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

Le 24 août 2022

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

Rapport explicatif

Référence : SG-DDPS-251.2-35/1/6/8

Condensé

Le 18 décembre 2020, l'Assemblée fédérale a adopté la loi sur la sécurité de l'information (LSI). Cette loi crée une base légale uniforme pour la sécurité de l'information au sein de la Confédération.

La présente législation d'exécution de la LSI a été élaborée avec des représentants des autres autorités fédérales et des cantons. Dans le message du 22 février 2017 concernant la loi sur la sécurité de l'information, le Conseil fédéral a annoncé qu'il consulterait les autres autorités fédérales et les cantons à propos de toutes les dispositions importantes. Cette procédure doit permettre 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, d'où son lancement.

Le droit d'exécution relatif à la LSI se compose de trois nouvelles ordonnances et de la modification d'une ordonnance en cours.

- Ordonnance sur la sécurité de l'information (OSI) : 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 de l'administration fédérale et de l'armée ; elle précise les tâches, compétences et responsabilités correspondantes ; le principal changement est l'introduction d'un système de management de la sécurité de l'information dans toutes les unités administratives.
- Ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP [nouvelle]) : elle compile les dispositions d'exécution sur les différents contrôles de sécurité relatifs aux personnes ; ces contrôles sont limités au strict minimum nécessaire à l'identification de risques considérables pour la Confédération et seront donc moins nombreux à l'avenir.
- Ordonnance sur la procédure de sécurité relative aux entreprises (OPSE) : elle régit les détails de la procédure de sécurité relative aux entreprises introduite par la LSI ; cette procédure s'applique à tous les mandats sensibles que la Confédération attribue.
- Ordonnance du 19 octobre 2016 sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération (OIAM) : la révision partielle de cette ordonnance élargit le champ d'application de l'ordonnance à toutes les unités administratives de l'administration fédérale décentralisée et apporte quelques modifications formelles et techniques.

L'entrée en vigueur de la LSI et des dispositions d'exécution est prévue à l'été 2023.

Table des matières

Rapport explicatif

1 Contexte

Le 18 décembre 2020, l'Assemblée fédérale a adopté la 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 englobe toutes les procédures de traitement, documents papier et déclarations orales compris, et ne se limite pas uniquement au traitement électronique. Dans le langage courant, les deux notions sont souvent utilisées comme synonyme.

La présente législation d'exécution de la LSI a été élaborée avec des représentants des autres autorités fédérales 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 et les cantons à propos de toutes les dispositions importantes (Cf. ch. 1.5, p. 2820). Cette consultation doit permettre 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.

2 Comparaison avec le droit étranger, notamment européen

Dans de nombreux pays européens, les bases légales de la sécurité de l'information sont adaptées aux nouvelles réalités de la société de l'information. En raison des ordres juridiques et des structures des États pour partie très hétérogènes, la hiérarchie normative des réglementations en question et leur champ d'application ne peuvent que difficilement être comparés. En revanche, on peut affirmer que les dispositions de la LSI et de sa législation d'exécution correspondent globalement aux réglementations des divers États analysés ou qu'elles sont pour le moins coordonnées avec elles. Sur le plan organisationnel, grâce au service spécialisé de la Confédération pour la sécurité de l'information, la Confédération dispose d'un interlocuteur unique au niveau international. La coopération dans ce domaine devrait s'en trouver simplifiée et gagner en efficacité.

3 Présentation du projet

3.1 Législation d'exécution relative à la LSI

Le droit d'exécution relatif à la LSI se compose de quatre ordonnances :

- L'ordonnance sur la sécurité de l'information (OSI, ch. 3.3);
- une modification de l'ordonnance du 19 octobre 2016 sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération[3] (OIAM, ch. 3.4) ;
- l'ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP, cf. ch. 3.5) ;
- l'ordonnance sur la procédure de sécurité relative aux entreprises (OPSE, ch. 3.6).

Le 12 janvier 2022, le Conseil fédéral a ouvert la procédure de consultation sur le projet d'une obligation de signaler les cyberattaques contre les infrastructures critiques. L'introduction d'une telle obligation de signalement entraîne la révision complète du chap. 5 de la LSI. Cette révision de la LSI et de son ordonnance doit entrer en vigueur à la fin 2023. Il n'est donc pas judicieux d'adopter une nouvelle ordonnance pour couvrir les besoins actuels, dès lors qu'il faudra la revoir intégralement au cours des prochains mois. D'où l'abandon temporaire de l'idée d'édicter des dispositions d'exécution concernant le chap. 5.

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

3.2 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 solutions du Conseil fédéral n'ont pas perdu en actualité. Ils fournissent la base conceptuelle du droit d'exécution relatif à la LSI. Il en va de même pour l'appréciation de la menace, la direction stratégique de la Suisse et les principes d'action que le Conseil fédéral a définis le 18 avril 2018 dans la Stratégie nationale de protection de la Suisse contre les cyberrisques 2018 à 2022. Pour 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 à 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 unités administratives sont responsables de l'exécution des tâches qui leur sont déléguées, de même que de la protection de leurs 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 rendus disponibles pour un usage partagé sur le principe *once only*. De ce fait, des menaces et 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

Obtenir une sécurité absolue relève de l'impossible. Les risques sont inévitables. Les mesures applicables à la protection de base de la Confédération 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 gérer activement les risques pour 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. Un niveau de sécurité approprié pourra ainsi être obtenu. Avec telle une approche fondée sur les risques, l'accent peut être mis tant sur les risques que sur les possibilités, les nouvelles idées, les applications ou les 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 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, concepts ou 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 définir en premier lieu les principes, tâches, compétences et responsabilités à leur niveau. Quant aux consignes liées aux technologies, elles doivent être définies au niveau des directives et des normes techniques.

e. Permettre la digitalisation

Les besoins en 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.

[4] RS **172.010.59**

[4] RS **172.010**

3.3 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 administratives 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 l'OSI que si leurs activités sont sensibles pour la sécurité ou peuvent représenter un risque considérable pour l'administration fédérale centralisée. Ces conditions sont remplies lorsque les unités décentralisées ont accès aux moyens informatiques de l'administration fédérale centralisée des catégories de sécurité « protection élevée » ou « protection très élevée », lorsqu'elles exploitent elles-mêmes de tels moyens informatiques ou lorsqu'elles traitent des informations classifiées de la Confédération. La ChF et les départements peuvent en outre proposer au Conseil fédéral d'assujettir d'autres unités décentralisées. Les organisations chargées de tâches administratives, mais n'appartenant pas à l'administration fédérale au sens de l'art. 2, al. 4, LOGA, sont totalement exclues du champ d'application de la LSI et donc de l'OSI. Elles sont considérées comme des tiers.

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, les dispositions de la LSI et de l'OSI relatives aux informations classifiées sont applicables. Il en va de même des dispositions sur la sécurité informatique si les cantons accèdent aux moyens informatiques de la Confédération. En pratique, les cantons seront comme aujourd'hui 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, les cantons peuvent s'affranchir des dispositions légales de la Confédération s'ils garantissent 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 normes fédérales déterminantes sont les prescriptions et exigences techniques pour la protection de base de l'informatique au sein de la Confédération et pour la protection des informations classifiées. 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 unités administratives sont tenues de sécuriser l'information au moyen d'un système de management de la sécurité de l'information approprié (SMSI). Un SMSI est un instrument de conduite servant à planifier, mettre en œuvre, vérifier et améliorer systématiquement la sécurité de l'information. Il englobe les prescriptions et procédures nécessaires et indique à qui sont dévolues, au sein de l'organisation, telles ou telles tâches, compétences et responsabilités. Cette abréviation renvoie implicitement à la norme ISO/IEC 27001 qui tend à se généraliser tant dans l'économie privée que dans les administrations publiques. Plusieurs unités administratives et départements ont déjà décidé d'appliquer systématiquement la norme ISO à leur processus visant à sécuriser l'information. Certaines ont reçu une certification formelle. L'OSI n'exige qu'un SMSI *light* des unités administratives : en d'autres termes, elles peuvent appliquer uniquement les principaux processus de gestion et non la norme ISO dans son intégralité. Ces processus principaux sont réglés dans l'SI. Une certification externe n'est pas exigée. Les unités administratives et les départements peuvent toutefois définir un niveau d'ambition supérieur.

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

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. Ces critères sont forcément imprécis et nécessitent une interprétation. Des outils seront créés pour leur application. La Confédération va réduire la quantité d'informations classifiées.

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 sur les exigences techniques actuellement manquantes sur le traitement électronique des informations classifiées, seront rédigées probablement d'ici fin 2023 et harmonisées avec les normes internationales dès lors que cela s'avère possible et judicieux.

f. Accréditation de sécurité des moyens informatiques

L'OSI introduit une obligation d'accréditation pour un nombre limité de systèmes d'information sensibles au sein desquels des informations classifiées CONFIDENTIEL ou SECRET sont traitées (p. ex. une application pour la communication vidéo confidentielle). L'OSI comble ainsi une lacune qui complique aujourd'hui la collaboration internationale dans le domaine de la sécurité. Une accréditation 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. Si l'accréditation de sécurité ne peut pas être accordée, le Conseil fédéral doit évaluer les risques résiduels et décider de l'utilisation des moyens informatiques.

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. 20a de la loi fédérale sur le personnel de la Confédération du 24 mars 2000[8] (LPers), introduit par la LSI, permet aux unités administratives d'exiger des candidats à un poste et de ses 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 correspondants 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 des faits de leur environnement privé et professionnel qui pourraient menacer la sécurité (p. ex. un chantage suite à de lourdes dettes dues à des jeux de hasard). Le traitement d'un risque potentiellement élevé ressort de la compétence de l'employeur. Celui-ci peut exiger des collaborateurs concernés les extraits visés à l'art. 20a 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 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). Les responsables de la sécurité 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. L'OSI fusionne les rôles actuels de *délégué à la sécurité informatique* et de *préposé à la protection des informations* dans 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 et 41–42 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 les chefs de département n'en décident pas autrement. Les préposés à la sécurité de l'information continuent d'assumer la coordination et la surveillance opérationnelles (art. 81 LSI).

[8] RS **172.220.1**

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

L'art. 83 LSI crée un service spécialisé de la Confédération pour la sécurité de l'information. L'OSI précise ses tâches pour le domaine de compétence du Conseil fédéral. Le service spécialisé émettra, sur la base de l'art. 85 LSI, 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. Sur le plan international, il jouera le rôle d'autorité nationale pour la sécurité[9].

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

Les art. 24 à 26 LSI ont créé la base légale formelle nécessaire au traitement des données sensibles et des profils de la personnalité dans les systèmes de gestion des données d'identification de la Confédération. La présente modification de l'OIAM est essentiellement d'ordre formel et technique. Le champ d'application de cette ordonnance est toutefois étendu aux unités de l'administration fédérale décentralisée.

3.5 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)[10]. 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 doit également servir à restreindre au strict minimum le recours aux CSP nécessaires à l'identification de risques considérables pour la Confédération. Une réduction d'au moins 30 % est ciblée, de sorte que les CSP puissent être effectués en temps utile avec les ressources actuelles. 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 relatifs aux personnes dans un seul acte. Elle remplace l'ordonnance du 4 mars 2011 sur les contrôles de sécurité relatifs aux personnes (OCSP)[11], l'ordonnance du 9 juin 2006 sur les contrôles de sécurité relatifs aux personnes dans le domaine des installations nucléaires (OCSPN)[12] ainsi que toutes les ordonnances départementales sur les contrôles de sécurité relatifs aux personnes[13].

