Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Secrétariat général du DDPS SG-DDPS
Digitalisation et cybersécurité DDPS

8 novembre 2023

Législation d'exécution relative à la loi sur la sécurité de l'information

Explications

Référence : SG-DDPS-251.2-35/1/6/8

Table des matières

Explications

1 Contexte

Le 18 décembre 2020, l'Assemblée fédérale a adopté la loi sur la sécurité de l'information (LSI)[1]. Le délai référendaire a expiré mi-avril 2021 sans avoir été utilisé. Cette nouvelle loi crée une base légale uniforme pour la sécurité de l'information au sein de la Confédération.

La notion de *sécurité de l'information* englobe toutes les exigences et mesures visant à protéger la confidentialité, l'intégrité, la disponibilité et la traçabilité des informations et données de tout type, de même que la disponibilité et l'intégrité des moyens informatiques. La plupart des informations étant aujourd'hui traitées sous forme électronique, un accent est mis sur la cybersécurité. Reste que cette notion ne se limite pas au traitement électronique, elle englobe toutes les procédures de traitement, documents papier et déclarations orales compris. Dans le langage courant, la sécurité de l'information et la cybersécurité sont souvent utilisées comme synonymes.

La législation d'exécution de la LSI a été élaborée avec des représentants des autres autorités fédérales soumises à la LSI et des cantons. Dans son message du 22 février 2017 concernant la loi sur la sécurité de l'information (message LSI)[2], le Conseil fédéral a annoncé qu'il consulterait les autres autorités fédérales concernées et les cantons à propos de toutes les dispositions importantes (cf. ch. 1.5, p. 2820) afin d'atteindre un degré de sécurité aussi homogène que possible et de répondre à satisfaction aux besoins de toutes les autorités fédérales et des cantons. Une procédure de consultation a donc été organisée, dont les résultats ont été intégrés dans les projets présentés ici.

2 Présentation des projets

2.1 Législation d'exécution relative à la LSI

La législation d'exécution relative à la LSI se compose de quatre ordonnances :

- l'ordonnance (nouvelle) sur la sécurité de l'information (OSI, ch. 3.1) ;
- ordonnance (modifiée) du 19 octobre 2016 sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération[3] (OIAM, ch. 3.2) ;
- l'ordonnance (nouvelle) sur les contrôles de sécurité relatifs aux personnes (OCSP, ch. 3.3) ;
- l'ordonnance (nouvelle) sur la procédure de sécurité relative aux entreprises (OPSEnt, ch. 3.4).

Le 29 septembre 2023, le Parlement a approuvé une modification de la LSI introduisant une obligation de signaler les cyberattaques menées contre les infrastructures critiques. Cela entraîne la révision complète du chap. 5 de la LSI. Le Département fédéral de la défense, de la protection de la population et des sports (DDPS) est en train d'élaborer l'ordonnance qui en découle.

2.2 Conditions générales et principes

Dans le message LSI, le Conseil fédéral a justifié la nécessité formelle et matérielle de cette loi. Le contexte et les objectifs et propositions de solutions du Conseil fédéral qui y sont liés n'ont pas perdu de leur actualité. Ils fournissent la base conceptuelle de la législation d'exécution relative à la LSI. Il en va de même pour l'appréciation de la menace, l'orientation stratégique de la Suisse et les principes d'action que le Conseil fédéral et les cantons ont définis en avril 2023 dans la Cyberstratégie nationale. S'agissant de la mise en œuvre de la sécurité de l'information au sein de l'administration fédérale et de l'armée, plusieurs autres stratégies sont à prendre en considération, notamment les stratégies informatiques nationales et internes de la Confédération.

Pour l'élaboration de ladite législation d'exécution, les cinq principes ci-après ont été définis comme orientations stratégiques.

a. Responsabilité partagée de la sécurité

Conformément à l'art. 45 de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[4], les directeurs des de groupement et d'office sont responsables de l'exécution des tâches qui leur sont déléguées, de même que de la protection de leurs

[1] FF **2020** 9665
[2] FF **2017** 2765
[3] RS **172.010.59**
[4] RS **172.010**

informations et moyens informatiques. Or cette responsabilité seule ne suffit pas dans un environnement numérisé interconnecté. Des informations sont échangées, des systèmes interconnectés et des fichiers mis à disposition pour un usage partagé sur le principe *once only*. De ce fait, des menaces et des attaques à l'encontre d'une organisation ou de ses fournisseurs peuvent se propager au domaine de compétence d'autres organisations. La sécurité de l'information est donc une tâche globale à responsabilité partagée qui exige des objectifs communs, une approche coordonnée et des normes minimales.

b. Approche fondée sur les risques

Parvenir à une sécurité absolue relève de l'impossible. Les risques sont inévitables. Les directives de la Confédération sur la protection de base protègent contre une multitude de menaces en fonction des risques encourus. Elles servent à la sécurité globale de l'information de la Confédération et doivent être respectées. De plus, les responsables doivent appliquer une gestion active des risques dans le domaine de la sécurité de l'information, en prenant en compte et en priorisant les vulnérabilités, les menaces et leurs éventuelles répercussions sur l'exécution des tâches. Avec pareille approche, l'accent peut être mis tant sur les risques que sur les possibilités, les opportunités et les nouvelles idées, applications ou technologies.

c. Harmonisation et standardisation

La confiance dans la cyberadministration passe par une sécurité de l'information appropriée. C'est vrai tant pour les affaires nationales que pour l'interconnexion internationale toujours croissante des autorités. Une harmonisation nationale et internationale des règlements et la standardisation des mesures de sécurité sont dès lors souhaitables. La standardisation présente d'autres avantages importants : les coûts de sécurité des projets sont plus faciles à calculer et à planifier ; de plus, la clarté des exigences en matière de sécurité aide les services de développement et d'acquisition à sécuriser les moyens informatiques.

d. Neutralité des technologies

De nouvelles technologies, de nouveaux concepts ou de nouvelles formes de travail en lien avec la sécurité apparaissent avec l'informatisation croissante. Les ordonnances doivent être en mesure d'intégrer des évolutions comme l'informatique en nuage, l'Internet des objets, l'intelligence artificielle ou l'informatique quantique sans nécessiter constamment des adaptations. Il convient donc de fixer en premier lieu à leur niveau les principes, tâches, compétences et responsabilités et de définir les consignes liées aux technologies au niveau des directives et des normes techniques.

e. Préparation à la digitalisation

Les besoins de la digitalisation doivent être intégrés de bonne heure dans les projets législatifs. Lorsque des tâches, processus et procédures sont vérifiés sur le plan juridique ou redéfinis, il faut s'assurer que les nouvelles consignes permettront la digitalisation.

2.3 Ordonnance sur la sécurité de l'information (OSI)

a. Objet

L'OSI remplace l'ordonnance du 27 mai 2020 sur les cyberrisques (OPCy)[5] et l'ordonnance du 4 juillet 2007 concernant la protection des informations (OPrI)[6]. Elle régit la gestion de la sécurité de l'information, la protection des informations classifiées, la sécurité informatique et les mesures de protection personnelle et physique. Elle précise les tâches, les compétences et les responsabilités correspondantes au sein de l'administration fédérale et de l'armée.

b. Champ d'application

L'OSI s'applique au Conseil fédéral, à l'administration fédérale et à l'armée. Les unités de l'administration fédérale décentralisée au sens de l'art. 7*a* de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration (OLOGA)[7] ne relèvent de la LSI et de l'OSI que lorsqu'elles traitent des informations classifiées de la Confédération, qu'elles accèdent à des moyens informatiques de l'administration fédérale centrale ou qu'elles délèguent la gestion de leurs moyens informatiques aux fournisseurs de prestations informatiques de la Confédération. Dans ces cas, elles ne doivent pas mettre en œuvre la LSI et l'OSI tout entières, mais seulement

[5] RS **120.73**
[6] RS **510.411**
[7] RS **172.010.1**

les dispositions concernant le traitement des informations classifiées ou garantissant la sécurité des moyens informatiques. Il en va de même des organisations visées à l'art. 2, al. 4, OLOGA auxquelles sont confiées des tâches administratives mais qui sont extérieures à l'administration fédérale. La Chancellerie fédérale (ChF) et les départements peuvent toutefois soumettre à l'ensemble de la LSI des unités administratives décentralisées qui exercent constamment des activités sensibles.

L'OSI s'applique par analogie à l'Assemblée fédérale, aux tribunaux fédéraux, au Ministère public de la Confédération et à son autorité de surveillance, ainsi qu'à la Banque nationale suisse, s'ils n'édictent pas leurs propres dispositions.

c. Collaboration avec les cantons

Dans la mesure où les cantons traitent des informations classifiées de la Confédération ou accèdent à des moyens informatiques de la Confédération, les dispositions de la LSI et de l'OSI sont applicables. La LSI et l'OSI intègrent également les exigences minimales en la matière du service spécialisé de la Confédération pour la sécurité de l'information, notamment les prescriptions et exigences techniques pour la protection informatique de base dans l'administration fédérale et pour la protection des informations classifiées. Les cantons seront comme jusqu'à présent tenus de satisfaire aux exigences de sécurité que l'office fédéral responsable du système informatique aura fixées en application des règles de la LSI et de l'OSI. Toutefois, ils peuvent s'affranchir des dispositions légales de la Confédération s'ils garantissent d'eux-mêmes une sécurité équivalente de l'information. Cela suppose qu'ils édictent leurs propres prescriptions de sécurité en s'appuyant sur la norme fédérale et les fassent appliquer dans leur domaine de compétence. Les cantons ne sont pas tenus de mettre en œuvre un système de management de la sécurité de l'information (SMSI).

d. Gestion de la sécurité de l'information

Les offices, les secrétariats généraux, les groupements et la ChF sont tenus de sécuriser l'information au moyen d'un SMSI approprié. Un SMSI n'est pas un système informatique, mais est un instrument de conduite servant à planifier, mettre en œuvre, vérifier et améliorer systématiquement la sécurité de l'information. Il englobe les prescriptions, les procédures, les mesures et les contrôles nécessaires et indique à qui sont dévolues telles ou telles tâches, compétences et responsabilités au sein de l'organisation. L'abréviation SMSI renvoie implicitement à la norme ISO/IEC 27001, qui tend à se généraliser tant dans l'économie privée que dans les administrations publiques. Plusieurs offices et départements ont déjà décidé d'appliquer systématiquement la norme ISO à leur processus visant à sécuriser l'information. Certains ont reçu une certification formelle. L'OSI n'exige qu'un SMSI *light* des offices, des secrétariats généraux, des groupements et de la ChF : en d'autres termes, ils peuvent n'appliquer que les principaux processus de gestion et ne doivent pas appliquer la norme ISO dans son intégralité. Ces processus sont réglés dans l'OSI. Une certification externe n'est pas exigée. Les unités administratives et les départements peuvent toutefois définir un niveau d'ambition plus élevé.

e. Protection des informations classifiées et sécurité informatique

Les critères de classification des informations et d'attribution d'une catégorie de sécurité aux moyens informatiques s'appuient sur les critères de gestion des risques de la Confédération, si bien que la Confédération réduira la quantité d'informations classifiées. Les critères sont volontairement formulés de manière ouverte et devront être interprétés. Des outils seront créés pour leur application.

Concernant les mesures concrètes de protection des informations classifiées et de garantie de la sécurité informatique, l'OSI reprend en majorité les règles actuelles de l'OPrI et de l'OPCy. Les consignes détaillées, y compris les exigences techniques actuellement manquantes sur le traitement électronique des informations classifiées, seront rédigées et harmonisées avec les normes de l'Union européenne et de l'OTAN.

f. Certification de sécurité des moyens informatiques

L'OSI introduit la possibilité de faire certifier les systèmes d'information sur le plan de la sécurité. Une certification de sécurité est exigée à l'étranger et sur le plan international quand des informations protégées d'une autorité (ou d'un État) doivent être traitées dans le système d'une autre autorité (ou d'un autre État). Elle atteste que le système de destination répond aux exigences de sécurité imposées et que les risques résiduels peuvent être supportés

conformément aux techniques les plus récentes. L'OSI comble ainsi une lacune qui compliquait jusqu'à présent la collaboration internationale dans le domaine de la sécurité. Contrairement à la majorité des pays qui exigent une certification pour le traitement électronique des informations classifiées, l'OSI ne prévoit de demander une certification que lorsqu'elle est nécessaire à la collaboration nationale ou internationale.

g. Sécurité des personnes

La prise de responsabilité vis-à-vis des risques de sécurité liés aux personnes est une tâche de direction permanente. Le nouvel art. 20*a* de la loi du 24 mars 2000 sur le personnel de la Confédération (LPers)[8], introduit par la LSI, permet aux employeurs d'exiger des candidats à un poste et de leurs employés qu'ils produisent un extrait de leur casier judiciaire et du registre des poursuites, si cela est nécessaire pour préserver leurs intérêts. La pratique a montré qu'une fois le contrôle de sécurité relatif aux personnes (CSP) effectué, les risques liés aux personnes ne donnaient souvent plus matière à discussion. Dans l'esprit d'un suivi largement répandu sur le plan international (appelé *aftercare*), les collaborateurs contrôlés doivent donc signaler à leur employeur les faits de leur environnement privé et professionnel susceptibles de menacer la sécurité (p. ex. dettes de jeu, relations problématiques ou voyages dans des pays particuliers). De tels faits peuvent être très pesants psychiquement pour les collaborateurs. Son devoir d'assistance impose à l'employeur en vertu de l'art. 4, al. 2, let. g, LPers d'écouter ses employés et d'essayer de trouver avec eux le moyen de réduire leur exposition aux risques. Le traitement d'un risque potentiellement élevé reste de la compétence de l'employeur. Celui-ci peut exiger des collaborateurs concernés les extraits visés à l'art. 20*a* LPers, y compris durant la période de répétition du CSP. Selon le cas, une telle annonce peut entraîner une répétition extraordinaire du CSP.

h. Responsables de la sécurité de l'information et préposés à la sécurité de l'information

Une nouveauté importante de l'OSI concerne les directions d'office. L'OSI leur délègue des tâches, compétences et responsabilités concrètes dans le domaine de la sécurité de l'information qu'elles peuvent, si nécessaire, confier à un membre de leur direction (responsable de la sécurité de l'information). Les responsables de la sécurité de l'information surveillent le SMSI de l'office et prennent toutes les décisions importantes relatives à la sécurité de l'information. Les activités de surveillance opérationnelles relèvent des préposés correspondants, conformément à l'art. 37 OSI. L'OSI fusionne les rôles existants de *délégué à la sécurité informatique* et de *préposé à la protection des informations* dans un nouveau rôle, celui de *préposé à la sécurité de l'information*. Ses tâches seront précisées en conséquence et complétées par la gestion du SMSI.

Au sens des art. 37, 38, 41 et 42 LOGA, les départements sont responsables du pilotage, de la coordination et de la surveillance de la sécurité de l'information en leur sein. Ils définissent notamment la politique de sécurité de l'information et l'organisation de la sécurité départementale. La responsabilité opérationnelle de la sécurité incombe au secrétaire général, pour autant que le chef de département n'en décide autrement. Les préposés à la sécurité de l'information continuent d'assumer la coordination et la surveillance opérationnelles (cf. art. 81 LSI).

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

La LSI crée un service spécialisé de la Confédération pour la sécurité de l'information. L'art. 83 LSI fixe les tâches de ce service qui lui permettront de collaborer avec les autorités soumises à la LSI indépendantes du Conseil fédéral. Ces tâches consistent essentiellement à apporter un soutien et à assurer la coordination. L'OSI précise ces tâches pour le domaine de compétence du Conseil fédéral. Le service spécialisé émettra, pour l'administration fédérale et l'armée, les directives nécessaires en matière d'organisation, de personnel et de construction, de même que sur le plan technique, pour garantir la sécurité de l'information en fonction de l'état d'avancement de la technologie. Il apportera en outre son aide à la ChF et aux départements dans la gestion de la sécurité. Sur le plan international, il jouera le rôle d'autorité nationale pour la sécurité (cf. message LSI, ch. 5.2 et art. 42, al. 3, OSI). Le service spécialisé de la Confédération pour la sécurité de l'information fait partie du Secrétariat d'État à la politique de sécurité (SEPOS) du DDPS. Il reprend les tâches de l'Office fédéral de la cybersécurité (OFCS) pour ce qui est de l'autoprotection de la Confédération (directives et conseils).

L'OFCS se concentre sur la protection de la Suisse face aux cyberrisques. Du fait que la LSI prévoit une obligation d'annoncer les cyberincidents, l'OFCS développera ses prestations au profit des

[8] RS **172.220.1**

infrastructures critiques, des milieux économiques et de la population. Il continuera cependant de conseiller et de soutenir la ChF, les départements et les offices dans les questions de cybersécurité, y compris lorsqu'il s'agira d'émettre des directives techniques. Les autorités fédérales sont de même tenues, en vertu des modifications de la LSI, d'annoncer les cyberincidents à l'OFCS. Si les départements et les offices ne sont pas en mesure de gérer eux-mêmes un incident, l'OFCS leur apportera son soutien ou, après avoir consulté le service spécialisé de la Confédération pour la sécurité de l'information, dirigera les opérations.

Étant donné que le service spécialisé de la Confédération pour la sécurité de l'information ne sera pas encore opérationnel au moment où la LSI entrera en vigueur, l'OFCS continuera d'assumer ses tâches jusqu'à l'été 2025 pour ce qui est de l'autoprotection de la Confédération (sécurité informatique de la Confédération).

2.4 Modification de l'ordonnance sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération (OIAM)

Jusqu'à présent, l'OIAM s'appuyait en premier lieu sur la LOGA. Les art. 24 à 26 LSI créent une base légale formelle spécifique sur laquelle l'OIAM se basera. En vertu de l'art. 20, al. 2, LSI, il sera en outre possible d'utiliser des données biométriques dans les systèmes IAM sous certaines conditions. L'OIAM doit donc être modifiée en ce sens.

Dans le cadre du service standard eIAM, l'administration fédérale a mis en place un service d'authentification permettant l'accès à ses applications spécialisées et à ses prestations de cyberadministration. L'utilité de ce service n'est plus à démontrer et l'objectif est désormais de le mettre à la disposition des cantons intéressés (et de leurs communes) pour que ceux-ci puissent y intégrer leurs propres applications, sur la base de la loi fédérale sur l'utilisation de moyens électroniques pour l'exécution des tâches des autorités (LMETA). L'OIAM doit donc être modifiée en ce sens.

Dans le cadre du présent projet, seules les modifications découlant de la LSI et de la LMETA sont prises en compte dans l'OIAM. Le reste des modifications nécessaires de l'OIAM est l'objet d'une révision totale que la ChF a déjà entamée.

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

a. Généralités

En adoptant la LSI, le législateur y a transposé les dispositions relatives aux CSP de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)[9]. Dans le même temps, les dispositions légales ont été adaptées aux besoins actuels de la sécurité de l'information. Pour certains motifs de contrôle n'ayant pas trait à la sécurité de l'information (p. ex. la lutte contre la corruption), de nouvelles bases légales ont été créées dans d'autres lois. Cette modernisation du droit des CSP vise également à renforcer leur efficacité en élargissant la palette des données auxquelles les services spécialisés CSP peuvent accéder afin d'évaluer les risques pour la sécurité. Le Conseil fédéral veut en contrepartie réserver les CSP, selon le nouveau droit, aux fonctions recelant effectivement un risque considérable pour la Confédération et l'armée. Leur nombre sera par conséquent nettement réduits. Les CSP doivent pouvoir être effectués de manière appropriée dans les délais à l'aide des ressources existantes. Le nouveau droit mise plus sur la qualité que sur la quantité. Les principales modifications apportées au cadre juridique des CSP sont contenues dans la LSI même.

b. Objet

L'OCSP (nouvelle) réunit les dispositions d'exécution sur les différents contrôles de sécurité relatifs aux personnes dans un seul acte. Elle remplace l'ordonnance du 4 mars 2011 sur les contrôles de sécurité relatifs aux personnes (OCSP)[10], l'ordonnance du 9 juin 2006 sur les contrôles de sécurité relatifs aux personnes dans le domaine des installations nucléaires (OCSPN)[11] et toutes les ordonnances départementales sur les contrôles de sécurité relatifs aux personnes[12].

L'ordonnance règle matériellement tant les CSP au sens de la LSI que tous les autres contrôles, appréciations et examens qui, sans être prévus par la LSI, doivent être effectués en appliquant la procédure des CSP de la LSI. Quelle que soit leur dénomination ou leur motif, ils visent tous

[9] RS **120**
[10] RS **120.4**
[11] RS **732.143.3**
[12] RS **120.421**–**120.427**

à juger la fiabilité des personnes concernées dans le cadre de l'exercice d'une activité déterminante. Les mêmes données sont collectées et la même méthode d'évaluation est appliquée au sein des mêmes degrés de contrôle.

c. Champ d'application

L'OCSP s'applique à toutes les autorités et à toutes les organisations soumises à la LSI. Son champ d'application est limité pour les unités administratives décentralisées et les organisations auxquelles sont confiées des tâches administratives au sens de l'art. 2, al. 4, LOGA : seules celles qui sont concernées par le champ d'application de l'OSI relèvent aussi de celui de l'OCSP pour ce qui est des CSP visés par la LSI. Les unités administratives décentralisées qui entrent dans le champ d'application de la LPers peuvent également être concernées par les contrôles inhérents aux contrôles de loyauté visée à l'art. 20*b* LPers et ainsi tomber sous le coup de l'OCSP.

L'OCSP s'applique également aux autorités soumises à la LSI visées à l'art. 2, al. 1, LSI qui sont indépendantes du Conseil fédéral. Le législateur a en effet octroyé à l'art. 48 LSI au seul Conseil fédéral la compétence de régler les modalités de la procédure de contrôle et de l'organisation des services spécialisés CSP. Les autorités concernées restent en revanche chargées d'émettre les listes des fonctions et de désigner les services qui demandent le contrôle et les instances décisionnelles.

d. Restriction des motifs de contrôle

La nouvelle législation restreint les motifs de contrôle. Les fonctions rattachées au degré de contrôle le plus élevé – le contrôle de sécurité élargi – doivent rester l'exception. Il y a cependant un risque que la valeur seuil légale des contrôles soit abaissée dans la pratique si les offices ne disposent pas d'autres instruments leur permettant de contrôler la loyauté de leur personnel. L'art. 20*a* LPers propose aux employeurs des moyens correspondants.

e. Listes de fonctions

Maintenir le nombre de contrôles dans le cadre ciblé exige un meilleur contrôle de la licéité de l'inscription des fonctions soumises au contrôle lors de l'établissement et de la mise à jour des listes desdites fonctions. Pour cette raison, le DDPS gérera ces listes de façon centralisée et les actualisera régulièrement à la demande des départements et de la ChF.

Les listes des fonctions soumises à contrôle selon la LSI sont sensibles du point de vue de la sécurité de l'information. Elles offrent la vue d'ensemble de toutes les fonctions au sein de l'administration et de l'armée qui ont accès à des informations classifiées ou qui gèrent ou exploitent des systèmes informatiques critiques de la Confédération. Même si ces listes ne contiennent pas les noms des chargés de fonction, c'est chose facile pour un attaquant potentiel, à l'époque des réseaux sociaux, de relier un nom à une fonction et d'obtenir ainsi une cible pour des actions d'espionnage ou de sabotage. Dans le domaine militaire, les listes de fonctions détaillées peuvent permettre de tirer des conclusions sur les détails non publiés de l'organisation de l'armée. Par conséquent, en vertu de l'art. 6 de la loi du 18 juin 2004 sur les publications officielles (LPubl)[13], les listes contenant les fonctions soumises à contrôle au sens de la LSI ne seront pas publiées. Pour les mêmes raisons, les listes des fonctions selon la loi du 23 mars 2007 sur l'approvisionnement en électricité (LApEl)[14] ne seront pas non plus publiées. En revanche, les listes des fonctions soumises à contrôle en premier lieu à des fins de lutte contre la corruption ou de protection de la réputation de la Confédération seront publiées comme à présent.

2.6 Ordonnance sur la procédure de sécurité relative aux entreprises (OPSEnt)

a. Généralités

La LSI (art. 49 à 72) introduit la procédure de sécurité relative aux entreprises. La procédure a pour objet la sécurité de l'information dans le cadre de l'attribution de mandats sensibles des autorités fédérales à des entreprises non soumises à leur surveillance directe. Elle sert à contrôler la fiabilité de l'entreprise pressentie. Les entreprises influencées par des services de renseignement étrangers ne doivent pas avoir accès aux informations sensibles ou aux moyens informatiques critiques de la Confédération. La procédure permet également de contrôler et de faire respecter la sécurité de l'information durant l'exécution du mandat.

[13] RS **170.512**
[14] RS **734.7**

b. Objet et champ d'application

L'OPSEnt règle les détails de la procédure et remplace l'ordonnance du 29 août 1990 concernant la sauvegarde du secret[15], qui se limitait aux mandats à contenu militaire classifié. L'OPSEnt s'applique à toutes les autorités et organisations qui tombent sous le coup de la LSI. Elle ne s'applique aux unités de l'administration fédérale décentralisée que dans la mesure où celles-ci tombent sous le coup de l'OSI (cf. ch. 2.3, let. b).

c. Acquisitions subordonnées

L'ordonnance définit les acquisitions auxquelles s'applique la procédure dans tous les cas. Sont concernés les mandats dont l'exécution requiert l'accès à des informations classifiées SECRET et les acquisitions de systèmes sensibles destinés à traiter des informations classifiées CONFIDENTIEL de plusieurs organisations ou qui seront utilisés par plusieurs offices et départements. Pour toutes les autres acquisitions, le service spécialisé chargé de la procédure de sécurité relative aux entreprises évaluera la nécessité d'une procédure avec l'adjudicateur.

d. Coordination avec le droit des marchés publics

Comme la LSI, la nouvelle ordonnance se recoupe à plusieurs occasions avec le droit de la Confédération sur les marchés publics. Ces recoupements ont été examinés en détail et réglés lors de l'élaboration de l'avant-projet, en collaboration avec des représentants des offices spécialisés. L'application en bonne et due forme de la procédure de sécurité relative aux entreprises suppose une étroite collaboration entre l'adjudicateur, le service d'achat et le service spécialisé chargé de ladite procédure. Cette collaboration doit s'opérer si possible au tout début du processus d'acquisition. Cela permet d'identifier et de réduire de bonne heure les risques liés à l'acquisition.

