Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Projet

Loi fédérale sur la sécurité de l'information au sein de la Confédération

(Loi sur la sécurité de l'information, LSI)

du …

L'Assemblée fédérale de la Confédération suisse,
vu les art. 54, al. 1, 60, al. 1, 101, 102, al. 1, et 173, al. 1, let. a et b, et 2, de la Constitution[1],
vu le message du Conseil fédéral du 22 février 2017[2],
arrête:

Chapitre 1 Dispositions générales

Art. 1 But

[1] La présente loi vise à garantir la sécurité du traitement des informations relevant de la compétence de la Confédération et la sécurité de ses moyens informatiques.

[2] Elle vise ainsi à protéger les intérêts publics suivants:

a. la capacité de décision et d'action des autorités et organisations de la Confédération;

b. la sécurité intérieure et extérieure de la Suisse;

c. les intérêts de la politique extérieure de la Suisse;

d. les intérêts économiques, financiers et monétaires de la Suisse;

e. l'accomplissement des obligations légales et contractuelles des autorités et organisations de la Confédération en matière de protection des informations.

Art. 2 Autorités et organisations concernées

[1] La présente loi s'applique aux autorités suivantes:

a. l'Assemblée fédérale;

b. le Conseil fédéral;

RS …
1 RS **101**
2 FF **2017** 2765

c. les tribunaux fédéraux;

d. le Ministère public de la Confédération et son autorité de surveillance;

e. la Banque nationale suisse.

2 Elle s'applique également aux organisations suivantes:

a. les Services du Parlement;

b. l'administration fédérale;

c. les services administratifs des tribunaux fédéraux;

d. l'armée;

e. les organisations visées à l'art. 2, al. 4, de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[3], pour leurs tâches administratives.

3 Le Conseil fédéral peut restreindre le champ d'application de la présente loi pour les organisations au sens de l'art. 2, al. 3 et 4, LOGA à celles qui:

a. exercent des activités sensibles, ou

b. recourent ou accèdent à des moyens informatiques de la Confédération dans l'accomplissement de leurs tâches.

4 Il peut limiter à certaines dispositions de la présente loi le champ d'application au sens de l'al. 3. Il tient compte à cet égard de l'autonomie d'exécution des organisations concernées selon les actes organisationnels qui les régissent.

5 Les organisations de droit public ou privé qui exploitent des infrastructures critiques sans être visées par les al. 1 à 3 sont soumises aux art. 75 à 81. La législation spéciale peut prévoir que d'autres dispositions de la présente loi leur sont applicables.

Art. 3 Application de la loi aux cantons

1 Les dispositions relatives aux informations classifiées et à la sécurité des moyens informatiques s'appliquent aux cantons dans la mesure où ces derniers traitent des informations classifiées de la Confédération ou accèdent à ses moyens informatiques dans le cadre de leur collaboration avec la Confédération ou de l'exécution du droit fédéral.

2 Elles ne s'appliquent pas lorsque les cantons garantissent une sécurité au moins équivalente de l'information.

Art. 4 Rapport avec d'autres lois fédérales

1 La loi du 17 décembre 2004 sur la transparence[4] prime la présente loi.

2 Lorsque la protection d'informations est également réglée dans d'autres lois fédérales, les dispositions de la présente loi s'appliquent à titre complémentaire.

3 RS **172.010**
4 RS **152.3**

Art. 5 Définitions

On entend par:

a. *moyen informatique:* moyen relevant des techniques de l'information et de la communication, notamment les applications, les systèmes d'information et les fichiers, ainsi que les installations, les produits et les services servant au traitement électronique des informations;

b. *activité sensible:*
   1. le traitement d'informations classifiées «confidentiel» ou «secret»,
   2. l'administration, l'exploitation, la maintenance et le contrôle de moyens informatiques relevant des catégories de sécurité «protection élevée» ou «protection très élevée»,
   3. l'accès à des zones de sécurité, en particulier aux zones de protection 2 ou 3 d'une installation au sens de la législation sur la protection des ouvrages militaires;

c. *infrastructure critique:* infrastructure d'information, de communication, d'énergie, de transport ou autre indispensable au fonctionnement de la société civile, de l'économie et de l'État.

Chapitre 2 Mesures générales

Section 1 Principes

Art. 6 Sécurité de l'information

1 Les autorités et organisations soumises à la présente loi veillent à ce que le besoin de protection des informations relevant de leur compétence soit évalué en fonction de l'atteinte potentielle aux intérêts définis à l'art. 1, al. 2.