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

c. 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 afin de contrôler la loyauté des membres de leur personnel. L'art. 20*a* LPers propose aux employeurs des moyens correspondants.

d. 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

[9] Cf. message LSI, ch. 5.2 et art. 41, al. 3, OSI.
[10] RS **120**
[11] RS **120.4**
[12] RS **732.143.3**
[13] RS **120.421**–**120.427**

contenant lesdites fonctions. Le DDPS doit gérer ces listes de façon centralisée et les actualiser régulièrement sur demande des départements et de la Chancellerie fédérale (ChF).

Les listes de 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, grâce aux réseaux sociaux, chose facile pour un attaquant potentiel de faire le lien entre une identité et une fonction et ainsi d'acquérir une cible pour des actions d'espionnage ou de sabotage. Dans le domaine militaire, les listes de fonctions détaillées permettent de tirer des conclusions sur les détails non publiés de l'organisation de l'armée. Par conséquent, les listes contenant les fonctions soumises à contrôle au sens de la LSI ne doivent pas être publiées en vertu de l'art. 6, al. 1, de la loi sur les publications officielles du 18 juin 2004[14] (LPubl). Pour les mêmes raisons, la liste des fonctions selon la loi sur l'approvisionnement en électricité du 23 mars 2007[15] (LApEl) ne doit pas non plus être publiée. Les listes des fonctions soumises à contrôle à des fins de lutte contre la corruption ou de protection de la réputation de la Confédération peuvent sans autre être publiées comme à présent.

Les listes de fonctions ne seront établies qu'à partir de l'ouverture de la procédure de consultation. Il faut déjà s'assurer que les critères de vérification soient bien acceptés. Il est en effet question de plusieurs milliers d'entrées potentielles à vérifier avant de les intégrer dans les listes de fonctions définitives. Des informations détaillées sur la charge de travail occasionnée par les CSP ne seront disponibles qu'après la consultation.

3.6 Ordonnance sur la procédure de sécurité relative aux entreprises (OPSE)

a. Généralités

La LSI (art. 49 à 72 LSI) 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. Cette nouvelle procédure abroge la méthode de gestion des risques visant à réduire l'espionnage industriel. Elle permet également de contrôler et de faire respecter la sécurité de l'information durant l'exécution du mandat.

b. Objet et champ d'application

L'OPSE règle les détails de la procédure et remplace l'ordonnance du 29 août 1990 concernant la sauvegarde du secret[16], laquelle se limitait aux mandats à contenu militaire classifié. L'OPSE 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. 3.3, 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 traitant des informations classifiées CONFIDENTIEL de plusieurs organisations ou qui sont 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 et le nouveau droit de la Confédération sur les marchés publics se recoupent à plusieurs occasions. Ces recoupements ont été contrôlés en détail et traités lors de l'élaboration de l'avant-projet, en collaboration avec des représentants des services 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 des acquisitions et le service spécialisé chargé de ladite procédure. Cette coopération doit s'opérer le plus rapidement

[14] RS **170.512**
[15] RS **734.7**
[16] RS **510.413**

possible dans le processus d'acquisition. Cela permet d'identifier et de réduire de bonne heure les risques liés à l'acquisition.

3.7 Coordination des tâches et des finances

La LSI et ses ordonnances d'exécution créent les bases d'une amélioration durable de la sécurité de l'information de l'administration fédérale et de l'armée. L'accent est mis sur les informations et les moyens informatiques les plus critiques. L'introduction du SMSI est essentielle : il relie, pilote et supervise l'ensemble des mesures et des processus de la nouvelle législation. Une gestion efficiente de la sécurité de l'information favorise une sécurité plus efficace, économique et durable que ne le feraient de simples investissements dans des mesures techniques.

Le niveau d'ambition a été défini tant pour le SMSI que pour les autres mesures en ménageant les ressources. La LSI et ses ordonnances auront globalement peu de répercussions sur le personnel et sur les finances. C'est aux unités administratives et aux départements de décider s'ils veulent appliquer ou non une sécurité de l'information plus élevée à leur propre domaine de compétence et débloquer les ressources correspondantes.

3.8 Mise en œuvre

L'entrée en vigueur de la LSI et de ses ordonnances est prévue pour l'été 2023. Les délais sont suffisants pour assurer la transition vers le nouveau droit, tant pour la LSI (art. 90) que pour ses ordonnances d'exécution (art. 48 OSI, 38 OCSP et 25 OPSE).

D'autres prescriptions devront être élaborées ou actualisées avant l'entrée en vigueur de la LSI et de ses ordonnances, notamment :

- des consignes sur la gestion de la sécurité de l'information au sein de la Confédération (art. 15 OSI) ;
- les catalogues de classification (art. 17, al. 2 et 3, OSI) ;
- des consignes sur la protection des informations classifiées (art. 21, al. 1, OSI) ;
- des consignes sur l'accréditation de sécurité des moyens informatiques (art. 23, al. 6, OSI) ;
- des consignes sur les exigences minimales auxquelles doivent répondre les catégories de sécurité informatique (art. 29, al 1, OSI) ;
- des consignes sur la protection physique et les zones de sécurité (art. 34 et 35 OSI) ;
- les listes de fonctions pour les contrôles de sécurité relatifs aux personnes (art. 2 OCSP).

Outre l'émission de dispositions légales et techniques, trois autres conditions doivent être remplies :

- Mettre en place et en service le service spécialisé de la Confédération pour la sécurité de l'information (art. 83 LSI). Celui-ci reprendra des tâches et ressources du domaine de compétences actuels du Secrétariat général du DDPS (Digitalisation et cybersécurité DDPS, DCS) et du Secrétariat général du DFF (Centre national pour la cybersécurité, NCSC). Le 18 mai 2022, le Conseil fédéral a décidé de faire du NCSC un office fédéral à part entière. Il a chargé le DFF de lui présenter, d'ici à la fin de l'année 2022, des propositions concernant l'organisation du futur office et son rattachement à l'un des départements. En parallèle, diverses questions concernant les structures de politique de sécurité de la Confédération, y compris les structures dans le domaine cyber, sont en cours d'examen. Le résultat de ces travaux en cours est déterminant pour le rattachement administratif et les ressources du service spécialisé de la Confédération pour la sécurité de l'information. Le Conseil fédéral décidera du rattachement administratif du service spécialisé après la procédure de consultation.
- Former les préposés à la sécurité de l'information et d'autres chargés de fonction.
- Adapter ou introduire plusieurs systèmes d'information ; cela concerne notamment SICSP, le système d'information du CSP, ainsi que ses systèmes environnants, de même que SIPSE, le futur système d'information de la PSE ; pour l'exploitation efficiente du SMSI par les offices, l'administration fédérale travaille sur l'acquisition et l'introduction d'une application SMSI standardisée pour numériser les tâches et processus de l'OSI ; cette application devrait être prête fin 2024 pour son introduction et utilisation par les offices et les départements.

Les travaux de mise en œuvre sont coordonnés avec les autres autorités fédérales et avec les cantons. Le Conseil fédéral décidera au besoin d'une entrée en vigueur échelonnée de la LSI et de ses ordonnances.

4 Commentaire des dispositions

4.1 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 ainsi que 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 de protection personnelle et physique. Comme dans la LSI même (message LSI, commentaire de l'art. 1), la notion d'*information* n'est pas définie par l'OSI. Celle de *données personnelles* fait référence à celles visées dans la législation sur la protection des données.

Le rapport entre la LSI et la loi du 19 juin 1992 sur la protection des données (LPD)[17] est détaillé dans le message LSI[18]. 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 5 – Une liste positive détaille les autorités et organisations tenues d'appliquer cette ordonnance (message LSI, commentaire de l'art. 2 LSI) et sous quelles conditions.

Concernant le champ d'application de la LSI et de l'OSI pour les unités administratives de l'administration fédérale décentralisée au sens de l'art. 7a OLOGA ainsi que pour les organisations au sens de l'art. 2, al. 4, LOGA qui sont chargées de tâches administratives, mais qui n'appartiennent pas à l'administration fédérale : cf. ch. 3.3, let. b.

Pour les autorités concernées au sens de l'art. 2, al. 1, let. a et c à e, LSI (Assemblée fédérale, tribunaux de la Confédération, 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 c'est le cas et qu'elles en font usage, elles sont affranchies de l'OSI (mais pas de la LSI).

Al. 6 – Les dispositions de la section 4 de cette ordonnance s'appliquent aux cantons qui 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 fassent appliquer dans leur domaine de compétence. Les normes fédérales déterminantes sont les prescriptions et exigences techniques pour la protection de base de l'informatique au sein de la Confédération et pour la protection des informations classifiées. Les cantons ne sont pas tenus de mettre en œuvre un système de management de la sécurité de l'information (SMSI) au sens des 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 cantons eux-mêmes (art. 3 Cst.)[19], mais aussi aux collectivités, instituts ou fondations de droit public qui relèvent du droit administratif du canton correspondant. Du côté des cantons, ils doivent vérifier dans chaque cas si une organisation ou un institut (p. ex. un hôpital, une centrale électrique, voire un institut financier) est considéré

[17] RS **235.1**
[18] FF **2017** 2789
[19] RS **101**

comme un canton au sens de la LSI ou de l'OSI. Si un canton ne tombe pas dans le champ d'application de la LSI, il est considéré comme tiers au sens de l'art. 9 LSI (cf. commentaire de l'art. 10).

Al. 6, 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, dans tous les cas, être examinée. La Confédération décide en dernier ressort de l'existence d'un accès.

Section 2 Principes

Art. 3 Objectifs de sécurité

Les interfaces techniques entre les moyens informatiques des organisations qui relèvent de l'OSI 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.

Al. 1 – 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 à un minimum 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) qui se présentent, les nouvelles idées, les applications ou les 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. Le NCSC fixe aujourd'hui un minimum de consignes en matière de sécurité de l'information qui servent à protéger l'ensemble de l'administration fédérale et que les unités administratives doivent appliquer avec une marge de manœuvre limitée. Toutefois, cela ne dégage pas les unités administratives de leur responsabilité dans l'évaluation continue des risques et de la prise de mesures qui peuvent s'imposer. Concernant la compétence des départements sur l'attribution autre de certaines tâches, voir le commentaire de l'art. 39, al. 3.

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 (commentaire de l'art. 4, al. 4, et art. 11 OSI).

On entend par *collaborateurs de l'administration fédérale* les membres du personnel internes et externes qui reçoivent des instructions de la Confédération : les collaborateurs *internes* sont des employés de la Confédération conformément à la LPers ; en revanche, 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 personnes privées indépendantes ou les collaborateurs d'entreprises qui, sur la base d'une relation contractuelle par exemple, donnent des conseils à 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 commentaire de l'art. 10. En ce qui les concerne, la gestion réglementaire des objets protégés doit être garantie, 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 ainsi que du contrôle du respect des consignes. Il incombe à ces supérieurs d'expliquer concrètement à leurs collaborateurs comment gérer les informations protégées, de les rendre attentifs au fait d'utiliser rigoureusement selon les directives les logiciels de codage et de veiller à ce qu'ils suivent les formations proposées. Voir commentaire de l'art. 11 OSI au sujet de la responsabilité des unités administratives.

Section 3 Gestion de la sécurité de l'information

Les art. 5 à 15 OSI définissent les exigences minimales dans 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, des départements et du service spécialisé de la Confédération pour la sécurité de l'information. Ce dernier édictera à ce sujet des consignes de traitement (art. 21, al. 1) ou des directives générales abstraites (cf. art. 29, al. 1) qui prendront en compte l'approche fondée sur les risques encourus.

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. La notion de *SMSI* renvoie implicitement à la norme ISO/IEC 27001 qui tend à se généraliser dans l'économie privée et dans les administrations publiques. Les unités administratives ne peuvent s'acquitter que d'un *SMSI light* ; en d'autres termes, elles ne sont pas obligées d'appliquer la norme ISO dans son intégralité et peuvent se contenter des principaux processus de management définis dans l'OSI ; des consignes viendront préciser ces processus. Une certification externe n'est pas exigée. Les unités administratives et les départements sont libres de définir un niveau d'ambition supérieur.