2.7 Délais transitoires

Afin d'assurer la fluidité du passage au nouveau droit, tant la LSI que ses ordonnances d'exécution prévoient des délais transitoires appropriés. Les délais transitoires s'appliquant aux offices, secrétariats généraux, aux groupements et à la ChF dès l'entrée en vigueur de la LSI sont les suivants :

- 1 an pour établir un catalogue indiquant comment classifier les informations relevant de leur compétence en vertu du nouveau droit (cf. art. 51, al. 5, OSI) ;
- 2 ans pour mener une analyse du besoin de protection et classer leurs moyens informatiques conformément au nouveau droit (cf. art. 90, al. 2, LSI) ;
- 3 ans pour
  - mettre en place leur SMSI (cf. art. 51, al. 4, OSI),
  - contrôler leur liste des fonctions relative aux CSP (cf. art. 6, al. 1, OCSP) ;
- 6 ans (un cycle de vie) pour mettre en œuvre les nouvelles prescriptions de sécurité techniques pour l'ensemble des moyens informatiques (cf. art. 90, al. 2, LSI).

[15] RS **510.413**

3 Commentaire des dispositions

3.1 Ordonnance sur la sécurité de l'information (OSI)

Préambule

Le préambule renvoie à toutes les normes légales qui attribuent au Conseil fédéral une compétence de légiférer dans le cadre de l'OSI.

Section 1 Dispositions générales

Art. 1 Objet

La notion de *sécurité de l'information* s'applique à la sécurité de toutes les informations, y compris des données personnelles visées par la législation sur la protection des données, dont sont responsables l'administration fédérale et l'armée. L'OSI règle les tâches, responsabilités et compétences et les procédures garantissant la sécurité de l'information dans l'administration fédérale et l'armée qui sont nécessaires, dans le cadre de la gestion de la sécurité de l'information, de la protection des informations classifiées, de la sécurité informatique et des mesures relatives à la sécurité des personnes et à la protection physique. Comme dans la LSI (cf. message LSI, commentaire de l'art. 1), la notion d'*information* n'est pas définie par l'OSI. Cette notion couvre aussi les données. Lorsque l'OSI fait mention de *données personnelles*, elle fait référence à celles visées dans la législation sur la protection des données.

Le rapport entre la LSI et la loi fédérale du 19 juin 1992 sur la protection des données (aLPD), qui n'est plus en vigueur, est détaillé dans le message LSI (cf. ch. 1.2.3, p. 2789). Les organes de sécurité selon les art. 36 ss OSI assureront, dans le cadre du SMSI, la coordination avec les conseillers en protection des données compétents.

Art. 2 Champ d'application

Al. 1 à 3 – L'OSI s'applique au Conseil fédéral, à l'administration fédérale centrale et à l'armée.

Toutes les unités de l'administration fédérale décentralisée au sens de l'art. 7*a* OLOGA[16] et les organisations visées à l'art. 2, al. 4, LOGA auxquelles sont confiées des tâches administratives mais qui ne font pas partie de l'administration fédérale entrent dans le champ d'application de la LSI (cf. art. 2, al. 2, LSI). L'art. 2, al. 3 et 4, LSI confère toutefois au Conseil fédéral la compétence de restreindre l'application de la loi à certaines organisations ou à certaines dispositions de la loi. La loi lui ménage une marge d'appréciation afin de tenir compte de l'autonomie des unités organisationnelles concernées en matière d'exécution. Par la réglementation de l'art. 2, al. 2 et 3, OSI, le Conseil fédéral fait usage de sa marge d'appréciation en ce que les organisations concernées sont exclues du champ d'application de la LSI pour ce qui est de l'utilisation de leurs propres moyens informatiques, indépendamment de leurs catégories de sécurité, mais restent soumises à la LSI dans deux autres domaines. En limitant les dispositions en vertu de l'art. 2, al. 4, LSI dans le domaine de compétence du Conseil fédéral, l'accent est mis sur la sécurité de l'information de l'administration fédérale centrale et de l'armée, afin de conserver leur autonomie d'exécution et de limiter les coûts.

Les unités de l'administration fédérale décentralisée ne relèvent dès lors de la LSI et de l'OSI que lorsqu'elles traitent des informations classifiées de la Confédération, qu'elles accèdent à des moyens informatiques de l'administration fédérale centrale ou qu'elles délèguent la gestion de leurs moyens informatiques aux fournisseurs de prestations informatiques de la Confédération. Dans ces cas, elles ne doivent pas mettre en œuvre la LSI et l'OSI tout entières, mais seulement les dispositions concernant le traitement des informations classifiées ou garantissant la sécurité des moyens informatiques. Il en va de même des organisations visées à l'art. 2, al. 4, OLOGA auxquelles sont confiées des tâches administratives mais qui sont extérieures à l'administration fédérale. Par cette solution pragmatique, les unités administratives décentralisées ne sont concernées que lorsque leurs activités peuvent représenter un danger pour l'administration fédérale décentralisée.

La ChF et les départements peuvent toutefois décider que les unités administratives décentralisées qui leur sont subordonnés sont soumises à l'ensemble de la LSI. La condition en est que ces unités administratives ou ces organisations exercent constamment des activités sensibles au sens de l'art. 5, let. b, LSI. S'agissant du DDPS, cela concerne par exemple l'Autorité de surveillance indépendante des activités de renseignement, qui traite quotidiennement des informations

[16] RS **172.010.1**

classifiées SECRET des services de renseignement. Cette subordination conduit aux mêmes tâches et responsabilités que celles qui incombent aux offices fédéraux de l'administration fédérale centrale en vertu de la LSI et de l'OSI. Ces unités administratives et ces organisations doivent en particulier également gérer un SMSI.

Pour les autres autorités visées à l'art. 2, al. 1, let. a et c à e, LSI (l'Assemblée fédérale, les tribunaux de la Confédération, le Ministère public de la Confédération et son autorité de surveillance ainsi que la Banque nationale suisse), l'OSI s'applique par analogie si elles n'édictent pas leurs propres dispositions d'exécution. Si elles le font, elles sont affranchies de l'OSI (mais pas de la LSI) (cf. au contraire l'application de l'OCSP et de l'OPSEnt).

Al. 4 – Les dispositions de la section 4 de cette ordonnance s'appliquent aux cantons lorsqu'ils traitent des informations classifiées de la Confédération. Si ceux-ci accèdent aux moyens informatiques de la Confédération, ils sont soumis aux dispositions sur les catégories de sécurité (art. 28), les mesures de sécurité (art. 29), la sécurité de l'exploitation (art. 30) et les mesures physiques de protection (art. 34). Toutefois, les cantons peuvent s'affranchir des dispositions légales s'ils garantissent une sécurité équivalente de l'information. Cela suppose qu'ils édictent leurs propres prescriptions de sécurité en se fondant sur les normes fédérales et les font appliquer dans leur domaine de compétence. Les normes fédérales déterminantes sont les prescriptions et les exigences techniques pour la protection informatique de base dans l'administration fédérale (Si001) et pour la protection des informations classifiées. Les cantons ne sont pas tenus de mettre en œuvre un SMSI visé aux art. 5 ss.

Il y a *sécurité équivalente de l'information* lorsque des mesures de sécurité autres que celles prévues dans l'OSI déploient un effet comparable et au moins aussi élevé et performant en fonction de l'avancement de la technologie selon l'art. 85, al. 1, LSI. Les cantons évaluent en premier lieu, selon leur propre appréciation, si la sécurité de l'information est équivalente.

La notion de *cantons* fait référence non seulement aux administrations cantonales, mais aussi aux collectivités, instituts ou fondations de droit public qui relèvent du droit administratif du canton correspondant. S'agissant des cantons, il faut vérifier dans chaque cas si une organisation ou un institut (p. ex. un hôpital, une centrale électrique, voire un institut financier) est considéré comme un canton au sens de la LSI ou de l'OSI. Si une organisation cantonale n'entre pas dans le champ d'application de la LSI, elle est considérée comme un tiers au sens de l'art. 9 LSI (cf. commentaire de l'art. 10).

Al. 4, let. b – On entend par *accès aux moyens informatiques* tous les types d'accès techniques aux moyens informatiques de la Confédération dont les cantons disposent. La question de l'accès doit être examinée dans tous les cas. La Confédération décide en dernier ressort de l'existence d'un accès.

Al. 5 – L'OSI s'applique aussi à l'armée. Les tâches, les compétences et les responsabilités sont assumées comme jusqu'à présent par l'administration militaire, ce que la nouvelle législation doit conserver.

Section 2 Principes

Art. 3 Objectifs de sécurité

Les interfaces techniques entre les moyens informatiques de l'administration fédérale centrale et de l'armée se multiplient. De ce fait, les menaces ou risques encourus par l'organisation ou ses fournisseurs ne peuvent pas être considérés isolément. La sécurité de l'information est forcément une tâche globale qui exige un objectif commun et une approche coordonnée.

Le Conseil fédéral aspire à garantir la protection des informations et des moyens informatiques par une approche fondée sur les risques encourus. La concrétisation de la sécurité sur la seule base d'une liste de contrôle ne suffit plus. Les responsables doivent plutôt gérer activement les risques, connaître les menaces qui pèsent sur la sécurité de l'information et leurs éventuelles répercussions, adapter la charge de travail pour réduire les risques en fonction de l'ampleur de ces risques et se concentrer sur les risques majeurs en les jugulant par les mesures les plus efficaces qui soient. Avec l'approche fondée sur les risques, l'accent doit être mis tant sur les risques encourus (répercussions négatives) que sur les possibilités et les occasions (répercussions positives) offertes par les nouvelles idées, applications et technologies. La *résilience* est la capacité d'une organisation à faire face à un incident de sécurité et à retourner à un fonctionnement normal.

Art. 4 Responsabilité

Al. 1 et 2 – Conformément à l'art. 45 LOGA, les directeurs des groupes et des offices sont responsables vis-à-vis de leurs supérieurs hiérarchiques de la conduite des unités administratives qui leur sont subordonnées et de l'exécution des tâches qui leur sont déléguées. Cela inclut donc la responsabilité de la sécurité de l'information. L'OFCS a certes fixé jusqu'à présent un minimum de consignes en matière de sécurité de l'information, notamment la protection informatique de base dans l'administration fédérale, qui servent à protéger l'ensemble de l'administration fédérale et que les offices, les secrétariats généraux, les groupements et la ChF doivent appliquer avec une marge de manœuvre limitée. Toutefois, cela ne les dégage pas l de leur responsabilité dans l'évaluation continue des risques et dans la prise des mesures qui peuvent s'imposer. Afin de garantir cette protection de l'ensemble de l'administration fédérale, les cantons traitant des informations classifiées de la Confédération oui qui accèdent à ses moyens informatiques, devront aussi respecter ces exigences (cf. commentaire de l'art. 49).

Al. 3 – Le personnel doit respecter les règles de comportement fixées pour le traitement des informations et l'utilisation des moyens informatiques de la Confédération. Il est donc indispensable qu'il reçoive une instruction appropriée à ce sujet et qu'il dispose des moyens nécessaires (cf. commentaire de l'art. 4, al. 4, et art. 11 OSI).

On entend par *collaborateurs de l'administration fédérale* les collaborateurs internes et externes qui reçoivent des instructions de la Confédération : les collaborateurs *internes* sont des employés de la Confédération conformément à la LPers, tandis que les collaborateurs *externes* sont des personnes embauchées dans le cadre d'un contrat de location de services. Ne sont pas considérés comme collaborateurs de la Confédération les indépendants ou les collaborateurs d'entreprises qui, sur la base d'une relation contractuelle par exemple, conseillent la Confédération ou lui fournissent des prestations de service ou matérielles (comme le développement de logiciels, l'extension du réseau, la construction d'un local de serveurs, la prise en charge de la direction d'un projet, etc.). Ces personnes sont des *tiers* ; voir le commentaire de l'art. 10. En ce qui les concerne, la gestion réglementaire des objets à protéger doit être garantie et contrôlée, le cas échéant, par des contrats au sens de l'art. 9 LSI.

Al. 4 – À chaque échelon hiérarchique, les supérieurs sont également responsables dans le domaine de la sécurité de l'information de l'instruction pratique et spécifique à la fonction de leurs collaborateurs et des militaires qui leur sont subordonnés ainsi que du contrôle du respect des consignes. Il leur incombe d'expliquer concrètement à leurs collaborateurs comment gérer les informations protégées, de les rendre attentifs à une utilisation rigoureusement conforme aux directives des logiciels de cryptage et de veiller à ce qu'ils suivent les formations proposées. Voir le commentaire de l'art. 11 OSI au sujet de la responsabilité des offices, des secrétariats généraux, des groupements et de la ChF.

Section 3 Gestion de la sécurité de l'information

Les art. 5 à 15 OSI définissent les exigences minimales à appliquer à la gestion de la sécurité de l'information au sein de l'administration fédérale et de l'armée. Ils précisent, pour les tâches essentielles de la sécurité de l'information, les responsabilités des offices, de la ChF, des départements et du service spécialisé de la Confédération pour la sécurité de l'information. Ce dernier édictera des consignes à ce sujet et mettra à disposition les outils nécessaires. L'OFCS fournit des prestations importantes servant à la gestion de la sécurité de l'administration fédérale, en particulier lorsqu'il s'agit de maîtriser les cyberincidents (cf. art. 12).

Art. 5 Système de management de la sécurité de l'information

Al. 1 – Un SMSI se compose de procédures et de règles qui expliquent comment la sécurité de l'information est organisée au sein d'un système et qui montrent quelles tâches, compétences et responsabilités relèvent de qui (cf. ch. 2.3, let. d).

Tandis que les responsables de la sécurité de l'information des unités administratives (cf. art. 36) garantissent la constitution, le fonctionnement, la vérification et l'amélioration continue du SMSI, l'exploitation à proprement parler de celui-ci incombe, sur mandat des premiers, aux préposés à la sécurité de l'information des unités administratives (cf. art. 37, al. 2, let. a). Selon l'art. 51, al. 4, un SMSI doit être mis sur pied au plus tard trois ans après l'entrée en vigueur de l'OSI.

Al. 2 – L'objectif d'un SMSI est la gestion et l'amélioration de la sécurité de l'information au sein de l'organisation. Des objectifs concrets sont nécessaires, sur la base desquels la direction de

l'office peut juger si l'effet souhaité est atteint. La définition et la mesure annuelles des objectifs sont une tâche de conduite qui incombe à la direction de l'office.

Al. 3 – Afin de garantir une certaine objectivité et comparabilité dans l'évaluation de la mise en œuvre et de l'efficacité du SMSI, une vérification périodique à effectuer par un service indépendant de l'office ou de la ChF ou par le département est exigée. Cette vérification indépendante du SMSI permet l'amélioration continue de la sécurité et met les partenaires de l'office en confiance. L'office ou la ChF décide de la manière dont elle entend utiliser les résultats de l'évaluation et des mesures à mettre en œuvre. Le processus d'amélioration continue est crucial pour garantir la sécurité de l'information. De tels contrôles permettent de tenir compte de ce processus.

La périodicité de trois ans s'oriente sur le cycle de certification officiel de la norme ISO (ISO/IEC 27001), mais l'ampleur de la vérification prescrite est nettement moins ambitieuse que celle de la norme ISO : un audit formel au sens de la norme ISO n'est pas forcément demandé, même si pareil audit serait le bienvenu. Selon le mandat, le SMSI peut être contrôlé dans son intégralité ou partiellement. L'unité administrative concernée a la compétence décisionnelle quant au choix de l'organisme de contrôle indépendant. Les vérifications peuvent être effectuées soit par les structures de surveillance internes des départements, soit par une entreprise externe (cf. commentaire du message LSI, p. 2829).

Al. 4 – Cet alinéa démontre le lien étroit entre le SMSI et la gestion des risques de la Confédération, la gestion de la continuité de l'exploitation et la gestion des crises. Il s'agit de tâches de gestion externes au champ d'application de l'OSI, mais que les unités administratives doivent harmoniser et coordonner étroitement.

Art. 6 Gestion des bases légales et des engagements contractuels

Une liste des bases légales déterminantes dans le propre domaine de compétences et des engagements contractuels dans le domaine de la sécurité de l'information est utile pour attester du respect des bases légales pertinentes qui sont vérifiées par exemple dans le cadre de la mesure de l'atteinte annuelle des objectifs du SMSI selon l'art. 5, al. 2, OSI ou de la vérification du SMSI selon l'art. 5, al. 3, OSI. Du fait de l'extension des chaînes d'approvisionnement dans le domaine de la sécurité de l'information, une vue d'ensemble des obligations à s'acquitter et des droits à faire valoir est indispensable et favorise notamment l'utilisation de synergies avec d'autres relations contractuelles existantes.

Le service spécialisé conseille les unités administratives sur les questions de sécurité et notamment lors de la gestion des consignes touchant la sécurité (p. ex. des directives ou des lignes directrices) ou des projets (p. ex. dans le domaine informatique et ayant de l'importance pour la sécurité) des unités administratives ou des départements.

Art. 7 Inventaire des objets à protéger

Al. 1 – Un inventaire liste tous les objets à protéger conformément à l'art. 7, al. 2, OSI à un moment donné (liste d'inventaire).

Al. 2 – L'OPCy ne connaissait que la notion d'*objet informatique à protéger* (cf. art. 3, let. h, OPCy), notion couverte par la let. b. Les informations ne sont toutefois pas toujours traitées dans un seul système d'information dédié. C'est par exemple le cas lorsqu'une tâche est effectuée en utilisant l'environnement informatique standard de la Confédération ou lorsque les informations sont traitées dans une solution informatique en nuage externe. La notion d'objet « informations » à protéger au sens de la let. a fait donc abstraction d'une quelconque dépendance à un système informatique pour ne tenir compte que de la protection des informations dont le traitement est nécessaire à l'accomplissement de la tâche. En principe, les mêmes critères et méthodes d'évaluation du besoin de protection que pour les objets informatiques à protéger sont applicables. Plusieurs objets à protéger de même nature ou connexes peuvent également être réunis pour n'en former qu'un. Les consignes du service spécialisé de la Confédération pour la sécurité de l'information (cf. art. 15) préciseront ces notions.

Al. 3 – Seule une liste d'inventaire à jour peut garantir le suivi de toutes les informations sur les objets à protéger conformément aux let. a à g.

Al. 3, let. c – L'aperçu des liens contractuels avec des tiers (cf. commentaire de l'art. 10, al. 1, OSI), par exemple avec des fournisseurs informatiques, sert à la bonne gestion des fournisseurs et permet d'identifier de bonne heure d'éventuelles dépendances de la Confédération à des

fournisseurs (avec l'évaluation du danger d'accumulation de risques). Il permet aussi d'identifier les risques qui, à travers ces fournisseurs, peuvent avoir un impact sur la Confédération.

Al. 3, let. e – La mise en œuvre des mesures de sécurité ne doit pas nécessairement être documentée dans l'inventaire même. L'inventaire doit au moins mentionner l'endroit où l'on peut trouver la documentation de sécurité et qui en est responsable.

Al. 3, let. f – Voir le commentaire de l'art. 13, en relation avec l'art. 5, al. 2 et 3, OSI.

Al. 3, let. g – La possibilité d'utilisation partagée des objets à protéger respectifs renvoie au principe du *once only*. Les unités administratives décident à leur seule discrétion des objets à protéger qui seront partagés avec d'autres unités administratives. Lorsque l'objet à protéger contient des données personnelles, toutes les unités administratives concernées doivent bien entendu disposer des bases légales nécessaires afin d'accéder à ces données et de les traiter.

Art. 8 Gestion des risques

Al. 1 – L'évaluation des risques est l'un des fondements d'une gestion efficace des risques et d'une sécurité de l'information adéquate et économique (cf. commentaire du message LSI, p. 2829 s.). Les directives en matière informatique applicables à la protection de base de la Confédération offrent, dans une approche spécifiquement axée sur les risques, une protection contre une multitude de menaces. Elles servent à la sécurité globale de l'information de la Confédération et doivent être respectées. Elles permettent le suivi de moyens informatiques peu sensibles avec une charge de travail réduite. Dans ce cas, les unités administratives n'ont pas besoin de procéder à des évaluations complexes des risques.

Al. 1, let. a – L'évaluation des risques à l'aune de leurs répercussions sur les objets à protéger (art. 7, al. 2, OSI) est, dans ce rapport, très liée à des mesures opérationnelles techniques et concerne, selon les besoins, la confidentialité, la disponibilité, l'intégrité ou la traçabilité des informations et du système informatique.

Al. 1, let. b – Le contrôle de l'efficacité des mesures de la sécurité de l'information peut par exemple prendre la forme de tests de pénétration ou s'effectuer par la collecte d'indicateurs-clés.

Al. 1, let. c – Voir le commentaire sur la gestion des bases légales et des engagements contractuels selon l'art. 6 OSI.

Al. 1, let. d – Il est demandé une décision consciente du responsable de la sécurité de l'information, c'est-à-dire l'acceptation démontrable des risques résiduels sur la base d'un processus d'analyse et de décision minutieux.

Le fait d'être démontrable n'est associé à aucune forme particulière. Dans le contexte de la numérisation, cela doit permettre de recourir à des méthodes de démonstration neutres sur le plan technologique.

Al. 3 – Les instructions sur la politique des risques de la Confédération et les directives et manuels qui y ont trait sont déterminants. Les offices rendent compte à leur département, qui fait ensuite rapport au Conseil fédéral. La consolidation est effectuée par le service de coordination Gestion des risques de la Confédération et la CSG.

Art. 9 Autorisation et liste des exceptions

Comme précédemment avec l'OFCS, le service spécialisé de la Confédération pour la sécurité de l'information déterminera à la suite de l'entrée en vigueur de l'OSI, sur la base de l'art. 85 LSI, les exigences de sécurité de l'information minimales qui doivent être satisfaites. Dans ses directives, il fixera également qui décidera des dérogations au respect des consignes minimales. La procédure des dérogations de l'OPCy valable jusqu'ici peut être reprise.

Art. 10 Collaboration avec les tiers

Al. 1 – La LSI qualifie de *tiers* toutes les autorités, organisations et personnes de droit public ou privé qui ne sont pas des autorités ou organisations qui lui sont soumises et qui agissent indépendamment de celles-ci. Les unités administratives décentralisées sont aussi considérées comme des tiers dans la mesure où elles ne sont pas concernées par la LSI (cf. message LSI, p. 2824 et 2831), ainsi que certaines organisations qui utilisent des infrastructures critiques (cf. art. 2, al. 5, LSI). L'évaluation des risques pour la sécurité est régie par l'art. 8 OSI.

Al. 3 – Plusieurs incidents survenus chez des partenaires externes de la Confédération ont montré qu'ils doivent respecter les mêmes normes de sécurité que les autorités fédérales lorsqu'ils traitent des informations de la Confédération ou fournissent des prestations informatiques à la Confédération. Les contrats passés avec des tiers doivent donc fixer des exigences claires en matière de sécurité de l'information et garantir leur vérification. Ils doivent entre autres contenir l'obligation de garantir la protection des informations et des données de la Confédération conformément aux normes fédérales (y c. exigences en matière de protection des données, cf. message LSI à propos de l'art. 9) et d'annoncer les incidents de sécurité. De même, ils doivent préciser les modalités visant à démontrer la mise en œuvre des consignes de sécurité et prévoir en particulier un droit d'audit pour la Confédération.

Art. 11 Formation et sensibilisation

Pour améliorer durablement leur sécurité, l'administration fédérale et l'armée doivent sensibiliser et former leurs collaborateurs et leurs militaires (dont les responsables hiérarchiques) sur le sujet de façon à ce qu'ils ne mettent pas seulement en œuvre les mesures préventives de sécurité dans le respect des prescriptions, mais qu'ils soient en mesure d'identifier eux-mêmes les dangers et les menaces, de réagir correctement et de diffuser les annonces de sécurité correspondantes.

Les unités administratives assurent la formation générale (par des campagnes régulières de sensibilisation ou des formations d'entrée) pour tous les collaborateurs et l'allocation du budget, du temps et des ressources requis. Ceci en complément des supérieurs hiérarchiques directs, qui sont responsables de la formation spécifique à la fonction de leurs collaborateurs (cf. commentaire de l'art. 4, al. 4, OSI).

Art. 12 Gestion des incidents

Al. 1 – Les unités administratives sont responsables de la maîtrise des incidents de sécurité et du traitement des failles de sécurité. Elles doivent donc prévoir, dans le cadre de leur SMSI, dans l'office et avec les fournisseurs de prestations d'annoncer les incidents de sécurité et déterminer la réponse à y apporter. Un *incident de sécurité* est un événement lors duquel une atteinte est ou a été portée à la sécurité de l'information ou aux consignes de sécurité. Une *faille de sécurité* est un défaut d'un moyen informatique qui, s'il est exploité, peut porter atteinte à la sécurité de l'information. Il est important de fixer au préalable qui, face à un événement, décide des mesures d'urgence et qui, pour une telle décision, doit être consulté ou informé. Celui qui détient la compétence décisionnelle en pareil cas doit nécessairement connaître les répercussions de ces mesures sur les affaires.

Al. 2 – Cette disposition et le droit en vigueur jusqu'ici se recoupent (cf. art. 14, al. 4, let. c, OPCy).

Al. 3 – S'agissant de la mise en place et de l'exploitation de leur SMSI, les offices, leurs départements et la ChF sont capables de maîtriser les incidents de manière professionnelle selon une approche systématique. Tant le service spécialisé de la Confédération que l'OFCS peuvent conseiller ou soutenir les unités administratives et les départements. La tâche de l'OFCS consistera comme jusqu'à présent essentiellement à fournir des conseils en matière de cybersécurité ; le service spécialisé proposera pour sa part des conseils généraux dans le domaine de la gestion de la sécurité et répondra aux questions techniques dans les domaines du droit de la sécurité, de la sécurité industrielle et de la sécurité des personnes. La disposition potestative souligne que le service spécialisé de la Confédération pour la sécurité de l'information et l'OFCS peuvent apporter leur soutien, mais n'y sont pas obligés. En principe, ces services apportent leur soutien à la demande des unités administratives ou des départements. Les priorités du soutien seront fixées en fonction de la criticité et de l'importance de l'incident et des ressources à disposition.