2 Elles veillent à ce que les informations, en fonction de leur besoin de protection:

a. ne soient accessibles qu'aux personnes autorisées (confidentialité);

b. soient disponibles en cas de besoin (disponibilité);

c. ne puissent être modifiées sans droit ou par mégarde (intégrité);

d. soient traitées de manière à être traçables (traçabilité).

3 Elles veillent à ce que les moyens informatiques auxquels elles recourent pour accomplir leurs tâches légales soient protégés contre les utilisations abusives et les perturbations.

4 Elles tiennent compte à cet égard des principes de la proportionnalité, de l'économicité et de la simplicité d'emploi.

Art. 7 Responsabilité des autorités soumises à la présente loi

[1] Les autorités soumises à la présente loi veillent, chacune dans son domaine de compétence, à ce que la sécurité de l'information soit organisée, mise en œuvre et contrôlée conformément à l'état des connaissances scientifiques et techniques.

[2] Elles fixent:

a. leurs objectifs en matière de sécurité de l'information;

b. les principes de gestion des risques;

c. les conséquences d'une violation des prescriptions.

Art. 8 Gestion des risques

[1] Les autorités et organisations soumises à la présente loi veillent, chacune dans son domaine de compétence, à ce que les risques en matière de sécurité de l'information soient constamment évalués.

[2] Elles prennent les mesures nécessaires pour éliminer les risques ou les ramener à un niveau acceptable.

[3] Les risques jugés acceptables doivent être formellement acceptés.

Art. 9 Collaboration avec les tiers

[1] Lorsque les autorités et organisations soumises à la présente loi collaborent avec des tiers, elles veillent à ce que les exigences et mesures prévues par la présente loi soient reprises dans les accords et les contrats qu'ils concluent à cet effet.

[2] Elles veillent à ce que la mise en œuvre des mesures soit contrôlée de manière adéquate.

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

[1] Les autorités et organisations soumises à la présente loi veillent à ce que les violations de la sécurité de l'information soient décelées rapidement, leurs causes clarifiées et leurs conséquences limitées au maximum.

[2] Les autorités soumises à la présente loi veillent à établir des plans d'action dans l'éventualité de graves violations de la sécurité de l'information susceptibles de menacer l'accomplissement de tâches indispensables de la Confédération; elles organisent des exercices à cet effet.

Section 2 Classification des informations

Art. 11 Principes régissant la classification

[1] Les autorités et organisations soumises à la présente loi veillent à ce que les informations qui remplissent les critères définis à l'art. 13 soient classifiées.

[2] La classification doit se limiter au strict nécessaire et être si possible temporaire.

Art. 12 Compétences

1 Les autorités soumises à la présente loi désignent les personnes ou services compétents pour classifier les informations (auteurs de la classification).

2 Seuls l'auteur de la classification ou les services auxquels il est subordonné peuvent modifier ou supprimer une classification.

3 Le Conseil fédéral règle la déclassification des archives.

Art. 13 Échelons de classification

1 Les informations susceptibles de nuire aux intérêts définis à l'art. 1, al. 2, let. a à d, si elles sont portées à la connaissance d'une personne non autorisée sont classifiées «interne».

2 Les informations susceptibles de nuire considérablement aux intérêts définis à l'art. 1, al. 2, let. a à d, si elles sont portées à la connaissance d'une personne non autorisée sont classifiées «confidentiel».

3 Les informations susceptibles de nuire gravement aux intérêts définis à l'art. 1, al. 2, let. a à d, si elles sont portées à la connaissance d'une personne non autorisée sont classifiées «secret».

4 Les échelons de classification sont indiqués en lettres majuscules sur les informations classifiées.

Art. 14 Accès aux informations classifiées

1 Seules peuvent accéder aux informations classifiées les personnes qui offrent toutes les garanties qu'elles les traiteront correctement et qui remplissent l'une des conditions suivantes:

a. elles ont besoin des informations en question pour accomplir une tâche légale;

b. elles disposent d'une autorisation d'accès qui leur a été conférée contractuellement et elles ont besoin des informations en question pour accomplir les tâches qui leur ont été confiées.