Tandis que les responsables de la sécurité des unités administratives (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, au préposé à la sécurité de l'information de l'unité administrative (art. 37, al. 2, let. a). Selon l'art. 48, 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'unité administrative. Des objectifs concrets sont nécessaires, sur la base desquels la direction de l'office peut juger si l'effet souhaité est atteint. Ces définition et mesure annuelles des objectifs sont une tâche directionnelle qui incombe à cette dernière et doit être distincte de l'établissement du plan de contrôle et d'audit visé à l'art. 13.

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 organisme indépendant de l'office ou le département est exigée. Cette vérification indépendante du SMSI met les autres offices en confiance, tout en permettant l'amélioration continue de la sécurité au sein de l'office même.

La périodicité de trois ans s'oriente sur le cycle de certification officiel de la norme ISO, 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. De telles vérifications peuvent être effectuées soit par les structures de surveillance internes des départements, soit par une entreprise externe (commentaire du message LSI, p. 3018). Le recours à un pool d'auditeurs SMSI issu d'unités administratives d'un département ou de la Confédération serait également envisageable. Le processus continu d'amélioration est crucial pour garantir la sécurité de l'information. De tels contrôles permettent d'en tenir compte.

Al. 4 – Il 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 du management 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

Al. 1 – un répertoire sur les bases juridiques déterminantes dans le propre domaine de compétences et les engagements contractuels dans le domaine de la sécurité de l'information atteste du respect des bases juridiques pertinentes qui doivent être 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, un aperçu 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.

Al. 2 – Le service spécialisé de la Confédération pour la sécurité de l'information a impérativement un rôle consultatif (devoir de consultation), mais n'est pas habilité à donner des instructions sur le contenu. Les évaluations et les estimations d'un service spécialisé de la Confédération ont tout de même un poids important. Les différences devraient toujours être bien justifiées et mises sur un pied d'égalité. Ce devoir de consultation est en lien avec les 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, let. a – L'OPCy ne connaît aujourd'hui que la notion d'*objet informatique à protéger* (cf. art. 3, let. h, OPCy), notion couverte par la lettre b. Les informations ne sont toutefois pas toujours traitées dans un seul système d'information spécifique. C'est par exemple le cas lors que tâche est effectuée en utilisant l'environnement informatique standard de la Confédération ou lors que les informations sont traitées dans une solution informatique en nuage externe. La notion d'objet « informations » à protéger au sens de la lettre 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. La notion de « tâche de la Confédération ne couvre pas toutes les tâches, mais bien les processus d'affaires importants d'une unité administrative. Les consignes du service spécialisé de la Confédération (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 – La possibilité d'utilisation partagée des objets à protéger respectifs (let. e) 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.

Al. 3, let. d – L'aperçu des liens contractuels avec des tiers (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 interdépendances entre la Confédération et les 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. f – Concernant les risques résiduels, voir le commentaire de l'art. 9 OSI.

Al. 3, let. g – Voir le commentaire de l'art. 14, en relation avec l'art. 6, al. 2 et 3, OSI.

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 (commentaire du message LSI, p. 3018 s). Les consignes 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.

Il va de soi que l'appréciation des risques doit être *justifiable.* Le fait d'être justifiable n'est associé à aucune forme particulière. Dans le contexte de la numérisation, cela doit permettre de recourir à des méthodes de justification neutres sur le plan technologique.

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 de la collection d'indicateurs-clés.

Al. 1, let. c – Voir le commentaire sur la gestion des consignes selon l'art. 6 OSI.

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

Al. 3 – Les instructions sur la politique des risques de la Confédération et les directives et manuels qui y ont trait sont déterminants.

Art. 9 Autorisation et exceptions

Il s'agit de la gestion des exceptions aux consignes sur la sécurité de l'information en vigueur. Comme le NCSC aujourd'hui, le service spécialisé de la Confédération pour la sécurité de l'information décidera à l'avenir, sur la base de l'art. 85 LSI, des exigences de sécurité minimales qui doivent être satisfaites. Si une unité administrative n'est pas en mesure d'observer une exigence minimale, elle peut solliciter une dérogation. Le service spécialisé peut déléguer la décision sur l'octroi de la dérogation. Ainsi, le service spécialisé lui-même, le département ou une personne particulière au sein de l'unité administrative peuvent octroyer des autorisations exceptionnelles. Le principe actuel des dérogations sur les exceptions peut être repris conformément aux dispositions actuelles de l'OPCy sur la sous-délégation au sens de l'al. 2.

Art. 10 Collaboration avec les tiers

Al. 1 – La LSI qualifie de *tiers* 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 (message LSI, p. 3013 et 3019 s), ainsi que certaines organisations qui utilisent des infrastructures critiques (art. 2, al. 5, LSI).

Al. 3 – Les clauses sur la sécurité de l'information dans les contrats doivent remplir les conditions, conformément à l'art. 9 LSI (message LSI sur l'art. 9).

Art. 11 Formation et sensibilisation

Pour améliorer durablement leur sécurité, l'administration fédérale et l'armée doivent sensibiliser et former leurs collaborateurs et leurs membres sur le sujet de façon à ce 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 qui concerne la sécurité de l'information (avec des campagnes régulières de sensibilisation ou des formations d'entrée) pour tous les collaborateurs en y allouant le budget, le temps et les ressources correspondantes (art. 4, al. 4, OSI). Au contraire, les supérieurs hiérarchiques directs sont, selon cette disposition, responsables de la formation spécifique à la fonction de leurs collaborateurs (commentaire de l'art. 4, al. 4, OSI).

Art. 12 Gestion des incidents

Al. 1 – Les unités administratives sont responsables de la gestion des incidents et failles de sécurité. Un *incident de sécurité* est un événement lors duquel une atteinte est portée à la sécurité de l'information ou aux consignes de sécurité correspondantes. Un *incident de sécurité non abouti* est aussi un incident de sécurité. On parle d'*incident de sécurité non abouti* lorsqu'une atteinte aurait pu être portée à la sécurité de l'information. En revanche, 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.

Al. 2 – Cette disposition et le droit actuel se recoupent (art. 14, al. 4, let. c, OPCy), hormis le fait que les *incidents de sécurité non aboutis* doivent eux aussi, désormais, être signalés.

Al. 3 et 6 – La disposition potestative souligne que le service spécialisé de la Confédération pour la sécurité de l'information peut apporter son soutien, mais n'y est pas obligé. En principe, il l'apporte sur demande des unités administratives ou des départements et, quel que soit l'importance du cas, en fonction de ses ressources (al. 6 également).

Al. 4 – Voir les nouvelles obligations d'annoncer les violations portées à la sécurité des données selon la nouvelle loi sur la protection des données (nLPD[20], cf. art. 24) qui devrait entrer en vigueur le 1er septembre 2023.

Al. 5, let. b et d – Voir le message LSI à propos des art. 17 et 88 LSI.

Al. 5, let. e: La haute importance politique dépend des intérêts politiques concernés. Celle-ci doit être examinée au cas par cas avec la personne responsable de la sécurité du département correspondant (art. 39 OSI).

Al. 7 – On entend par *responsabilité* la compétence décisionnelle opérationnelle. Toutefois, l'unité administrative ou le département concerné reste responsable de la sécurité de l'information (commentaire de l'art. 4 OSI). Si la responsabilité relève du service spécialisé de la Confédération pour la sécurité de l'information, celui-ci peut ordonner seul des mesures immédiates ou avoir recours à des spécialistes (y compris à des tiers selon l'art. 10 OSI). Les coûts engagés dans ce cas sont entièrement à la charge de l'unité administrative responsable ou du département et s'effectuent en concertation avec celui-ci. La prise en charge de la responsabilité doit être justifiée (commentaire de l'art. 8, al. 1, OSI).

Art. 13 Planification des contrôles et des audits

Le manque de contrôles et d'audits est une lacune essentielle 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 (message LSI, p. 2978). Cette disposition exige que les unités administratives et les départements définissent annuellement les contrôles et les audits fondés sur les risques qu'ils effectueront l'année prochaine 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'unité administrative (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 qui ont un champ d'application limité ; ils peuvent être effectués de façon informelle par quelques personnes et au coût souvent inférieur à celui des audits. Une unité administrative 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 une organisation indépendante. Ils examinent si des systèmes, des processus ou des systèmes de gestion respectent les consignes en vigueur ou les normes exigées.

Al. 2 – Les contrôles et les audits peuvent, si les contrats avec des tiers l'autorisent, porter sur le respect des consignes par des tiers, notamment des fournisseurs. Si un tel contrôle est prévu et si le tiers dispose d'une déclaration de sécurité (art. 61 ss LSI), une coordination avec le service spécialisé chargé de la procédure de sécurité relative aux entreprises permet d'éviter que la Confédération contrôle plusieurs fois les mêmes éléments chez un partenaire.

Al. 3 – Sur demande des autorités fédérales, le service spécialisé de la Confédération pour la sécurité de l'information peut procéder à des vérifications (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 de qualité et à des examens transversaux 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

Al. 1 et 2 – 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 relative aux entreprises effectués pour le département ou la ChF ; les conclusions sur les incidents et failles

[20] FF **2020** 7397

de sécurité ainsi que les mesures d'amélioration prises ou prévues ; les conclusions des contrôles et des audits ainsi que les mesures d'amélioration prises ou prévues.

Al. 3 – Pour améliorer sur le long terme la sécurité de l'information au niveau de la Confédération, l'examen critique continu de l'efficacité de la sécurité de l'information et une adaptation permanente et judicieuse des mesures de sécurité sont nécessaires.

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

Cet article se réfère à l'art. 85 LSI. Le service spécialisé du Conseil fédéral obtient la compétence d'édicter les directives concernant le management de la sécurité de l'information (art. 5 à 14). Ces directives ne s'appliquent aux organes selon l'art. 2, al. 1 à 3, à savoir le domaine de compétence du Conseil fédéral.

Section 4 Informations classifiées

Les art. 18 à 20 décrivent les conditions matérielles de la classification des informations (message LSI à propos de l'art. 13). Par rapport à l'OPrI, les seuils de classification INTERNE, CONFIDENTIEL et SECRET ont été augmentés. En augmentant ces seuils pour les informations classifiées, il devra être possible de procéder à une classification ciblée. Ainsi, il devrait globalement y avoir dans l'administration fédérale un moins grand nombre d'informations classifiées, avec l'effet que cela implique sur les ressources. De plus, cette mesure influe directement sur le nombre de CSP. Cette augmentation devrait réduire les fonctions dont l'exercice est nécessaire au traitement des informations classifiées CONFIDENTIEL (OCSP et commentaire à ce propos).

Art. 16 Principes

Al. 1 – La classification est obligatoire dès lors que les critères correspondants conformément 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 compris les consignes de l'OCSP et de l'OPSE ; cf. message LSI, p. 3020).

Al. 2 – La collecte d'informations ou de supports d'informations classifiés ou non classifiés (p. ex. papier, matériel informatique, appareils de radio) 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 (p. ex. le produit deepl.com comme solution de cloud ou l'hébergement de l'Intranet de la Confédération puisque l'hébergement peut s'effectuer dans le nuage). De même, des informations isolées simples risquent de plus en plus d'évoluer vers des recueils de données à classifier du fait de la mise en œuvre de produits recourant à l'intelligence artificielle.

Al. 3 – Le fait de devoir remettre ou non un document à un demandeur (p. ex. un journaliste) sur le principe de la transparence ne dépend pas de son éventuelle mention de classification, s'évalue uniquement en fonction des critères de la Loi sur la transparence du 17 décembre 2004[21] (LTrans).