Al. 5 à 7 – Si un incident a atteint ou pourrait atteindre une dimension importante, les offices et les départements doivent l'annoncer au service spécialisé. Les critères visés à l'al. 5 concernent des incidents pouvant impacter non seulement les intérêts et les tâches de l'office ou du département mais encore l'ensemble de l'administration fédérale. La haute importance politique d'un incident dépend tant des informations, des systèmes informatiques ou des organisations concernés que des circonstances dans lesquelles il s'est produit. L'importance politique d'un incident a tendance à évoluer de manière dynamique. Celle-ci est examinée avec la personne responsable de la sécurité de l'information de l'office ou du département concerné.

Lorsque qu'un incident est critique au sens des critères de l'al. 5, le service spécialisé examine avec l'unité administrative concernée et, lorsque la cybersécurité est en jeu, également avec l'OFCS, s'il est nécessaire d'apporter un soutien, voire de prendre la tête des opérations.

Lorsqu'il y a péril en la demeure, cette décision est prise très rapidement. Selon l'ampleur de l'incident ou des vulnérabilités décelées, les opérations peuvent être dirigées soit par le service spécialisé, soit par l'OFCS. On entend par *direction des opérations*, la compétence décisionnelle opérationnelle. Toutefois, l'unité administrative ou le département concerné reste responsable de la sécurité de l'information (cf. commentaire de l'art. 4 OSI). Si le service spécialisé ou l'OFCS prend la direction des opérations, il peut ordonner des mesures immédiates ou avoir recours à des spécialistes. Les coûts engagés dans ce cas sont à la charge de l'unité administrative responsable ou du département et sont l'objet d'une concertation avec ceux-ci.

À la suite de l'introduction d'une obligation d'annoncer les cyberincidents (cf. ch. 2.1 plus haut), les autorités fédérales, comme toutes les autres infrastructures critiques, doivent signaler à l'OFCS qu'elles sont victimes d'une cyberattaque. Le DDPS veillera à ce que l'annonce à l'OFCS et au service spécialisé soit coordonnée et à ce que les processus de maîtrise des incidents de sécurité soient clairs, efficients et efficaces. S'agissant du traitement des données dans le cadre de la gestion des incidents, voir les art. 44 à 46 OSI.

Art. 13 Planification des contrôles et des audits

Le manque de contrôles et d'audits est une lacune considérable dans la gestion de la sécurité de l'information de l'administration fédérale et de l'armée. Seuls des audits adéquats permettent aux organisations de connaître le niveau de sécurité de leurs informations, de savoir quels risques elles encourent et quelles mesures s'imposent (cf. message LSI, p. 2790). Cette disposition demande donc que les unités administratives et les départements définissent annuellement les contrôles et les audits fondés sur les risques qu'ils effectueront l'année suivante et pourquoi. Une vérification du SMSI planifiée en vertu de l'art. 5, al. 3, OSI doit être inscrite sur le plan de contrôle et d'audit. Le plan d'audit et les ressources nécessaires seront approuvés par le responsable de la sécurité de l'information de l'unité administrative (cf. art. 36, al. 3, let. d, OSI). L'art. 13 ne précise pas le nombre de contrôles et d'audits à effectuer. Cette décision relève uniquement de l'unité administrative. Avec le plan de contrôle et d'audit à élaborer obligatoirement, la direction de l'office doit prendre une décision positive traçable.

Les *contrôles* au sens de cette ordonnance sont des vérifications ponctuelles au champ d'application limité ; ils peuvent être effectués de façon informelle en mobilisant moins de ressources et à un coût souvent inférieur à celui des audits. Un office ou la ChF peut, par exemple, planifier le contrôle de l'actualité de la documentation sur la sécurité ou le contrôle du respect de la *politique du bureau bien rangé*. En revanche, les *audits* suivent une procédure formalisée et sont souvent réalisés par un service indépendant. Ils examinent si les systèmes, les processus ou les systèmes de gestion respectent les consignes en vigueur ou les normes exigées.

Al. 2 – Les contrôles et les audits concernent aussi le respect des consignes par des tiers, notamment les fournisseurs. Tous les contrats passés avec des tiers devraient prévoir un droit d'audit pour la Confédération (cf. art. 10, al. 3). Si un tel contrôle est prévu et si le tiers dispose d'une déclaration de sécurité (cf. art. 61 ss LSI), une coordination avec le service spécialisé chargé de la procédure de sécurité relative aux entreprises permet à la Confédération d'engager pertinemment ses ressources en évitant de contrôler plusieurs fois les mêmes éléments chez un partenaire.

Al. 3 – À la demande des autorités fédérales, le service spécialisé de la Confédération pour la sécurité de l'information peut procéder à des contrôles (cf. art. 83, al. 1, let. c, LSI). Le niveau d'ambition est volontairement peu élevé et l'extension de la capacité d'audit du service spécialisé de la Confédération pour la sécurité de l'information n'est pas envisagée actuellement. Depuis des années, le Contrôle fédéral des finances (CDF) procède à des audits et à des examens transversaux de qualité dans le domaine de la sécurité de l'information. Ces audits ont en point de mire les risques que cible le service spécialisé de la Confédération pour la sécurité de l'information et couvrent ainsi les besoins au niveau de la Confédération.

Art. 14 Compte rendu

Pour améliorer à long terme la sécurité de l'information au niveau de la Confédération, il est nécessaire de contrôler en permanence et de manière critique l'efficacité de la sécurité de l'information et d'adapter régulièrement et judicieusement les mesures de sécurité. Le compte rendu couvre notamment les points suivants : l'état et l'efficacité du SMSI des unités administratives ; l'état des objets à protéger, de la mise en œuvre des mesures de sécurité et de la prise en charge des risques résiduels ; l'état de la formation ; des indications sur les contrôles

de sécurité relatifs aux personnes et sur les procédures de sécurité relatives aux entreprises effectués pour la ChF ou le département ; les conclusions sur les incidents et les failles de sécurité et les mesures d'amélioration prises ou prévues ; les conclusions des contrôles et des audits et les mesures d'amélioration prises ou prévues. Le service spécialisé de la Confédération pour la sécurité de l'information fixe les modalités du compte rendu.

Al. 3 – Selon l'art. 83, al. 1, let. h, LSI, le compte rendu à l'intention du Conseil fédéral porte également sur la situation en matière de sécurité des autres autorités soumises à la LSI, si bien qu'il doit être établi en coordination avec elles. Cette coordination a essentiellement lieu lors de la conférence visée à l'art. 82 LSI.

Art. 15 Directives relatives à la gestion de la sécurité de l'information

Cet article se réfère à l'art. 85 LSI. Le service spécialisé se voit confier par le Conseil fédéral la tâche d'édicter les directives concernant la gestion de la sécurité de l'information (cf. art. 5 à 14) pour l'administration fédérale et l'armée. Concernant la disposition transitoire, voir l'art. 50, al. 6.

Section 4 Informations classifiées

Les art. 18 à 20 décrivent les conditions matérielles de la classification des informations (cf. message LSI à propos de l'art. 13). Elles concordent largement avec les critères appliqués à l'évaluation de l'ampleur des dégâts dus à un événement dans le cadre de la gestion des risques de la Confédération. Par rapport à l'OPrI, les seuils de classification INTERNE, CONFIDENTIEL et SECRET sont relevés. Ce relèvement vise à rendre possible une classification plus ciblée des informations et à améliorer leur protection.

Art. 16 Principes

Al. 1 – La classification est obligatoire dès lors que les critères visés aux art. 18 ss OSI sont remplis. Le principe du *besoin d'en connaître* précisé à l'art. 14 LSI doit être strictement respecté. La classification de matériel est un cas concret de classification des informations auquel s'appliquent les mêmes méthodes d'évaluation et mesures de protection (y c. les consignes de l'OCSP et de l'OPSEnt ; cf. message LSI, p. 2832).

Al. 2 – Le regroupement d'informations ou de supports d'informations classifiés ou non classifiés (p. ex. papier, appareils de stockage de données texte, image et son) peut donner naissance à une compilation qui a besoin d'être davantage protégée qu'une information isolée qu'elle contient. C'est typiquement le cas des bases de données.

Le fait de remettre ou non un document officiel à un demandeur (p. ex. un journaliste) sur le principe de la transparence ne dépend pas de son éventuelle mention de classification, mais s'évalue uniquement en fonction des critères de la loi du 17 décembre 2004 sur la transparence (LTrans)[17]. Les critères sur lesquels se fonde la classification des informations sont harmonisés avec ceux figurant à l'art. 7 LTrans, qui prévoient de limiter, de différer et de refuser l'accès aux documents officiels. La jurisprudence du Tribunal fédéral en matière de secret est déterminante dans tous les cas, en particulier lorsqu'il s'agit de distinguer le secret formel du secret matériel.

Pour le reste, les lois cantonales sur la transparence ne s'appliquent pas aux documents officiels de la Confédération comme les informations classifiées. Les demandes d'accès sont exclusivement régies par le droit fédéral. Si par exemple un canton reçoit une demande d'accès à une information classifiée de la Confédération, c'est le service fédéral responsable de la protection de l'information classifiée qui doit être consulté.

Art. 17 Auteurs de la classification

Al. 1 – Les offices, les secrétariats généraux, les groupements, la ChF et les départements (plus précisément les organes agissant pour eux) sont les services le mieux à même d'évaluer, dans leur domaine de compétence, les informations devant être protégées pour des raisons objectives. Ils sont ainsi les services ayant les compétences générales de classifier les informations (auteurs de la classification à proprement parler) et de modifier et de supprimer la classification (cf. art. 12, al. 2, LSI). En vertu de l'al. 1, ils sont chargés d'indiquer de manière aussi détaillée possible dans un catalogue de classification les informations à classifier qui relèvent de leur domaine de compétence. Ils indiquent également la durée probable de la classification. Étant donné que les données à classifier sont régulièrement traitées, il est généralement possible de déterminer à l'avance

[17] RS **152.3**

jusqu'à quand elles doivent être classifiées et à quel échelon. L'ordonnance ne fixe aucun délai minimal ou maximal. Le fait de fixer un délai de classification ne dégage pas de l'obligation visée à l'art. 25 de contrôler tous les cinq ans, le cas échéant, le besoin de protection d'un document déterminé.

Les catalogues de classification des unités administratives sont matériellement contraignants pour les collaborateurs. Ceux-ci doivent formellement classifier les informations qui y sont contenues en marquant le document (cf. al. 5). Lorsque la classification est manifestement erronée, il convient d'appliquer la réglementation figurant à l'art. 24 OSI.

Al. 2 – Ce contrôle vise à garantir que lors de l'établissement des catalogues de classification les critères légaux de la classification au sein de l'administration fédérale sont appliqués selon des principes comparables. La compétence de décider de manière définitive dont jouissent les offices, les secrétariats généraux, les groupements, la ChF et les départements est conservée.

Al. 3 – Dans l'administration fédérale et à l'armée, de nombreuses informations sont traitées qui ne peuvent pas être affectées spécifiquement à un office ou à un département (p. ex. protection des objets et des personnes, moyens informatiques, affaires du Conseil fédéral). Il est prévu que le service spécialisé de la Confédération pour la sécurité de l'information s'occupe de ce catalogue de classification obligatoire pour tous.

Al. 4 – Les catalogues de classification visés aux al. 1 et 3 ne sont pas exhaustifs. Quiconque traite des informations sera forcément confronté à la situation dans laquelle une information qu'il considère sensible ne figure pas dans un catalogue. Il revient alors aux collaborateurs de la Confédération et aux militaires (let. a) d'intégrer cette information par analogie à ce qui figure dans un catalogue de classification ou de la classifier directement en vertu des critères définis aux art. 18 à 20. Les mandants sont soumis à la même obligation lorsqu'ils chargent des tiers de traiter des informations sensibles (let. b).

Al. 5 – De manière générale, il faut s'assurer que l'information sensible soit protégée (p. ex. classifiée) dès le moment où elle est visible ou audible. C'est le cas dès qu'elle se trouve sur un support d'informations. Il est par conséquent important que la protection soit prise immédiatement à la source et qu'elle soit apportée par toutes les personnes traitant l'information au moyen du marquage formel (mentionner la classification). Une forme particulière du marquage s'applique à l'échange oral d'informations, qui consiste à rendre son interlocuteur attentif au fait que des informations classifiées sont sur le point d'être échangées. Les personnes visées à l'al. 5 ne sont pas habilitées à réduire ou à supprimer une classification de l'information. Cette compétence demeure celle des offices, de la ChF et des départements.

Art. 18 Échelon de classification « interne »

Pour qu'une classification INTERNE se justifie, deux conditions doivent se cumuler : l'accès aux informations par des personnes non autorisées doit pouvoir entraîner un *potentiel* préjudice de causalité des intérêts publics de la Suisse et le préjudice ne doit pas être simplement négligeable, sans qu'il y ait des indications concrètes d'un dommage financier. Ces intérêts publics sont mentionnés à l'art. 1, al. 2, let. a à d, LSI ; la let. e n'est pas un intérêt propre à l'institution fédérale (cf. message LSI, p. 2833 s.). De telles informations sont protégées par la loi ou par un accord ; de même, le secret de fonction visé à l'art. 320 du code pénal (CP)[18] ou la LTrans assurent la protection de certaines informations dans les cas prévus par ces lois.

Art. 19 Échelon de classification « confidentiel »

Pour qu'une classification CONFIDENTIEL se justifie, deux conditions doivent se cumuler : l'accès aux informations par des personnes non autorisées doit pouvoir entraîner un préjudice de causalité potentiellement *considérable* des intérêts publics de la Suisse. Ces intérêts sont mentionnés à l'art. 1, al. 2, let. a à d, LSI. *Considérable* signifie que la Suisse ou la Confédération pourraient subir un préjudice significatif.

Art. 20 Échelon de classification « secret »

Pour qu'une classification SECRET se justifie, deux conditions doivent se cumuler : l'accès aux informations par des personnes non autorisées doit pouvoir entraîner un préjudice de causalité potentiellement *grave* des intérêts publics de la Confédération. Ces intérêts sont mentionnés à l'art. 1, al. 2, let. a à d, LSI. *Grave* signifie que la Suisse pourrait subir un préjudice catastrophique.

[18] RS **311.0**

Art. 21 Directives relatives au traitement

Al. 1 et 2 – Sur la base de l'art. 85 LSI, le service spécialisé de la Confédération pour la sécurité de l'information édicte des directives sur le traitement des informations classifiées et sur les mesures prises pour leur protection au niveau de l'organisation, du personnel et des constructions, de même que sur le plan technique. Il s'agit de consignes minimales uniformes s'alignant sur celles des partenaires étrangers de la Suisse (cf. al. 3 et art. 3, al. 3, OSI). Les unités administratives décentralisées et les organisations visées à l'art. 2, al. 4, OLOGA appliquent les exigences lorsqu'elles traitent des informations classifiées de la Confédération ou si le département les soumet au champ d'application la LSI. Les unités administratives et l'armée peuvent déterminer une protection plus élevée dans leur domaine de compétence. Elles ne peuvent cependant pas demander aux autres organisations de la Confédération de respecter des mesures de protection plus élevées lorsqu'elles souhaitent échanger leurs informations classifiées avec d'autres organes, étant donné que cela porterait atteinte au principe d'une norme uniforme.

Al. 3 – En application de l'art. 84, al. 1, LSI, le Conseil fédéral délègue à la ChF la compétence de régler le traitement des affaires classifiées du Conseil fédéral.

Al. 4 – Les traités internationaux en matière de sécurité de l'information, comme ceux conclus avec l'UE ou l'OTAN, contiennent des listes de concordance concernant l'application des classifications, des normes de sécurité dans le domaine informatique ou de la sécurité des communications et des réglementations sur l'exécution de contrôles mutuels (cf. message LSI à propos de l'art. 88).

Art. 22 Mesures de sécurité liées à l'engagement

Il arrive parfois que le besoin d'échanger rapidement des informations au sein d'un groupe prime le besoin d'en assurer la confidentialité. C'est en particulier le cas lors d'engagements des services de sécurité ou de police. Dans ces cas, une simplification ciblée des prescriptions de sécurité ordinaires peut faciliter l'accomplissement de la mission sans pour autant entraîner un risque trop élevé pour la sécurité. Selon le droit en vigueur jusqu'à présent (cf. art. 18, al. 3, OPrI), les services de renseignement et fedpol peuvent traiter des informations classifiées de manière simplifiée. D'autres unités administratives de la Confédération chargées de tâches de sécurité, en particulier le Groupement Défense, ont un besoin semblable, raison pour laquelle d'autres services doivent pouvoir profiter de la possibilité du traitement simplifié. Il faut toutefois éviter qu'en conséquence les offices fédéraux les plus sensibles soient *généralement* assujettis à des exigences de sécurité plus basses que les autres offices. Pour cette raison, les conditions et les modalités liées au traitement simplifié sont légèrement durcies.

Art. 23 Certification de sécurité des moyens informatiques

La certification de sécurité est généralement exigée à l'étranger lorsque des informations classifiées à compter de l'échelon CONFIDENTIEL sont traitées dans un système informatique. Sur le plan international, cette certification est toujours demandée lorsque des informations protégées d'un État doivent être traitées dans le système d'un autre État. Si une telle certification est requise pour un système d'information suisse, par exemple parce que des informations classifiées de l'UE doivent y être traitées, le service spécialisé de la Confédération pour la sécurité de l'information peut examiner et certifier ce système en collaboration avec les cryptologues de l'armée et les spécialistes de la sécurité d'armasuisse. La preuve du respect des exigences minimales visées à l'art. 21, al. 1, OSI est déterminante pour la certification. L'OSI comble une lacune qui, jusqu'à présent, compliquait la collaboration internationale dans le domaine de la sécurité. Jusqu'à présent, aucune certification visée à l'art. 23 OSI n'était nécessaire pour la collaboration nationale. Les systèmes informatiques devant accéder à un système informatique certifié doivent, selon les circonstances, également être certifiés. L'OSI ménage la possibilité de rendre obligatoire la certification pour la collaboration nationale également.

Art. 24 Protection en cas de menace pour des informations classifiées

Cette disposition correspond au droit en vigueur (art. 15 OPrI). Le signalement aux organes de sécurité responsables s'effectue selon la disposition relative à la gestion des incidents (cf. art. 12 OSI).

Art. 25 Contrôle du besoin de protection et cercle des personnes autorisées

Cette disposition correspond au droit en vigueur (cf. art. 14 OPrI).

Art. 26 Archivage

Al. 1 – Les dispositions sur l'archivage s'appliquent à la sauvegarde des documents dignes d'archivage de la Confédération (y c. des documents classifiés) et à leur publication en tenant compte des intérêts légitimes de la protection de la personnalité et de l'État, ainsi que de la transparence et de la traçabilité. Les informations classifiées de la Confédération restent des documents fédéraux au sens de la législation sur l'archivage, même lorsqu'elles sont traitées par des cantons et des tiers dans le cadre d'un échange d'informations. La procédure d'archivage au niveau fédéral reste ainsi régie par la législation sur l'archivage.

Al. 2 – Les Archives fédérales ont pour tâche de garantir la protection des archives classifiées et archivées de manière centralisée. Elles peuvent donc déroger aux exigences et mesures standard du service spécialisé de la Confédération pour la sécurité de l'information selon l'art. 85 LSI. Elles doivent cependant protéger les archives classifiées de telle sorte que la sécurité mise en œuvre serve de pendant au risque inhérent aux documents archivés.

Al. 3 – Le délai de protection des archives (y c. des archives classifiées) ne se prolonge pas automatiquement à son expiration. Par contre, la classification est automatiquement supprimée à l'échéance du délai de protection. En d'autres termes, après expiration de ce délai, les archives peuvent être consultées (art. 10, al. 1, de l'ordonnance du 8 septembre 1999 sur l'archivage [OLAr][19]). Après expiration du délai de 30 ou de 50 ans, il n'est pas prolongé pour la plupart des informations classifiées. En revanche, le prolongement du délai de protection avant son expiration peut se justifier pour certaines constructions ou projets militaires (art. 12 de la loi fédérale du 26 juin 1998 sur l'archivage [LAr][20], en relation avec l'art. 14 OLAr).

La responsabilité de demander dans les temps le prolongement du délai de protection incombe à l'office compétent. Les délais de protection des documents versés figurent sur le bordereau correspondant que l'unité administrative compétente administre dans les systèmes GEVER. Les fonds à protéger plus longtemps du fait d'intérêts publics et privés sensibles prépondérants (art. 12 LAr et art. 14 OLAr) sont mentionnés à l'annexe 3 de l'OLAr (art. 14, al. 5).

Section 5 Sécurité des moyens informatiques

Art. 27 Procédure de sécurité

La procédure de sécurité selon les art. 14*b* à 14*e* OPCy en vigueur a été reprise dans les grandes lignes.

Al. 1 – Le besoin de protection actuel doit être déterminé sur la base des critères des catégories de sécurité visés à l'art. 28.

Al. 2 – Les dérogations aux consignes exigent toujours une autorisation expresse du service ayant émis la directive (cf. commentaire relatif à l'autorisation d'exceptions selon l'art. 9 OSI).

La méthode de gestion des risques visant à protéger de l'espionnage mentionnée jusqu'à présent dans les directives informatiques est couverte par les règles sur la procédure de sécurité relative aux entreprises et n'exige plus de règles séparées (cf. art. 55 à 58 LSI).

Al. 3 – Un risque résiduel peut être un risque accepté ou un risque inconnu (cf. manuel sur la gestion des risques de la Confédération). L'OSI précise qu'un risque résiduel ne peut être qu'un risque accepté. Il est question de risque résiduel lorsque le risque initial peut être réduit à un niveau approprié par des mesures de pilotage (pour éviter les risques, les diminuer ou les transférer).

Al. 4 – L'acceptation *démontrable* (cf. commentaire de l'art. 8, al. 1, let. d, OSI) des risques résiduels est importante, car elle confirme un processus d'analyse et de décision minutieux et donc une décision consciente sur les risques résiduels que l'on est prêt à accepter. Cette décision peut être déléguée d'une manière générale par une instruction ou peut être déléguée au cas par cas (p. ex. dans le cadre d'un projet informatique) à un autre membre de la direction (de façon également démontrable).

Al. 5 et 6 – Une menace nouvelle ou récurrente peut remettre en question, entièrement ou partiellement, une analyse des risques déjà effectuée, d'où la nécessité d'adapter le concept de risque. C'est à l'office qu'il revient d'évaluer si un changement de la menace est considérable.

[19] RS **152.11**
[20] RS **152.1**

Du fait de la progression rapide des technologies et de la complexification des menaces dans le domaine de la sécurité de l'information, il s'agit de vérifier chaque année si un changement affectant la sécurité s'est produit. Le délai fixé à cinq ans pour la répétition de la procédure de sécurité au sens de l'art. 14*e*, al. 1, OPCy ne s'applique donc plus.

Al. 7 – Le service spécialisé de la Confédération pour la sécurité de l'information émet des consignes minimales en matière de cybersécurité. Ces consignes s'appliquent d'ailleurs également aux unités administratives décentralisées et aux organisations visées à l'art. 2, al. 4, LOGA, lorsqu'elles accèdent aux moyens informatiques des fournisseurs internes de prestations informatiques ou leur délèguent la gestion de leurs moyens informatiques.

Art. 28 Attribution des catégories de sécurité « protection élevée » et « protection très élevée »

Les moyens informatiques (définition légale à l'art. 5, let. a, en relation avec l'art. 17 LSI) seront subdivisés en trois catégories de sécurité : « protection de base », « protection élevée » et « protection très élevée » à la différence de l'OPCy actuelle qui ne prévoit que deux catégories de sécurité : « protection de base » et « protection accrue ». Le classement dans l'une des trois nouvelles catégories est fonction des intérêts publics de la Confédération, d'après l'art. 1, al. 2, let. a à e, LSI.

Les critères matériels de la classification des informations s'appliquent aussi à la catégorisation des moyens informatiques.

Ils concordent largement avec les critères appliqués à l'évaluation de l'ampleur des dégâts dus à un événement dans le cadre de la gestion des risques de la Confédération.

Contrairement aux critères de classification des informations classifiées, la catégorisation des moyens informatiques peut s'appuyer sur l'aspect financier. En effet, une violation de la disponibilité ou de l'intégrité d'informations traitées par des moyens informatiques est plus facilement quantifiable que, par exemple, une violation de la confidentialité d'un document classifié.

Art. 29 Mesures de sécurité

Al. 1 – Les directives émises jusqu'à présent par à l'OFCS sur les exigences minimales pour chaque catégorie de sécurité selon l'art. 17 LSI pour l'administration fédérale et l'armée seront édictées à compter de 2025 par le service spécialisé de la Confédération pour la sécurité de l'information. Les unités administratives décentralisées, qui ne sont pas soumises à toute la LSI par leur département, et les organisations visées à l'art. 2, al. 4, LOGA appliquent ces consignes lorsqu'elles accèdent aux moyens informatiques des fournisseurs internes de prestations informatiques de l'administration fédérale ou leur délèguent la gestion de leurs moyens informatiques (p. ex. l'Office fédéral de l'informatique et de la télécommunication). La « protection de base » s'applique aussi aux cantons (art. 3 LSI) dans la mesure où ils entrent dans le champ d'application de la LSI.

Al. 2 – Concernant les questions en lien avec la protection des données et leur sécurité fondée sur les risques, le service spécialisé veille à établir une coordination efficace avec le proposé fédéral à la protection des données et à la transparence (PFPDT) et les conseillers en protection des données, conformément à la LPD (cf. également art. 82, al. 1, LSI). Les directives visées à l'al. 1 doivent être harmonisées avec les dispositions en vigueur sur la protection des données. À cet égard, il faut être attentif au fait que les notions « protection élevée » et « protection très élevée » selon l'art. 17 LSI ne correspondent pas avec, par exemple, les notions propres à la législation sur la protection des données de « risque », « risque faible » ou « risque élevé ».