2 L'accès aux archives classifiées est réglé par la législation sur l'archivage.

3 Les limitations d'accès prévues dans des traités internationaux au sens de l'art. 88 sont réservées.

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

1 L'accès à des informations classifiées relevant de l'Assemblée fédérale, des Services du Parlement, des tribunaux et des ministères publics est régi par le droit de procédure applicable.

2 Avant toute décision donnant accès à une information au sens de l'al. 1, l'organe parlementaire ou le tribunal compétent peut consulter l'auteur de la classification.

Section 3 Sécurité des moyens informatiques

Art. 16 Procédure de sécurité

1 Pour garantir la sécurité de l'information lors de l'utilisation de moyens informatiques, les autorités soumises à la présente loi élaborent, chacune dans son domaine de compétence, une procédure de sécurité.

2 La procédure de sécurité définit:

a. les critères permettant d'évaluer le besoin de protection des informations avant la mise en service des moyens informatiques;

b. les modalités de mise en œuvre des mesures de sécurité et leur contrôle;

c. la compétence d'autoriser les moyens informatiques;

d. la procédure à suivre en cas de modification des risques.

3 L'exécution de la procédure de sécurité incombe aux autorités et organisations soumises à la présente loi qui décident de l'engagement de moyens informatiques.

Art. 17 Catégories de sécurité

1 Les moyens informatiques relèvent de la catégorie de sécurité «protection de base», à moins qu'ils relèvent d'une catégorie de sécurité supérieure.

2 Ils relèvent de la catégorie de sécurité «protection élevée» dans les cas suivants:

a. une violation de la confidentialité, de la disponibilité, de l'intégrité ou de la traçabilité des informations qu'ils servent à traiter risque de nuire considérablement aux intérêts définis à l'art. 1, al. 2;

b. leur utilisation abusive ou leur perturbation sont susceptibles de nuire considérablement aux intérêts définis à l'art. 1, al. 2.

3 Ils relèvent de la catégorie de sécurité «protection très élevée» dans les cas suivants:

a. une violation de la confidentialité, de la disponibilité, de l'intégrité ou de la traçabilité des informations qu'ils servent à traiter risque de nuire gravement aux intérêts définis à l'art. 1, al. 2;

b. leur utilisation abusive ou leur perturbation sont susceptibles de nuire gravement aux intérêts définis à l'art. 1, al. 2.

Art. 18 Mesures de sécurité

1 Les autorités soumises à la présente loi fixent les exigences de sécurité minimales applicables aux catégories de sécurité définies à l'art. 17.

2 Tous les moyens informatiques doivent satisfaire aux exigences minimales de la catégorie de sécurité «protection de base».

3 L'efficacité des mesures applicables aux moyens informatiques de la catégorie de sécurité «protection très élevée» doit faire l'objet de contrôles périodiques.

Art. 19 Sécurité de l'exploitation de moyens informatiques

1 Les autorités et organisations soumises à la présente loi garantissent la sécurité des moyens informatiques qu'elles exploitent pour elles-mêmes ou sur mandat d'une autre autorité ou organisation.

2 Les art. 57*i* à 57*q* LOGA[5] s'appliquent par analogie au traitement des données personnelles dans le cadre de la surveillance des réseaux.

Section 4 Mesures relatives aux personnes

Art. 20 Conditions d'accès aux informations et aux moyens informatiques de la Confédération

1 Les autorités et organisations soumises à la présente loi veillent à ce que les personnes qui accèdent à des informations, des moyens informatiques, des locaux et d'autres infrastructures de la Confédération:

a. soient choisies avec soin;

b. soient identifiées en fonction de la sensibilité de l'activité concernée;

c. reçoivent une formation et une formation continue adaptées à leur niveau de responsabilité;

d. soient le cas échéant tenues contractuellement au maintien du secret.

2 Elles peuvent recourir à des méthodes biométriques de vérification pour identifier les personnes, si la sensibilité de l'activité concernée le requiert. Les données biométriques sont détruites à l'échéance de l'autorisation d'accès.

Art. 21 Délivrance restrictive des autorisations

1 Les autorités et organisations soumises à la présente loi veillent à ce que des autorisations d'accès à des informations, des moyens informatiques, des locaux ou d'autres infrastructures de la Confédération ne soient délivrées qu'aux personnes qui en ont besoin pour accomplir leurs tâches.