Art. 17 Auteurs de la classification

Al.1 –Tous les collaborateurs de la Confédération (art. 4, al. 3, OSI) et les militaires peuvent être auteurs de la classification au sens de la présente ordonnance. Les tiers ne sont pas auteurs de classification. Les personnes citées aux let. a à c sont compétentes pour la classification et pour la déclassification. Des cas particuliers sont à observer, comme dans le cadre de la gestion de projets : d'après HERMES, c'est par exemple le donneur d'ordre du projet (et non le chef de projet) qui doit s'assurer de la vérification des collectes d'informations éventuellement créées en vue d'un recueil à classifier.

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 plus souvent déjà trop tard si la protection n'a pas lieu directement à la source. Les supérieurs hiérarchiques des auteurs de classification ou les mandants ont le droit de modifier la classification. Mais en cas de pareille substitution qui inclut une prise de responsabilité quant à l'exactitude de la classification, ils doivent apparaître clairement comme auteurs de la classification. Si l'auteur de la classification n'est plus identifiable, il est possible de retrouver l'autorité supérieure par le truchement des Archives fédérales (AFS).

[21] RS **152.3**

Al. 2 – Les directives actuelles sur la classification (catalogue de classification) du 26 septembre 2011 (art. 8 OPrI) seront révisées d'ici à l'entrée en vigueur de la LSI.

Al. 4 – Cette disposition correspond à l'actuel article 8 OPrI, la compétence de la Conférence des secrétaires généraux étant déléguée au service spécialisé de la Confédération pour la sécurité de l'information.

Art. 18 Échelon de classification « interne »

Pour que se justifie la classification INTERNE, 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 ; l'OPrI ne précise pas le degré d'*atteinte*. 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 (message LSI, p. 3022 s.). De telles informations sont protégées par la loi ou par un accord ; de même, le secret de fonction selon l'art. 321 du Code pénal suisse du 21 décembre 1937[22] (CP) ou la LTrans doivent assurer la protection de certaines informations dans les cas prévus par ces lois.

Art. 19 Échelon de classification « confidentiel »

Pour que se justifie la classification CONFIDENTIEL, 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 que se justifie la classification SECRET, 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.

Art. 21 Directives relatives au traitement

Al. 1 – 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 d'informations classifiées ainsi que sur les mesures prises pour leur protection au niveau de l'organisation, du personnel et des constructions, de même que sur le plan technique. Ces consignes ne s'appliquent qu'aux organes visés l'art. 2, al. 1 à 3.

Al. 4 – 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. 5 – Les traités internationaux en matière de sécurité de l'information contiennent par exemple des listes de concordance concernant le traitement des informations classifiées, des normes de sécurité dans le domaine informatique ou de la sécurité des communications et des réglementations sur l'exécution de contrôles mutuels (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 prime le besoin d'en protéger la confidentialité. C'est en particulier le cas lors d'engagement de 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 actuel (cf. art. 18, al. 3, OPrI), les services de renseignements et la police fédérale (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 serait toutefois absurde que 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.

[22] RS **311.0**

Art. 23 Accréditation de sécurité des moyens informatiques

Al. 1 – L'OSI introduit, et c'est une nouveauté, une obligation d'accréditation pour un nombre limité de systèmes d'information sensibles (let. a à c) dans lesquels sont traitées des informations classifiées CONFIDENTIEL ou SECRET de plusieurs organisations (p. ex. une application pour la communication vidéo confidentielle). Avant une accréditation de sécurité, le moyen informatique correspondant ne doit pas être utilisé. Une telle accréditation est exigée à l'étranger et sur le plan international dès que 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). L'OSI comble ainsi une lacune qui, jusqu'à présent, compliquait la collaboration internationale dans le domaine de la sécurité.

Al. 2 à 4 – L'accréditation de sécurité doit rassurer sur le fait qu'un moyen informatique répond aux exigences imposées à la sécurité de l'information de la Confédération. Si elle ne peut pas être délivrée, le Conseil fédéral peut décider de supporter les risques résiduels.

Al. 5 et 6 – L'étendue de l'accréditation devra toujours être définie pour chaque cas concret. Cette tâche sera attribuée au service spécialisé de la Confédération pour la sécurité de l'information en tant que futur service d'accréditation ; une sous-délégation correspondante dans le domaine des systèmes militaires est prévue à la let. c.

Art. 24 Protection en cas de menace des informations classifiées

Le droit est d'ores et déjà en vigueur (art. 15 OPrI). Le signalement aux organes de sécurité responsables s'effectue selon la disposition relative à la gestion des incidents (art. 12 OSI).

Art. 25 Contrôle du besoin de protection et personnes autorisées

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

Art. 26 Archivage

Al. 1 – Les clauses sur l'archivage s'appliquent à la sauvegarde des documents dignes d'archivage de la Confédération (y compris 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.

Al. 2 – Les AFS ont pour tâche de garantir la protection des archives classifiées et archivées de manière centralisée. Elles peuvent donc se distancier des 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 compris des archives classifiées) ne se prolonge pas automatiquement à leur expiration. Par contre, la classification tombe automatiquement 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 [LOAr][23]). 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][24], en relation avec l'art. 14 LOAr).

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 (ActaNova). Les fonds à protéger plus longtemps du fait d'intérêts publics et privés sensibles prépondérants (art. 12 LAr et art. 14 LOAr) sont mentionnés à l'annexe 3 de la LOAr (art. 14, al. 5).

Section 5 Sécurité des moyens informatiques

Art. 27 Procédure de sécurité

La procédure de sécurité actuelle selon les art. 14*b* à 14*e* OPCy est repris 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. 27.

[23] RS **152.11**
[24] RS **152.1**

Al. 2 – Les écarts par rapport aux consignes exigent toujours un consentement exprès de l'instance habilitée à éditer des directives (commentaire sur l'autorisation d'exceptions selon l'art. 9 OSI).

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

Al. 3 – Un risque résiduel peut être un risque accepté ou un risque inconnu (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 *justifiable* (commentaire de l'art. 8, al. 2, OSI) des risques résiduels est importante, car celle-ci 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. La délégation de cette décision peut généralement s'effectuer par une instruction ou au cas par cas (p. ex. dans le cadre d'un projet informatique) à un autre membre de la direction (de façon également justifiable).

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.

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.

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

Désormais, les moyens informatiques (définition légale à l'art. 5, let. a, en relation avec l'art. 17 LSI) sont subdivisés en trois catégories de sécurité : « protection de base », « protection élevée » et « protection très élevée ». Par contre, l'actuelle OPCy 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. La « protection de base » s'applique désormais aussi aux cantons (art. 3 LSI) dans la mesure où ils entrent dans le champ d'application de la LSI.

Contrairement aux critères de classification des informations classifiées, la catégorisation des moyens informatiques s'appuie 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. Les critères financiers s'appuient sur les critères de la matrice d'évaluation de la gestion des risques de la Confédération.

Art. 29 Mesures de sécurité

Al.1 – Sur la base de l'art. 85 LSI, le service spécialisé de la Confédération pour la sécurité de l'information édicte des directives sur les exigences minimales pour chaque échelon de sécurité selon l'art. 17. Ces consignes doivent s'appliquer à tous les organes, selon l'art. 2, al. 1 à 3.

Al. 2 – Concernant les questions en lien avec la protection des données et leur sécurité fondée sur les risques, le service spécialisé de la Confédération pour la sécurité de l'information 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 (également art. 82, al. 1, LSI). Concernant l'approche fondée sur les risques, voir le commentaire de l'art. 4, al. 1, OSI. Les directives de ce service spécialisé, selon l'al. 1, doivent être harmonisées avec les dispositions en vigueur sur la protection des données. À cet égard, il faut veiller à ce que les notions « protection élevée » et « protection très élevée » selon l'art. 17 LSI ne se confondent 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 est due dès que des évolutions sensibles des risques s'esquissent, mais au plus tard tous les cinq ans. La base juridique de la vérification périodique figure à l'art. 18, al. 3, LSI.

Al. 4 – Voir le commentaire de l'art. 5, al. 4, OSI.

Art. 30 Sécurité de l'exploitation

Al. 1 à 4 – Les prestataires internes 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 administratives normales qui doivent mettre en œuvre l'OSI comme toutes les autres unités administratives. 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 prestataires 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. Les unités administratives (généralement les bénéficiaires de prestations) sont 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. 5 – 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

Al.1 – Sur la base de l'art 85 LSI, le service spécialisé de la Confédération pour la sécurité de l'information édicte des directives sur les exigences minimales pour la vérification fondée sur les risques de l'identité des personnes et des machines nécessitant un accès à des informations, des moyens informatiques, des locaux et d'autres infrastructures de la Confédération. Il consulte au préalable le délégué DTI. Ces consignes ne s'appliquent qu'aux organes visés l'art. 2, al. 1 à 3.

Il s'agit de définir ici comment une personne peut 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*.

Art. 32 Sécurité relative aux personnes

Al. 1 – Les unités administratives doivent 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 s'assurer que celle-ci fasse partie intégrante des 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.

Al. 2 – la pratique a montré que les risques de sécurité liés aux personnes, une fois le contrôle de sécurité relatif effectué, ne donnaient plus souvent 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. Il peut s'agir d'incidents susceptibles de soumettre concrètement une personne à un chantage (p. ex. de grosses dettes contractées dans le cadre de jeux de hasard, une dépendance à l'alcool ou aux stupéfiants découverte par une tierce personne, une relation extra-conjugale dévoilée). Si un signalement a lieu, la procédure sera coordonnée avec le service du personnel.

Art. 33 Soupçons de comportement répréhensible

Al. 1 – Cette disposition doit garantir que de possibles infractions soient communiquées aussi vite que possible aux autorités de poursuite pénale compétentes sans que les départements doivent se perdre en conjectures détaillées de nature pénale, voire judiciaire. Ainsi la notion d'acte délictueux sera *prise en considération* 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 mise en sûreté 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 mise en sûreté des preuves, les unités administratives n'effacent pas, ne laissent pas ou ne créent pas de traces

physiques ou électroniques. La mise en sûreté 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 physiques de protection

Al. 1 – Sur la base de l'art 85 LSI, le service spécialisé de la Confédération pour la sécurité de l'information édicte des directives sur les mesures minimales nécessaires à prendre pour protéger physiquement les informations et les moyens informatiques. Il consulte au préalable des organes de l'administration fédérale et de l'armée compétents pour la sécurité des objets. Ces consignes ne s'appliquent qu'aux organes visés l'art. 2, al. 1 à 3.

Al. 1 et 2 – Les mesures de protection physiques peuvent être la mise en place de zones de sécurité (art. 35 OSI et message LSI, p. 3032 ss), des contrôles d'accès dans des bâtiments, la surveillance par caméra de certains secteurs, des dispositifs de destruction de supports d'informations ou des contrôles des postes de travail. Le préposé à la sécurité de l'information des unités administratives a désormais la compétence pour réaliser ces derniers (art. 37, al. 2, let. j, OSI).

Art. 35 Zones de sécurité

Al. 1 – La création de zones de sécurité doit réduire les potentiels de dommages suite à un espionnage ou sabotage dans des zones très sensibles (comme les locaux abritant des serveurs ou certaines salles de conduite) (message LSI, p. 3015, 3032 ss).

Al. 2 – La confirmation des exigences de sécurité pour les zones de sécurité ne signifie pas une accréditation de sécurité au sens de l'art. 23 OSI. Les zones de sécurité ne doivent pas être confondues avec des locaux anti-écoute pour lesquels des mesures de construction et d'organisation plus complexes sont nécessaires.

Al. 3 – Sur la base de l'art 85 LSI, le service spécialisé de la Confédération pour la sécurité de l'information édicte des directives sur les exigences de sécurité pour les zones de sécurité et leurs installations. Il consulte au préalable des organes de l'administration fédérale et de l'armée compétents pour la sécurité des objets. Ces consignes ne s'appliquent qu'aux organes visés l'art. 2, al. 1 à 3.