Al. 3 – Les let. a et b distinguent deux types de risques qui exigent une attention particulière par rapport à l'efficacité des mesures de sécurité. De ce fait, une vérification doit avoir lieu dès que des évolutions sensibles des risques s'esquissent, mais au plus tard tous les cinq ans. La base légale de la vérification périodique figure à l'art. 18, al. 3, LSI.

Al. 4 – Voir l'art. 10, al. 2, LSI et le commentaire de l'art. 5, al. 4, OSI.

Art. 30 Sécurité de l'exploitation

Al. 1 à 3 – Les fournisseurs internes de prestations de la Confédération ont un double rôle dans la mise en œuvre de la sécurité de l'information. D'une part, ce sont des unités organisationnelles normales qui doivent mettre en œuvre l'OSI comme toutes les autres unités organisationnelles. D'autre part, ils jouent aussi un rôle central pour la sécurité des bénéficiaires des prestations. Il

est donc déterminant pour la sécurité que le partage des tâches et des compétences soit clair. Les fournisseurs internes de prestations ont comme obligation générale de fournir leurs prestations informatiques conformément aux techniques les plus récentes et de mettre à la disposition des bénéficiaires de prestations les informations nécessaires relatives à la sécurité en temps opportun. Parmi ces informations figurent les mécanismes de protection mis en place, qui comprennent plusieurs niveaux comme la *security*, la *compliance* et le *backup* et permettent non seulement de déjouer les attaques par maliciel et rançongiciel, mais offrent aussi une protection contre les dommages résultant par exemple de pannes de système ou d'erreurs humaines (p. ex. droits d'accès erronés ou anciens) ou dus à des utilisateurs malintentionnés dans leurs propres organisations. Les bénéficiaires de prestations sont toutefois responsables de la définition claire des responsabilités pour la sécurité au niveau de l'exploitation, y compris pour la gestion des vulnérabilités, dans les conventions correspondantes. Elles sont notamment responsables de la sécurité de leurs données et de leurs tâches.

Al. 4 – Cette surveillance relève purement de la technique de sécurité et il ne s'agit pas d'une éventuelle surveillance des collaborateurs. Les tiers peuvent être des personnes qui interviennent dans le cadre d'un programme de prime de bogues par exemple.

Section 6 Mesures relatives aux personnes et protection physique

Art. 31 Vérification de l'identité des personnes et des machines

Il s'agit de définir ici dans quelle mesure une personne doit prouver son identité physique ou électronique afin d'avoir accès à des informations, des moyens informatiques, des locaux et d'autres infrastructures de la Confédération. Le niveau de sécurité requis (*level of assurance*) sera plus élevé pour les systèmes sensibles que pour les applications normales. Les personnes, mais aussi les ordinateurs et même les processus doivent pouvoir dès lors *prouver leur identité*. Ces directives faisaient, en vertu du droit en vigueur jusqu'à présent, partie de la protection informatique de base dans l'administration fédérale édictée par l'OFCS. Il n'est pour l'heure pas nécessaire de créer une réglementation séparée mais cela pourrait le devenir en raison de l'importance croissante de ce niveau de sécurité.

Art. 32 Sécurité relative aux personnes

La pratique a montré que les risques de sécurité liés aux personnes, une fois le CSP effectué, ne donnaient souvent plus matière à discussion. Dans l'esprit d'un suivi classique sur le plan international (appelé *aftercare*), les collaborateurs disposant d'un certificat de sécurité doivent signaler à leur employeur des faits de leur environnement privé ou professionnel qui menacent la sécurité. De telles circonstances rendent les collaborateurs particulièrement vulnérables (p. ex. des dettes contractées dans le cadre d'une addiction au jeu, une dépendance à l'alcool ou aux stupéfiants découverte par une tierce personne, une relation extra-conjugale dévoilée) ou relèvent d'activités auxquelles des risques élevés sont attachés (p. ex. voyages dans des pays particulièrement critiques ou contacts intensifs avec des ressortissants de ces pays). Pour les collaborateurs, la vulnérabilité ressentie peut être particulièrement pesante psychiquement. Pour ce qui est de l'employeur, il ne s'agit pas d'espionner les collaborateurs, de les surveiller constamment ou de les punir, mais de convenir avec eux dans un rapport de confiance d'éventuelles mesures ou stratégies appropriées afin de réduire les risques. En cas de signalement épineux, il faut convenir de la procédure avec le service du personnel ou un service de médiation.

Les offices, les secrétariats généraux, les groupements et la ChF doivent en outre assurer chaque année la sensibilisation des collaborateurs soumis à un contrôle de sécurité. Les supérieurs doivent assumer activement la responsabilité vis-à-vis des risques de sécurité liés aux personnes et l'intégrer dans les tâches de direction permanentes. Ainsi, une telle sensibilisation pourrait se dérouler dans le cadre de l'entretien avec les collaborateurs. Ce point serait ainsi abordé au moins une fois par an.

Art. 33 Soupçon de comportement répréhensible

Al. 1 – Cette disposition vise à garantir que de possibles infractions soient communiquées aussi vite que possible aux autorités de poursuite pénale compétentes sans que la ChF et les départements doivent se perdre en conjectures détaillées de nature pénale, voire judiciaire. Ainsi, un acte délictueux *paraît* déjà *constituer une infraction* si le moindre des signes indique un agissement répréhensible, même s'il n'est pas pleinement établi.

Al. 2 – Il s'agit ici de la conservation rapide de preuves tangibles et en partie fugaces. Les obstacles à celle-ci doivent être réduits. Il est important que, dans le cadre de la conservation des preuves, les unités administratives n'effacent pas, ne laissent pas ou ne créent pas de traces physiques ou électroniques. La conservation de preuves dont il est ici question n'implique pas leur analyse, laquelle est du ressort des autorités de poursuite pénale sur ordre d'un juge.

Art. 34 Mesures de protection physique

Al. 1 – Les consignes permettant de garantir la protection physique des informations et des moyens informatiques sont aujourd'hui fixées à la Confédération par plusieurs services (par fedpol et l'Office fédéral des constructions et de la logistique [OFCL] pour l'administration fédérale civile et par l'État-major de l'armée pour le Groupement Défense et l'armée). Les consignes actuelles sont pour l'heure suffisantes pour couvrir le besoin de protection. Si des consignes supplémentaires ou à l'échelon fédéral devaient être nécessaires, par exemple en rapport avec l'harmonisation internationale des prescriptions de protection, le service spécialisé de la Confédération pour la sécurité de l'information pourrait fixer pour l'administration fédérale et l'armée des exigences minimales pour protéger physiquement les informations et les moyens informatiques après avoir consulté les organes mentionnés. Les unités administratives décentralisées et les organisations visées à l'art. 2, al. 4, LOGA ne doivent appliquer ces consignes que lorsqu'elles traitent des informations classifiées de la Confédération, lorsqu'elles accèdent aux moyens informatiques des fournisseurs internes de prestations informatiques ou délèguent la gestion de leurs moyens informatiques à ces fournisseurs de prestations.

Al. 1 et 2 – Les mesures de protection physiques peuvent être la mise en place de zones de sécurité (cf. art. 35 OSI et message LSI, p. 2843 ss), des contrôles d'accès aux bâtiments, la surveillance par caméra de certains secteurs, des dispositifs de destruction de supports d'informations ou des contrôles des postes de travail.

Art. 35 Zones de sécurité

Al. 1 et 3 – La création de zones de sécurité vise à réduire le potentiel de dommages par suite d'espionnage ou de sabotage dans des zones très sensibles (comme les locaux abritant des serveurs, les salles de conduite ou les locaux anti-écoute) (cf. message LSI, p. 2827, 2843 ss). Si des personnes ou des entreprises doivent entrer dans une zone de sécurité au sens de l'OSI, elles doivent préalablement passer un CSP ou une procédure de sécurité relative aux entreprises. Il doit donc être garanti que les zones de sécurité soient établies conformément au droit et de manière adéquate. Il est par conséquent exigé qu'un contrôle ait lieu avant la mise en service qui doit être renouvelé périodiquement. Le service spécialisé de la Confédération pour la sécurité de l'information édictera les consignes nécessaires.

Al. 4 – La protection des informations et des moyens informatiques dans une zone de sécurité commence déjà en dehors de cette zone. Les attaquants potentiels disposent aujourd'hui de moyens leur permettant d'espionner des signaux électromagnétiques à distance. Les unités administratives doivent par conséquent être autorisées à placer des capteurs à proximité immédiate de la zone de sécurité pour détecter les tentatives d'espionnage et les écarter. Les organes de sécurité de la Confédération émettent généralement des recommandations visant la mise en place de ces mesures. Leur mise en œuvre relève toutefois de la responsabilité de l'unité administrative établissant la zone de sécurité.

Section 7 Organisation de sécurité

Une nouveauté importante de l'OSI concerne les directions des offices. L'OSI leur confie des tâches, compétences et responsabilités concrètes dans le domaine de la sécurité de l'information. Le directeur d'office peut déléguer ces tâches à un membre de sa direction (le responsable de la sécurité de l'information). Les responsables de la sécurité de l'information supervisent le SMSI de leur office et prennent toutes les décisions importantes dans le domaine de la sécurité de l'information. Les activités de surveillance opérationnelles incombent en revanche aux préposés à la sécurité de l'information. Avec l'OSI, les rôles de *délégué à la sécurité informatique* et de *préposé à la protection de l'information* sont réunis en un seul et même rôle, celui de *préposé à la sécurité de l'information*. Ses tâches seront précisées, puis complétées par d'autres tâches relevant du SMSI.

Un modèle analogue est appliqué à l'échelon des départements. Ceux-ci sont responsables en leur sein du pilotage, de la coordination et de la surveillance de la sécurité de l'information dans le

sens des art. 37, 38, 41 et 42 LOGA. Ils définissent en particulier la politique de la sécurité de l'information et l'organisation de la sécurité départementale. La responsabilité opérative de la sécurité incombe au secrétaire général. Les préposés à la sécurité de l'information continuent d'assumer les tâches de coordination et de surveillance opérationnelles (cf. art. 81 LSI).

La section 7 décrit les différents rôles et fonctions prévus dans l'organisation de la sécurité. Certains rôles, comme ceux des préposés à la sécurité de l'information des unités administratives (art. 37 OSI), peuvent être confiés à plusieurs personnes, selon le thème, en fonction des besoins d'un office. Il en va de même de tous les autres rôles visés aux art. 37 ss OSI. Aucun rôle n'est lié à une seule personne en particulier, sauf celui du responsable de la sécurité de l'information, qui ne peut être assumé que par une seule personne.

Les suppléants doivent être qualifiés techniquement et personnellement pour assurer toutes les tâches du rôle primaire. Ils doivent avoir été formés pour pouvoir suppléer le rôle primaire à tout moment et avant tout en cas d'urgence à un niveau raisonnable.

Le système fondé sur les rôles de l'OSI est conçu pour la grande majorité des unités administratives pour lesquelles la sécurité de l'information est une tâche commune à plusieurs services. Pour les fournisseurs de prestations TIC de la Confédération, la garantie de la sécurité au sein de l'organisation est en revanche une tâche principale. Généralement, les fournisseurs de prestations disposent aussi d'une division de sécurité dirigée par un membre de la direction. Étant donné que la sécurité est déjà organisée et mise en œuvre hiérarchiquement chez les fournisseurs de prestations, il peut être envisageable, dans certaines circonstances, de fusionner les rôles de « responsable de la sécurité » et de « préposé à la sécurité ».

Art. 36 Responsables de la sécurité de l'information des unités administratives visées à l'art. 2, al. 1, let. c

Al. 1 – *Responsable* signifie ici l'obligation personnelle de rendre des comptes à l'organe supérieur. Elle suppose que la personne responsable a les pouvoirs, en particulier financiers, de prendre, de contrôler ou de corriger des mesures. Ceci doit être distingué du devoir d'exécution des mesures de surveillance. Dans ce cas, la personne mandatée est responsable de l'exécution et est la seule à devoir rendre des comptes.

Al. 2 – L'obligation personnelle de rendre compte est déléguée avec la délégation de la responsabilité de la sécurité de l'information. De ce fait, la délégation devrait être démontrable (cf. commentaire de l'art. 8, al. 1, let. d, OSI).

Al. 3, let. b – En principe, toutes les décisions importantes qui concernent la sécurité de l'information doivent être prises par ce rôle.

Al. 4 – Le mandat confié aux préposés à la sécurité de l'information visés à l'art. 37 OSI peut, par exemple, prendre la forme de directives internes ou d'objectifs annuels au sens de l'art. 5, al. 2, OSI. Concernant la notion de *conflit d'intérêts*, voir le message LSI à propos de l'art. 82, al. 3.

Art. 37 Préposés à la sécurité de l'information des unités administratives visées à l'art. 2, al. 1, let. c

La désignation d'une suppléance officielle est nouvelle. Ce rôle correspond pour une bonne partie à celui de délégué à la sécurité informatique des unités administratives (DSIO) utilisé jusqu'à présent.

Le préposé à la sécurité de l'information de la ChF vérifie en vertu de l'art. 8 OCSP si des tiers exercent une activité sensible au cas où cette vérification n'aurait pas lieu dans le cadre de la procédure de sécurité relative aux entreprises. S'agissant des départements, cette tâche revient au préposé à la sécurité de l'information du département.

Art. 38 Sécurité de l'information dans les services standard

En principe, ce rôle auprès des services standard a les mêmes tâches que le rôle de préposé à la sécurité de l'information des unités administratives selon l'art. 37 OSI.

Art. 39 Responsabilité des départements en matière de sécurité de l'information

Al. 1 à 2 – Le pilotage et la surveillance de la sécurité de l'information sont des tâches stratégiques et des tâches essentielles des départements (cf. art. 38 LOGA, commentaire de l'art. 5, al. 1).

En vertu de l'art. 47, al. 4, LOGA, les départements peuvent pour le reste en tout temps prendre la responsabilité de tâches et compétences attribuées aux offices, aux secrétariats généraux, aux groupements et à la ChF par l'OSI. Ainsi, un département dont l'organisation est centralisée comme le DFAE peut mettre en œuvre ses besoins internes d'organisation dans le cadre de l'OSI.

Al. 4 – Les consignes, mesures et audits valables à l'échelle du département sont décidés par le secrétaire général. Lorsque la responsabilité en matière de sécurité dans les l'offices est assumée par les directeurs d'office, ceux-ci attendent que la personne qui dispose de la compétence décisionnelle à l'échelon du département ait une position élevée. Le cas Xplain survenu dans l'administration fédérale a en outre montré qu'il pouvait être nécessaire que le suivi politico-stratégique incombe au secrétaire général. La solution d'impliquer le secrétaire général présente par ailleurs l'avantage que la coordination interdépartementale se fait dans le cadre de la Conférence des secrétaires généraux.

Art. 40 Préposés à la sécurité de l'information des départements

La désignation d'une suppléance officielle est nouvelle (cf. art. 81, al. 1, LSI). Ce rôle réunit celui de délégué à la sécurité informatique (DSID) et celui de préposé à la protection des informations des départements. En plus des tâches et compétences listées, il a également la compétence d'effectuer la nouvelle tâche prévue dans le domaine des CSP, notamment celle de vérifier, s'agissant des tiers, s'il existe une activité sensible conformément à l'art. 8 OCSP ne donnant pas lieu à une procédure de sécurité relative aux entreprises.

Let. f – Puisque les préposés à la sécurité de l'information doivent collaborer étroitement selon les art. 37 et 40, le préposé à la sécurité de l'information du département visé à l'art. 40 devrait être associé au choix d'une nouvelle personne pour le rôle de préposé à la sécurité de l'information de l'unité administrative visé à l'art. 37. Il peut notamment évaluer la compétence technique de la personne à choisir. Les modalités de l'obligation de consulter doivent être définies par les offices et le département.

Let. g – La procédure de contrôle des documents SECRET est reprise sans changement.

Let. h – Jusqu'à présent, les rapports annuels des DSID devaient être envoyés à l'OFCS. À l'avenir, les titulaires du rôle, selon cette disposition, devront rendre des comptes à la personne responsable de la sécurité de l'information du département selon l'art. 39 OSI (cf. art. 14 OSI). Cette dernière transmet ensuite le rapport au service spécialisé de la Confédération pour la sécurité de l'information pour que celui-ci, de son côté, puisse établir un rapport annuel sur l'état de la sécurité de l'information à l'intention du Conseil fédéral (cf. art. 83, al. 1, let. h, LSI).

Art. 41 Préposé à la sécurité de l'information du Conseil fédéral

En tant qu'autorité soumise à la LSI, le Conseil fédéral obtient un préposé à la sécurité de l'information et son suppléant conformément à l'art. 81 LSI. Ce préposé nommé prend également la direction, en vertu de l'art. 83, al. 3, LSI, du service spécialisé de la Confédération pour la sécurité de l'information. Étant donné que ce service spécialisé est rattaché au SEPOS du DDPS, c'est au DDPS qu'il incombe de désigner le préposé à la sécurité de l'information.

Art. 42 Service spécialisé de la Confédération pour la sécurité de l'information

Al. 1 – Les tâches générales et relevant largement du soutien et de la coordination du service spécialisé de la Confédération pour la sécurité de l'information sont décrites aux art. 83 LSI et 41 OSI ; les tâches contextuelles figurent dans d'autres dispositions de l'OSI (p. ex. les consignes concernant la gestion de la sécurité de l'information visées à l'art. 15, d'autres consignes relevant d'autres domaines à l'art. 17, 21, 23, 27, 29, 31, 34 et 35). Concernant la collaboration entre le service spécialisé et l'OFCS, voir le ch. 2.3, let. i.

Let. f – Le secteur Transformation numérique et gouvernance de l'informatique (secteur TNI) de la ChF gère les services standard (art. 4, al. 4, de l'ordonnance du 25 novembre 2020 sur la transformation numérique et l'informatique [OTNI][21]). Il s'agit de prestations fournies de manière centralisée au sein de l'administration fédérale, qui sont souvent utilisées et qui répondent aux mêmes besoins ou à des besoins semblables. Dans ce contexte, il assure aussi des services de sécurité, comme l'utilisation de Threema, l'application de la Confédération permettant une communication sûre sur les appareils mobiles. S'agissant des solutions de sécurité utilisées par plusieurs départements et l'armée et certifiées au sens de l'art. 23 OSI afin de traiter des

[21] RS **172.010.58**

informations classifiées CONFIDENTIEL ou SECRET, il manquait jusqu'à présent un service demandeur au niveau fédéral. Cette situation a rendu difficile l'acquisition, l'entretien et le développement de telles solutions servant à crypter les fichiers ou à assurer la sécurité des vidéoconférences. Le service spécialisé de la Confédération devra donc en assumer la responsabilité. Cela n'entame ni ne remet en question la compétence du secteur TNI de la ChF en matière de services standard.

Al. 2 – La Conférence des préposés à la sécurité de l'information visée à l'art. 82, al. 2, let. c, LSI conseille le service spécialisé de la Confédération pour la sécurité de l'information sur tous les aspects de la coordination de l'exécution et sur tous les points d'importance stratégique.

Al. 3 – Le rôle d'autorité nationale de sécurité, assumé jusqu'à présent par le Secrétariat général du DDPS, sera attribué au service spécialisé de la Confédération pour la sécurité de l'information. Les tâches et compétences visées aux let. d et f font l'objet des traités internationaux selon l'art. 87 LSI (cf. message LSI à propos de l'art. 88, p. 2881 ; p. 2900).

Art. 43 Tâches et compétences de l'OFCS

L'Office fédéral de la cybersécurité (OFCS) est le centre de compétences fédéral en matière de cybersécurité. Il a pour tâche d'assurer la cybersécurité en Suisse ; la Confédération est l'un de ses nombreux « clients ». L'OFCS assume plusieurs tâches en faveur des autorités fédérales, notamment en lien avec la gestion des incidents (cf. art. 12 OSI). Il conseillera et soutiendra en outre les autorités fédérales et siégera dans les organes fédéraux.

Afin d'améliorer la cybersécurité de la Confédération, il est habilité à rechercher les menaces et les vulnérabilités techniques sur les réseaux de l'administration fédérale et sur Internet. Il peut également déléguer cette tâche à des tiers, par exemple dans le cadre d'un programme de prime de bogues. L'OFCS ne peut bien entendu pas faire de recherches sur les réseaux de l'armée ou du service de renseignement sans y être autorisé.

L'OFCS et le service spécialisé de la Confédération pour la sécurité de l'information coordonnent leurs activités afin d'éviter les doublons et d'engager les ressources d'une manière aussi efficace que possible. Tous deux sont rattachés au DDPS, ce qui simplifie la collaboration. Voir aussi le ch. 2.3, let. i.

Section 8 Coûts et évaluation

Art. 44 Coûts

Les unités administratives supportent les coûts de leur propre sécurité. Ces coûts doivent être pris en compte et déclarés lors de la planification de projets. C'est en particulier le cas des coûts afférents aux mesures de sécurité informatique.

Art. 45 Évaluation

Voir le message LSI, commentaire de l'art. 89 LSI, p. 2881.

Section 9 Traitement des données personnelles

Les art. 46 à 48 règlent le traitement des informations et des données personnelles dans le cadre de la gestion de la sécurité de l'information selon l'OSI. La maîtrise des incidents de sécurité implique le traitement de données personnelles relatives aux auteurs potentiels d'infraction qui pourraient faire l'objet de poursuites ou de sanctions pénales ou administratives et qui sont, dès lors, des données sensibles au sens de l'art. 5, let. c, LPD. La législation sur la protection des données requiert pour leur traitement une base légale au sens formel explicite qui faisait défaut jusqu'à aujourd'hui. La base légale nécessaire est créée dans le cadre de la révision en cours de la LSI (cf. ch. 2.1) (cf. art. 10*a* LSI).

Art. 46 Généralités

Al. 1 et 2 – Sans échange mutuel d'informations et de données personnelles, les unités administratives et leurs organes de sécurité ne peuvent pas s'acquitter de leurs tâches. Concernant le traitement des données sensibles lors de la gestion des incidents, voir le commentaire de la section 9. Le traitement des données personnelles requises lors de l'utilisation de l'infrastructure électronique de la Confédération est réglé aux art. 57*i* à 57*q* LOGA. Le nouvel art. 10*a* LSI constituera toutefois la base légale nécessaire au traitement des données sensibles, cette base

s'appliquant également au traitement non électronique des données et améliorant les modalités de l'échange des données.

Al. 4 et 5 – Il est fréquent en cas de cyberattaque que l'auteur de l'infraction publie les données volées sur Internet si la victime ne verse pas la somme exigée. Indépendamment de toute enquête pénale potentielle, les unités administratives de la Confédération et en particulier leurs organes de sécurité doivent pouvoir télécharger et analyser ces données afin d'évaluer le dommage pour la Confédération et de lancer les mesures visant à limiter les dommages (p. ex. informer les personnes concernées). Si la cyberattaque vise une entreprise travaillant pour la Confédération, les données touchées ne sont pas seulement celles de la Confédération mais aussi celles des autres clients, pour le traitement desquelles la Confédération ne dispose pas de base légale. Ces dispositions autorisent les offices fédéraux à traiter ces données. Le traitement des données de tiers n'est autorisé que si elles sont nécessaires à l'évaluation du dommage pour la Confédération.

Art. 47 Application SMSI

Cette disposition crée la base légale nécessaire à l'exploitation d'applications SMSI. Celles-ci permettent la digitalisation des tâches et des processus de l'OSI. Concernant le traitement de données sensibles, voir le commentaire de la section 9.

Art. 48 Services électroniques de formulaire

Al. 1 – Un service de formulaire est une petite application simple avec laquelle des formulaires numériques sont remplis puis envoyés. Les services de formulaire mentionnés à l'al. 1 servent à automatiser la délivrance de demandes de visite (*request for visit*, al. 1, let. a), de certificats internationaux de sécurité (cf. al. 1, let. b) et de certificats de sécurité dans le contexte international (*facility security clearances*, al. 1, let. c).

Al. 2 – Concernant les données de l'annexe 2, il s'agit de données personnelles qui sont exigées comme lors d'une demande d'autorisation de voyage ESTA pour les voyages aux États-Unis. Les données suivies d'un astérisque (*) sont transmises aux autorités étrangères. Les dispositions de la législation sur la protection des données relatives à la transmission de données à l'étranger sont respectées (cf. notamment les art. 16, al. 1, et 17 LPD). Les personnes qui demandent l'accès à des projets classifiés à l'étranger ne l'obtiennent pas si elles refusent de transmettre ces données.

Al. 3 à 6 – Des informations classifiées ou des données personnelles peuvent être traitées dans le cadre d'une annonce de sécurité. Dès que l'annonce est envoyée, les données alimentent immédiatement l'application SMSI, où l'annonce et l'incident sont traités. Pour des raisons de sécurité de l'information et de protection des données, les données potentiellement sensibles ne peuvent pas être conservées plus de 24 heures dans le service de formulaire. Concernant le traitement de données sensibles lors de la gestion des incidents, voir le commentaire de la section 9.

Section 10 Dispositions finales

Art. 49 Dispositions d'exécution particulières

Dans la mesure où la loi ne le prévoit pas explicitement, seul le Conseil fédéral ou le département compétent est autorisé à émettre des directives contraignantes pour les cantons (cf. art. 48, al.1, LOGA). Étant donné que le service spécialisé de la Confédération pour la sécurité de l'information ne possède pas la compétence légale formelle nécessaire, le DDPS doit déclarer ses directives techniques contraignantes. Cela concerne notamment celles émises en vertu des art. 21 et 29 OSI.

Art. 50 Abrogation et modification d'autres actes

L'OPCy est abrogée. L'OPrI est valable jusqu'au 31 décembre 2023, ce qui assure une transition fluide vers le nouveau droit (cf. plus bas).