2 Les autorisations sont retirées à la fin de l'engagement ou du contrat ou dès que la tâche concernée a été exécutée. Elles peuvent être bloquées ou retirées sans préavis lorsque des indices concrets donnent à penser que la sécurité est menacée.

5 RS **172.010**

Section 5 Protection physique

Art. 22 Principe

Les autorités et organisations soumises à la présente loi veillent à assurer une protection physique adéquate des informations et moyens informatiques dont elles sont responsables contre les utilisations abusives et les perturbations.

Art. 23 Zones de sécurité

1 Les autorités et organisations soumises à la présente loi peuvent instituer des zones de sécurité dans des locaux ou des espaces dans les cas suivants:

a. des informations classifiées «confidentiel» ou «secret» y sont fréquemment traitées;

b. des moyens informatiques des catégories de sécurité «protection élevée» ou «protection très élevée» y sont exploités.

2 Elles peuvent prendre les mesures suivantes dans les zones de sécurité:

a. soumettre certains objets à autorisation , en particulier les appareils de prises de vue et de son;

b. surveiller les secteurs sensibles avec des appareils de prises de vue;

c. procéder à des fouilles;

d. procéder à des contrôles inopinés, même en l'absence des employés.

3 Elles peuvent au surplus exploiter, conformément à l'art. 34, al. 1ter, de la loi du 30 avril 1997 sur les télécommunications[6], une installation perturbatrice dans les zones de sécurité où des informations classifiées «secret» sont fréquemment traitées ou des moyens informatiques de la catégorie de sécurité «protection très élevée» sont exploités.

4 Les dispositions particulières relatives aux zones de sécurité établies en vertu des traités internationaux au sens de l'art. 88 et les dispositions applicables aux zones de protection des installations au sens de la législation sur la protection des ouvrages militaires sont réservées.

Section 6 Systèmes de gestion des données d'identification

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

1 Les autorités soumises à la présente loi peuvent exploiter des systèmes permettant une gestion centralisée des données servant à identifier les personnes qui ont accès aux informations, aux moyens informatiques, aux locaux et à d'autres infrastructures (systèmes de gestion des données d'identification).

6 RS **784.10**

2 Les systèmes de gestion des données d'identification vérifient l'identité des personnes et les critères d'accès aux machines et aux systèmes. Ils transmettent le résultat aux systèmes d'information raccordés pour la délivrance des autorisations.

3 Les autorités soumises à la présente loi désignent un service responsable pour chaque système de gestion des données d'identification.

Art. 25 Échange et harmonisation des données

1 Les systèmes de gestion des données d'identification permettent d'échanger des données et de les harmoniser avec les systèmes d'information raccordés, avec les répertoires de personnes et d'utilisateurs et avec d'autres systèmes de gestion des données d'identification exploités par des autorités soumises à la présente loi.

2 L'échange et l'harmonisation sont limités aux données dont le traitement est autorisé dans le système concerné.

Art. 26 Utilisation du numéro AVS

1 Le service responsable peut utiliser temporairement le numéro AVS prévu à l'art. 50c de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants[7] dans le système de gestion des données d'identification des personnes pour générer un numéro personnel dérivé du numéro AVS selon un processus unidirectionnel et irréversible.

2 Le numéro AVS est effacé dès la création du numéro personnel dérivé.

Art. 27 Dispositions d'exécution

Les autorités soumises à la présente loi édictent des dispositions d'exécution notamment dans les domaines suivants:

a. la protection et la sécurité des données;

b. les données personnelles traitées;

c. l'échange et l'harmonisation des données avec d'autres systèmes;

d. la journalisation et la transmission des données de journalisation aux systèmes d'information raccordés;

e. le contrôle périodique réalisé par un organe indépendant du traitement des données personnelles.

7 RS **831.10**

Chapitre 3 Contrôle de sécurité relatif aux personnes
Section 1 Dispositions générales

Art. 28 But et objet du contrôle

1 Le contrôle de sécurité relatif aux personnes vise à déterminer si l'exercice d'une activité sensible par une personne dans le cadre de sa fonction ou d'un mandat pose un risque pour la sécurité de l'information.

2 À cette fin, les services compétents collectent des données pertinentes pour la sécurité touchant au mode de vie de la personne concernée, notamment à ses liaisons personnelles étroites et à ses relations familiales, à sa situation financière et à ses rapports avec l'étranger.