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 qu'ils peuvent déléguer au besoin à un membre de leur direction (le responsable de la sécurité). Les responsables de la sécurité 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 opératives sont des tâches qui incombent aux préposés à la sécurité de l'information. Avec l'OSI, les rôles actuels de *délégué à la sécurité informatique* et de *préposé à la protection de l'information* sont condensés en un seul et même rôle, celui de *préposé à la sécurité de l'information*. Ses tâches vont être 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 au sein du département dans le sens des art. 37 à 38 et 41 à 42 LOGA. Ils définissent en particulier la politique de la sécurité de l'information et l'organisation de la sécurité départementale. La responsabilité opérative pour la sécurité incombe au secrétaire général. Les préposés à la sécurité de l'information continuent d'assumer les tâches opératives de coordination et de surveillance (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 pour tous les autres rôles, conformément aux art. 37 ss OSI. Aucun rôle n'est lié à une seule personne en particulier. N'est pas concerné celui précisé à l'art. 35 OSI : le responsable de la sécurité de la ChF et des unités administratives ne peut être attribué qu'à une seule personne.

Les personnes suppléantes doivent être à la hauteur techniquement et personnellement pour assurer toutes les tâches du rôle primaire. La personne suppléante doit avoir été formée pour pouvoir suppléer le rôle primaire à tout moment et avant tout en cas d'urgence à un niveau raisonnable.

Art. 36 Responsables de la sécurité de la ChF et des unités administratives

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 ce fait, la délégation devrait être justifiée (commentaire de l'art. 8, al. 2, let. a, 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 selon 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, art. 82, al. 3.

Art. 37 Préposés à la sécurité de l'information des unités administratives

La désignation d'une suppléance officielle est nouvelle. Ce rôle correspond largement à celui actuel de délégué à la sécurité informatique des unités administratives (DSIO).

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

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

Al. 3 – Cette disposition permet aux départements avec une organisation plus centralisée (comme le DFAE) de concrétiser leurs besoins internes d'organisation dans le cadre de l'OSI.

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

La désignation d'une suppléance officielle est nouvelle (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.

Let. e – Puisque les rôles doivent travailler en étroite collaboration selon les art. 37 et 40, le rôle visé à l'art. 40 devrait être associé au choix d'une nouvelle personne pour le rôle visé à l'art. 37.

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

Let. g – Ce rôle se voit attribuer une tâche supplémentaire dans le domaine des CSP. Les détails seront précisés par voie de directives et les titulaires du rôle seront formés en conséquence.

Let. h – Aujourd'hui, les rapports annuels des DSID doivent être envoyés au NCSC. Désormais, les titulaires du rôle, selon cette disposition, devront rendre des comptes à la personne responsable de la sécurité du département selon l'art. 39 OSI (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 (art. 83, al. 1, let. h, LSI).

Art. 41 Service spécialisé de la Confédération pour la sécurité de l'information

Al. 1 – Les tâches générales du service spécialisé de la Confédération pour la sécurité de l'information sont décrites aux art. 83 LSI et 41 OSI ; les tâches contextuelles, dans d'autres dispositions de l'OSI.

Al. 3 – La Conférence des préposés à la sécurité de l'information au sens de 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. 4 – Le rôle d'autorité nationale de sécurité est à présent attribué au service spécialisé de la Confédération pour la sécurité de l'information. Aujourd'hui, il est exercé par le domaine

Digitalisation et cybersécurité DDPS au sein du Secrétariat général du DDPS. Les tâches et compétences visées aux let. d et f font l'objet des traités internationaux selon l'art. 87 LSI (message LSI sur l'art. 88, p. 3071 ; p. 3090).

Section 8 Coûts et évaluation

Art. 42 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 pour les coûts afférents aux mesures de sécurité informatique.

Art. 43 Évaluation

Voir le message LSI, commentaire de l'art. 89 LSI, page 3071.

Section 9 Traitement des informations et des données personnelles

Les art. 44 à 46 règlent le traitement d'informations et de 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 à des 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. 3, let. c, LPD. La législation sur la protection des données requiert pour leur traitement une base légale au sens formel explicite qui fait aujourd'hui défaut. La base légale nécessaire sera créée dans le cadre de la révision en cours de la LSI (cf. ch. 3.1).

Art. 44 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 de données personnelles lors de la gestion des incidents, voir le commentaire de la section 9.

Art. 45 Application SMSI

Cette disposition crée la base légale nécessaire à l'exploitation d'applications SMSI. Celles-ci permettent la digitalisation des tâches et processus de l'OSI (cf. ch. 3.8). Concernant le traitement de données personnelles lors de la gestion des incidents, voir le commentaire de la section 9.

Art. 46 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), d'attestations de sécurité (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 nLPD). Les personnes qui demandent 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 doivent pas être conservées plus de 24 heures dans le service de formulaire. Concernant le traitement de données personnelles lors de la gestion des incidents, voir le commentaire de la section 9.

Section 10 Dispositions finales

Art. 47 Abrogation et modification d'autres actes

L'OPCy et l'OPrI sont abrogées.

Art. 48 Dispositions transitoires

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

Art. 49 Entrée en vigueur

La nécessité d'une entrée en vigueur partielle est en cours d'examen.

Annexe 1

Le [département compétent] s'occupe de l'annexe 1.

Annexe 2

Voir le commentaire relatif à l'art. 46.

Annexe 3

Ch. 1 – Modification de l'ordonnance sur la coordination de la transformation numérique et de la gouvernance de l'informatique dans l'administration fédérale du 25 novembre 2020[25] (OTNI) : l'OPCy est remplacée par l'OSI.

Ch. 2 – Ordonnance sur l'organisation du DDPS du 7 mars 2003[26] (Org-DDPS): la notion de *secret militaire* ne s'applique plus avec la LSI et l'OSI. L'organe de coordination pour la protection des informations au sein de la Confédération est dissout et ses tâches sont assumées par le service spécialisé de la Confédération pour la sécurité de l'information.

Ch. 3 – Ordonnance concernant les relations militaires internationales du 24 juin 2009[27] (ORMI) : les organes et ordonnances concernés devront être actualisés suite à la LSI et à ses ordonnances d'exécution.

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

Préambule

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 générale d'organisation du Conseil fédéral et indirectement sur les bases légales des systèmes d'information raccordés. Grâce à l'art. 20, al. 2, LSI, il sera désormais possible, sous réserve de certaines conditions, de traiter des données biométriques dans les systèmes de gestion des données d'identification (systèmes IAM). Celles-ci sont considérées comme des données sensibles au sens de la nLPD (cf. 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 toutefois toujours possible de traiter des données sensibles dans les systèmes IAM en s'appuyant sur une base légale formelle autre que la LSI. Les profils de personnalité n'ont plus d'importance particulière dans la nLPD et ne doivent donc plus être mentionnés. Un profilage au sens de l'art. 5, let. f, nLPD n'a pas lieu au sein des systèmes IAM ou des services d'annuaires, car ceux ne servent pas à *évaluer* des aspects personnels relatifs à des personnes physiques.

Art. 2 Champ d'application

La notion d'*administration fédérale* utilisée à l'art. 2, al. 2, let. b, LSI comprend aussi bien l'administration fédérale centralisée que celle décentralisée (message LSI, p. 3012), d'où la nécessité d'étendre le champ d'application aux unités administratives de cette dernière, dans la mesure où elles ont accès aux systèmes informatiques de l'administration fédérale centralisée.

Le contenu de l'actuel al. 2 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, sans base légale explicite).

[25] RS **172.010.58**
[26] RS **172.214.1**
[27] RS **510.215**

Art. 3, al. 1

Jusqu'ici, les données sur les identités ne sont proposées que sur demande aux systèmes IAM en aval ou autres systèmes d'enregistrement des identités, lesquels les utilisent selon leurs propres rythmes et besoins. Dans le cadre de mesures de protection réactives (p. ex. modification immédiate d'autorisations ou blocages d'urgence), il n'est plus possible de se reposer sur la date de la mise en œuvre de l'annonce dans des applications ; il s'agit au contraire d'être réactif et d'approvisionner les systèmes IAM en aval avec ces informations intéressant la sécurité. Ce nouveau mode d'alimentation est important et doit donc être ancré dans l'OIAM. La formulation actuelle qui prévoit qu'un système IAM ne mette les données à la disposition des systèmes en aval ou d'autres systèmes IAM que *sur demande* est donc adaptée en conséquence, d'où la suppression de *sur demande*.

Art. 5 Systèmes IAM

Al. 1 – Les autres organes de la Confédération responsables des systèmes IAM (let. c et g) sont mentionnés en plus des organes de la Confédération responsables déjà mentionnés dans l'IAM.

Al. 2 – Actuellement, le traitement des données personnelles dans les systèmes IAM n'est pas contrôlé. L'art. 26, let. e, LSI exige à présent explicitement, et pas uniquement en lien avec les systèmes IAM, qu'un contrôle périodique du traitement des données personnelles par un service externe soit prévu. Un alinéa supplémentaire est inséré en conséquence à l'art. 5.

Al. 3 – Vu l'art. 84, al. 3, LSI, l'OIAM s'applique 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. 4 – Du fait des nouveaux al. 2 et 3, l'actuel al. 2 devient l'al. 4, sans changement de contenu.

Art. 11, al. 2 et 3

Vu l'art. 20, al. 2, LSI et sur la base de la nLPD, les actuels al. 2 et 3, d'après lesquels aucun profil de la personnalité et, sans base juridique particulière, aucune donnée personnelle sensible ne peut être traité dans les systèmes IAM, doivent être doublement contrôlés (cf. les explications sous ch. 3.4). Premièrement, la disposition interdisant le traitement des profils de la personnalité est remplacée par une interdisant le profilage (art. 5, let. f, de la nouvelle loi sur la protection des données). Deuxièmement, les données biométriques permettant d'identifier clairement une personne sont désormais considérées d'emblée comme des données sensibles ; pour leur traitement, une base générale est créée dans l'art. 20, al. 2, LSI. Ces données biométriques doivent donc désormais, selon l'annexe (let. a, ch. 11), être traitées en principe dans tous les systèmes IAM dans lesquels cela s'avère nécessaire pour identifier des personnes sous l'angle des risques.

Art. 13, al. 4

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

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 sur les systèmes d'information de l'armée du 3 octobre 2008[28] (LSIA), 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.

Art. 20 Système global IAM

Conformément à l'art. 20 actuel, 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

[28] RS **510.91**

permettre une répartition efficace des tâches. Cela signifie qu'ils peuvent échanger entre eux des données d'utilisateurs à l'instar d'une fédération. Désormais, les systèmes IAM mentionnés peuvent aussi être reliés aux systèmes IAM visés à l'art. 21, raison pour laquelle l'art. 20 est complété en conséquence. Une nouveauté formelle tient dans le fait que tous les systèmes IAM externes à l'administration fédérale – c'est-à-dire aussi les systèmes IAM des Services du Parlement et de l'armée énumérés jusqu'ici dans l'art. 20 – sont repris dans l'art. 21.

Art. 21 Conditions pour le raccordement de systèmes IAM externes

Phrase introductive – Quand un système IAM externe au sens de l'art. 21 doit être relié aux systèmes IAM de l'administration fédérale, des Services du Parlement ou de l'armée, il est impératif, pour des raisons de sécurité, de soumettre les exploitants en question à l'OIAM. La phrase est donc complétée en conséquence.

Let. a et b – Désormais, les systèmes IAM des Services du Parlement et de l'armée, mentionnés jusqu'ici dans l'art. 20, sont aussi repris dans la liste.

Les let. c à f correspondent aux actuelles let. a à d.