Art. 51 Dispositions transitoires

Outre ces dispositions transitoires, d'autres figurent dans la LSI, dans l'OCSP et l'OPSEnt. Les dispositions transitoires permettront de planifier et de mettre en œuvre la nouvelle législation de façon systématique et ordonnée dans les six ans qui suivront l'entrée en vigueur (cf. art. 90 LSI).

Al. 1 et 2 – Les consignes existantes du NCSC ne sont pas toutes abrogées et remplacées à l'entrée en vigueur de la nouvelle loi. Certaines ont été modifiées peu avant l'entrée en vigueur du nouveau droit et tiennent donc compte d'un grand nombre des nouvelles exigences (p. ex.

directives de la protection de base de la Confédération). Durant le délai transitoire, les décisions relatives aux exceptions seront prises, selon le domaine de compétence visé par l'OSI, soit par le service spécialisé de la Confédération pour la sécurité de l'information, soit par l'OFCS. Ces deux organes décideront des mesures dans le cas d'espèce.

Al. 3 et 5 – La CSG a émis le catalogue de classification de la Confédération, qui sera remplacé par ceux qui sont visés à l'art. 17 OSI et qui devront être terminés durant l'année suivant l'entrée en vigueur de l'OSI (cf. art. 51, al. 4). La CSG a en outre repris les directives en matière de protection de l'information de l'Organe de coordination pour la protection des informations au sein de la Confédération pour ce qui est des prescriptions de traitement détaillées. Ces directives seront entièrement remaniées, puis approuvées par le service spécialisé de la Confédération pour la sécurité de l'information dans un intervalle de deux ans.

Al. 4 – Il n'est pas possible de mettre rapidement en place un SMSI. Il convient d'effectuer au préalable des analyses et d'établir des concepts, ce qui requiert un certain temps. En outre, la Confédération disposera d'une application SMSI, probablement à compter de 2025, afin de digitaliser les processus de gestion de la sécurité de l'information. Le délai visé à l'al. 4 laissera suffisamment de temps aux offices, à la ChF et aux départements pour planifier et mettre en œuvre les travaux avec soin.

Al. 6 et 7 – À compter de l'entrée en vigueur de la LSI et de l'OSI, le service spécialisé de la Confédération pour la sécurité de l'information sera progressivement mis en place au sein du SEPOS. Par conséquent, l'OFCS continuera d'accomplir ses tâches jusqu'à l'été 2025 dans le domaine de la sécurité informatique, voire d'émettre des directives. Celle-ci auront toutefois une durée de validité limitée qui correspondra au délai visé à l'al. 3.

Art. 52 Entrée en vigueur

L'OSI entrera en vigueur en même temps que la LSI et les autres ordonnances le 1er janvier 2024.

Annexe 1

Voir le commentaire de l'art. 48.

Annexe 2

L'abrogation de l'OPrI et de l'OPCy entraîne la mise à jour des renvois au nouveau droit dans plusieurs ordonnances. Le terme « sécurité informatique » sera remplacé par « sécurité de l'information » s'il y a lieu.

Ch. 31 – Ordonnance du 24 juin 2009 concernant les relations militaires internationales (ORMI)[22] : les organes et ordonnances concernés doivent être actualisés à la suite de la LSI et de ses ordonnances d'exécution.

[22] RS **510.215**

3.2 Modification de l'ordonnance sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération (OIAM)

Remarques préliminaires

Dans le cadre du présent projet, seules les modifications découlant de la LSI et de la loi fédérale sur l'utilisation de moyens électroniques pour l'exécution des tâches des autorités (LMETA) sont prises en compte dans l'OIAM. Le reste des modifications nécessaires de l'OIAM est l'objet d'une révision totale que la ChF a déjà entamée.

Modifications découlant de la LSI

L'OIAM se fondait jusqu'à présent essentiellement sur la LOGA. Les art. 24 à 26 LSI ont créé la base légale formelle sur laquelle l'OIAM se basera en premier lieu. En vertu de l'art. 20, al. 2, LSI, l'utilisation des données biométriques sera en outre autorisée en général dans les systèmes IAM sous certaines conditions. L'OIAM doit donc être modifiée en ce sens.

Modifications découlant de la LMETA

Dans le cadre du service standard eIAM, l'administration fédérale a mis en place un service d'authentification permettant l'accès à ses applications spécialisées et à ses prestations administratives en ligne (prestations de cyberadministration). Ce service est aujourd'hui largement utilisé (plus de 10 millions d'accès par mois, plus de 800 applications intégrées au système, environ 2 millions d'identités) et son utilité n'est plus à démontrer. L'objectif est désormais de le mettre à la disposition des cantons intéressés (et de leurs communes) pour que ceux-ci puissent y intégrer leurs propres applications, sur la base de la LMETA. Cette démarche permettra de mettre en place une procédure de connexion intégrale donnant accès aux prestations de cyberadministration de tous les niveaux administratifs (fédéral, cantonal et communal) et d'exploiter les synergies qui en découleront.

Ce service, qui sera mis à la disposition des cantons à partir du 1er janvier 2024 sous le nom d'AGOV, présente les avantages suivants :

- les personnes physiques peuvent générer une identité électronique qui leur permet d'accéder à toutes les applications de cyberadministration intégrées au système ;
- elles peuvent utiliser leurs identités électroniques existantes, une fois que celles-ci sont acceptées par AGOV, pour accéder à toutes les applications de cyberadministration intégrées au système ;
- les fournisseurs de prestations de cyberadministration peuvent authentifier leurs clients de manière sûre sans avoir à développer et gérer eux-mêmes les outils nécessaires ;
- les administrations de toute la Suisse sont préparées à utiliser la future e-ID comme moyen d'identification sûr, ce qui favorisera son utilisation à large échelle.

La mise à disposition de ce service nécessite plusieurs changements au niveau de l'OIAM.

Préambule

Modifications découlant de la LSI

Une base légale formelle spécifique pour l'OIAM existante a été créée aux art. 24 à 26 LSI ; les dispositions fondamentales de l'ordonnance ont été transférées dans la loi. Jusqu'à présent, l'OIAM s'appuyait sur la compétence d'organisation du Conseil fédéral et indirectement sur les bases légales de tous les systèmes d'information raccordés aux systèmes IAM. L'OIAM ne se fondera plus sur la LOGA comme jusqu'à présent mais principalement sur les articles mentionnés de la LSI. Les systèmes IAM de la base centralisée des identités sont ainsi aussi inclus. La LSI ne porte en revanche pas sur les services d'annuaires, si bien que la LOGA reste mentionnée à leur propos.

En vertu de l'art. 20, al. 2, LSI, il sera en outre autorisé, sous certaines conditions, de traiter des données biométriques dans les systèmes IAM. Celles-ci sont considérées comme des données sensibles au sens de la LPD (cf. FF *2020* 7397, art. 5, let. c, ch. 4). Ainsi, le principe selon lequel aucune donnée sensible ne peut être traitée dans les systèmes IAM est relativisé (cf. art. 11, al. 3, OIAM). Il est de plus toujours possible de traiter des données sensibles dans les systèmes IAM en s'appuyant sur des dispositions légales spécifiques autres que celles de la LSI. Les profils de la personnalité n'ont plus d'importance particulière dans la LPD et ne doivent donc plus être mentionnés. Un profilage au sens de l'art. 5, let. f et g, LPD n'a pas lieu dans les systèmes IAM ou les services d'annuaires, car ceux-ci ne servent pas à *évaluer* des aspects personnels relatifs à des personnes physiques.

Modifications découlant de la LMETA

L'OIAM traite aujourd'hui déjà de l'interconnexion de systèmes IAM, notamment de la possibilité de raccorder des systèmes IAM externes aux systèmes IAM de la Confédération (art. 21 ss) ou vice versa (art. 24). La LMETA, en particulier son art. 11, crée la base légale qui permet à la Confédération de mettre à la disposition des cantons des prestations rendant cette interconnexion possible. Le service AGOV fait partie du service standard eIAM et son extension aux cantons et aux communes constitue un cas typique de mise en œuvre de l'art. 11 LMETA. En ce qui concerne AGOV, l'OIAM règle notamment l'exécution de l'art. 11, al. 3 à 5, LMETA. La présente révision introduit dans l'OIAM les nouvelles dispositions rendues nécessaires par AGOV.

L'***art. 1*** (objet) n'est *pas* modifié car tous les services qui devront être soumis à l'OIAM (cf. commentaire de l'art. 2 ci-dessous) sont compris dans l'expression « de la Confédération ». Cela s'applique en particulier aussi aux organisations visées à l'art. 2, al. 4, LOGA qui relèvent de l'administration fédérale, vu qu'elles accomplissent des tâches administratives.

Art. 2 Champ d'application

Al. 1 – La *let. a* découle de l'art. 2, al. 2, let. b, LSI et correspond à l'al. 1 en vigueur jusqu'ici.

Let. b – Le champ d'application pour l'armée est nouveau et découle de l'art. 2, al. 2, let. d, LSI.

Al. 2 – La notion d'*administration fédérale* utilisée à l'art. 2, al. 2, let. b, LSI comprend aussi bien l'administration fédérale centrale que l'administration fédérale décentralisée (cf. message LSI, p. 2824), d'où la nécessité d'étendre le champ d'application aux unités de l'administration fédérale décentralisée. Le Conseil fédéral peut cependant restreindre le champ d'application de la LSI en vertu de l'art. 2, al. 3 et 4, LSI. À l'instar de l'administration fédérale décentralisée, les organisations visées à l'art. 2, al. 4, LOGA sont soumises à la LSI pour ce qui est de leurs tâches administratives (cf. art. 2, al. 2, let. e, LSI ; le terme de *tâches administratives* ne comprend que celles qui relèvent de la souveraineté de l'État ; les tâches de l'administration auxiliaire peuvent le cas échéant en faire partie lorsqu'elles relèvent des pouvoirs publics [p. ex. procédures d'acquisition], ce qui devrait toutefois rester l'exception). Le Conseil fédéral a là aussi toutefois la possibilité de restreindre le champ d'application de la LSI en vertu de l'art. 2, al. 3, LSI aux organisations ayant de l'importance pour la sécurité. Tant pour l'administration fédérale décentralisée que pour les organisations visées par la LOGA, le champ d'application de l'OIAM et des autres ordonnances d'exécution de la LSI doit être fixé de manière uniforme dans l'OSI, de sorte que l'OIAM ne contienne qu'un renvoi à cet égard.

Le contenu de l'al. 2 en vigueur jusqu'ici n'est pas une liste positive exhaustive et peut être supprimé sans remplacement (une autorité ou un service peut s'engager sur une base volontaire à respecter l'OIAM, pour autant qu'aucune disposition du droit fédéral n'en dispose autrement).

Art. 5 Systèmes IAM

Al. 1 – Les autres organes de la Confédération responsables des systèmes IAM de l'administration fédérale centrale (let. a, ch. 2, d et f) sont mentionnés en plus des organes de l'administration fédérale centrale responsables déjà mentionnés dans l'OIAM.

Let. a, ch. 1 – Puisque le secteur TNI de la ChF est responsable du service standard eIAM dans l'administration fédérale, il est logique de lui confier également la responsabilité de la partie AGOV de ce service, afin de garantir un pilotage cohérent.

Let. c – Le Groupement Défense remplace ici la Base d'aide au commandement (BAC), étant donné que c'est à lui que reviendra la responsabilité des systèmes IAM d'une manière générale ; la

façon dont sera ensuite réglée la responsabilité au sein de la Défense n'est pas l'objet de l'OIAM.

Al. 2 – Actuellement, le traitement des données personnelles dans les systèmes IAM n'est pas contrôlé. En vertu de l'art. 26, let. e, LSI, qui prévoit un contrôle périodique du traitement des données personnelles par un service externe, un alinéa supplémentaire est introduit concernant les systèmes IAM de l'administration fédérale centrale.

Al. 3 – Tenant compte de la relative autonomie organisationnelle de l'armée, des unités de l'administration fédérale décentralisée et des organisations visées à l'art. 2, al. 4, LOGA, il faut simplement fixer au niveau de l'ordonnance que les services cités sont responsables de leurs propres systèmes IAM. Pour cette même raison, cet alinéa ne prévoit pas de faire impérativement contrôler périodiquement par un service externe le traitement des données personnelles par ces services.

S'agissant des systèmes IAM de l'armée, il convient en outre de retenir qu'ils alimentent les systèmes de l'armée importants pour l'engagement, tandis que les systèmes IAM visés à l'art. 5, al. 1, let. c, alimentent les systèmes de l'administration militaire. Les systèmes IAM dont il est question ici se distinguent par des normes légales différentes en matière de traitement des données et de responsabilité et doivent être soumis séparément à l'OIAM.

Al. 4 – Vu l'art. 84, al. 3, LSI, l'OIAM s'applique par analogie aussi aux autorités visées à l'art. 2, al. 1, let. a et c à e, LSI, dans la mesure où elles n'édictent pas leurs propres dispositions. Pour que cela fonctionne, les autres autorités doivent pour le moins définir qui, dans leur domaine, est responsable en matière de législation sur la protection des données.

Al. 5 – Du fait des nouveaux al. 2 à 4, l'al. 2 devient l'al. 5, sans changement de contenu.

Art. 6, let. b, ch. 3

Le Groupement Défense remplace là aussi la BAC (cf. commentaire de l'art. 5, al. 1, let. c, plus haut).

Art. 7, let. b

Les personnes utilisant AGOV pour recourir à des prestations de cyberadministration doivent disposer d'un interlocuteur clair auprès de qui exercer leur droit de rectification et de suppression. Comme pour le droit d'accès, cet interlocuteur est l'organe responsable du service prévu à l'art. 5.

Art. 9, let. b

Dans le cadre d'AGOV, le système eIAM gérera non seulement les données personnelles des utilisateurs des systèmes de cyberadministration de la Confédération, mais aussi celles des utilisateurs des systèmes d'information des cantons et des communes. À noter que ces deux cercles d'utilisateurs peuvent se recouper, une même personne utilisant tantôt une application de la Confédération, tantôt une application des cantons ou des communes pour recourir à des prestations de cyberadministration. L'objectif d'AGOV est justement de faire en sorte que les utilisateurs n'aient pas besoin de créer un compte et de s'identifier séparément pour chaque service.

Art. 11, al. 2 et 3

Les al. 2 et 3 en vigueur jusqu'ici, d'après lesquels aucun profil de la personnalité et, sans base légale particulière, aucune donnée sensible ne peuvent être traités dans les systèmes IAM, doivent être doublement remaniés, d'une part vu l'art. 20, al. 2, LSI et, d'autre part, sur la base de la révision totale de la loi fédérale sur la protection des données.

Al. 2 – La disposition interdisant le traitement des profils de la personnalité est remplacée par une interdiction du profilage et du profilage à risque élevé (cf. art. 5, let. f et g, LPD). Cela concerne tous les types de traitement automatisé des données personnelles. Le traitement automatisé consiste à utiliser ces données afin d'en évaluer certains aspects personnels se rapportant à une personne physique, notamment pour analyser ou prédire la performance professionnelle, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, le lieu de séjour ou le changement de lieux de la personne physique concernée. Lorsque par exemple des données secondaires et le comportement des utilisateurs sont analysés pour déceler des irrégularités et des cyberattaques potentielles (*fraud detection*), ces processus de traitement des données ne relèvent pas de la notion de profilage au sens de la LPD, vu que l'accent est mis sur la sécurité de l'information et non sur le regroupement et l'analyse des différents aspects personnels d'une personne déterminée.

Étant donné que l'al. 2 a été abrogé au 1er septembre 2023 par la nouvelle ordonnance du 31 août 2022 sur la protection des données, il existe une lacune du 1er septembre 2023 au 31 décembre 2023 (il est prévu que la présente modification entre en vigueur le 1er janvier 2024) quant à l'interdiction de traiter les profils de la personnalité et d'effectuer du profilage et du profilage à risque élevé, ce qui devrait toutefois être gérable sur cette courte période.

Al. 3 – Les données biométriques permettant d'identifier clairement une personne sont maintenant considérées d'emblée comme des données sensibles ; pour leur traitement, une base générale est créée à l'art. 20, al. 2, LSI. Ces données biométriques peuvent donc, selon l'annexe (let. a, ch. 13), être traitées en principe dans tous les systèmes IAM dans lesquels cela est nécessaire pour identifier des personnes sous l'angle des risques. Voir le commentaire relatif à l'annexe, let. a.

Art. 12, al. 4

Pour que le service IAM de la Confédération puisse, dans le cadre d'AGOV, assumer la fonction d'intermédiaire pour les identités reconnues, y compris celles des cantons (ID-Broker), il faut qu'il puisse reprendre automatiquement les données des systèmes IAM de ces derniers. Les processus, interfaces et mesures de sécurité nécessaires sont détaillés dans les directives visées à l'art. 24, al. 2, et dans la convention visée à l'art. 24, al. 2, let. b.

Art. 13, al. 4, let. a

Pour des raisons de clarté, la let. a précise explicitement que la base légale en question doit (aussi) prévoir le traitement des données à transmettre.

Art. 14, al. 2

Cette disposition ne change pas en substance ; cependant, il n'est plus question de renvoyer à l'art. 2*a* de la loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée et du DDPS (LSIA)[23], mais à la LSI.

Titre précédant l'art. 18 et art. 18, al. 1 et 2

La sécurité de l'information et le respect de ses consignes ne doivent pas s'appliquer uniquement aux systèmes IAM mêmes. Ils concernent également les services d'annuaires. C'est également valable pour les prestataires de services d'annuaires externes à la Confédération, notamment si ces prestataires n'exploitent pas déjà un système IAM. Le texte de l'ordonnance est donc complété en conséquence.

En outre, dans la dernière partie de la phrase de l'al. 2, l'adjectif *prédéfinie*, qui n'apporte pas de plus-value, est supprimé de manière à ce que seules les *exigences minimales* soient prises en compte. Le sens de la disposition reste inchangé.

Art. 20 Système global IAM

Conformément à l'art. 20 en vigueur jusqu'ici, les systèmes IAM de l'administration fédérale peuvent être reliés entre eux ainsi qu'avec les systèmes IAM des Services du Parlement et de l'armée pour permettre un partage efficace des tâches. Cela signifie qu'ils peuvent échanger entre eux des données d'utilisateurs à l'instar d'une fédération. Les systèmes IAM mentionnés devront pouvoir aussi être reliés aux autres systèmes IAM de la Confédération (p. ex. ceux des tribunaux fédéraux), si bien qu'il est maintenant question des systèmes IAM *de la Confédération*.

Comme jusqu'à présent, il sera possible de relier les systèmes IAM externes aux systèmes IAM de la Confédération (un système déterminé ou un système global) (cf. actuel art. 21, qui prévoit que des systèmes IAM externes peuvent être raccordés aux systèmes IAM de la Confédération sous certaines conditions). Ceci doit être prévu à l'art. 20 déjà.

Art. 21 Phrase introductive et let. a

Généralités : l'art. 21 règle les conditions auxquelles les systèmes IAM externes (à la Confédération) peuvent être raccordés aux systèmes IAM de la Confédération. Ce raccordement sera toujours complet, ce qui ne signifie toutefois en aucun cas une perte de souveraineté sur les données. En vertu de l'art. 9, let. a, par exemple, les données personnelles ne peuvent être traitées qu'avec les ressources de l'administration fédérale ; il s'agit aussi d'une condition supplémentaire pour l'art. 21. Exemple : un canton se raccorde certes au système IAM de la Confédération,

[23] RS **510.91**

mais ne donne que les données personnelles nécessaires à l'utilisation de la ressource fédérale, en aucun cas toutes les données. En plus, l'article ne prévoit pas de mise à disposition passive, mais un envoi proactif des données par le système IAM cantonal. Le canton détermine donc toujours quelles données il communique et sur quelles personnes.

Phrase introductive – Quand un système IAM externe au sens de l'art. 21 doit être relié aux systèmes IAM de la Confédération, il est impératif, pour des raisons de sécurité, de soumettre les exploitants en question à l'OIAM, à l'exception des cantons. Les systèmes IAM des cantons raccordés à ceux de la Confédération doivent absolument garantir une sécurité de l'information qui soit au moins équivalente à celle des systèmes fédéraux. Il n'est toutefois pas nécessaire que les cantons soient soumis à l'ensemble des autres dispositions de l'OIAM. Cette manière de faire est cohérente avec la répartition des compétences entre cantons et Confédération prévue par la Constitution. La phrase est complétée en ce sens.

La *let. a* correspond à la version en vigueur jusqu'ici, complétée toutefois des systèmes IAM de la Principauté de Liechtenstein, ce qui permet de donner suite à la demande du Liechtenstein.

Art. 24, al. 1, let. a

Pour qu'AGOV puisse déployer toute son utilité, il faut que le système IAM de la Confédération puisse être relié à ceux des cantons et des communes intéressés. Ce cas de figure est désormais prévu à l'art. 24. Pour des raisons systématiques, l'al. 1, let. a, est donc complété dans ce sens. Une convention régissant les relations sur le plan juridique, organisationnel et technique est conclue avant le raccordement (al. 1, let. b). Le plan organisationnel inclut aussi les aspects financiers, pour lesquels le principe défini à l'art. 11, al. 4, LMETA s'applique. Le raccordement n'est possible que si les systèmes à raccorder disposent des bases légales nécessaires, notamment lorsque les droits et obligations des personnes privées en matière de protection des données ou de procédure sont concernés (art. 11, al. 5, LMETA).

Annexe

Modifications découlant de la LSI

Let. a – Sur la base de l'art. 20, al. 2, LSI, les données biométriques peuvent être traitées tant pour les personnes qui sont gérées dans les systèmes utilisés par l'armée que pour toutes les personnes gérées dans les systèmes IAM (jusqu'à présent ceci n'était possible que pour les systèmes de l'armée sur la base de l'art. 2*a* LSIA). Les données biométriques, mentionnées actuellement à la let. g, sont donc intégrées dans la let. a (ch. 13) ; la let. g peut par conséquent être abrogée. Ces données ne peuvent pas forcément être reprises systématiquement dans tous les systèmes IAM et utilisées dans tous les cas. Il s'agit plutôt d'examiner, pour chaque système IAM et chaque scénario d'application, si l'utilisation de données biométriques est indispensable pour identifier des personnes sous l'angle du risque. De plus, faute de base légale formelle, les données biométriques ne peuvent pas faire l'objet de communications entre les systèmes de différents responsables. Enfin, les données biométriques doivent être détruites après l'échéance du droit d'accès (cf. art. 20, al. 3, LSI et art. 14, al. 2, OIAM).

Le ch. 11 (image du visage pour pièces d'identité) figurera dans un chiffre séparé (cf. ch. 14), étant donné que l'image du visage non biométrique, soit la simple photographie, doit être mentionnée dans tous les systèmes IAM (et par conséquent dans les trois colonnes). On ne parle plus que de *photo du visage* vu qu'il ne s'agit pas que de la photo figurant sur les documents d'identité mais aussi, par exemple, des photos utilisées dans Skype.

Let. c – Il est prévu d'indiquer dans les systèmes IAM le numéro de bureau des personnes visées aux art. 8 et 9, let. b, du fait que cette information est nécessaire aux processus d'assistance du poste de travail numérique.

Let. e – Il est précisé au ch. 7 que les mots de passe doivent être protégés cryptographiquement, soit par un chiffrement suffisamment confidentiel ou par salage et hachage suffisamment confidentiels, bien que cela semble aller de soi (toutes les règles internes de gestion des mots de passe prévoient que ces derniers soient impérativement chiffrés ou protégés par salage ou hachage). Il arrive toutefois que les mots de passe soient mal sécurisés et puissent être craqués.

Let. f – Deux modifications linguistiques sont apportées au contenu (phrase introductive et ch. 2), conformément au libellé de la LSI.

La let. g est abrogée (cf. commentaire ci-dessus).

Modifications découlant de la LMETA

Annexe, let. a, ch. 4 et 5, c, ch. 2, et e, ch. 11

Parmi les données personnelles gérées dans AGOV figurent désormais également la nationalité, le lieu de naissance, l'adresse postale privée et la qualité de l'authentification. Ces données sont transmises aux systèmes d'information consommateurs dans le cadre de la prestation d'authentification. Les applications spécialisées les utilisent pour le traitement des affaires (autorisations, décisions de taxation, aides financières, prestation de services, etc.). La nationalité et le lieu de naissance figureront également dans la future e-ID (cf. art. 2, al. 2, let. e et f, de l'avant-projet de loi fédérale sur l'identité électronique et les autres moyens de preuve électroniques [loi sur l'e-ID, LeID] du 29 juin 2022). Quant à qualité de l'authentification, cette information est nécessaire dans le cadre des applications de cyberadministration pour permettre le traitement ultérieur par les applications spécialisées. Les exigences régissant la qualité de l'authentification peuvent en effet varier en fonction des applications ou du type de prestation.

Pour pouvoir traiter ces données, les systèmes consommateurs doivent disposer des bases légales nécessaires, notamment en matière de protection des données (art. 11, al. 5, LMETA). Les cantons doivent donc prévoir les dispositions requises dans leur législation.

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

Titre

La notion de *contrôles de sécurité relatifs aux personnes* regroupe, outre les contrôles de sécurité relatifs aux personnes (CSP) au sens de la LSI, l'ensemble des vérifications, évaluations et contrôles visés par d'autres lois, auxquels s'applique, directement ou par analogie, la procédure de contrôle de sécurité relatif aux personnes prévue par la LSI.

Préambule

Le préambule renvoie à toutes les normes légales qui attribuent au Conseil fédéral la compétence de légiférer dans le domaine des CSP.

Section 1 Dispositions générales

Art. 1 Objet

L'OCSP, qui est une ordonnance du Conseil fédéral, porte sur toutes les compétences d'exécution relatives aux CSP qui entrent dans le cadre de l'art. 48 LSI et sur les vérifications, évaluations et contrôles visés par d'autres lois.