3 Les données sur l'exercice des droits constitutionnels ne peuvent être traitées que s'il existe un soupçon concret que la personne soumise au contrôle exerce ces droits pour préparer ou accomplir des actes susceptibles de nuire considérablement aux intérêts définis à l'art. 1, al. 2.

Art. 29 Liste des fonctions

1 Les autorités soumises à la présente loi édictent, chacune dans son domaine de compétence, une liste des fonctions qui impliquent l'exercice d'une activité sensible.

2 Elles contrôlent périodiquement l'exactitude de la liste et y apportent les corrections nécessaires.

Art. 30 Personnes soumises au contrôle

1 Les personnes suivantes sont soumises à un contrôle de sécurité:

a. les personnes qui exercent une fonction figurant sur l'une des listes visées à l'art. 29;

b. les personnes engagées par un canton qui exercent une activité sensible dans le cadre de la collaboration avec la Confédération ou dans l'exécution du droit fédéral;

c. les personnes qui exécutent pour une autorité ou une organisation soumise à la présente loi un mandat qui implique l'exercice d'une activité sensible;

d. les personnes soumises à un contrôle de sécurité en vertu d'un traité international au sens de l'art. 88.

2 Toute personne appelée à exercer une activité sensible pour le compte d'une autorité étrangère ou d'une organisation internationale est soumise à un contrôle de sécurité pour autant que la Suisse ait conclu un traité international au sens de l'art. 88 avec l'État ou l'organisation internationale en question.

3 Les personnes qui exercent une fonction qui ne figure pas encore sur l'une des listes visées à l'art. 29 peuvent exceptionnellement, sur approbation de l'autorité concernée, être soumises à un contrôle de sécurité. La liste des fonctions doit être complétée dès que possible.

4 Les candidats aux fonctions suivantes ne sont pas soumises à un contrôle de sécurité:

a. membre de l'Assemblée fédérale;

b. membre du Conseil fédéral et chancelier de la Confédération;

c. juge auprès d'un tribunal fédéral;

d. procureur de la Confédération;

e. membre de l'autorité de surveillance du Ministère public de la Confédération;

f. général;

g. membre d'un gouvernement cantonal et juge auprès d'un tribunal cantonal.

Art. 31 Degrés de contrôle

Les autorités soumises à la présente loi attribuent les degrés de contrôle suivants aux activités sensibles définies ci-après:

a. contrôle de sécurité de base: activités sensibles dont l'exercice inadéquat ou contraire aux prescriptions est susceptible de nuire considérablement aux intérêts définis à l'art. 1, al. 2;

b. contrôle de sécurité élargi: activités sensibles dont l'exercice inadéquat ou contraire aux prescriptions est susceptible de nuire gravement aux intérêts définis à l'art. 1, al. 2.

Section 2 Procédure

Art. 32 Services compétents

1 Les autorités soumises à la présente loi et les cantons désignent les services qui ont les compétences suivantes:

a. ouvrir la procédure du contrôle de sécurité;

b. décider de confier l'activité sensible (instances décisionnelles).

2 Le Conseil fédéral met en place un ou plusieurs services spécialisés chargés de réaliser les contrôles de sécurité relatifs aux personnes (services spécialisés CSP). Ces derniers réalisent l'évaluation du risque pour la sécurité sans aucune instruction.

Art. 33 Consentement et collaboration

1 Aucun contrôle de sécurité ne peut être réalisé sans le consentement de la personne soumise au contrôle.

2 Les conscrits, les militaires et les membres de la protection civile peuvent être soumis à un contrôle de sécurité sans leur consentement.

3 La personne soumise au contrôle est tenue de collaborer à l'établissement des faits.

Art. 34 Moment du contrôle

1 Pour les personnes visées à l'art. 30, al. 1, let. a et b, la procédure de contrôle de sécurité doit être ouverte avant l'attribution de la fonction.

2 Pour les personnes visées à l'art. 30, al. 1, let. a, qui doivent être nommées par le Conseil fédéral, le contrôle de sécurité doit être achevé avant le dépôt de la proposition de nomination.

3 Pour les personnes visées à l'art. 30, al. 1, let. c, le contrôle de sécurité doit être achevé avant que l'activité sensible ne leur soit confiée.

4 Pour les personnes visées à l'art. 30, al. 1, let. d, le contrôle de sécurité a lieu au moment prévu par le traité applicable.