Annexe

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 (aujourd'hui, ceci n'est possible que pour les systèmes de l'armée sur la base de l'art. 2*a* LSIA). Les données biométriques, mentionnées actuellement sous la let. g, intègrent donc la let. a ; la let. g peut donc être abrogée.

Ces données ne doivent 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 l'identification de personnes sous l'angle des risques. À noter que ces données doivent être détruites après l'échéance du droit d'accès (art. 20, al. 3, LSI et art. 14, al. 2, OIAM).

Par ailleurs, les colonnes *services d'annuaires* et *systèmes IAM avec personnes selon art. 8 et 9, let. a* sont regroupées. Une différenciation entre les services d'annuaires et les systèmes IAM en question s'est révélée, par le passé, extrêmement gênante dans l'offre de prestations IAM à des processus de gestion, c'est pourquoi, à l'avenir, tous les destinataires doivent divulguer les règlements complets de traitement lors d'une connexion à des services IAM (comme c'était uniquement le cas jusqu'ici pour les systèmes IAM).

Enfin, deux modifications linguistiques sont apportées au contenu de la let. f (phrase introductive et ch. 2), conformément au libellé de la LSI.

4.3 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

Al. 1 et 2 – l'OCSP porte sur toutes les compétences d'exécution relatives aux CSP qui entrent dans le cadre de l'art. 48 LSI ainsi qu'aux vérifications, évaluations et contrôles visés par d'autres lois.

Al. 3 – L'autorité soumise à la présente loi, le Conseil fédéral, a des tâches d'exécution spécifiques pour l'administration fédérale, d'après l'art. 2, al. 1, LSI.

Art. 2 Champ d'application

L'art. 2 LSI est transposé par le Conseil fédéral dans l'art. 2 OSI. Cette disposition est donc aussi déterminante pour le champ d'application de l'OCSP.

Section 2 Listes des fonctions

Art. 3 Attribution

Al. 1 à 3 – Une liste des fonctions doit être 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[29] et l'art. 6*a,* al. 2 de la loi du 22 juin 2001 sur les documents d'identité[30], des contrôles de sécurité pourraient être effectués pour certaines personnes dans le domaine de la délivrance de documents d'identité au sens de l'art. 6 de l'OCSP actuelle. C'est sciemment qu'aucune liste de fonctions n'est dressée dans l'OCSP pour ces contrôles. En cas de besoin impératif de CSP, ceux-ci seraient couverts via une procédure de sécurité relative aux entreprises auprès des entreprises correspondantes.

Les listes des fonctions ne doivent 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 de fonctions.

Al. 4 – Cet alinéa correspond par son contenu à la réglementation en vigueur de l'art. 1, al. 3, OCSPN.

Art. 4 Modification

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 contenant lesdites fonctions. Le DDPS gérera ces listes de façon centralisée et les actualisera régulièrement sur demande des départements et de la Chancellerie fédérale (ChF). Il consultera le service spécialisé de la Confédération pour la sécurité de l'information.

Art. 5 Publication, conservation et communication

Concernant la sensibilité des listes des fonctions en termes de sécurité, voir ch. 3.5 let. d. 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 organes requérants et des organes de sécurité selon l'OSI.

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 au moins une fois par législature 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 des 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 correspondante pour un contrôle extraordinaire soit déléguée au DDPS, lequel consulte le service spécialisé de la Confédération pour la sécurité de l'information. Les listes des

[29] RS **142.20**
[30] RS **143.1**

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 ou une organisation engagée 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.

Art. 9 Contrôle de fiabilité extraordinaire de l'IFSN

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

Section 4 Degrés de contrôle

Le rattachement du contrôle de la loyauté selon la loi sur l'asile au sujet du 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[31] (LAsi) 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. Si de telles informations ne sont traitées qu'exceptionnellement et que le traitement d'informations classifiées ne concerne pas une fonction à proprement parler, un CSP n'est pas nécessaire.

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 sont associées à 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 porter fortement atteinte aux intérêts par le vol de données ou le sabotage selon l'art. 1, al. 2, LSI. Seuls les contenus des informations traitées décident si les utilisateurs des moyens informatiques exercent une activité sensible. De ce fait, ce sont surtout les administrateurs et les responsables des applications des systèmes qui sont recensés. La notion d'*exploitation* se réfère à l'activité des fournisseurs de prestations au sens de l'art. 19 LSI. Il doit être clairement distingué de l'expression *exploiter un système d'information* que l'on trouve dans la législation sur la protection des données et qui ne vise en fait qu'à 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 délimitation de zones ou de locaux en zones de sécurité constitue une mesure physique en faveur de 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 de telles zones font l'objet d'un contrôle de sécurité de base.

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

Al. 2, let. a et b – Voir commentaire de l'al. 1, let. a et b.

Al. 2, let. c et d – 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 Centre des opérations électroniques de la Base d'aide au commandement le font

[31] RS **142.31**

régulièrement dans des domaines très sensibles. Leurs activités doivent donc être rattachées au degré de contrôle du contrôle de sécurité élargi.

Al. 2, let. e – Voir 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 concernant l'ordonnance sur le personnel de la Confédération[32]) 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 – D'après la matrice d'évaluation actuellement en vigueur de la gestion des risques de la Confédération, une conséquence *considérable* correspond à des conséquences financières potentielles de l'ordre de 50 millions 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 être limité aux tâches qui peuvent compromettre considérablement les intérêts publics de la Confédération.

Al. 1, let. d – Les personnes qui travaillent dans l'entourage rapproché d'un chef de département peuvent régulièrement porter un grave préjudice en cas d'exercice inadéquat de leur fonction. Elles doivent donc sans exception être soumises à un contrôle de sécurité de base.

Al. 2, let. a à c – 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, respectivement de l'art. 2, al. 1bis, de l'ordonnance sur le personnel de la Confédération du 3 juillet 2001[33] (OPers) répondent au moins régulièrement à 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, OPers. 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. d – D'après la matrice d'évaluation actuellement en vigueur de la gestion des risques de la Confédération, une conséquence *importante* correspond à des conséquences financières potentielles dépassant les 500 millions de francs, tandis qu'une conséquence *très importante* dépasse un milliard de francs.

Al, 2, let. e – Les activités du personnel des services spécialisés CSP selon l'art. 16, al. 1, sont aussi soumis à un contrôle de sécurité élargi afin de garantir leur fiabilité vis-à-vis des personnes à contrôler.

Art. 12 Contrôles selon la loi sur l'armée du 3 février 1995[34] (LAAM)

Al. 1, let. a – Les activités normales de militaires en uniforme à l'étranger 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.

Al. 1, let. b –Voir 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 s'il faut renoncer à recruter un conscrit, dégrader un militaire ou l'exclure de l'armée.

Al. 2 – Actuellement, les aspirants peuvent être soumis à un CSP, indépendamment d'une raison matérielle justifiant le contrôle. Cette possibilité tombe avec la présente ordonnance. Désormais, ils ne doivent être contrôlés que s'il existe une raison matérielle selon la LSI ou la LAAM pour un tel contrôle. Si la personne concernée est déjà au bénéficie d'un CSP valable et si l'aspirant a une fonction exigeant un CSP, le CSP peut être répété par anticipation dans la mesure où le délai minimal au sens de l'art. 43, al. 1, LSI est écoulé.

[32] RS **172.220.111.343.3**
[33] RS **172.220.111.3**
[34] RS **510.10**

Art. 13 Contrôles de fiabilité selon la loi sur l'énergie nucléaire du 21 mars 2003[35]

Cet article correspond par son contenu à la réglementation en vigueur de l'art. 3 OCSPN.

Art. 14 Contrôles de loyauté selon 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.

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. Suite à de précédentes expériences, il vaut mieux renoncer volontairement à 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 si le délai est très court, à une multiplication des constatations parce que les signes de risques n'ont pas pu être clarifiés de façon approfondie ou parce que les données n'étaient pas 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 – Cet alinéa correspond par son contenu à l'art. 2, al. 2 et 4, al. 1, OCSPN.

Al. 5 – Pour que les services spécialisés CSP puissent être efficaces dans leur travail, 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.

Art. 16 Services spécialisés CSP

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

Le service spécialisé CSP de la ChF contrôle, selon l'art. 16, al. 2, let. d, les *fonctions du Secrétariat général du DDPS avec tâches de conduite vis-à-vis du service spécialisé CSP du DDPS*. Il s'agit, en l'occurrence, de contrôler le secrétaire général, son suppléant et le chef du service spécialisé CSP du DDPS. Hormis ces trois fonctions du SG-DDPS, le service spécialisé CSP de la ChF ne contrôle pas d'autres fonctions visées à la let. d.

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 correspondante 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. 4, al. 5, LPD.

Art. 18 Collaboration

Le contrôle de sécurité serait illusoire si, sous le couvert des droits fondamentaux, la personne concernée pouvait refuser de répondre à des demandes de renseignements sur d'éventuels abus d'alcool ou de stupéfiants, des dettes personnelles, des occupations accessoires, etc., et si des faits de cette nature n'entraient pas dans l'appréciation du risque pour la sécurité. 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) : ils disposent d'une

[35] RS **732.1**

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 – La consultation d'une base de données est, en principe, le fait des deux services spécialisés CSP via le service spécialisé CSP du DDPS. Les services spécialisés CSP ne doivent pas obligatoirement recourir à tous les moyens disponibles pour évaluer le risque. Cette règle est particulièrement importante pour le contrôle élargi parce que la réduction du nombre des degrés de contrôle ne doit pas entraîner une augmentation massive des coûts des CSP. Il est donc possible de renoncer à déterminer 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 selon 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 des frais 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, l'audition n'est pas absolument nécessaire si le risque a peu changé.

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 interroger 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. Les bases juridiques ne prévoient pas d'obligation à cet égard. Les tiers concernés peuvent donc refuser de communiquer des informations à tout moment.

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 plusieurs motifs justifient qu'une personne soit contrôlée par les deux services spécialisés CSP, seul le service spécialisé CSP de la 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 qui sont adaptées, du point de vue des services spécialisés CSP, 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 à ces recommandations. Elles peuvent suivre les conditions recommandées, en prévoir d'autres ou y renoncer.

Art. 23 Communication

Al. 1 – Si, pour plusieurs motifs de contrôle, des personnes sont soumises à un contrôle effectué à différents moments, les constats relatifs aux risques 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 au sens de l'art. 113 LAAM, auxquels tous les militaires sont soumis. Si l'on constate, dans le cadre

d'un autre contrôle, un risque par rapport à l'arme personnelle, les services spécialisés CSP sont autorisés à communiquer la déclaration 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 provisoires 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 psychologues lors du recrutement.

Section 6 Conséquences de la déclaration

Art. 24 Exercice de l'activité

Al. 1 – L'instance décisionnelle assume la responsabilité des activités 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 (art. 22). Elles peuvent suivre les conditions recommandées, en prévoir d'autres ou y renoncer entièrement. 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.

Al. 2 – La communication de la décision de l'instance décisionnelle est nécessaire pour donner accès à des installations militaires ou à des zones de sécurité. Elle est également déterminante pour l'établissement du certificat international 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 est au bénéfice d'une déclaration pour un degré de contrôle au moins équivalent et que celle-ci est encore valable, un nouveau contrôle doit être évité pour des raisons d'économies. La décision à ce sujet dépend de celui qui assume le risque.

Al. 2 – Utiliser la déclaration d'un ancien contrôle 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 pour l'ancien contrôle est plus strict que pour le nouveau contrôle. En effet, des données collectées dans le cadre du contrôle plus strict et qui ne devraient pas l'être dans le cadre d'un degré moins strict viennent alors alimenter une 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 à des règles restrictives sur l'utilisation de découvertes fortuites dans d'autres bases juridiques, une utilisabilité clairement restreinte doit être possible.

