en question uniquement pour des activités qui sont réellement plus sensibles s'agissant de la sécurité. Malgré la loi, 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 concernées ne disposent pas d'autres instruments afin de contrôler la fiabilité de personnes postulant un emploi et de membres de leur personnel. Le nouvel art. 20*a* LPers fournit à l'employeur des moyens correspondants: il aura la possibilité d'exiger des personnes postulant un emploi et des membres du personnel qu'ils produisent un extrait du casier judiciaire et du registre des poursuites. Cette exigence ne devrait toutefois pas constituer la norme, mais être mise en œuvre uniquement dans la mesure où cela est nécessaire à la défense des intérêts de l'employeur. Le Conseil fédéral doit édicter des dispositions d'exécution à ce sujet.

Art. 20b

La LSI limite sa réglementation du CSP aux activités sensibles dans le cadre du traitement d'informations classifiées et de l'administration de moyens TIC ainsi qu'en cas d'accès à certaines zones de sécurité. Ces activités devraient concerner la majorité des CSP nécessaires. Il subsiste néanmoins d'autres activités dans le domaine des tâches des autorités fédérales dans le cadre desquelles des intérêts importants de la Confédération peuvent être fortement mis en péril sans que les activités en question soient directement liées au traitement d'informations ou de moyens TIC. S'agissant du personnel de la Confédération (à l'exception de l'armée et de la Banque nationale), ce genre de réglementations doit figurer dans la LPers. L'introduction d'une nouvelle disposition concernant le contrôle de fiabilité à l'art. 20*b* LPers doit permettre de couvrir un besoin identifié en matière de contrôle.

- En vertu de la let. a, le Conseil fédéral peut assujettir à un contrôle les personnes postulant un emploi et les membres du personnel qui doivent régulièrement représenter la Suisse à l'étranger et pourraient, alors, porter une atteinte considérable à l'image la Confédération. Il s'agit en premier lieu du personnel diplomatique et consulaire du DFAE, mais cela peut aussi concerner le personnel d'autres départements qui assume des fonctions similaires (p. ex. auprès du SECO).
- En vertu de la let. b, le Conseil fédéral peut également assujettir à un contrôle les personnes postulant un emploi et les membres du personnel qui doivent assumer des compétences décisionnelles ou des tâches de surveillance dans d'importantes affaires financières ou fiscales et pourraient, alors, porter une atteinte

considérable aux intérêts financiers de la Confédération (p. ex. 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).

Conformément à l'al. 2, le Conseil fédéral doit, dans la législation d'exécution de la LPers, déterminer les groupes de personnes devant être soumis à un contrôle de fiabilité. Ce dernier ne doit être ordonné qu'en cas de besoin avéré. La présente disposition ne saurait servir à déroger à la limitation des motifs de contrôle au sens de la LSI.

L'al. 3 dispose qu'il ne serait pas judicieux de prévoir une procédure spécifique pour le contrôle de fiabilité, car les points à élucider sont en principe les mêmes que ceux relevant de la sécurité de l'information. L'exécution du 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 récolte de données et des dispositions relatives aux conséquences de l'évaluation.

En vertu de l'al. 4, si la personne faisant l'objet d'un contrôle au sens de la présente disposition est simultanément assujettie à un CSP au sens de la LSI, les deux procédures doivent, dans l'intérêt de l'économie de procédure, être combinées.

2.5 Code pénal

Art. 365, al. 2, let. d

La modification de cet article revêt un caractère purement formel. 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 ainsi que le but de la récolte de données du casier judiciaire doivent être adaptées en conséquence. L'évaluation du risque pour la sécurité dans le cadre de contrôles de fiabilité au sens de la législation spéciale sera désormais aussi indiquée en tant qu'objectif de la récolte de données. En revanche, la mention de l'examen de dangerosité est déjà réglée aux let. n et p.

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

Voir le commentaire de l'art. 365, al. 2, let. d.

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

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

La modification de ces deux articles revêt un caractère purement formel. Puisque le CSP sera désormais réglé dans la LSI et non plus dans la LMSI, les dispositions concernant les services bénéficiant d'un droit d'accès ainsi que le but de la récolte de données du système de recherches informatisées et de l'index national de police doivent être adaptées en conséquence. L'évaluation du risque pour la sécurité dans le cadre de contrôles de fiabilité au sens de la législation spéciale ainsi que l'évaluation du potentiel de violence dans le cadre d'examens de dangerosité seront désormais aussi indiquées en tant qu'objectifs de la récolte de données.