Art. 35 Collecte des données

1 Les services spécialisés CSP peuvent collecter les données suivantes relatives à une personne pour réaliser un contrôle de sécurité de base:

a. données du casier judiciaire;

b. données sur des procédures pénales en cours, classées ou suspendues, auprès des autorités pénales;

c. données nécessaires à l'évaluation du risque, auprès des organes de sécurité de la Confédération, du Service de renseignement de la Confédération (SRC), des organes de l'armée et d'autres organes de la Confédération;

d. données des registres et dossiers des organes de sécurité des cantons et des organes de police;

e. données des registres des offices des poursuites et des faillites;

f. données des dossiers établis lors de contrôles de sécurité antérieurs;

g. données de sources d'information publiques.

2 Ils peuvent au surplus collecter les données suivantes relatives à une personne pour réaliser un contrôle de sécurité élargi:

a. données détenues par les autorités fiscales fédérales et cantonales;

b. données du registre du contrôle des habitants;

c. données détenues par les établissements financiers et banques entretenant des relations d'affaires avec la personne concernée;

d. données fournies par la personne concernée au cours d'une audition.

3 Lorsque des indices concrets fondés sur les données collectées donnent à penser qu'il existe un risque pour la sécurité ou lorsque les données collectées sont insuffisantes ou ne s'étendent pas sur une période suffisante pour réaliser le contrôle, les services spécialisés CSP peuvent auditionner la personne concernée. Ils peuvent également interroger des tiers moyennant le consentement de la personne soumise au contrôle de sécurité; ils indiquent aux tiers concernés qu'ils sont libres de donner des renseignements ou non.

4 Les données relatives à des tiers qui sont indissociables des données relatives à la personne soumise au contrôle de sécurité peuvent être traitées si elles sont indispensables pour réaliser le contrôle. Les services spécialisés CSP informent les tiers concernés du traitement de leurs données.

Art. 36 Assistance administrative

1 L'autorité ou l'organisation concernée au sens de l'art. 35 collecte les données détenues par une autorité étrangère ou une organisation internationale.

2 Lorsque les données collectées fournissent des indices concrets de crime organisé ou de criminalité internationale, le service spécialisé CSP consulte les Offices centraux de police criminelle de la Confédération. Les offices centraux ne communiquent au service spécialisé CSP que les données personnelles pertinentes pour la sécurité.

Art. 37 Prise en charge des coûts

1 Les autorités et organisations de droit public auprès desquelles les services spécialisés CSP peuvent collecter des données ou qui sont tenues de participer à la procédure prêtent leur concours gratuitement.

2 Les tiers auxquels la procédure occasionne une charge considérable sont indemnisés.

3 La Confédération supporte les coûts du contrôle pour les employés des cantons visés à l'art. 30, al. 1, let. b.

Art. 38 Classement de la procédure

1 Les services spécialisés CSP classent la procédure lorsque la personne concernée revient sur son consentement ou qu'elle n'entre plus en considération pour exercer la fonction prévue ou pour exécuter le mandat.

2 Ils notifient le classement de la procédure à la personne concernée et au service qui a demandé son ouverture. La personne concernée est réputée ne pas avoir été contrôlée.

Section 3 Évaluation du risque pour la sécurité

Art. 39 Risque pour la sécurité

1 Il existe un risque pour la sécurité lorsque des indices concrets fondés sur les données collectées laissent supposer avec une probabilité élevée que la personne contrôlée exécutera l'activité sensible de manière inadéquate ou contraire aux prescriptions.

2 La probabilité d'un exercice inadéquat ou contraire aux prescriptions d'une activité sensible peut notamment être jugée élevée lorsque des indices donnent à penser que la personne présente l'une des caractéristiques suivantes:

a. elle manque d'intégrité ou de loyauté;

b. elle est susceptible de céder au chantage ou à la corruption;

c. elle ne dispose pas d'une pleine capacité de jugement ou de décision.

3 L'évaluation doit se fonder sur des faits concernant la situation personnelle de la personne soumise au contrôle, indépendamment de toute faute commise.

Art. 40 Résultat de l'évaluation

1 Les services spécialisés CSP rendent l'une des déclarations suivantes, qui a la signification indiquée ci-après:

a. déclaration de sécurité: il n'existe aucun risque pour la sécurité;

b. déclaration de sécurité sous réserve: il existe un risque pour la sécurité, mais celui-ci peut être ramené à un niveau acceptable en respectant certaines conditions; les services spécialisés CSP recommandent les conditions à fixer;

c. déclaration de risque: il existe un risque pour la sécurité;

d. constatation: les données sont insuffisantes ou ne s'étendent pas sur une période suffisante pour évaluer le risque pour la sécurité.