Art. 26 Répétition ordinaire du contrôle

La LSI ne prescrit pas de délais de répétition ordinaires fermes 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 renoncer à une répétition du 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.

Art. 27 Répétition exceptionnelle du contrôle

Al. 1 – La répétition exceptionnelle 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 exceptionnelle 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 exceptionnelle peut aussi être engagée.

Art. 28 Effet de la répétition

L'effet de la répétition vaut tant pour une répétition ordinaire qu'exceptionnelle. Comme la répétition sert de nouvelle évaluation de la personne à contrôler, l'ancienne évaluation 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, 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 la tenue de procédures de recours sur les évaluations afin que les organes supérieurs aux services spécialisés CSP ne puissent pas influencer indirectement les évaluations suite au refus de la tenue d'un recours. Les services spécialisés CSP doivent donc pouvoir décider eux-mêmes s'ils veulent exercer un recours contre des décisions du Tribunal administratif fédéral.

Art. 30 Certificat international 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 selon 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.

Section 7 Traitement des données personnelles

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

En application de l'art. 16, al. 2, 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.

Section 8 Dispositions finales

Art. 33 Gestion électronique des affaires

À l'avenir, les affaires seront traitées électroniquement dans la mesure du possible.

Art. 34 Émoluments

Les coûts pour les contrôles issus de l'administration fédérale centrale doivent être budgétisés de façon centralisée par le DDPS. Les coûts pour les contrôles effectués par des services externes à l'administration fédérale centrale doivent être supportés par ceux-ci de façon décentralisée et donnent lieu à des émoluments. Par l'octroi correspondant de personnes et de ressources 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 pour leur propre sécurité de l'information, moyennement rémunération, dans la mesure où le Conseil fédéral le précise. Il ressort clairement de l'art. 16 que le service spécialisé CSP du 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 du DDPS doit être techniquement à la hauteur 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 chaque canton 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 doivent nécessiter des moyens supplémentaires des services spécialisés, les prestations ne pourront être apportées que si les moyens supplémentaires sont effectivement octroyés aux services spécialisés. Une compensation interne à la Confédération de ces moyens est exclue.

Art. 36 Abrogation 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 doivent donc être abrogées. Doit également être abrogée l'ordonnance sur les contrôles de sécurité relatifs aux personnes, laquelle est entièrement revue par la présente ordonnance. L'ordonnance sur les contrôles de sécurité relatifs aux personnes dans le domaine des installations nucléaires doit, elle aussi, être abrogée car ses contenus, s'ils sont encore nécessaires, sont intégrés dans la présente ordonnance.

Art. 37 Modification d'autres actes

Du fait de l'ampleur de la modification des autres actes, la réglementation sur ce sujet apparaît à l'annexe 9. L'explication correspondante suit ci-après.

Art. 38 Dispositions transitoires

Les déclarations sur les contrôles actuels 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 requérants qu'aux services spécialisés CSP. Elle ménage par ailleurs une marge de manœuvre suffisante pour faire contrôler 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 également une réglementation spéciale qui permette de mettre un terme au contrat en cours de façon ordonnée.

Art. 39 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 être publiées (commentaire de l'art. 5).

Annexe 7 Collecte et traitement des données

Les détails sur la collecte et le traitement des données nécessaires aux contrôles sont précisés à l'annexe 7. Les barrières légales qui fixent la LSI pour le traitement des données (p. ex. art. 27, al. 3, ou art. 34, al. 4, LSI) ne sont pas répétées ici. La liste des données n'est pas exhaustive, comme l'indique l'adverbe *notamment*. Il s'agit, pour ces deux chiffres, de dispositions potestatives. Les services spécialisés ne doivent pas obligatoirement recourir à tous les moyens disponibles pour évaluer le risque. Par exemple, il est peu judicieux de collecter des données fiscales sur des conscrits étant donné que ces personnes n'ont pas ou peu remis de déclarations fiscales pertinentes vu leur jeune âge. Cette règle est particulièrement importante pour le degré de contrôle du contrôle de sécurité élargi parce que la réduction du nombre de ces degrés ne doit pas entraîner une augmentation inutilement massive des coûts des CSP.

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. À défaut 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

d'obtention et de traitement d'informations qui gagne en importance du fait de la progression de la numérisation.

Annexe 8 Modification d'autres actes

1. Org-DDPS

Les services spécialisés CSP réalisent l'évaluation sans aucune instruction, conformément à l'art. 31, al. 2, LSI. Selon les art. 7 ss de l'ordonnance sur l'organisation du gouvernement et de l'administration, ils font partie de l'administration fédérale centrale et ne peuvent pas être rattachés administrativement. Le rattachement administratif du service spécialisé CSP du DDPS contenu dans l'art. 6, let. c, Org-DDPS en vertu de l'art. 21, al. 1, LMSI doit donc être abrogé.

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. La notion d'*intérêt politique* protège en particulier la bonne réputation de la Confédération. Cette mesure de l'art. 94e 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 plus tôt que cinq ans. Il incombe à l'employeur de décider si une inscription aux 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 être intégralement contenue dans l'OCSP.

3. ORMI

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

4. Ordonnance sur les systèmes d'information de l'armée du 16 décembre 2009[36] (OSIAr)

L'art. 67 et l'annexe 30 correspondants 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 la présente ordonnance. Par ailleurs, les renvois actuels à l'OCSP en vigueur doivent être adaptés à la nouvelle législation.

5. Ordonnance sur les obligations militaires du 22 novembre 2017[37]

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

6. Ordonnance sur l'énergie nucléaire du 10 décembre 2004[38] (OENu)

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 à 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.

[36] RS **510.911**
[37] RS **512.21**
[38] RS **732.11**

4.4 Ordonnance sur la procédure de sécurité relative aux entreprises (OPSE)

Notes introductives

Pour comprendre le sujet, de courts commentaires s'affichent à cet endroit au moins sur les dispositions de la LSI.

- La définition de *mandat sensible* est donnée dans les définitions légales de 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 de la catégorie 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 protégées 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'OPSE fait référence à des entreprises, des parties d'entre elles ou des sous-contractants qui exécutent des mandats publics qui impliquent une activité sensible (art. 49, LSI).
- On entend par adjudicateurs au sens de l'OPSE les autorités et organisations soumises à la présente loi d'après l'art. 2 LSI (art. 50, al. 1, let. a, LSI).

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 correspondante. L'art. 84, al. 1, LSI contient la compétence fondamentale des autorités soumises à la présente loi sur l'établissement des dispositions d'exécution de la LSI. L'art. 73 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'OPSE.

Al. 2 – Dans la mesure où les autorités et 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'OPSE doit donc correspondre à celui de la LSI et de l'OSI (cf. aussi ch. 3.6, let. a).

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 constitue l'énoncé de fait légal de base pour 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 du droit public et 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'OPSE porte sur des critères nationaux. L'exécution de la procédure de sécurité relative aux entreprises ayant leur siège à l'étranger dépend des traités internationaux correspondants.

Art. 3 Autorité compétente

Al. 1 – L'autorité appelée service spécialisé Procédure de sécurité relative aux entreprises (service spécialisé PSE) doit être affectée sur le plan organisationnel. La décision correspondante sera prise avec la décision sur le rattachement administratif du service spécialisé de la Confédération pour la sécurité de l'information (ch. 3.8).

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 phrase, 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.

Art. 4 Demande d'ouverture de la procédure

Al. 1, let. a et b – 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. 1, let. c – Les entreprises qui attribuent un contrat de sous-traitance jouent alors le rôle d'adjudicateur. Dans la mesure où leur propre adjudicateur les autorise à sous-traiter, il leur appartient de demander l'ouverture de la procédure. Le préposé à la sécurité relative aux entreprises est compétent à cet égard, selon l'art. 12.

Al. 2 – Concernant les autorités soumises à la présente loi selon 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'OPSE, il demande uniquement aux autorités soumises à la présente loi d'indiquer qui est le service compétent.

Al. 3, let. a – La description des travaux de construction, de la livraison ou des prestations sert notamment au service spécialisé PSE comme critère d'identification, surtout 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 au moins doit indiquer dans quelles mesures les conditions de l'art. 5, let. b, LSI sont remplies. L'allègement de la preuve par une justification uniquement sommaire doit notamment servir à ce qu'une ouverture de procédure puisse avoir lieu relativement tôt dans le but d'affecter le moins possible les déroulements de la procédure d'adjudication.

Al. 3, let. c – La procédure de sécurité doit être coordonnée individuellement et de bonne heure aux 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 toujours exercer en accord avec l'adjudicateur, suisse ou étranger (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 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 sont toujours soumises aux dispositions de l'OPSE, 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 sur plusieurs autorités ou départements est, sans exception, un cas de procédure de sécurité relative aux entreprises.
- Let. c – Comme pour la let. b, l'utilisation, 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 sûreté étrangères

Al. 1 – Si l'adjudicateur envisage de confier un mandat sensible (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 s'effectuent par le truchement du service spécialisé de la Confédération pour la sécurité de l'information (art. 83 LSI).

Al. 2 – En présence d'un traité international correspondant, à la demande du service spécialisé de la Confédération pour la sécurité de l'information (art. 87 LSI), l'autorité de sécurité étrangère 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 à 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. 5, 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 devrait 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 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 au plan de la procédure. Les tâches de coordination correspondantes 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 d'aptitude, 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 d'aptitude. Ce nombre peut être augmenté, mais uniquement dans des cas justifiés. Cette clause d'exception doit constituer une issue lors d'évolutions non prévues dans la procédure d'adjudication et permettre des annonces tardives.

Al. 2 – L'accord de l'entreprise pour la réalisation de la procédure est la condition d'ouverture (art. 50, al. 2, LSI) et doit donc être examiné d'office par le service spécialisé PSE. Cet accord 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.

Al. 2 – La collecte des données au sens de l'art. 6, al. 1, let. a, de la loi sur le renseignement du 25 septembre 2015[39] (LRens) est de la compétence du SRC. Il est ici examiné si l'entreprise est apparue en lien avec le terrorisme, un service de renseignement interdit, la prolifération, des attaques d'infrastructures critiques ou l'extrémisme violent. Le SRC s'occupe de collecter les données.

Al. 3, let. a – Conformément à l'art. 56, al. 1, let. a, LSI, le service spécialisé PSE peut collecter les données correspondantes directement auprès des entreprises afin d'évaluer leur aptitude. Celles-ci ont l'obligation de collaborer, comme précisé à l'art. 9, al. 1, let. a à g. Tout manque de volonté en ce sens de sa 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.

Al. 3, let. b – Contrairement au refus de fournir des renseignements (let. a), 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.

Art. 10 Exclusion de la procédure

Al. 1 – Tant l'art. 44 de la loi fédérale sur les marchés publics du 21 juin 2019[40] (LMP) 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 d'aptitude, 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 d'aptitude. D'autre part, le service spécialisé PSE doit informer le plus rapidement possible l'adjudicateur si, suite aux données collectées, des informations apparaissent qui peuvent inciter l'adjudicateur à exclure l'entreprise.

Al. 2 – L'échange continu d'informations justifie que le service spécialisé PSE contrôle dans un premier temps l'adéquation 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 stoppée 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 d'aptitude 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 Préposé à la sécurité de l'entreprise

Al. 1 – Une entreprise pour laquelle l'adjudicateur a demandé un examen d'aptitude 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 gestion de l'entreprise puisse être responsabilisée 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 avoir un impact sur les décisions ou alors ils agissent au moins sur ordre direct d'une telle personne.

[39] RS **121**
[40] RS **172.056.1**

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 pour déposer la demande d'ouverture de la procédure de sécurité pour le sous-contractant auprès du service spécialisé PSE (art. 4, al. 1, let. c).

Art. 13 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 sécuritaire de l'entreprise.