Dans la systématique de la LSI, le Conseil fédéral est l'une des autorités visées à l'art. 2, al. 1, LSI, lesquelles sont placées sur un pied d'égalité. En tant qu'autorité soumise à la LSI visée à l'art. 84, al. 1, LSI, il est chargé d'édicter les dispositions d'exécution pour son domaine de compétence. Afin d'harmoniser les niveaux de sécurité entre les autorités concernées, le législateur prévoit à l'art. 84, al. 3, LSI que les dispositions d'exécution que le Conseil fédéral édicte dans son domaine de compétence s'appliquent par analogie également aux autres autorités soumises à la LSI, pour autant qu'elles n'émettent pas leurs propres directives. Il existe toutefois des domaines pour lesquels la LSI retire cette compétence « opt-out » aux autres autorités concernées. Il n'est donc pas pertinent que tant le Conseil fédéral que par exemple le Parlement, les tribunaux fédéraux ou la Banque nationale fixent chacun une procédure de contrôle ou règlent l'organisation des services spécialisés CSP. Une seule règle doit exister à ce sujet et le législateur a expressément attribué cette compétence de réglementation au Conseil fédéral. Si ce dernier, en tant qu'« autorité soumise » à la LSI édicte des dispositions d'exécution (cf. p. ex. art. 26 et 28 LSI), les autres autorités concernées peuvent émettre leurs propres dispositions d'exécution. Si la loi donne expressément une compétence d'exécution au Conseil fédéral (cf. p. ex. art. 48, 73, 80 ou 83, al. 3, LSI), cette compétence lui revient à lui seul. Dans ce cas, les autres autorités fédérales ne disposent d'aucune compétence propre de réglementation.

À l'art. 48 LSI, le législateur a expressément donné *au seul Conseil fédéral* la compétence d'émettre des dispositions d'exécution concernant les points de réglementation visés aux al. 1 et 2. Le Conseil fédéral a en revanche, en tant qu'autorité soumise à la LSI visée à l'art. 2, al. 1, LSI, des tâches spécifiques d'exécution pour son propre domaine, à savoir l'administration fédérale et l'armée. Voir également le commentaire de l'art. 2 à ce sujet.

Art. 2 Champ d'application

L'OCSP s'applique à toutes les autorités et à toutes les organisations soumises à la LSI. Son champ d'application est limité pour les unités administratives décentralisées et les organisations ayant des tâches administratives visées à l'art. 2, al. 4, LOGA : seules celles qui entrent dans le champ d'application de l'OSI sont concernées par le champ d'application de l'OCSP pour ce qui est des CSP selon la LSI. Les unités administratives décentralisées qui sont couvertes par le champ d'application de la LPers peuvent également être concernées par les contrôles de loyauté visés à l'art. 20*b* LPers et entrer ainsi dans le champ d'application de l'OCSP.

L'OCSP s'applique également aux autorités fédérales indépendantes du Conseil fédéral soumises à la LSI visées à l'art. 2, al. 1, LSI. À l'art. 48 LSI, le législateur a en effet octroyé au seul Conseil fédéral la compétence de régler les modalités de la procédure de contrôle et l'organisation des services spécialisés CSP. Les autorités concernées restent en revanche chargées d'édicter leurs listes des fonctions et de désigner les services qui demandent le contrôle et les instances décisionnelles (cf. commentaire de l'art. 1).

Section 2 Listes des fonctions

Art. 3 Attribution

Al. 1 à 3 – Une liste des fonctions est établie en annexe à l'ordonnance pour chaque type de CSP. Conformément à l'art. 41*b,* al. 2, de la loi du 16 décembre 2005 sur les étrangers et l'intégration[24] et à l'art. 6*a,* al. 2, de la loi du 22 juin 2001 sur les documents d'identité[25], des contrôles de sécurité au sens de l'art. 6 de l'OCSP actuelle peuvent être effectués pour certaines personnes dans le domaine de la délivrance de documents d'identité. C'est sciemment qu'aucune liste des fonctions n'est dressée dans l'OCSP pour ces contrôles. En cas de besoin impératif de CSP, celui-ci serait couvert via une procédure de sécurité relative aux entreprises dans les entreprises correspondantes.

Les listes des fonctions ne peuvent pas contenir de fonctions qui ne se conforment pas aux strictes conditions des art. 10 à 14 OCSP.

Les autorités soumises à la présente loi selon l'art. 2 LSI qui ne relèvent pas du domaine de compétence du Conseil fédéral (p. ex. le Ministère public de la Confédération) doivent établir elles-mêmes leurs listes des fonctions.

Al. 4 – Cet alinéa correspond pour l'essentiel à la réglementation en vigueur de l'art. 1, al. 3, OCSPN. Durant la phase du projet, les responsables de projet traitent déjà des informations classifiées CONFIDENTIEL ou SECRET. De ce fait, un contrôle de fiabilité est déjà nécessaire à ce moment-là. En prenant en compte les responsables de projet d'une nouvelle installation nucléaire et les titulaires d'une autorisation générale, le cycle entier au cours duquel des informations classifiées CONFIDENTIEL ou SECRET doivent être traitées est couvert.

Art. 4 Modification

Maintenir le nombre de contrôles dans le cadre ciblé exige un meilleur contrôle que celui effectué jusqu'à présent de la légalité de l'inscription des fonctions soumises au contrôle lors de l'établissement et de la mise à jour des listes des fonctions. Le DDPS gérera donc ces listes de façon centralisée et les actualisera régulièrement à la demande des départements et de la ChF. Il consultera le service spécialisé de la Confédération pour la sécurité de l'information. Conformément à la LApEl, la société nationale du réseau de transport n'adresse au Département fédéral de l'environnement, des transports, de l'énergie et de la communication ses demandes visant à modifier la liste des fonctions qu'après avoir consulté la Commission de l'électricité.

Art. 5 Publication, conservation et communication

Les organes et les personnes qui, pour l'exécution de leurs tâches, doivent avoir accès à des listes des fonctions non publiées doivent pouvoir les consulter par l'intermédiaire du DDPS. Il s'agit, en l'occurrence des services qui demandent le contrôle et des organes de sécurité selon l'OSI. Concernant la sensibilité des listes des fonctions en termes de sécurité, voir le ch. 2.5, let. e.

Art. 6 Contrôle de l'actualité

Al. 1 – Le contrôle de l'exactitude des listes des fonctions est fastidieux, mais il est nécessaire de maintenir les listes des fonctions à jour et de remettre en question des classifications de fonctions déjà effectuées afin de ne contrôler que les personnes dont la fonction exige un contrôle du fait d'un risque potentiel. Il faut donc définir une approche pragmatique, avec une vérification générale des listes des fonctions tous les trois ans et une vérification spécifique lors de réorganisations ou de changements des tâches.

Al. 2 – Sur la base des expériences précédentes, il faut s'assurer que le contrôle de l'exactitude des listes des fonctions a bien lieu. Un rapport doit être rendu au DDPS. Les changements dans les listes des fonctions qui s'avèrent nécessaires à l'issue d'un contrôle de l'exactitude des listes des fonctions doivent être traités en conséquence.

Art. 7 Contrôle extraordinaire

Si une fonction remplit les critères d'un contrôle, mais n'a pas encore été intégrée dans la liste des fonctions correspondante, le contrôle peut, sur la base de l'art. 29, al. 3, LSI, être réalisé avec l'accord de l'autorité soumise à la LSI. Pour l'administration fédérale, il faut que la compétence décisionnelle concernant un contrôle extraordinaire soit déléguée au DDPS, qui consulte le

[24] RS **142.20**
[25] RS **143.1**

service spécialisé de la Confédération pour la sécurité de l'information. La demande est adressée par la ChF ou les départements, qui consultent leur préposé à la sécurité de l'information au préalable. Les listes des fonctions doivent être mises à jour en conséquence. Les autres autorités soumises à la LSI règlent elles-mêmes les compétences.

Art. 8 Contrôle du personnel cantonal et des tiers

Al. 1 – La définition des fonctions d'employés cantonaux qui sont soumis à un contrôle conformément à l'art. 29, al. 1, let. b, LSI est en principe du ressort des cantons. Pour garantir un traitement homogène, le DDPS doit assumer ici une fonction de pilotage. Pour ce faire, il consulte le service spécialisé de la Confédération pour la sécurité de l'information.

Al. 2 –Les fonctions des tiers qui exécutent pour une autorité soumise à la LSI ou une organisation un mandat qui inclut l'exercice d'une activité sensible ne peuvent pas être définies à l'avance, mais résultent des nécessités des différents mandats. Pour que la nécessité du contrôle soit aussi garantie ici, les décisions doivent être centralisées. Lors de la décision, il s'agit de s'assurer de la légalité du contrôle et de répondre à cette question : sommes-nous réellement en présence d'une activité sensible ?

Art. 9 Contrôle de fiabilité extraordinaire de l'IFSN

Cet article correspond de par son contenu à la réglementation en vigueur de l'art. 5 OCSPN.

Section 4 Attribution aux degrés de contrôle

Le rattachement du contrôle de la loyauté selon la loi sur l'asile au degré de contrôle du contrôle de sécurité de base est déjà précisé à l'art. 29*a* de la loi du 26 juin 1998 sur l'asile (LAsi)[26] et ne nécessite donc pas d'être précisé dans l'ordonnance.

Art. 10 Contrôles de sécurité relatifs aux personnes selon la LSI

Al. 1, let. a – La notion de *traitement* fait ici référence à tout rapport avec des informations, indépendamment des moyens et procédés utilisés, notamment l'obtention, la conservation, l'enregistrement, l'utilisation, le remaniement, la communication, l'archivage, la suppression ou la destruction d'informations. Ce qui est décisif, c'est de savoir si le traitement des informations classifiées est nécessaire pour l'accomplissement des tâches dans le cadre de la fonction concernée. Concernant le critère de la régularité pour les CSP, voir le ch. 1.2.5 du message LSI, p. 2797 et le commentaire de l'art. 29 LSI, p. 2847 et 2848.

Al. 1, let. b – Les notions que sont *l'administration, l'exploitation, la maintenance et le contrôle de moyens informatiques* couvrent toutes les activités visées à l'art. 5, let. b, LSI qui impliquent des droits d'accès particuliers aux moyens informatiques de la Confédération ou qui placent les personnes chargées de les exercer dans une situation où elles pourraient nuire considérablement aux intérêts publics par le sabotage selon l'art. 1, al. 2, LSI. La décision de savoir si les utilisateurs des moyens informatiques exercent une activité sensible est prise uniquement en fonction de la classification des informations à traiter. De ce fait, ce sont surtout les administrateurs et les responsables des applications des systèmes qui sont concernés. La notion d'*exploitation* se réfère à l'activité des fournisseurs de prestations au sens de l'art. 19 LSI. Elle doit être clairement distinguée de l'expression *exploiter un système d'information* que l'on trouve dans la législation sur la protection des données pour régler le recours à un système d'information par un bénéficiaire de prestations (p. ex. art. 24, al. 1, LSI). Les activités sensibles dans le cadre du développement ou de la construction de systèmes d'information sont incluses à la let. b comme partie de l'administration et de l'exploitation.

Al. 1, let. c – La caractérisation de zones ou de locaux en zones de sécurité constitue une mesure physique favorisant la sécurité de l'information, notamment pour protéger les locaux abritant des serveurs ou certaines salles de conduite. Une zone de sécurité exige une protection conséquente. Les personnes qui doivent accéder à la zone de sécurité 1 font donc l'objet d'un contrôle de sécurité de base.

Al. 1, let. d – Si des traités internationaux prévoient un contrôle, le degré de contrôle dépend des consignes du traité. Si le traité ne contient pas de réglementation spécifique, on effectuera toujours un contrôle de sécurité de base.

[26] RS **142.31**

Al. 2, let. a à c – Voir le commentaire de l'al. 1, let. a à c.

Al. 2, let. d et e – Les personnes qui exercent des activités sensibles pour le Service de renseignement de la Confédération (SRC) ou son autorité de surveillance, le Renseignement militaire et le service Actions dans le cyberespace et dans l'espace électromagnétique (ACEM) le font régulièrement dans des domaines très sensibles. Leurs activités doivent donc être rattachées au degré de contrôle du contrôle de sécurité élargi.

Al. 2, let. f – Voir le commentaire de l'al. 1, let. d.

Art. 11 Contrôle de loyauté selon la LPers

Al. 1, let. a – Lors de leurs activités officielles, le personnel fédéral affecté à l'étranger et celui du DFAE soumis à la discipline des transferts (cf. art. 3, let. a et b, de l'ordonnance du DFAE du 20 septembre 2002 concernant l'ordonnance sur le personnel de la Confédération[27]) peuvent porter un préjudice considérable à des intérêts prépondérants de la Confédération. Les personnes exerçant de telles activités sont soumises au contrôle de sécurité de base.

Al. 1, let. b – Dans le contexte actuel, une conséquence considérable correspond à un préjudice financier potentiel de l'ordre de 50 à 500 millions de francs.

Al. 1, let. c – La portée des tâches relevant de la poursuite pénale ou des tâches policières peut être très grande selon l'interprétation de ces notions. Le champ d'application de ce motif de contrôle doit donc être limité aux tâches et aux organisations qui peuvent compromettre considérablement les intérêts publics de la Confédération.

Al. 2, let. a et b – Les titulaires de fonction pour lesquels le Conseil fédéral ou le chef de département est compétent pour la conclusion, la modification et la résiliation des rapports de travail en vertu de l'art. 2, al. 1, ou de l'art. 2, al. 1*bis*, de l'ordonnance du 3 juillet 2001 sur le personnel de la Confédération (OPers)[28] répondent régulièrement à au moins l'un des motifs de contrôle visés à l'art. 20*b*, al. 1, let. a et b, LPers. Cela concerne aussi les titulaires de fonction au sens de l'art. 2, al. 1, let. e, LPers. Du fait du risque d'atteinte élevée à la réputation en cas de manquements de ces titulaires, ces personnes sont soumises au contrôle de sécurité élargi.

Al. 2, let. c – Par *responsables des unités administratives décentralisées*, on entend les directeurs. Ceux-ci doivent également passer un contrôle de sécurité élargi en raison de l'atteinte élevée à la réputation pouvant résulter d'un manquement de ces titulaires de fonctions (cf. art. 11, al. 2, let. a et b). Toutefois, seuls ceux qui sont soumis à la LPers sont concernés par ces lettres. Par exemple, la LPers ne s'applique pas à la direction des commissions extraparlementaires, ni à la direction de la FINMA. Les motifs de contrôle visés dans la LSI sont déterminants pour les autres unités administratives décentralisées.

Al. 2, let. d – Dans ce contexte, une conséquence *importante* correspond à un préjudice financier potentiel dépassant 500 millions de francs, tandis qu'une conséquence *très importante* dépasse un milliard de francs.

Al. 2, let. e – Si le personnel de fedpol agit de manière inadéquate ou de façon contraire aux prescriptions dans la lutte contre la grande criminalité qui relève de la compétence de la Confédération, comme la lutte contre le terrorisme, l'extrémisme violent, la criminalité organisée et d'autres formes de criminalité transnationale, une atteinte considérable peut être portée à l'intérêt public de la Confédération.

Al. 2, let. f – Le personnel des services spécialisés CSP visés à l'art. 16, al. 1, dont les activités sont considérées comme étant des activités de police de sécurité, est aussi soumis à un contrôle de sécurité élargi.

Art. 12 Contrôles visés dans la loi du 3 février 1995 sur l'armée (LAAM)[29]

Al. 1, let. a – Les activités exercées à l'étranger par des militaires en uniforme n'entrent pas toutes dans le cadre de la *représentation officielle* de la Suisse. La représentation purement visuelle de la Suisse ou des activités entrant dans le cadre de contingents de troupes internationaux ne suffisent pas à motiver un contrôle de loyauté. Il doit s'agir d'activités officielles incluant des compétences décisionnelles qui ont un impact extérieur sur la représentation de la Suisse.

[27] RS **172.220.111.343.3**
[28] RS **172.220.111.3**
[29] RS **510.10**

Al. 1, let. b – Voir le commentaire de l'art. 11, al. 2, let. b.

Al. 1, let. c – Au besoin, un contrôle de sécurité de base suffit lorsqu'il s'agit de décider de ne pas recruter un conscrit, de dégrader un militaire ou de l'exclure de l'armée.

Al. 2 – Jusqu'à présent, les aspirants pouvaient être soumis à un CSP, indépendamment d'une raison matérielle justifiant le contrôle. Cette possibilité est supprimée avec la présente ordonnance. Ils ne peuvent être contrôlés que s'il existe une raison matérielle selon la LSI ou la LAAM pour un tel contrôle. Si la personne concernée a déjà fait l'objet d'un CSP valable et qu'elle est candidate à une fonction exigeant un CSP, le CSP ne peut être répété par anticipation que si le délai minimal fixé à l'art. 43, al. 1, LSI est échu.

Al. 3 et 4 – Cet alinéa reprend pour l'essentiel le contenu de l'art. 5, al. 2 et 3, OCSP.

Art. 13 Contrôles de fiabilité visés dans la loi du 21 mars 2003 sur l'énergie nucléaire (LENu)[30]

Cet article correspond pour l'essentiel à la réglementation en vigueur de l'art. 3 OCSPN, auquel sont ajoutés les responsables de projet d'une nouvelle installation nucléaire et les titulaires d'une autorisation générale. L'al. 1, let. b, remplace plusieurs catégories de personnes pour lesquelles un CSP était nécessaire en vertu de l'OCSPN en vigueur jusqu'ici, les activités sensibles devenant un motif de contrôle par analogie avec les autres dispositions de l'OCSP en lien avec les activités. La formulation *compromettre considérablement* exclut les activités dont le potentiel de dommage résultant d'un exercice déloyal ne justifie pas un CSP. L'al. 1, let. b, suit les principes de la sécurité nucléaire et de l'utilisation de l'énergie nucléaire, selon lesquels, au titre de la prévention, on prendra toutes les mesures qui s'imposent en vertu de l'expérience et de l'état de la science et de la technique et toutes les mesures supplémentaires qui contribuent à diminuer le danger, pour autant qu'elles soient appropriées (art. 4, al. 3, LENu). S'agissant du cercle des personnes, cette disposition correspond à la pratique.

Art. 14 Contrôles de loyauté visés dans la LApEl

Conformément à la stratégie nationale pour la protection des infrastructures critiques 2018–2022, les informations critiques sont toutes des informations essentielles au bon fonctionnement de la sécurité d'approvisionnement, des applications critiques ou des infrastructures critiques. Les informations très critiques sont, quant à elles, toutes des informations hautement essentielles au bon fonctionnement de la sécurité d'approvisionnement, des applications critiques ou des infrastructures critiques.

Sont par exemple soumises à un contrôle de sécurité relatif aux personnes les personnes qui peuvent accéder de manière autonome à une installation électrique du fait qu'elles sont en mesure d'impacter en peu de temps la sécurité de l'approvisionnement.

Section 5 Procédure

Dans le cadre des travaux préalables au présent projet d'ordonnance, il a été suggéré de prévoir des délais maximaux pour la durée d'évaluation du risque pour la sécurité afin que les résultats soient disponibles dans un délai raisonnable. Du fait des précédentes expériences, il a été décidé de ne pas fixer de tels délais. La durée de l'évaluation dépend essentiellement de la disponibilité des données à collecter et de leur contenu effectif. Un délai absolu conduirait, surtout s'il est trop court, à une multiplication des constatations parce que les signes de risques n'auraient pas pu être clarifiés de façon approfondie ou parce que les données n'auraient pas été disponibles dans les temps.

Art. 15 Services qui demandent le contrôle et instances décisionnelles

Al. 1 – Pour l'administration fédérale, les départements et la ChF doivent pouvoir définir eux-mêmes le rattachement des compétences le plus approprié pour leur organisation.

Al. 3 – Lors d'une procédure de sécurité relative aux entreprises, le service spécialisé chargé de la procédure de sécurité (service spécialisé PSE) est à la fois le service qui demande le contrôle et l'instance décisionnelle. Mais si, en vertu de l'art. 53, al. 2, LSI, la procédure n'a pas lieu et que seul le CSP est effectué, l'adjudicateur engage le CSP après que le préposé à la sécurité de l'information

[30] RS **732.1**

du département a vérifié que les tiers employés exerçaient bien une activité sensible. L'adjudicateur est en outre aussi l'instance décisionnelle et habituellement le service d'achat.

Al. 4 – Cet alinéa correspond à l'art. 2, al. 2 et 4, al. 1, OCSPN, auquel sont ajoutés les responsables de projet d'une nouvelle installation nucléaire et les titulaires d'une autorisation générale (cf. commentaire de l'art. 4, al. 4).

Al. 6 – Pour que les services spécialisés CSP puissent être efficaces, ils doivent connaître qui, au sein des diverses autorités, est compétent pour engager les procédures de contrôle et pour décider de l'exercice ou non d'une fonction.

Al. 7 – Étant donné qu'il est encore nécessaire de compléter des formulaires physiques pour lancer un contrôle, le service qui demande le contrôle doit conserver ces documents originaux. Il les conserve tant que la personne concernée exerce son activité sensible, mais pas plus de dix ans.

Art. 16 Services spécialisés CSP

Il faut maintenir le système éprouvé des deux services spécialisés CSP aux compétences différentes.

Le service spécialisé CSP ChF contrôle, selon l'art. 16, al. 3, let. d, les fonctions du SEPOS du DDPS impliquant des tâches de conduite envers le Service spécialisé CSP DDPS. Il s'agit, en l'occurrence, de contrôler le secrétaire d'État, son suppléant et le chef du service spécialisé CSP DDPS. Hormis ces trois fonctions du SG-DDPS, le service spécialisé CSP ChF ne contrôle pas d'autres fonctions visées à la let. d.

Pour le reste, les prescriptions sur la récusation visées à l'art. 10 de la loi fédérale du 20 décembre 1968 sur la procédure administrative[31] s'appliquent.

Art. 17 Contrôle des conditions du contrôle

Les autorités soumises à la LSI sont responsables de l'évaluation de la sensibilité des fonctions. Les listes des fonctions sont donc contraignantes pour les services spécialisés CSP. Ils ne peuvent pas vérifier pour chaque CSP requis si la fonction est effectivement sensible. La charge de travail serait disproportionnée. Par contre, ils peuvent et doivent contrôler si la procédure a été correctement ouverte. De plus, le service qui demande le contrôle a pour tâche de justifier que la personne a consenti au contrôle et que ce consentement répond aux exigences de l'art. 6, al. 6, LPD.

Les services spécialisés contrôlent en outre que les données nécessaires au contrôle ont été communiquées. Il s'agit notamment des données permettant d'identifier la personne, de celles qui concernent les anciens lieux de domicile et des coordonnées électroniques telles que l'adresse e-mail.

Art. 18 Collaboration

Le contrôle de sécurité serait inefficace si, sous le couvert des droits fondamentaux, la personne concernée pouvait refuser de répondre à des demandes de renseignements sur d'éventuels abus d'alcool ou de stupéfiants, des dettes personnelles, des activités accessoires, etc., et si des faits de cette nature n'entraient pas dans l'appréciation du risque pour la sécurité. Dans le cadre de l'obligation de collaborer à la procédure, la personne contrôlée doit donc participer à l'établissement des faits. Elle peut toutefois déclarer ne pas vouloir répondre à certaines questions. Il appartient alors aux services spécialisés d'apprécier le refus de répondre ou le refus de fournir d'autres documents (tels des rapports médicaux ou des dépistages de drogues), car ils disposent d'une certaine liberté pour poser des questions en rapport avec la vie privée. Les éventuelles obligations légales de garder le secret de la personne à contrôler doivent être prises en compte.

Art. 19 Collecte des données

Al. 1 – Selon le droit en vigueur, la consultation d'une base de données est principalement le fait du Service spécialisé CSP DDPS. À la suite de l'entrée en vigueur de la LSI et de l'OCSP, les deux services spécialisés CSP collecteront eux-mêmes les données des cas leur ayant été confiés. Ils ne doivent pas obligatoirement recourir à tous les moyens disponibles pour évaluer le risque. Cette règle est particulièrement importante pour le contrôle élargi parce que la réduction du nombre

[31] RS **172.021**

des degrés de contrôle ne doit pas entraîner une augmentation massive des coûts des CSP. Par conséquent, c'est volontairement que cette disposition ne fixe pas quelles données devront être collectées et traitées, et à quel moment. Les services spécialisés CSP sont les mieux placés pour évaluer quelles données sont nécessaires aux évaluations des risques.

Al. 2 et 3 – L'audition de la personne concernée visée à l'art. 34, al. 2, let. d, LSI sert à vérifier des faits qui ne ressortent pas ou pas clairement des données collectées. Elle peut être menée sans indice d'un risque pour la sécurité et sa portée n'est pas limitée. Du fait de la charge de travail qu'elle occasionne, elle doit être restreinte à un minimum de fonctions. La liste est donc exhaustive. Pour toutes les fonctions énumérées, les collaborateurs internes et externes sont traités de la même manière. En cas de répétition ordinaire du contrôle selon l'art. 26, les services spécialisés décident eux-mêmes si l'audition est nécessaire si le risque a peu changé. Cela sera généralement l'exception.

Al. 4 – Pour faire la lumière sur des éléments particulièrement pertinents pour la sécurité ou pour obtenir un complément de données sur une plus longue période, les services spécialisés CSP peuvent aussi auditionner des tiers. L'al. 4 cite aux let. a à c les groupes de personnes les plus importants connus de la pratique. À côté de cela, il y a aussi d'autres personnes qui disposent d'informations utiles (p. ex. des membres de la famille ou d'anciens partenaires professionnels). Celles-ci sont incluses dans la formulation générale de la let. d. À plusieurs reprises, il a été suggéré d'obliger par l'ordonnance les tiers qui peuvent être auditionnés à dire la vérité. Or les bases légales ne prévoient pas d'obligation à cet égard. Les tiers concernés peuvent donc refuser à tout moment de communiquer des informations.

Art. 20 Assistance administrative

Les services spécialisés CSP ne collectent pas toutes les données de façon autonome, notamment pas les données collectées à l'étranger. Cette collecte passe usuellement par fedpol et le SRC. Seuls ces services sont en mesure d'apprécier à leur juste valeur la fiabilité des données et des sources de données.