2 Dans les cas visés à l'al. 1, let. b à d, ils donnent au préalable la possibilité à la personne soumise au contrôle de donner son avis.

Art. 41 Notification

1 Les services spécialisés CSP notifient par écrit à la personne concernée et à l'instance décisionnelle la déclaration qu'ils ont rendue.

2 Pour les nominations par le Conseil fédéral, les services spécialisés CSP notifient leur déclaration au département qui propose la nomination.

3 Ils peuvent notifier la déclaration à une autre instance décisionnelle dans les cas suivants:

a. la personne soumise au contrôle est appelée à exercer une autre activité sensible au sens de la présente loi qui requiert un contrôle de sécurité;

b. la personne est soumise à un contrôle de loyauté en vertu d'une autre loi fédérale;

c. le potentiel de violence de la personne doit être évalué en vertu de l'art. 113 de la loi du 3 février 1995 sur l'armée[8].

4 Si les services spécialisés CSP disposent, avant la clôture de l'évaluation, d'indices concrets d'un risque pour la sécurité, ils peuvent communiquer leurs constatations intermédiaires par écrit aux autorités et instances visées aux al. 1 à 3 et à la personne contrôlée.

8 RS **510.10**

Section 4 Conséquences de la déclaration

Art. 42 Exercice de l'activité sensible

1 Les déclarations des services spécialisés CSP ont valeur de recommandation.

2 L'instance décisionnelle décide sur la base des résultats de l'évaluation si la personne contrôlée peut exercer l'activité sensible en question.

3 Elle peut fixer des conditions à l'exercice de l'activité.

4 Elle communique sa décision au service spécialisé CSP.

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

Il n'est pas nécessaire de réaliser un nouveau contrôle de sécurité lorsque la personne concernée a déjà obtenu une déclaration pour un degré de contrôle au moins équivalent:

a. en vue d'une autre activité sensible au sens de la présente loi;

b. dans le cadre d'un contrôle de loyauté en vertu d'une autre loi fédérale.

Art. 44 Répétition du contrôle

1 Le contrôle de sécurité relatif aux personnes est répété comme suit:

a. contrôle de sécurité de base: au plus tôt après cinq ans, au plus tard après dix ans;

b. contrôle de sécurité élargi: au plus tôt après trois ans, au plus tard après cinq ans.

2 Le Conseil fédéral peut prévoir qu'il n'est pas nécessaire de répéter le contrôle de sécurité de base pour les personnes exerçant certaines fonctions militaires ou certaines fonctions de la protection civile.

3 Lorsque le service qui a demandé le contrôle ou l'instance décisionnelle ont des raisons de penser que de nouveaux risques sont apparus depuis le dernier contrôle, ils peuvent demander la répétition du contrôle de sécurité au service spécialisé CSP compétent; ils motivent leur demande par écrit.

Art. 45 Voies de droit

1 La personne contrôlée dispose d'un délai de 30 jours à compter de la réception d'une déclaration au sens de l'art. 40, al. 1, pour utiliser les voies de droit suivantes:

a. consulter le dossier du contrôle;

b. demander la rectification des données erronées ou la destruction des données obsolètes;

c. demander que l'on ajoute à une donnée la mention de son caractère litigieux.

2 Les restrictions à la communication de renseignements sont régies par l'art. 9 de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[9].

3 La déclaration constitue un acte matériel au sens de l'art. 25*a* de la loi fédérale du 20 décembre 1968 sur la procédure administrative[10]. La personne contrôlée peut recourir contre une déclaration au sens de l'art. 40, al. 1, let. b à d, auprès du Tribunal administratif fédéral dans un délai de 30 jours à compter de sa notification.

4 Si l'instance décisionnelle est le Tribunal fédéral ou le Tribunal administratif fédéral, l'art. 36, al. 2 et 4, de la loi du 24 mars 2000 sur le personnel de la Confédération[11] s'applique par analogie.

5 La procédure de recours est régie au surplus par les dispositions générales de la procédure fédérale.

Section 5 Traitement des données personnelles

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

1 Les services spécialisés CSP exploitent un système d'information pour réaliser les contrôles de sécurité relatifs aux personnes.