2.7 Loi sur l'armée

Art. 14

Le projet de LSI limite sa réglementation du CSP à certaines activités sensibles (cf. l'art. 20*b* LPers ci-dessus). Cependant, l'armée connaît aussi d'autres activités dans le cadre desquelles l'image de la Confédération et de ses institutions ou des intérêts financiers importants de la Confédération peuvent être fortement mis en péril.

C'est pourquoi l'al. 1 prévoit, sur la base de l'art. 20*b* LPers proposé, que le Conseil fédéral peut soumettre à un contrôle de fiabilité deux domaines de tâches dans le cadre des dispositions d'exécution de la LAAM.

- En vertu de la let. a, le Conseil fédéral peut assujettir à un contrôle des militaires qui doivent régulièrement représenter la Suisse à l'étranger et pourraient, alors, porter une atteinte considérable à l'image de la Confédération. Il est principalement question de militaires qui, dans le cadre d'engagements à l'étranger, représentent la Suisse ou assument des tâches dans le domaine de la diplomatie militaire.
- En vertu de la let. b, le Conseil fédéral peut assujettir à un contrôle des militaires qui doivent assumer des compétences décisionnelles ou des tâches de surveillance dans d'importantes affaires financières et pourraient, alors, porter une atteinte considérable aux intérêts financiers de la Confédération.

Conformément à l'al. 2, le Conseil fédéral doit, dans la législation d'exécution de la LAAM, déterminer les groupes de personnes devant être soumis à un tel contrôle. Ce dernier doit être ordonné uniquement en cas de besoin avéré afin d'éviter que l'on ne déroge à la limitation des motifs de contrôle au sens de la LSI.

Comme dans le cas de la réglementation proposée dans la LPers, l'al. 3 dispose qu'il ne serait pas judicieux de prévoir une procédure spécifique pour le contrôle en question, car les points à élucider sont en principe les mêmes que ceux relevant de la sécurité des informations. L'exécution de ce contrôle doit dès lors se fonder sur la LSI. En reprenant la procédure, on tiendra compte notamment des règles régissant la récolte de données et des dispositions relatives aux conséquences de l'évaluation.

En vertu de l'al. 4, si la personne soumise à un contrôle au sens de la présente disposition est simultanément assujettie à un CSP au sens de la LSI, les deux procédures doivent, dans l'intérêt de l'économie de procédure, être combinées.

Art. 113, al. 5

La LSI prévoit une limitation du CSP aux activités sensibles en rapport avec le traitement d'informations et la gestion de moyens TIC; cette limitation exige une base légale de droit spécial pour le contrôle du potentiel de violence que présentent les militaires porteurs d'une arme. Dans le cadre de la procédure, la réglementation de la LSI doit être appliquée par analogie. Si deux procédures sont introduites, elles doivent, pour des raisons d'économie de procédure, être combinées.

Art. 150, al. 4 Abrogation

La compétence de conclure avec des Etats étrangers des traités visant au maintien du secret militaire figurera désormais à l'art. 90 LSI. En outre, on distingue de plus en plus rarement entre secret civil et militaire, de sorte que les conventions couvrent les deux secteurs ou concernent le maintien du secret en général. Pour garantir l'unicité du droit, l'art. 150, al. 4, de la loi sur l'armée doit être abrogé.

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

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

Les systèmes d'information sur le CSP et la PSE sont actuellement réglés dans la LSIA. Ces deux systèmes d'information seront désormais directement réglés dans la LSI (art. 52 à 54 pour le CSP et art. 77 à 79 pour la PSE). C'est pourquoi les deux sections correspondantes de la LSIA doivent être abrogées.

2.9 Loi sur l'énergie nucléaire

Art. 5, al. 3

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

Art. 24

La réglementation en vigueur de l'art. 24 LENu prévoit déjà des contrôles de fiabilité pour des personnes exerçant des fonctions essentielles pour la sécurité nucléaire et pour la sûreté de l'installation nucléaire. Ces personnes sont, conformément à l'OCSPN, assujetties à un CSP. Dans la nouvelle teneur de l'art. 24 LENu, la formulation a été adaptée à la nouvelle terminologie pour les contrôles de fiabilité, car le contrôle est exécuté par analogie avec les dispositions de la LSI concernant le CSP.