Art. 21 Regroupement des procédures de contrôle

Certaines fonctions regroupent diverses activités susceptibles de motiver des contrôles. Si plusieurs motifs justifient de contrôler une personne, les contrôles doivent être regroupés pour des raisons d'économie de procédure. Si une personne doit ainsi être contrôlée par les deux services spécialisés CSP, seul le service spécialisé CSP ChF réalise le contrôle. La raison de l'engagement de ce service tient dans l'art. 16, al. 2, selon lequel il existe une liste exhaustive des fonctions qui doit être respectée. Le regroupement évite une surcharge inutile des coûts. Les résultats du contrôle pour chaque motif doivent apparaître séparément.

Art. 22 Conditions

Les services spécialisés CSP recommandent aux instances décisionnelles des conditions adaptées pour réduire à un niveau acceptable le risque pour la sécurité qui existe de l'avis des services spécialisés CSP. Les instances décisionnelles ne sont pas liées par ces recommandations. Elles peuvent suivre les conditions recommandées, en prévoir d'autres ou ne pas en tenir compte. Ces mesures qui visent à réduire les risques et qui relèvent du droit du personnel se fondent sur l'art. 39, al. 1, let. b, et sur l'art. 41, al. 3, LSI (cf. message LSI à propos de l'art. 42) et sont spécifiées à l'art. 22, let. b, OCSP. L'employeur peut ordonner de telles mesures en vertu de l'art. 24, al. 2, LPers. La base légale permettant de traiter les données sensibles découle pour la Confédération de l'art. 27, al. 2, LPers, dans la mesure où cela est nécessaire pour la sauvegarde d'intérêts importants.

Art. 23 Communication

Al. 1 – Si, pour plusieurs motifs de contrôle, des personnes sont soumises à plusieurs contrôles effectués à des moments différents, les risques constatés lors d'un contrôle ultérieur doivent pouvoir être communiqués aux instances décisionnelles du contrôle antérieur afin que des mesures de sécurité puissent être prises en cas de besoin. La précision est importante notamment pour les contrôles visés à l'art. 113 LAAM, auxquels tous les militaires sont soumis. Si l'on constate un risque par rapport à l'arme personnelle dans le cadre de l'un des contrôles, les services spécialisés CSP sont autorisés à le communiquer aux autorités militaires compétentes.

Al. 2 – Lorsque les services spécialisés CSP disposent d'indices fondés d'un risque pour la sécurité et qu'il y a urgence, ils peuvent informer à titre préventif les organes compétents avant même l'achèvement de la procédure. Ces organes peuvent alors prendre les mesures de sécurité provisionnelles qui s'imposent. C'est notamment important pour le recrutement de conscrits, qui dure au maximum trois jours. Les réserves pour la sécurité (p. ex. la consommation antérieure de stupéfiants) peuvent être importantes pour l'évaluation de l'aptitude au service militaire par les médecins et les psychologues lors du recrutement.

Section 6 Conséquences de la déclaration

Art. 24 Communication de la décision sur l'exercice de l'activité

L'instance décisionnelle assume la responsabilité de la personne contrôlée et prend donc une décision sur l'exercice de l'activité concernée. Les éventuelles conditions recommandées par les services spécialisés CSP ne sont pas contraignantes pour les instances décisionnelles (cf. art. 22). Ces dernières peuvent suivre les conditions recommandées, en prévoir d'autres ou ne pas du tout en tenir compte. Si l'instance décisionnelle associe l'exercice d'une activité sensible à des conditions, elle doit aussi définir qui supporte les coûts de ces conditions. Les consignes de droit du travail ou de droit des contrats sont à respecter. Si les éventuelles conditions ne sont pas remplies, la personne contrôlée se verra démise de son activité sensible, le risque pour la sécurité ne pouvant pas être réduit à un niveau acceptable.

La communication rapide de la décision sur l'exercice de l'activité est notamment nécessaire pour donner accès à des installations militaires ou à des zones de sécurité. Elle est également déterminante pour l'établissement du certificat de sécurité au sens de l'art. 30, al. 2, let. b.

Art. 25 Utilisation de la déclaration pour d'autres activités sensibles

Al. 1 – En règle générale, lorsque la personne concernée fait l'objet d'une déclaration pour un degré de contrôle au moins équivalent et que celle-ci est encore valable, un nouveau contrôle doit être évité pour des raisons d'économies. La décision à ce sujet dépend de celui qui assume le risque. S'agissant des militaires, l'évaluation du potentiel d'abus ou de dangerosité visé à l'art. 113, al. 4, let. d, LAAM équivaut à un contrôle de sécurité de base au sens de la LSI.

Al. 2 – Utiliser la déclaration d'un contrôle antérieur pour un nouveau contrôle peut poser problème d'un point de vue de la législation sur la protection des données si le degré de contrôle de l'ancien contrôle est supérieur au degré de contrôle du nouveau contrôle. En effet, des données collectées dans le cadre d'un degré de contrôle supérieur et qui ne devraient pas l'être dans le cadre d'un degré de contrôle inférieur viennent alors alimenter l'évaluation. Ignorer ce savoir comme ordonné par la législation sur la protection des données peut, le cas échéant, aboutir à des résultats contraires à la politique de sécurité. Par analogie avec des règles restrictives sur l'utilisation de découvertes fortuites dans d'autres bases légales, une utilisabilité clairement restreinte doit être possible.

Art. 26 Répétition ordinaire du contrôle

La LSI ne prescrit pas de délais de répétition ordinaires du contrôle. Elle ne donne que des grandes lignes. Pour pouvoir, ici aussi, gérer le volume contrôlé, des délais clairs doivent être précisés pour la répétition du contrôle en fonction des besoins de sécurité. La LSI donne en outre au Conseil fédéral la compétence de pas répéter le contrôle d'un militaire ou d'un membre de la protection civile. Cela doit être mis en œuvre pour les cas où la répétition semble disproportionnée au vu du temps de service restant. Il s'agit par exemple des évaluations du potentiel d'abus ou de dangerosité visé à l'art. 113, al. 4, let. b, LAAM qui ne sont qu'exceptionnellement répétées, par exemple en cas de soupçons visés à l'art. 12, al. 3, let. c, OCSP.

Art. 27 Répétition extraordinaire du contrôle

Al. 1 – La répétition extraordinaire d'un contrôle ne se justifie que par l'apparition de nouveaux risques qui sont importants pour l'évaluation des risques liés à l'exercice de l'activité. En revanche, les manquements à des conditions d'embauche ne justifient pas l'ouverture d'une répétition anticipée du contrôle. Le droit du personnel prévoit des mesures pour pareils manquements.

Al. 2 – La LSI prévoit une répétition extraordinaire uniquement en cas de soupçons justifiés de nouveaux risques. La suppression de risques constatés antérieurement peut aussi être importante pour l'employeur car d'éventuelles restrictions ne sont alors plus nécessaires pour l'exercice d'activités sensibles. Dans pareils cas, une répétition extraordinaire peut aussi être engagée.

Art. 28 Effet de la répétition

L'effet de la répétition vaut tant pour une répétition ordinaire qu'extraordinaire. Comme la répétition sert de nouvelle évaluation de la personne à contrôler, l'évaluation précédente est déterminante pour l'exercice des activités sensibles jusqu'à ce que soit disponible la nouvelle évaluation. Si de nouveaux risques sont identifiés pendant le contrôle de répétition, l'instance décisionnelle doit veiller, par des mesures adaptées visées à l'art. 21, al. 2, LSI, à ce que ces risques ne puissent pas se réaliser d'ici à la fin du contrôle. Cela peut s'effectuer par le retrait temporaire de certaines activités ou des changements temporaires du cahier des charges.

Art. 29 Voies de droit

Les services spécialisés CSP réalisent l'évaluation sans aucune instruction selon l'art. 31, al. 2, LSI. Cela doit aussi valoir pour les procédures de recours concernant les évaluations afin que les organes supérieurs des services spécialisés CSP ne puissent pas influencer indirectement les évaluations en refusant qu'une procédure de recours ait lieu. Les services spécialisés CSP doivent donc pouvoir décider eux-mêmes s'ils veulent recourir contre des décisions du Tribunal administratif fédéral.

Art. 30 Certificat de sécurité

Les autorités de sécurité étrangères n'autorisent l'accès à des informations classifiées, à du matériel classifié et à des zones de sécurité qu'aux personnes disposant d'un certificat de sécurité. La procédure doit être définie pour la délivrance d'une *personnel security clearance*. La décision de l'instance décisionnelle visée à l'art. 24 est déterminante pour la *clearance* et non le résultat de l'évaluation par les services spécialisés CSP. Si la *clearance* ne relève pas de l'intérêt de la Confédération, le certificat de sécurité doit être payant. Jusqu'à présent, une *clearance* n'était demandée que dans un contexte international. Les services suisses attendent de plus en plus que les personnes qui participent à des projets ou à des séances classifiées présentent un certificat de sécurité. Une *clearance* peut être demandée et établie à ces deux fins.

Section 7 Traitement des données personnelles

Art. 31 Responsabilité en matière de protection et de sécurité des données

En application de l'art. 33 LPD, l'organisation des compétences et des responsabilités pour la protection des données qui exige aussi la sécurité des données doit être réglementée en lien avec le système d'information visé à l'art 45 LSI. Le principe selon lequel le maître des données est responsable doit être applicable.

Art. 32 Contrôle périodique du traitement des données personnelles

Les données traitées dans le cadre des contrôles étant sensibles, la légalité de leur traitement doit être vérifiée périodiquement par un service indépendant de ceux impliqués dans la procédure de contrôle. De tels services indépendants peuvent par exemple être la Révision interne, des auditeurs externes, des conseillers en protection des données ou le PFPDT.

Section 8 Dispositions d'exécution

Art. 33 Communication électronique

Les employés de la Confédération sont tenus de communiquer par voie électronique avec les services CSP. Selon la pratique actuelle, il n'est toutefois pas possible d'obliger la population générale à correspondre électroniquement (cf. message concernant la loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités ; FF *2022* 804). Les personnes qui ne sont pas des employés de la Confédération peuvent par conséquent demander que la correspondance avec elles s'effectue en format papier. La correspondance entre autorités continue de se dérouler par voie électronique. S'agissant de la correspondance juridique par voie électronique avec les tribunaux, l'art. 48 LSI, en relation avec l'art. 35 OCSP, constitue une disposition légale spéciale conformément à l'art. 1, al. 2, Règlement d'exécution du Tribunal administratif fédéral sur la communication électronique avec les parties[32].

[32] RS **173.320.6**

Art. 34 Émoluments

Les coûts des contrôles issus de l'administration fédérale centrale et de l'armée doivent être budgétisés de façon centralisée par le DDPS. En font également partie les contrôles imposés par la LSI et la LPers à toutes les autorités et organisations concernées. Les coûts des contrôles effectués pour des services externes à l'administration fédérale centrale doivent être supportés par ceux-ci de façon décentralisée et donner lieu à des émoluments. Par l'octroi de ressources humaines et financières au DDPS, le Conseil fédéral doit veiller à l'équilibre constant entre ces ressources et le nombre de contrôles à effectuer.

Art. 35 Prestations des services spécialisés CSP en faveur des cantons

Conformément à l'art. 86, al. 4, LSI, les cantons peuvent faire appel aux prestations des services spécialisés visés par la LSI pour leur propre sécurité de l'information, moyennant paiement, dans la mesure où le Conseil fédéral le précise. Il ressort de l'art. 16 que le service spécialisé CSP DDPS est compétent pour accomplir les contrôles de sécurité relatifs aux personnes des cantons. Pour pareille utilisation, les cantons doivent disposer de leurs propres bases légales pour les contrôles et le service spécialisé CSP DDPS doit être techniquement qualifié pour procéder aux évaluations demandées. Comme il s'agit de fait de prestations à caractère commercial de la Confédération, les conditions habituelles pour de telles prestations s'appliquent, notamment le principe de la couverture des frais. Le DDPS conclut avec les cantons concernés un accord de prestations pour que la quantité des contrôles – et donc la charge que doit assumer le DDPS – soit prévisible et planifiable. Si les prestations à fournir nécessitent des moyens supplémentaires du service spécialisé, les prestations ne pourront être apportées que si les moyens supplémentaires sont effectivement octroyés au service spécialisé. Une compensation de ces moyens interne à la Confédération est exclue.

Section 9 Dispositions finales

Art. 36 Abrogation et modification d'autres actes

Pour maintenir un nombre raisonnable de contrôles, une discipline stricte s'impose dans l'élaboration et l'actualisation des listes des fonctions. Le DDPS, qui supporte les coûts des CSP, gérera donc ces listes de façon centralisée. En tant que porteurs des risques à proprement parler, les départements et la ChF demandent d'apporter les changements nécessaires à ces listes au fur et à mesure. Les ordonnances départementales correspondantes en vigueur jusqu'ici sont donc abrogées. Est également abrogée l'ordonnance en vigueur sur les contrôles de sécurité relatifs aux personnes, qui est entièrement revue par la présente ordonnance. L'ordonnance sur les contrôles de sécurité relatifs aux personnes dans le domaine des installations nucléaires est, elle aussi, abrogée car ses contenus, s'ils sont encore nécessaires, sont intégrés dans la présente ordonnance. Du fait de l'ampleur de la modification des autres actes, la réglementation sur ce sujet apparaît à l'annexe 8. L'explication correspondante suit plus bas.

Art. 37 Dispositions transitoires

Si des contrôles sont encore pendants à l'entrée en vigueur de l'ordonnance, les services spécialisés CSP doivent vérifier en collaboration avec les services qui demandent le contrôle si le contrôle doit encore être effectué et, le cas échéant, à quel degré de contrôle. Les contrôles qui ne sont plus effectués sont classés selon l'art. 17, al. 3. Les contrôles de sécurité élargis avec audition pratiqués jusqu'ici seront intégrés dans les contrôles de sécurité élargis. Ces contrôles seront marqués dans le SICSP afin qu'il soit visible qu'une audition a eu lieu.

Les déclarations sur les contrôles effectués jusqu'à présent ne connaissent pas de date d'expiration formelle ; le contrôle est simplement répété après un certain délai. La réglementation proposée offre une continuité tant aux services qui demandent le contrôle qu'aux services spécialisés CSP. Elle ménage par ailleurs une marge de manœuvre suffisante pour faire recontrôler en priorité les fonctions les plus critiques. Concernant les contrôles visés par la LApEl effectués jusqu'alors sur une base de droit privé, il faut en outre une réglementation spéciale qui permette de mettre un terme au contrat en cours de façon régulière.

Art. 38 Entrée en vigueur

La date d'entrée en vigueur a pour le moment valeur d'objectif. Elle dépendra pour beaucoup de la suite de la procédure législative et des délais pour la mise en œuvre technique des nouvelles réglementations dans le système d'information sur le CSP.

Annexes 1 à 6 Listes des fonctions

Pour protéger la sécurité intérieure et extérieure de la Suisse, les annexes 1, 4 et 6 ne seront pas publiées (cf. commentaire du chap. 2.5, let. e et de l'art. 5).

Annexe 7 Collecte et traitement des données

Un CSP implique naturellement de collecter et traiter des données très personnelles concernant le mode de vie de la personne soumise au contrôle, notamment sur ses relations personnelles étroites et ses relations familiales, sa situation financière et ses rapports avec l'étranger (cf. art. 27, al. 2, LSI). Sans ces données, il n'est pas possible d'évaluer de manière fiable les risques pour la sécurité. La LSI fixe les limites nécessaires au traitement de ces données, qui ne peuvent être collectées et traitées que si elles sont importantes pour la sécurité (cf. p. ex. art. 27, al. 2 et 3, et art. 34 LSI). Les données concernant l'exercice des droits constitutionnels ne peuvent par exemple être traitées qu'en cas de soupçons concrets indiquant que la personne soumise au contrôle exerce ces droits afin de préparer ou de faire des activités menaçant les intérêts publics visés à l'art. 1, al. 2, LSI (p. ex. la capacité de décision et d'action des autorités et des organisations de la Confédération ou la sécurité intérieure et extérieure de la Suisse). Ces données sont collectées et traitées en tenant compte des risques. Par exemple, il est peu judicieux de collecter des données fiscales des conscrits étant donné qu'ils n'ont pas encore remis de déclarations fiscales ou n'ont pas remis de déclarations fiscales pertinentes vu leur jeune âge. La collecte de données qui ne sont pas utiles pour évaluer les risques pour la sécurité génère un surplus de travail inutile pour les services spécialisés CSP. Ainsi, tant le droit que ces services veillent à ne collecter et traiter que les données nécessaires.

Concernant la collecte et le traitement de données à partir de sources d'information publiques (*open source information,* OSINF), il est clair qu'il ne s'agit jamais d'informations privées ou confidentielles. De ce fait, les enquêtes OSINF ne touchent ni à la sphère privée protégée par la Constitution ni au secret des télécommunications. Il ne s'agit pas non plus d'une mesure secrète de surveillance. En l'absence d'une prise de contact directe par l'enquêteur avec la personne ciblée, il n'y a pas non plus de recherches secrètes. Les enquêtes OSINF sont une méthode légitime de recherche et de traitement d'informations qui gagne en importance du fait de la progression de la numérisation.

Annexe 8 Abrogation et modification d'autres actes

1. OMAH

Une base légale est nécessaire pour que les services spécialisés puissent consulter les données d'Hoogan.

2. OPers

Art. 94e Extrait du casier judiciaire et du registre des poursuites

La possibilité qu'a un employeur de demander un extrait du casier judiciaire et du registre des poursuites n'est donnée que lorsque l'employeur peut se prévaloir d'un intérêt légitime au sens de l'al. 1. Cette mesure de l'art. 94*e* OPers doit être comprise comme le moyen, parmi les contrôles de sécurité, qui porte le moins atteinte aux droits de la personnalité des personnes contrôlées. Elle ne s'applique en principe que lorsque la fonction en question n'est pas couverte par les contrôles selon l'OCSP. Il est toutefois possible d'y faire recours lorsque le CSP a été effectué il y a longtemps déjà et que l'employeur a un soupçon fondé que la personne concernée présente un risque. On ne doit toutefois pas aboutir automatiquement à la demande d'extraits de registres pour toutes les fonctions non soumises à un autre contrôle. C'est seulement lorsqu'une fonction satisfait clairement aux conditions de l'al. 1 en raison de son cahier de charges que l'employeur est en droit d'exiger des extraits. Pour des raisons importantes – par exemple une mission concrète ou un mandat particulier –, un nouvel extrait peut être exigé déjà avant cinq ans. Il incombe à l'employeur de décider si une inscription sur les registres signifie un risque et, le cas échéant, quelles mesures en matière de droit du personnel doivent être prises.

Art. 94f Contrôle de loyauté

Les conditions de contrôle de la loyauté au sens de l'art. 20*b* LPers doivent être définies dans l'OPers. La procédure de contrôle doit cependant être intégralement contenue dans l'OCSP.

3. Ordonnance SNE

La LSI constitue une nouvelle base légale pour les services spécialisés impliquant la modification de l'ordonnance SNE.

4. ORMI

Le renvoi actuel à l'OCSP en vigueur doit être adapté à la nouvelle législation.

5. Ordonnance du 16 décembre 2009 sur les systèmes d'information de l'armée et du DDPS (OSIAr)[33]

L'art. 67 et l'annexe 30 de l'OSIAr doivent être abrogés du fait de la réglementation sur le Système d'information sur le contrôle de sécurité relatif aux personnes de la LSI et de la présente ordonnance. Par ailleurs, les renvois actuels à l'OCSP en vigueur doivent être adaptés à la nouvelle législation.

6. *Ordonnance du 22 novembre 2017 sur les obligations militaires*[34]

Les renvois actuels à l'OCSP en vigueur doivent être adaptés à la nouvelle législation.

7. *Ordonnance du 10 décembre 2004 sur l'énergie nucléaire (OENu)*[35]

Du fait de l'abrogation de l'ordonnance sur les contrôles de sécurité relatifs aux personnes dans le domaine des installations nucléaires et de l'intégration de celle-ci dans l'OCSP, l'OENu doit contenir un renvoi à l'OCSP de manière à ce que le lecteur intéressé puisse trouver plus facilement les dispositions correspondantes. En revanche, la prise en charge des coûts doit être traitée dans l'OENu.

[33] RS **510.911**
[34] RS **512.21**
[35] RS **732.11**

3.4 Ordonnance sur la procédure de sécurité relative aux entreprises (OPSEnt)

Notes introductives

Pour comprendre le sujet, il semble indiqué ici de donner au moins quelques brèves explications sur les dispositions suivantes de la LSI.

- La définition de *mandat sensible* est donnée à l'art. 5, let. b, LSI. De tels mandats incluent ainsi le traitement d'informations classifiées CONFIDENTIEL ou SECRET selon l'art. 13 LSI, l'administration, l'exploitation et le contrôle de moyens informatiques relevant des catégories de sécurité « protection élevée » ou « protection très élevée », conformément à l'art. 17 LSI, et l'accès à des zones de sécurité, en particulier à des zones de protection au sens de la législation sur la protection des ouvrages militaires. La forme juridique des mandats importe peu.
- La notion d'entreprise au sens de l'OPSEnt fait référence aux entreprises, aux parties d'entre elles ou aux sous-contractants qui exécutent des mandats publics qui impliquent l'exercice d'une activité sensible (cf. art. 49, LSI).
- On entend par adjudicateurs au sens de l'OPSEnt les autorités et les organisations visées à l'art. 2 LSI (cf. art. 50, al. 1, let. a, LSI).
- La réglementation de la procédure de sécurité relative aux entreprises s'applique parallèlement à celle des marchés publics. L'OPSEnt est élaborée en étroite collaboration avec les services d'achat centraux (Office fédéral des constructions et de la logistique, armasuisse) de manière à garantir que les procédures de sécurité relatives aux entreprises et d'acquisition sont coordonnées de façon optimale.

Préambule

La procédure de sécurité relative aux entreprises forme, au sein du chap. 4 de la LSI, un ensemble de règles fermé en soi qui constitue la base de la législation d'exécution en la matière. L'art. 84, al. 1, LSI contient la compétence fondamentale des autorités soumises à la LSI d'édicter les dispositions d'exécution de la LSI. L'art. 73 LSI attribue au Conseil fédéral les domaines à réglementer individuellement.

Section 1 Dispositions générales

Art. 1 Objet et champ d'application

Al. 1 – La disposition s'appuie sur les mandats législatifs imposés au Conseil fédéral par l'art. 73 LSI à propos de la description de la matière normative de l'OPSEnt.

Al. 2 et 3 – Dans la mesure où les autorités et les organisations sont concernées par le champ d'application de la LSI ou de l'OSI, elles entrent aussi en ligne de compte comme émettrices de mandats sensibles. Le champ d'application de l'OPSEnt doit donc correspondre à celui de la LSI et de l'OSI (cf. ch. 2.6, let. b). S'agissant de l'application aux autorités soumises à la LSI, voir le commentaire de l'art. 1 OCSP. Cette correspondance à la LSI et à l'OSI mentionnée à l'al. 2 doit se référer également à l'administration fédérale décentralisée. Le champ d'application de l'OPSEnt s'inspire de celui qui figure dans l'OSI concernant le même sujet.

Art. 2 Entreprises concernées

Al. 1 – L'attribution de mandats sensibles par des autorités et des organisations suisses à des entreprises ayant leur siège en Suisse déclenche l'exécution de la procédure de sécurité. Les sous-contractants qui ont leur siège en Suisse sont mis sur le même plan que ces entreprises. La notion d'entreprise est à comprendre au sens large. Ni la forme juridique ni la taille ne jouent un rôle. Seule la sensibilité du mandat et l'assujettissement de l'entreprise au droit suisse sont décisifs.

Des unités administratives décentralisées de l'administration fédérale et des organisations et personnes de droit public ou privé à qui sont confiées des tâches de la Confédération peuvent aussi être considérées comme des entreprises dans la mesure où elles ne relèvent pas du champ d'application de la LSI.

Al. 2 – L'OPSEnt porte sur des états de fait nationaux. L'exécution de la procédure de sécurité relative aux entreprises pour les entreprises ayant leur siège à l'étranger dépend des traités internationaux correspondants.

Art. 3 Autorité compétente

Al. 1 – L'art. 51, al. 2, LSI détermine déjà que le service spécialisé PSE est le service spécialisé chargé de mener la procédure de sécurité relative aux entreprises. La disposition de l'ordonnance ne fait que préciser que ce service sera rattaché au DDPS.

Al. 2 – Dans le cadre de procédures de sécurité transfrontalières, le service spécialisé PSE doit pouvoir collaborer avec l'autorité de sécurité suisse désignée ayant l'exclusivité de l'entretien des contacts avec l'étranger. La coordination de la procédure de sécurité relative aux entreprises avec les procédures de ladite autorité incombe au service spécialisé PSE.

Section 2 Ouverture de la procédure

Note introductive sur la section 2

La procédure doit être ouverte aussi tôt que possible au sein du processus d'acquisition. Dans cette première phase, il s'agit avant tout de clarifier si le mandat à confier est sensible et si la condition essentielle au processus est remplie. La procédure d'adjudication ne doit subir aucun préjudice.

La nouvelle procédure de sécurité relative aux entreprises remplace entièrement la méthode de gestion des risques visant à réduire les activités d'espionnage de services de renseignement.

Art. 4 Demande d'ouverture de la procédure

Al. 1 – Les préposés à la sécurité de l'information garantissent que les réflexions sur l'attribution du marché à des tiers intègrent de bonne heure les aspects relatifs à la sécurité de l'information.

Al. 2 – Concernant les autorités soumises à la LSI visées à l'art. 2, al. 1, LSI, aucune compétence n'est dévolue au Conseil fédéral (hormis pour lui-même) pour la définition des compétences sur l'ouverture de la procédure. Dans l'OPSEnt, il demande uniquement aux autorités soumises à la LSI d'indiquer qui est le service compétent.

Al. 3, let. a – La description aussi précise que possible des travaux de construction, de la livraison ou de la prestation sert notamment de critère d'identification au service spécialisé PSE quand une entreprise exécute plusieurs mandats sensibles.

Al. 3, let. b – Comme la sensibilité du mandat est la condition d'ouverture d'une procédure, une justification sommaire doit au moins indiquer dans quelle mesure les conditions de l'art. 5, let. b, LSI sont remplies.