A. 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 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. 14 Contenu et examen du plan de sécurité

Al. 1 – L'examen mené sur place garantit que les mesures du plan de sécurité nécessaires, appropriées et adaptées à la situation peuvent être imposées à l'entreprise de façon ciblée. Il favorise la sécurité de l'information tout en épargnant à l'entreprise une charge de travail disproportionnée.

A. 2 – Le service spécialisé PSE donne à l'entreprise un cadre pour l'élaboration du 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 (p. ex. gestion des clés, surveillance des locaux), personnelles (contrôles de sécurité relatifs aux personnes), techniques (p. ex. utilisation des moyens informatiques) et physiques (protection contre les effractions).

Al. 3 – L'élaboration de plans de sécurité peut s'avérer complexe, notamment parce qu'une certaine marge de manœuvre doit être accordée à l'entreprise. Si le plan de sécurité proposé ne passe pas d'emblée l'examen du service spécialisé PSE (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. 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 de façon exhaustive 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

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 prévu 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 de 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 – L'action dès un premier soupçon, sans attendre les conséquences d'un incident, peut favoriser une intervention en temps utile. Ainsi, un tel soupçon est réputé soumis à l'obligation d'annoncer.

Al. 4 – 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 pour les 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. 5 – Cette disposition doit permettre d'éviter qu'une déclaration de sécurité relative aux entreprises arrive à expiration durant un mandat en cours, que le rapport contractuel devienne subitement illicite et qu'il doive donner lieu à une rédhibition. La situation peut être contournée 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 d'urgence incombe également à l'adjudicateur.

Al. 2, let. a – Les faits cités 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 d'annuler 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 les commentaires ci-avant sur la let. b.

Art. 19 Certificat international de sécurité

Al. 1 – L'établissement d'un certificat international de sécurité est un acte administratif sans spécificités et charges significatives, c'est pourquoi une taxe forfaitaire de 100 francs est prélevée.

Al. 2 – Il en va autrement lorsque l'entreprise n'est pas encore au bénéfice d'une déclaration de sécurité suisse. La réalisation nécessaire au préalable de la procédure de sécurité relative aux entreprises représente une charge dans laquelle le temps consacré à la procédure doit être pris en compte. La marge tarifaire à ce sujet 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 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 faits répréhensibles constatés 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 prononcées les décisions prises sur 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 annuler l'adjudication (décision), ce qui s'ensuit par la résiliation d'un contrat de droit privé. 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. 2c, de la loi du 20 décembre 1968 sur la procédure administrative[41]. La décision peut ainsi être exécutée sans retard. 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 pour 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 concilie les deux procédures de recours. À la demande d'une partie, les demandes de droit civil peuvent aussi être examinées dans la même procédure (art. 40, al. 1, de la loi du 17 juin 2005 sur le Tribunal administratif fédéral[42]).

Al. 3 – Ce délai d'ordre doit 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 (art. 65 LSI), l'ensemble de la procédure (y compris l'examen d'aptitude) 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 procédure de répétition, 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 arrêtée pour d'autres raisons. Il s'agit de décisions qui, toutes, mettent un terme au prolongement de la durée de validité selon l'al. 2. La rédhibition des rapports juridiques suit les règles applicables en cas de révocation de la déclaration de sécurité (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 correspondante se trouve dans l'annexe de l'OPSE.

Art. 23 Contrôle périodique du traitement des données personnelles

Le système d'information au sens de l'art. 70, al. 1, LSI, qui est utilisé pour la procédure de sécurité relative aux entreprises, peut, selon les circonstances, contenir des données personnelles sensibles. Il convient donc de le soumettre à un organe de surveillance indépendant. Le

[41] RS **172.021**
[42] RS **173.32**

département compétent dispose d'un certain pouvoir d'appréciation quant au choix de l'organe de révision.

Section 7 Dispositions finales

Art. 24 Abrogation et modification d'autres actes

A. 1 – La procédure de sauvegarde du secret uniquement applicable au sein du DDPS est réglée par l'ordonnance concernant la sauvegarde du secret. La procédure de sécurité relative aux entreprises applicable à l'échelle fédérale couvre la matière normative de l'ordonnance concernant la sauvegarde du secret et peut donc être abrogée sans être remplacée.

Al. 2 – L'ORMI renvoie à l'ordonnance concernant la sauvegarde du secret à abroger, ce qui doit être rectifié.

Al. 3 – 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 l'effectue dans l'annexe 3 de l'ordonnance du 16 août 2017 sur le service de renseignement[43] qui ne mentionne pas encore le service spécialisé PSE. Le ch. 10.6 y remédie ; quant au ch. 10.5, seul un changement d'ordre typographique est apporté.

Al. 4 – Les art. 3 et 6 de l'ordonnance sur la sécurité militaire du 21 novembre 2018[44] (OSM) attribuent aux organes de la sécurité militaire certaines tâches en lien avec l'industrie qui, d'après le nouveau droit, sont du ressort exclusif du service spécialisé PSE. Les dispositions correspondantes doivent donc être biffées (art. 3 OSM) ou reformulées (art. 6 OSM).

Al. 5 – L'art. 68 et l'annexe 31 de l'OSIAr peuvent être abrogés. Leur contenu est désormais repris dans l'art. 22 et l'annexe de l'OPSE.

Art. 25 Dispositions transitoires

Une rétroactivité sur des mandats qui ont été attribués avant l'entrée en vigueur de l'OPSE pourrait modifier les conditions de l'appel d'offres et de l'adjudication du mandat, ce qui pourrait entraîner au final son annulation, 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'OPSE. Les déclarations de sécurité établies d'après l'ancien droit resteront valables pendant cinq ans après leur établissement (art. 90, al. 3, LSI).

Art. 26 Entrée en vigueur

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

Annexe

L'annexe comporte désormais les données du Système d'information sur le contrôle de sécurité industrielle qui ont été retirées de l'OSIAr, conformément à l'art. 26, al. 5, OPSE.

5 Conséquences sur le personnel et les finances

5.1 Conséquences pour la Confédération

a. SMSI et gestion de la sécurité de l'information (art. 5 à 15 OSI)

La mise en place et l'introduction d'un SMSI *light* par les offices (et la ChF) entraîneront une charge de travail initiale unique modérée équivalent à 0.5 place à plein-temps (FTE) en moyenne. Cette charge de travail « de projet » se répartira au sein de l'office sur plusieurs services internes (notamment la direction de l'office, le service informatique, le service juridique, les ressources humaines et les responsables d'application). La majeure partie échoira aux préposés à la sécurité de l'information (art. 36 OSI). Pour un fonctionnement minimal correct du SMSI *light* au sein des offices, il faut compter pour les préposés à la sécurité de l'information sur une charge

[43] RS **121.1**
[44] RS **513.61**

supplémentaire d'environ 0,2 FTE par rapport à aujourd'hui. L'application SMSI (ch. 3.8) améliorera l'efficience du SMSI.

Les offices n'auront pas tous la même charge de travail supplémentaire. En effet, les départements et les offices peuvent définir un niveau d'ambition supérieur, avec les répercussions correspondantes sur les coûts. Par ailleurs, certains offices et départements répondent déjà aux consignes : armasuisse, swisstopo, l'OFSPO, l'OFIT et ASTRA sont, par exemple, des offices certifiés ISO. Le DDPS applique un SMSI complet depuis plusieurs années déjà. Le DFI a aussi décidé de demander à ses offices la mise en œuvre d'un SMSI.

b. Accréditation de sécurité de moyens informatiques (art. 23 OSI)

La charge de travail associée à l'accréditation de moyens informatiques ne peut pas encore être chiffrée. Il s'agit d'une nouvelle tâche pour laquelle l'administration fédérale n'a pas encore de recul. Après l'ouverture de la procédure de consultation, le Conseil fédéral examinera les compétences et les ressources nécessaires à l'accomplissement de cette tâche.

c. Préposés à la sécurité de l'information des départements (art. 40 OSI)

Le nouveau droit accroîtra légèrement la charge de travail des préposés, soit 0,2 FTE. Cette charge supplémentaire est due en partie aux tâches de pilotage et de coordination définies dans la LSI. De plus, ils devront désormais approuver l'ouverture de CSP auprès des tiers qui ne sont pas pris en compte par la procédure de sécurité relative aux entreprises. Les départements qui attribuent de nombreux mandats sensibles auront une charge de travail légèrement supérieure.

d. Service spécialisé de la Confédération pour la sécurité de l'information (art. 41 OSI)

Les ressources de ce service ne seront établies qu'après la procédure de consultation (cf. ch. 3.8). Si des ressources supplémentaires devaient s'avérer nécessaires, ce qui n'est pas prévisible actuellement, la charge supplémentaire sera modérée.

e. Application des mesures techniques de sécurité et contrôle de celles-ci

Les coûts de l'application des mesures techniques de sécurité et leur contrôle, notamment dans le domaine de la cybersécurité, représentent aujourd'hui déjà des coûts normaux de projets et d'utilisation. Ils doivent être planifiés en conséquence et inscrits au budget ordinaire (art. 42 OSI), ce qui inclut les coûts de réalisation des contrôles et des audits selon l'art. 13 OSI et les contrôles d'efficacité selon l'art. 29, al. 3, OSI (art. 18, al. 3, LSI).

f. Modification de l'OIAM

Le champ d'application de l'OIAM s'étend aux unités administratives de l'administration fédérale décentralisée. Si ces dernières veulent utiliser un système IAM, elles devront répondre aux exigences de l'OIAM. Les coûts correspondants doivent être planifiés dans ce cadre et inscrits au budget ordinaire.

g. Ordonnance sur les contrôles de sécurité relatifs aux personnes

Les indications détaillées sur la charge de travail liée aux CSP ne seront disponibles qu'après la procédure de consultation, car les listes de fonctions déterminantes seront établies à partir de l'ouverture de la consultation.

h. Ordonnance sur la procédure de sécurité relative aux entreprises

Pour la réalisation de la procédure de sécurité relative aux entreprises, le DDPS a déjà augmenté les ressources du service spécialisé chargé de cette procédure de 1,5 équivalent plein temps. Aucune ressource supplémentaire n'est nécessaire.

5.2 Conséquences pour les cantons

Les coûts de mise en œuvre par les cantons sont encore incertains. L'application de la LSI et des ordonnances au niveau des cantons est toutefois limitée. Ces coûts s'appliqueront majoritairement dans le cadre de projets ou lors du recours à des prestations de la Confédération. Ils devront être évalués dans ce contexte. Les séances de travail avec les cantons ont montré que la pratique était hétérogène. Évaluer la charge pour les cantons est un objectif important de la consultation.

5.3 Conséquences pour les milieux économiques

Les conséquences pour les milieux économiques ont été présentées dans le message LSI. Elles sont très faibles. Les milieux économiques sont concernés par la LSI et ses dispositions

d’exécution lorsqu’ils travaillent pour la Confédération. Les autorités fédérales s’engagent à préciser la garantie de la sécurité de l’information dans le cadre de la collaboration avec des tiers et à veiller à un contrôle approprié du respect des consignes. La fiabilité des entreprises à qui des mandats sensibles de la Confédération sont confiés sera examinée dans le cadre de la procédure de sécurité relative aux entreprises (ch. 4.4, commentaire de l’OPSE), puis contrôlée régulièrement. Les coûts de la procédure s’élèvent généralement à moins de 0,5 % du volume du marché et sont directement ou indirectement répercutés sur l’adjudicateur. Quelque 700 entreprises sont concernées par ce contrôle. Les conséquences pour les milieux économiques restent donc globalement très faibles.

5.4 Autres conséquences

Les ordonnances n’ont pas de conséquences sur la société, l’environnement ou d’autres domaines importants. Elles révèlent clairement, dans un sens positif, quelles mesures de sécurité sont nécessaires à l’ère numérique pour garantir la sécurité de la Confédération, et dès lors de la Suisse.