2.10 Loi sur l'approvisionnement en électricité

Art. 26a

La société nationale du réseau de transport, qui exploite le réseau de transport d'électricité à l'échelon de la Suisse (Swissgrid), exige depuis plusieurs années que des CSP soient effectués pour certaines catégories de personnel. Au vu du caractère critique du réseau de transport et du besoin correspondant de se protéger contre le sabotage, une nouvelle disposition concernant l'exécution de contrôles de fiabilité pour certains groupes de personnes doit être introduite dans la LApEl.

L'al. 1 inscrit dans la loi le principe de contrôler la fiabilité des membres du personnel de la société nationale du réseau de transport appelés à exercer des tâches importantes pour la sécurité du réseau de transport à l'échelon de la Suisse et pour la fiabilité et la performance de son exploitation.

En vertu de l'al. 2, le Conseil fédéral doit désigner les groupes de personnes devant être contrôlés. Dans ce cadre, il doit limiter ce contrôle à des fonctions susceptibles de causer un dommage considérable en cas de sabotage dû à des actions ou à des négligences.

L'al. 3 dispose que la procédure de contrôle est régie par les dispositions de la LSI concernant le CSP.

L'al. 4 suit la même réglementation que l'art. 25 LENu. La direction de Swissgrid ainsi que les régulateurs (OFEN et ElCom), en leur qualité d'instances de décision, doivent avoir accès aux données du contrôle.

2.11 Loi sur la Banque nationale

Art. 16, titre et al. 5

En raison de ses tâches de politique monétaire (voir aussi l'art. 1, al. 2, let. d), la Banque nationale est considérée comme une autorité concernée au sens de l'art. 2, al. 1, LSI. La modification de l'art. 16 LBN indique expressément que la LSI s'applique à la Banque nationale. Le titre de l'article sera adapté en conséquence.

3 Conséquences

3.1 Conséquences pour la Confédération

Les informations sont protégées parce qu'une atteinte à leur confidentialité, à leur disponibilité, à leur intégrité ou à leur traçabilité (cf. art. 4) peut violer les droits de tiers (p. ex. des données personnelles ou des secrets d'affaires et de fabrication), mettre en péril des intérêts publics d'importance (p. ex. la capacité d'action des autorités fédérales, la sécurité nationale, les relations internationales ou l'approvisionnement du pays) ou porter préjudice aux organisations concernées (p. ex. perte de productivité ou perturbations du service). La sécurité de l'information vise à réduire le plus efficacement et le plus avantageusement possible la probabilité et, le cas échéant, l'ampleur d'un tel dommage (notamment financier). Ses coûts doivent donc être mis en relation avec la réduction correspondante du risque.

La présente loi apportera une amélioration sensible et durable de la sécurité de l'information au sein de la Confédération. En premier lieu, elle règle la gestion de la sécurité de l'information et augmente son efficacité. En effet, une gestion optimale améliore souvent la sécurité de manière plus efficace, plus économique et plus durable que des investissements dans des mesures techniques. La pratique a également montré qu'une optimisation de la gestion de la sécurité de l'information peut même contribuer à réaliser des économies à moyen terme, en particulier si cette gestion se fonde sur une gestion efficace des risques. 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 relatives si elles sont mises en œuvre de manière conséquente. 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 (cf. ch. 1.2.3.4). S'agissant de contrôles de sécurité relatifs aux personnes (CSP), la valeur seuil pour l'exécution d'un CSP augmentera, tandis que le nombre d'activités pour lesquelles un CSP est nécessaire (et admis) diminuera. A l'avenir, le nombre de CSP effectués devrait donc baisser (cf. ch. 1.2.4). En outre, la standardisation proposée des exigences et des mesures de sécurité (cf. art. 88), l'amélioration de l'échange d'informations entre les autorités fédérales et le soutien apporté aux autorités fédérales par le service spécialisé de la Confédération en matière de sécurité de l'information (cf. art. 84 à 86) doivent notamment permettre d'éviter de se voir contraint de réinventer la roue dans le cadre de chaque projet. Enfin, la nouvelle réglementation facilitera la collaboration internationale dans le domaine de la sécurité (cf. ch. 4.2).