Al. 3, let. c – La procédure de sécurité doit être coordonnée individuellement et de bonne heure avec les dispositions procédurales des marchés publics. L'économie de procédure y gagnera si l'adjudicateur peut se faire rapidement une représentation nette de la procédure d'adjudication applicable.

Art. 5 Examen de la demande

Al. 1 – Le service spécialisé PSE dispose, pour l'ouverture de la procédure, d'une marge d'appréciation assez importante qu'il doit cependant toujours exercer en accord avec l'adjudicateur, suisse ou étranger (cf. art. 53, al. 2, LSI).

Al. 2 – Par cette disposition, le Conseil fédéral restreint la marge d'appréciation du service spécialisé PSE et définit de façon exhaustive les faits qui doivent impérativement donner lieu à l'ouverture d'une procédure de sécurité. Il s'agit des quatre cas de figure ci-après.

- Let. a – Les entreprises qui travaillent dans le domaine des besoins de protection très élevés des informations et des moyens informatiques doivent toujours être contrôlées, quel que soit le type ou le lieu d'exécution du mandat.
- Let. b – Le Conseil fédéral définit ici que le traitement d'informations classifiées CONFIDENTIEL pour lesquelles l'intérêt au maintien du secret est réparti entre plusieurs autorités ou départements est, sans exception, un cas de procédure de sécurité relative aux entreprises.
- Let. c – Comme pour la let. b, l'exploitation, la maintenance ou le contrôle de moyens informatiques relevant de la catégorie de sécurité « protection élevée », lorsqu'ils sont répartis entre plusieurs autorités ou départements, doivent, sans exception, déclencher la procédure de sécurité.
- Let. d – Un certificat international de sécurité doit disposer d'une base solide pour laquelle seule la réalisation de la procédure d'après la LSI garantit la sécurité nécessaire et suffisante. Même si elle doit prendre en charge les coûts de la procédure, l'entreprise ne peut pas

simplement *acheter* de cette façon un label de qualité garanti par l'État. Le service spécialisé PSE n'entrera en matière sur la procédure qu'en présence d'une demande en ce sens d'une autorité étrangère ou d'une organisation internationale et d'un mandat effectivement sensible.

Al. 3 – Ce délai d'ordre doit donner aux adjudicateurs un point de repère pour la planification et la coordination de la procédure d'adjudication et engager le service spécialisé PSE à observer le principe de célérité.

Art. 6 Examen de la demande avec des autorités de sécurité étrangères

Al. 1 – Si l'adjudicateur envisage de confier un mandat sensible (cf. art. 49 LSI) à une entreprise étrangère qui ne relève donc pas du droit suisse, il soumettra la demande correspondante au service spécialisé PSE. Les étapes nécessaires de la procédure avec l'autorité de sécurité étrangère sont alors effectuées par le service spécialisé de la Confédération pour la sécurité de l'information (cf. art. 83 LSI).

Al. 2 – En présence d'un traité international correspondant (cf. art. 87 LSI), l'autorité de sécurité étrangère, à la demande du service spécialisé de la Confédération pour la sécurité de l'information, soit confirmera que l'entreprise dispose d'une déclaration de sécurité, soit ouvrira la procédure de sécurité. Cette procédure relève entièrement du droit de l'État où l'entreprise a son siège, tout comme la déclaration de sécurité correspondante.

Art. 7 Définition des exigences en matière de sécurité

Al. 1 – L'OSI et l'OCSP sont les deux actes déterminants nommés à prendre en compte au cas par cas dans la définition des exigences en matière de sécurité.

Al. 2 – Dans les rapports internationaux, le traité international a la priorité sur l'OSI et l'OCSP.

Al. 3 – L'adjudicateur et le service spécialisé PSE peuvent s'accorder sur l'ouverture de la procédure, sous réserve de l'art. 6, al. 2. De même, après l'ouverture, tous deux doivent pouvoir s'entendre sur une répartition des tâches tant dans la procédure d'adjudication que pour la réalisation du mandat. Cette procédure pourrait être judicieuse là où des mesures de contrôle étendues ou durables sont indiquées après établissement de la déclaration de sécurité pendant la durée de celle-ci. Il est de l'intérêt direct de l'adjudicateur (maître du secret) de pouvoir effectuer des contrôles indépendamment du service spécialisé PSE. Les mesures de contrainte des autorités ne peuvent pas être déléguées à l'adjudicateur.

Al. 4 – Entre la procédure d'adjudication et la procédure de sécurité, la première reste toujours la procédure directrice. En tant qu'instrument de la sécurité de l'information, la procédure de sécurité suit toujours les déroulements de la procédure d'adjudication. Pour cette dernière, les étapes de la procédure de sécurité doivent être intégrées dans le plan de la procédure. Les tâches de coordination incombent par conséquent à la principale partie intéressée de la procédure directrice, à savoir l'adjudicateur.

Section 3 Évaluation des entreprises

Art. 8 Indication des entreprises qualifiées

Al. 1 – Avec l'examen de la qualification, le service spécialisé PSE s'occupe d'actes administratifs largement plus complexes et plus approfondis que l'examen sur la simple ouverture de la procédure. Pour des raisons juridiques et économiques, il est indispensable, à ce stade de la procédure, que seules les entreprises toujours en lice pour l'adjudication du point de vue de l'adjudicateur soient soumises à ces examens. Par principe, il ne faut pas présenter au service spécialisé PSE plus de cinq entreprises pour l'examen de la qualification. Ce nombre peut être augmenté, mais uniquement dans des cas justifiés. Cette clause d'exception vise à offrir une issue lors d'évolutions non prévues dans la procédure d'adjudication et permettre des annonces tardives.

Al. 2 – Le consentement de l'entreprise à la réalisation de la procédure est la condition d'ouverture (cf. art. 50, al. 2, LSI) et doit donc être examiné d'office par le service spécialisé PSE. Ce consentement peut être explicite ou résulter des conditions de participation précisées dans les dossiers d'appel d'offres et acceptées par l'entreprise.

Al. 3 – Par analogie avec l'art. 5, al. 3, ce délai d'ordre doit donner aux adjudicateurs un point de repère pour la planification et la coordination de la procédure d'adjudication et engager le service spécialisé PSE à observer le principe de célérité.

Art. 9 Collecte des données

Al. 1, let. a à g – Ces dispositions concrétisent l'art. 56 LSI et énumèrent de façon non exhaustive les points qui paraissent appropriés pour évaluer, sur le plan de la sécurité, une entreprise quant à sa loyauté et à ses relations avec des États et des organisations étrangères. Le service spécialisé PSE s'occupe de collecter les données. Conformément à l'art. 56, al. 1, let. a, LSI, le service spécialisé PSE peut collecter les données directement auprès des entreprises afin d'évaluer leur qualification. Tout manque de volonté en ce sens de leur part est assimilé à un refus de la procédure. La procédure est donc arrêtée pour l'entreprise correspondante, les conditions au processus n'étant pas réunies.

Contrairement au refus de fournir des renseignements, les données erronées ne constituent pas un empêchement de procéder, mais le fait doit être pris en compte dans les réflexions pour évaluer la loyauté. Généralement, l'entreprise est alors classée dans la catégorie des risques pour la sécurité.

Al. 2 – La collecte des données visée à l'art. 6, al. 1, let. a, de la loi fédérale du 25 septembre 2015 sur le renseignement (LRens)[36] est de la compétence du SRC. Il est ici examiné si l'entreprise est apparue en lien avec le terrorisme, l'espionnage, la prolifération, des attaques visant des infrastructures critiques ou l'extrémisme violent. Le SRC s'occupe de collecter les données.

Art. 10 Exclusion de la procédure

Al. 1 – Tant l'art. 44 de la loi fédérale du 21 juin 2019 sur les marchés publics (LMP)[37] que l'art. 57 LSI énumèrent différents faits en présence desquels l'adjudicateur peut ou doit exclure une entreprise de la procédure d'adjudication. Pour que cette procédure et celle de sécurité ne se bloquent pas inutilement, le fait que seuls existent des indices laissant supposer la présence de motifs d'exclusion d'après l'art. 44 LMP ne doit pas empêcher l'adjudicateur de signaler au service spécialisé PSE une telle entreprise pour la réalisation de l'examen de la qualification, avant d'avoir à se prononcer sur une exclusion. Il doit toutefois communiquer ses informations sur le sujet au service spécialisé PSE aux fins de l'examen de la qualification. Par ailleurs, le service spécialisé PSE doit aussi informer le plus rapidement possible l'adjudicateur si, compte tenu des données collectées, des informations apparaissent qui peuvent inciter l'adjudicateur à exclure l'entreprise.

Al. 2 – Cet échange continu d'informations justifie que le service spécialisé PSE contrôle dans un premier temps la qualification d'une entreprise douteuse avant que l'adjudicateur décide d'une éventuelle exclusion.

Al. 3 – Si, au cours de la procédure d'adjudication, l'adjudicateur exclut une entreprise, la procédure de sécurité devient sans objet. Le cas s'inscrit alors clairement dans le cadre de l'art. 51, al. 1, let. c, LSI et la procédure de sécurité doit être tout simplement arrêtée pour l'entreprise concernée.

Art. 11 Échange d'informations

Cette disposition s'exprime sur le contenu de l'échange mutuel d'informations. Il est précisé qu'il faut mettre à la disposition du service spécialisé PSE pour l'examen de la qualification des informations utiles relatives au droit des marchés publics et, à celle de l'adjudicateur, des informations sur la sécurité qui lui serviront pour sa décision d'exclusion selon l'art. 44 LMP.

Section 4 Plan de sécurité

Art. 12 Contenu et contrôle du plan de sécurité

Al. 1 – Le service spécialisé PSE donne à l'entreprise un cadre pour élaborer le plan de sécurité, dans lequel elle doit prendre et documenter les mesures de sécurité adaptées à la situation. Il y a lieu de documenter les mesures organisationnelles (gestion des clés, surveillance des locaux), personnelles (instruction, contrôles de sécurité relatifs aux personnes), techniques (utilisation des moyens informatiques) et physiques (protection contre les effractions). Les risques constatés dans le cadre du contrôle de la qualification visé aux art. 55 à 58 LSI qui ne peuvent être suffisamment réduits par des mesures organisationnelles sont intégrés dans le plan de sécurité.

Al. 2 – Le contrôle mené sur place garantit que les mesures du plan de sécurité nécessaires, appropriées et adaptées à la situation globale peuvent être imposées à l'entreprise de façon

[36] RS **121**
[37] RS **172.056.1**

ciblée. Il favorise la sécurité de l'information tout en épargnant à l'entreprise une charge de travail disproportionnée.

Al. 3 – L'élaboration de plans de sécurité peut s'avérer complexe, notamment parce qu'une certaine marge d'appréciation doit être accordée à l'entreprise. Si le plan de sécurité proposé ne passe pas d'emblée le contrôle du service spécialisé PSE (cf. art. 59, al. 2, LSI), ce dernier doit accorder à l'entreprise un délai supplémentaire pour l'améliorer et donner des consignes concrètes sur ce qui doit être amélioré et comment.

Al. 4 – Par analogie avec l'art. 5, al. 3, ce délai d'ordre doit donner aux adjudicateurs un point de repère pour la planification et la coordination de la procédure d'adjudication et engager le service spécialisé PSE à observer le principe de célérité.

Art. 13 Préposé à la sécurité de l'entreprise

Al. 1 – Une entreprise pour laquelle l'adjudicateur a demandé un examen de la qualification doit nommer un préposé à la sécurité qu'elle déclarera au service spécialisé PSE. Pour que les exigences définies en matière de sécurité puissent avoir l'effet nécessaire, il faut que la direction de l'entreprise soit associée à la responsabilité à ce sujet. Les préposés doivent donc disposer de certains droits de donner des instructions au sein de l'entreprise, au moins dans le domaine de la sécurité. Idéalement, ils sont eux-mêmes membres de la direction et peuvent ainsi influer sur les décisions ou alors ils agissent au moins sur son mandat direct.

Al. 2, let. a – Pour pouvoir influer efficacement sur la sécurité de l'information de l'entreprise, le service spécialisé PSE a besoin d'un interlocuteur par lequel passent tous les contacts.

Al. 2, let. b – Le préposé à la sécurité doit rendre des comptes au service spécialisé PSE sur la mise en œuvre du plan de sécurité. Le service spécialisé PSE veille à ce que les préposés reçoivent une formation initiale et continue appropriée.

Al. 2, let. c – Dans les cas où l'entreprise a été autorisée par l'adjudicateur à faire appel à des sous-contractants, le préposé à la sécurité a la légitimité de déposer la demande d'ouverture de la procédure de sécurité pour le sous-contractant auprès du service spécialisé PSE (cf. art. 4, al. 1, let. c).

Art. 14 Communication de l'adjudication

Al. 1 – Les contrats-cadres sont en général l'élément qui déclenche l'établissement d'une déclaration de sécurité. En revanche, les spécificités d'un mandat associées au contrat-cadre peuvent parfois tant influer sur le risque pour la sécurité de l'information qu'il devient nécessaire d'ajuster le plan de sécurité. Il est dès lors décisif que le service spécialisé PSE soit toujours mis au courant de la situation de l'entreprise en matière de mandats sensibles.

Al. 2 – Les informations que doit fournir l'adjudicateur pour l'élaboration du plan de sécurité comprennent notamment :

- des indications sur le niveau de sensibilité du mandat selon l'art. 5, let. b, LSI ;
- le nom des personnes à qui est confiée l'exécution du mandat sensible (pour effectuer les contrôles de sécurité relatifs aux personnes) ;
- des indications sur l'utilisation des moyens informatiques de l'entreprise, notamment si ceux-ci fonctionnent en réseau ou isolément.

Art. 15 Contrôles de sécurité relatifs aux personnes

Al. 1 – L'entreprise doit s'organiser pour l'exécution d'un mandat sensible de façon à ce que seul un nombre minimal de personnes absolument nécessaires à l'accomplissement du mandat soient soumises à un CSP. Les demandes de contrôle pour des personnes qui n'exercent que des activités potentiellement sensibles sont illicites et seront rejetées par le service spécialisé PSE.

Al. 2 – Pour des raisons économiques, il peut être judicieux d'autoriser les grandes entreprises à engager elles-mêmes des CSP. Ceci ne change rien au fait que le service spécialisé PSE définira en définitive qui sera vraiment contrôlé.

Section 5 Déclaration de sécurité relative aux entreprises et répétition de la procédure

Art. 16 Établissement de la déclaration de sécurité relative aux entreprises

La possibilité de limiter la déclaration de sécurité relative aux entreprises à quelques éléments d'activités sensibles au sens de l'art. 5, let. b, LSI n'est pas prévue par la loi, mais est compatible avec les objectifs de la LSI, voire dicté par le principe de proportionnalité. D'une part, il est clair que l'on ne peut pas, par exemple, imposer à une entreprise des mesures de protection aussi étendues pour le traitement d'informations classifiées CONFIDENTIEL que pour le traitement d'informations classifiées SECRET. D'autre part, il faut impérativement adapter un plan de sécurité axé sur CONFIDENTIEL si des informations classifiées SECRET sont nouvellement concernées. La sécurité du droit doit être établie par décision sur le niveau de traitement autorisé.

Art. 17 Information de la part de l'entreprise

Al. 1 et 2 – Ces listes non exhaustives concrétisent l'art. 63, al. 2, LSI sur le contenu de l'obligation d'annoncer des changements affectant la sécurité au sein de l'entreprise.

Al. 3 – Les changements et les incidents peuvent non seulement toucher l'entreprise, mais aussi les sous-contractants ou les fournisseurs. Tandis que les sous-contractants agréés sont soumis à l'obligation primaire d'annoncer conformément aux al. 1 et 2, cela n'est pas le cas des fournisseurs, qui ne sont qu'indirectement en contact avec l'activité sensible. L'entreprise doit également annoncer si ces derniers sont concernés par un incident pouvant avoir des répercussions sur l'activité sensible.

Al. 4 – Cette disposition vise à éviter qu'une déclaration de sécurité relative aux entreprises arrive à échéance durant un mandat en cours et que le rapport contractuel devienne alors subitement illicite et doive donner lieu à une rédhibition. La situation peut être gérée en demandant à temps un renouvellement de la déclaration de sécurité (cf. aussi commentaire de l'art. 20, al. 2).

Art. 18 Devoirs de l'adjudicateur

Al. 1 – Les adjudicateurs sont fréquemment en contact étroit avec les entreprises, si bien qu'il est très probable qu'ils remarquent d'éventuels faits répréhensibles. L'obligation d'annoncer de l'entreprise est donc étendue à l'adjudicateur pour les changements ou incidents touchant la sécurité, dans la mesure où il fait de pareils constats dans l'entreprise. La prise de mesures immédiates incombe également à l'adjudicateur.

Al. 2, let. a – Les faits visés à l'art. 44 LMP peuvent avoir un impact négatif sur la mise en œuvre du plan de sécurité et doivent donc, selon les circonstances, être appréciés sous l'angle de la sécurité de l'information. L'adjudicateur doit donc signaler au service spécialisé PSE quand il fait pareils constats. Cette obligation d'annoncer s'applique aussi quand l'adjudicateur ne prévoit pas de révoquer l'adjudication.

A. 2, let. b – Les changements impactant la sécurité apportés au mandat ont souvent des répercussions sur le plan de sécurité, d'où la nécessité de tenir le service spécialisé PSE au courant.

Al. 2, let. c – Ce qui vaut pour le changement d'un mandat s'applique par analogie à l'octroi d'un nouveau mandat. Voir le commentaire de la let. b ci-avant.

Art. 19 Certificat international de sécurité

Al. 1 – L'établissement d'un certificat international de sécurité est un acte administratif sans spécificités ni charges significatives, c'est pourquoi un émolument forfaitaire de 100 francs est prélevé.

Al. 2 – Il en va autrement lorsque l'entreprise ne dispose pas encore de déclaration de sécurité suisse. La réalisation nécessaire au préalable de la procédure de sécurité relative aux entreprises représente une charge qui doit être facturée selon le temps consacré. Le taux horaire varie selon l'urgence et la qualification exigée du personnel exécutant.

Al. 3 – L'établissement d'un certificat international de sécurité est un acte administratif entre le service spécialisé PSE et l'entreprise. Souvent, l'autorité de sécurité étrangère s'adressera cependant à son homologue suisse pour faire vérifier la validité des certificats qui lui ont été présentés. Il est donc judicieux que le service spécialisé PSE communique ou fasse communiquer sur demande à l'autorité de sécurité étrangère l'établissement d'un certificat international

correspondant par l'intermédiaire du service spécialisé de la Confédération pour la sécurité de l'information.

Art. 20 Révocation de la déclaration de sécurité et retrait du mandat

Al. 1 – Si la sécurité de l'information n'est pas gravement menacée, il faut commencer par accorder à l'entreprise la possibilité de corriger les irrégularités constatées en suivant le principe de proportionnalité. Comme l'adjudicateur jouit exceptionnellement des droits d'une partie habilitée à recourir, il doit être entendu avant que soient rendues les décisions concernant la procédure.

Al. 2 – Dans les rares cas de révocation de la déclaration de sécurité, il faut garder à l'esprit que deux autres éléments contestables sur le plan juridique sont alors déclenchés : l'adjudicateur doit révoquer l'adjudication (décision) et la résiliation d'un contrat de droit privé s'ensuit. Pour garantir la sécurité de l'information, le service spécialisé PSE retirera généralement à titre préventif l'effet suspensif d'un recours contre la révocation d'une déclaration de sécurité en se fondant sur l'art. 55, al. 2, de la loi fédérale du 20 décembre 1968 sur la procédure administrative[38]. La décision peut ainsi être exécutée sans délai. Dans la mesure où il n'en appelle pas à la clause d'exception de l'art. 58, al. 3, LSI, l'adjudicateur doit retirer le mandat sensible et garantir que l'entreprise ne dispose plus d'aucune possibilité de porter préjudice à la sécurité de l'information. Si la révocation de la déclaration de sécurité est contestée, cela s'appliquera aussi à la révocation de l'adjudication. Force est de supposer que le Tribunal administratif fédéral réunira les deux procédures de recours. À la demande d'une partie, les demandes de droit civil peuvent aussi être examinées dans la même procédure (cf. art. 40, al. 1, de la loi du 17 juin 2005 sur le Tribunal administratif fédéral[39]).

Al. 3 – Ce délai d'ordre vise à permettre au service spécialisé PSE d'obtenir dans un délai raisonnable des informations claires sur l'élimination d'un risque pour la sécurité et de décider si sa propre intervention relevant de la puissance publique est encore nécessaire.

Art. 21 Répétition de la procédure

Al. 1 – La présente disposition attribue au service spécialisé PSE la compétence d'ouvrir la procédure de répétition. Elle intervient d'office. Contrairement à la procédure simplifiée (cf. art. 65 LSI), l'ensemble de la procédure (y c. l'examen de la qualification) est opéré dans ce cas.

Al. 2 – Cette disposition a pour but d'empêcher l'interruption et la rédhibition de mandats en cours lorsque la procédure de répétition se prolonge au-delà de la date d'expiration de la déclaration de sécurité. L'acte formel enregistré au dossier d'ouverture de la procédure par le service spécialisé PSE doit suffire à prolonger jusqu'à la nouvelle décision la durée de validité de la déclaration arrivant à échéance.

Al. 3 – Dans le cadre de la répétition de la procédure, le service spécialisé PSE peut conclure que les conditions nécessaires au renouvellement d'une déclaration de sécurité ne sont pas réunies ou que la procédure doit être classée pour d'autres raisons. Il s'agit de décisions qui, toutes, mettent un terme au prolongement de la durée de validité visé à l'al. 2. La rédhibition des rapports juridiques suit les règles applicables en cas de révocation de la déclaration de sécurité (cf. art. 20).

Section 6 Traitement des données personnelles

Art. 22 Système d'information sur la procédure de sécurité relative aux entreprises

Les données personnelles et des entreprises pour la procédure de sécurité relative aux entreprises doivent être définies au niveau de l'ordonnance. La liste se trouve dans l'annexe de l'OPSEnt.

Art. 23 Contrôle périodique du traitement des données personnelles

Le système d'information visé à l'art. 70, al. 1, LSI, qui est utilisé pour la procédure de sécurité relative aux entreprises, peut, selon les circonstances, contenir des données sensibles. Il convient donc de le soumettre à un organe de surveillance indépendant. Le DDPS dispose d'un certain pouvoir d'appréciation quant au choix de l'organe de révision.

[38] RS **172.021**
[39] RS **173.32**

Section 7 Prestations du service spécialisé PSE en faveur des cantons

Art. 24

Conformément à l'art. 86, al. 4, LSI, moyennant un émolument, les cantons peuvent recourir aux prestations des services spécialisés visés par la LSI afin d'assurer leur propre sécurité de l'information, dans la mesure où le Conseil fédéral le définit. Selon la Confédération, il n'est pas pertinent de procéder à une vérification complète et à un contrôle permanent des entreprises recevant des mandats cantonaux. Elle n'estime pas nécessaire d'établir une déclaration de sécurité pour ces entreprises. En revanche, il peut être utile de vérifier la loyauté des entreprises en collaboration avec le SRC. Les cantons doivent en avoir la possibilité pour autant qu'ils possèdent une base légale formelle à ce sujet et qu'ils aient conclu avec le DDPS une convention de prestations réglant le financement des prestations et ses modalités.

Section 8 Dispositions finales

Art. 25 Abrogation et modification d'autres actes

Voir le commentaire de l'annexe 2 plus bas.

Art. 26 Dispositions transitoires

Une rétroactivité sur des mandats qui ont été attribués avant l'entrée en vigueur de l'OPSEnt pourrait modifier les conditions de l'appel d'offres et de l'adjudication du mandat, ce qui pourrait entraîner au final sa révocation, voire une nouvelle attribution. Cette insécurité juridique ne se justifie pas ; il faut dès lors s'en tenir à l'adéquation relative au droit des marchés publics dans pareils cas. Pour les rares cas où des procédures de sauvegarde du secret du DDPS sont en cours au moment de l'entrée en vigueur, il existe déjà des consignes de sécurité sur ce thème sur le plan matériel et il convient donc, pour des raisons économiques, de renoncer aux nouvelles étapes de procédure définies dans l'OPSEnt. Les déclarations relatives à la sécurité des entreprises rendues selon l'ancien droit restent valables cinq ans à compter de leur établissement (cf. art. 90, al. 3, LSI).

Art. 27 Entrée en vigueur

L'entrée en vigueur sera coordonnée avec celle de l'OSI et de l'OCSP.

Annexe 1

L'annexe comporte les données du Système d'information sur la procédure de sécurité relative aux entreprises qui ont été retirées de l'OSIAr, conformément à l'art. 25, al. 5, OPSEnt.

Annexe 2

I : Abrogation d'autres actes

La procédure de sauvegarde du secret uniquement applicable au sein du DDPS était réglée par l'ordonnance du 29 août 1990 concernant la sauvegarde du secret. La procédure de sécurité relative aux entreprises désormais applicable à l'échelle fédérale couvre la matière normative de l'ordonnance concernant la sauvegarde du secret, qui est donc abrogée sans être remplacée.

II : Modification d'autres actes

1. Ordonnance du 16 août 2017 sur le renseignement (ORens)[40]

L'art. 56 LSI mentionne expressément le SRC comme source d'information du service spécialisé PSE. L'art. 60 LRens précise que le SRC communique des données personnelles à des autorités nationales lorsque ceci est nécessaire pour garantir la sûreté intérieure et extérieure. Le Conseil fédéral spécifie les autorités concernées. Il le fait dans l'annexe 3 de l'ORens, qui ne mentionne pas encore le service spécialisé PSE. Le ch. 10.6 y remédie.

2. ORMI

L'ORMI renvoie à l'ordonnance du 29 août 1990 concernant la sauvegarde du secret à abroger, ce qui doit être rectifié.

3. OSIAr

[40] RS **121.1**

Les données citées dans l’OSIAr figureront dans l’annexe de l’OPSEnt si bien qu’il est possible de procéder aux suppressions requises.