L'amélioration nécessaire de la sécurité de l'information au sein de la Confédération engendrera des coûts. Ceux-ci ne pourront toutefois être estimés correctement qu'après la procédure de consultation. Cela nécessite des variantes concernant l'organisation et l'allocation des ressources s'agissant des préposés à la sécurité de l'information et du service spécialisé de la Confédération en matière de sécurité de l'information, ainsi que des données plus précises quant au nombre de moyens TIC existants qui appartiendront à l'avenir à la catégorie de sécurité «protection très élevée». Dans son message, le Conseil fédéral exposera de façon transparente les conséquences du projet en matière de finances et de personnel.

Les coûts engendrés directement par la loi doivent être clairement distingués des coûts des différentes mesures pouvant être librement adoptées par les autorités fédérales compétentes dans le cadre de la mise en œuvre. En effet, la loi règle uniquement la gestion de la sécurité de l'information et ne fixe ni un niveau de sécurité à atteindre, ni des mesures détaillées – à quelques exceptions près (voir ci-après). Elle n'est donc pas directement applicable: les autorités fédérales doivent édicter leurs propres dispositions d'exécution pour leur domaine de compétences et disposent pour cela d'une marge de manœuvre quasi illimitée (cf. art. 87, al. 1) – hormis pour ce qui a trait à l'organisation. Dans ce cadre, elles doivent déterminer le niveau de sécurité qu'elles souhaitent atteindre (cf. art. 5, al. 3, let. a) et décider, au niveau de l'ordonnance, des directives ou même du projet, des exigences et des mesures requises pour y parvenir en matière d'organisation, de personnel, de technique et de constructions. Plus le niveau à atteindre est élevé, plus les coûts des mesures de

sécurité seront importants. La loi elle-même n'exerce aucune influence sur ces coûts. Ils ne peuvent donc pas non plus être chiffrés lors de l'évaluation des conséquences de la loi en matière de finances et de personnel.

Toutes les autorités fédérales sont aujourd'hui déjà tenues de prendre des mesures afin de garantir la sécurité de l'information. Pour l'évaluation des coûts, sont donc déterminantes les dispositions de la loi qui fixent de nouvelles tâches ou modifient des tâches et des processus existants. Les cinq générateurs de coûts les plus importants sont énumérés ci-dessous.

1. *Organisation, pilotage, mise en œuvre et contrôle de la sécurité de l'information (art. 5, al. 1, let. a):* la nouvelle organisation exigée par la loi engendrera une charge organisationnelle qui ne doit pas être sous-estimée et nécessitera des ressources financières. Plus particulièrement lors des phases de conception et de mise en place, il conviendra d'acquérir des connaissances spécialisées dont les autorités fédérales sont aujourd'hui partiellement dépourvues. Les préposés à la sécurité de l'information répondront de la gestion et de l'exploitation d'une telle organisation interne. La loi prévoit deux préposés au minimum pour chaque autorité ainsi que pour les départements et la Chancellerie fédérale. Ces tâches devraient en majorité être accomplies au moyen des ressources en personnel existantes. Le besoin réel en matière de personnel variera néanmoins et dépendra de la taille de l'autorité ou de l'organisation (effectifs), de son domaine de tâches ainsi que du nombre et de la criticité des moyens TIC qu'elle engage.
2. *Contrôles et audits renforcés (art. 11, al. 2, et p. ex. art. 24, al. 2):* la ligne répond en principe de l'exécution des contrôles, une tâche normale de conduite. Les préposés à la sécurité de l'information effectueront aussi eux-mêmes des contrôles et des audits sur mandat de leur autorité ou de leur organisation. La loi prévoit cependant deux nouveaux types de contrôles qui auront des conséquences en matière de finances ou de personnel: une vérification périodique par un service indépendant de l'efficacité des mesures prises (art. 11, al. 2) ainsi qu'une vérification technique de l'efficacité des moyens TIC les plus critiques (art. 24, al. 2). Les coûts ainsi engendrés dépendront de la fréquence de telles vérifications. Les données ci-dessous fournissent un ordre de grandeur.
   - *Audits externes (art. 11, al. 2)*: selon les données du CDF, l'expérience montre qu'environ 100 jours-personnes sont nécessaires pour une petite vérification transversale, tandis qu'une grande vérification transversale requiert quelque 300 jours-personnes.
   - *Vérifications techniques de l'efficacité (art. 24, al. 2)*: selon les estimations brutes, la Confédération engage entre 50 et 70 systèmes TIC qui seront à l'avenir attribués à la nouvelle catégorie de sécurité «protection très élevée» et devront donc être soumis à une telle vérification. L'expérience montre que les coûts liés aux audits (coûts en personnel) représentent généralement entre 0,5 % et 2 % des coûts d'investissement totaux du système TIC devant faire l'objet d'un audit.
3. *Contrôles de sécurité relatifs aux personnes (CSP; art. 32 à 55)*: l'un des objectifs de la présente loi est d'harmoniser et de simplifier les CSP. Les adaptations proposées permettront à l'avenir d'effectuer moins de CSP et de réduire ainsi les coûts correspondants à moyen terme.
4. *Procédures de sécurité relatives aux entreprises (PSE; art. 56 à 80)*: le DDPS utilise aujourd'hui deux postes à plein temps pour l'exécution des PSE pour des mandats militaires classifiés. L'élargissement de ces procédures au domaine civil et aux autres autorités fédérales, tel que proposé par le Conseil fédéral, conduira à une augmentation du nombre d'entreprises prises en charge et, par conséquent, à des besoins supplémentaires sur le plan du personnel. Les entreprises qui soumissionnent pour des mandats d'autorités étrangères et ont besoin pour cela d'une déclaration de sécurité devront supporter les coûts de la PSE requise (art. 57, al. 3).
5. *Service spécialisé de la Confédération en matière de sécurité de l'information (art. 86)*: la création de ce nouveau service spécialisé entraînera des coûts de réorganisation. Ces derniers dépendront du rattachement administratif du service spécialisé ainsi que de l'ampleur du regroupement d'organes spécialisés existants. Bien que le service spécialisé doive majoritairement assumer ses tâches au moyen de ressources en personnel existantes de l'administration fédérale, un besoin supplémentaire en personnel sera présent. En effet, le service spécialisé agira au profit non seulement de l'administration fédérale, mais aussi des autres autorités fédérales. De plus, il devra assumer de nouvelles tâches, à savoir:
   - mener des contrôles et des audits (art. 86, al. 1, let. c): voir ci-dessus «*Contrôles et audits renforcés*»;
   - examiner l'adéquation de certains processus, moyens et prestations sous l'angle de la sécurité (art. 86, al. 1, let. e): cette nouvelle tâche est nécessaire pour la standardisation visée et la collaboration internationale;
   - gérer et coordonner la sécurité de l'information dans le cadre de projets transversaux importants (art. 86, al. 1, let. f): cette nouvelle tâche permettra de garantir que les responsabilités sont clairement

réglées pour des projets de ce type et que des experts reconnus encadrent les projets sur le plan de la sécurité;

- élaborer ou fixer des exigences en termes de sécurité ainsi que des mesures standard en fonction de l'état d'avancée des connaissances et de la technologie (art. 88, al. 1 et 2): cette mesure est nécessaire pour une exécution aussi uniforme que possible, mais peut aussi permettre de réaliser des économies (voir plus haut).

Le Conseil fédéral réglera l'organisation du service spécialisé au niveau de l'ordonnance (art. 86, al. 3). Dans ce cadre, il décidera également quels organes existants seront regroupés et avec quels moyens le service spécialisé remplira ses tâches.

3.2 Conséquences pour les cantons et les communes

Les cantons ne sont concernés que dans la mesure où ils exercent des activités sensibles sur mandat direct de la Confédération et sous la surveillance de cette dernière (cf. art. 2, al. 2, let. f, et art. 89). Ils doivent alors appliquer les mesures de sécurité exigées par la présente loi et désigner un service qui servira d'interlocuteur aux autorités fédérales compétentes. Le Conseil fédéral devra régler par voie d'ordonnance l'exécution des CSP par des agents cantonaux ainsi que la vérification de la mise en œuvre des mesures par les cantons. Dans ce cadre, il prendra en considération l'autonomie des cantons. Les conséquences pour les cantons seront donc minimes.

3.3 Conséquences pour l'économie

La loi ne s'applique qu'indirectement aux tiers, plus précisément lorsque ces derniers doivent traiter des informations ou utiliser ou gérer des moyens TIC 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 soumises à la procédure uniforme de sécurité relative aux entreprises introduite par la présente loi. Ce changement ne devrait occasionner qu'un faible accroissement de la charge administrative. A 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 au bénéfice de particuliers qui soumissionnent pour des mandats classifiés d'autorités étrangères ou d'organisations internationales et ont besoin à ce titre d'une déclaration de sécurité (cf. art. 56 à 80). En outre, l'économie profitera de l'amélioration de la protection des secrets d'affaires et de fabrication qu'elle confie aux autorités fédérales.

3.4 Conséquences pour la société

La société est concernée de deux points de vue. D'une part, elle aura davantage confiance dans le traitement des informations par les autorités fédérales. Elle acquerra la certitude que la Confédération juge importantes et protège en conséquence les informations qui la concernent (notamment les données personnelles et les secrets d'affaires et de fabrication). D'autre part, les principes de classification des informations seront affichés de manière transparente, ce qui revêt une importance particulière s'agissant du principe de transparence, qui n'est nullement remis en question par la présente loi.

3.5 Rapports avec les stratégies nationales du Conseil fédéral

3.5.1 Stratégie pour une société de l'information en Suisse

Le présent projet est inscrit au catalogue des projets relatifs à la société de l'information 2011–2015 (situation en juin 2013) dans le champ d'action «Sécurité et confiance». La loi fournira des bases claires pour la mise en œuvre des exigences de sécurité dans les projets réalisés par la Confédération. A propos de la stratégie, cf. le ch. 1.2.1.1.

3.5.2 Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)

A propos de la SNPC, cf. le ch. 1.1.2.2; à propos des liens entre la SNPC et le projet, cf. le ch. 1.2.6; à propos du soutien aux opérateurs d'IC dans le domaine de la sécurité des informations, cf. les art. 81 à 83.

3.5.3 Stratégie nationale de protection des IC (stratégie PIC)

La stratégie PIC du 27 juin 2012 (FF 2012 7173) vise à renforcer la capacité de résistance de la Suisse au niveau des infrastructures critiques. Elle propose différentes mesures afin de consolider la protection intégrale dans deux domaines. L'autoprotection sera renforcée par l'élaboration et l'application de concepts de protection intégrale par les organes compétents. Cela 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 tout en diminuant la vulnérabilité de la société, de l'économie et des pouvoirs publics en cas de défaillance grave. A cette fin, on élabore-

ra des planifications pour la maîtrise de défaillances graves et pour l'aide subsidiaire apportée aux exploitants lors de tels événements. Le Conseil fédéral souhaite assister les exploitants d'IC dans leurs efforts de protection. Dans ce cadre, il convient également d'atteindre la plus grande capacité de résistance possible en matière de sécurité de l'information.

Plusieurs mesures de la stratégie PIC visent directement à améliorer la sécurité de l'information. C'est le cas notamment de la mesure 7, qui prévoit la création de bases légales formelles permettant de soumettre certaines catégories de personnel des exploitants d'IC à un contrôle de sécurité. En principe, l'exécution de contrôles de sécurité doit être prévue dans la législation spéciale au sens de la SNPC (cf. ch. 1.1.2.2 et art. 3, al. 3). Parallèlement au projet, il est également demandé la création d'une base dans la LApEl pour l'exécution de contrôle de fiabilité de certains employés de Swissgrid (cf. art. 26*a* LApEl). La LSI soutient donc aussi la mise en œuvre de la stratégie PIC.

4 Aspects juridiques

4.1 Constitutionnalité

En vertu de l'art. 42 Cst., le législateur fédéral doit disposer pour ses réglementations d'une base constitutionnelle (explicite ou implicite). Des bases constitutionnelles suffisantes fondent la législation proposée dans le domaine de la sécurité de l'information. Formellement, les réglementations proposées sont avant tout des dispositions d'organisation pour les autorités fédérales. Dans la Constitution, le droit de l'organisation de la Confédération ne figure certes pas sous une forme explicite au catalogue de la répartition des compétences entre la Confédération et les cantons, mais l'art. 164, al. 1, let. g, Cst., dans son énumération des compétences de l'Assemblée fédérale, inclut «l'organisation et […] la procédure des autorités fédérales» aux objets devant être réglés par une loi fédérale (voir p. ex. le préambule de la LParl). De plus, dans la législation d'organisation en vigueur, on renvoie également à l'art. 173, al. 2, Cst., qui attribue à l'Assemblée fédérale tous les objets qui relèvent de la compétence de la Confédération et qui ne ressortissent pas à une autre autorité fédérale (voir p. ex. le préambule [avec note de bas de page 1] de la LOGA, celui de la LTrans et celui de la LFRC).

Sur le fond, cette loi 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. A cet égard, les dispositions 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 et à la protection de la population dans les limites de leurs compétences respectives» (voir p. ex. le préambule de la LMSI).

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 d'organisations internationales. Cette réglementation est couverte par l'art. 101 Cst., qui forme la base de la sauvegarde des intérêts de l'économie suisse à l'étranger. Les dispositions relatives à la protection des IC 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.

4.2 Compatibilité avec les obligations internationales de la Suisse

La Suisse a conclu avec divers Etats et organisations internationales des conventions de protection des informations ou des accords techniques de sécurité (*security agreements* ou *security arrangements*; cf. RS 0.514). Par ces traités, la Suisse s'engage à respecter certaines normes visant à protéger les informations classifiées. Outre la convention avec l'UE, la Suisse a également conclu des conventions de protection des informations avec l'OTAN (1997) dans le cadre de l'engagement «partenariat pour la paix» ainsi qu'avec l'ASE (2004). D'une part, ces conventions comportent des dispositions matérielles concernant par exemple des mécanismes de protection uniformes pour le traitement d'informations classifiées ou la reconnaissance mutuelle de certificats de sécurité. D'autre part, elles contiennent également des normes organisationnelles et structurelles et précisent notamment les organismes chargés de la mise en œuvre des mesures de sécurité (*national security authority* ou *designated security authority*). Des interlocuteurs nationaux chargés d'élaborer des normes homogènes en matière de TIC (*national accreditation authority* ou *security accreditation authority*) sont exigés notamment dans le domaine COMSEC. Le service spécialisé de la Confédération en matière de sécurité de l'information (art. 86) assumera ces tâches et en prendra la responsabilité dans le contexte international.

4.3 Forme de l'acte à adopter

Dans sa décision du 12 mai 2011 relative à l'élaboration de bases légales formelles pour la protection des informations, le Conseil fédéral était déjà parti de l'idée que les réglementations 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 importantes pour les autorités fédérales (art. 164, al. 1, let. g, Cst.) qui, en raison de la nécessité d'une applicabilité uniforme, doivent déployer des effets transversaux. D'autre part, il s'agit de dispositions susceptibles d'empiéter fortement sur les droits fondamentaux, notamment dans le domaine des contrôles de sécurité.

4.4 Délégation de compétences législatives

Les autorités concernées au sens de la loi devront édicter des dispositions d'exécution dans leur domaine de compétence respectif, notamment pour ce qui est de la réglementation des tâches et des compétences, de même que des mesures d'organisation. Globalement, il ne s'agit pas d'édicter des ordonnances de substitution au sens des principes de délégation admis, mais bien d'une compétence autonome d'édicter des dispositions d'exécution, dont les bases matérielles figurent dans la loi et ne créent aucun droit ni aucune obligation pour les particuliers. En principe, la Constitution attribue elle-même aux autorités concernées la compétence d'édicter de telles dispositions d'exécution. C'est pourquoi le projet de loi ne s'étend pas sur cette délégation de manière détaillée. En revanche, la loi contient des normes de délégation lorsque:

- les autorités concernées sont tenues d'édicter des dispositions d'exécution ou des ordonnances de substitution (p. ex. art. 5, al. 1, art. 19, al. 1, art. 22, al. 1, etc.);
- le Conseil fédéral est habilité à conclure des conventions internationales de droit public de sa propre compétence (art. 90).