2 Chaque service spécialisé CSP est responsable de la licéité du traitement des données personnelles qu'il effectue dans le système d'information.

3 Les données sensibles et les profils de la personnalité au sens de l'art. 3, let. c et d, LPD[12] peuvent être traités dans le système d'information dans la mesure où ils sont nécessaires à l'évaluation du risque pour la sécurité.

4 Le système d'information contient les données suivantes:

a. les données d'identité des personnes à contrôler ou des personnes qui ont été contrôlées, y compris le numéro AVS et le numéro de passeport;

b. les données visées aux art. 35 et 36;

c. les données relatives à l'évaluation du risque pour la sécurité;

d. le résultat de l'évaluation visé à l'art. 40, al. 1;

e. la décision de l'instance décisionnelle;

f. les données et les dossiers relatifs aux procédures de recours;

g. des listes et statistiques contenant les données visées aux let. a à f.

5 Le traitement des données visées à l'al. 4 en dehors du système d'information doit être mentionné dans le système.

9 RS **235.1**
10 RS **172.021**
11 RS **172.220.1**
12 RS **235.1**

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

a. casier judiciaire informatisé au sens des art. 365 à 371*a* du code pénal[13];

b. index national de police au sens de l'art. 17 de la loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération[14];

c. système d'indexation des données du SRC au sens de l'art. 51 de la loi fédérale du 25 septembre 2015 sur le renseignement[15].

Art. 47 Consultation et communication des données

1 Les organes suivants peuvent consulter en ligne les données ci-après contenues dans le système d'information:

a. les services qui ont demandé le contrôle: les données visées à l'art. 46, al. 4, let. b, qu'ils ont saisies eux-mêmes lors de l'ouverture de la procédure de contrôle, ainsi que les données visées à l'art. 46, al. 4, let. a, d et e;

b. les instances décisionnelles: les données visées à l'art. 46, al. 4, let. a, d et e;

c. les préposés à la sécurité de l'information au sens de l'art. 82, pour l'exécution de leurs tâches de contrôle: les données visées à l'art. 46, al. 4, let. a, d et e;

d. les services de la Confédération et des cantons auprès desquels les données visées à l'art. 38 sont collectées: les données visées à l'art. 46, al. 4, let. a.

2 Les organes suivants peuvent consulter les données ci-après contenues dans le système d'information:

a. le service spécialisé chargé de mener la procédure de sécurité relative aux entreprises (service spécialisé PSE) au sens de l'art. 52, al. 2, par une interface liée au système d'information visé à l'art. 71, pour mener la procédure de sécurité relative aux entreprises au sens des art. 50 à 74: les données visées à l'art. 46, al. 4, let. a, d et e;

b. le Groupement Défense:

1. par une interface liée au système d'information visé à l'art. 12 de la loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée (LSIA)[16], dans les buts définis à l'art. 13 LSIA: les données visées à l'art. 46, al. 4, let. a, d et e,

2. par une interface liée au système d'information visé à l'art. 18 LSIA, dans les buts définis à l'art. 19 LSIA: les données visées à l'art. 46, al. 4, let. a et e;

3. par une interface liée au système d'information visé à l'art. 156 LSIA, dans le but visé à l'art. 157 LSIA: les données visées à l'art. 46, al. 4, let. a et e,

13 RS **311.0**
14 RS **361**
15 RS **121**
16 RS **510.91**

4. par une interface liée au système d'information visé à l'art. 162 LSIA, dans le but visé à l'art. 163 LSIA: les données visées à l'art. 46, al. 4, let. a et e;

c. le service compétent pour délivrer des certificats internationaux de sécurité au sens de l'art. 49, let. c, par une interface: les données visées à l'art. 46, al. 4, let. a, d et e.

3 Les services spécialisés CSP peuvent au surplus communiquer électroniquement les données visées à l'art. 46, al. 4, let. a et e, à d'autres services de la Confédération dans la mesure où ces données sont nécessaires pour contrôler l'accès aux zones de sécurité.

4 Ils peuvent communiquer aux autorités et organisations soumises à la présente loi les listes et statistiques visées à l'art. 46, al. 1, let. g, dans la mesure où elles en ont besoin pour exécuter les tâches de contrôle prévues par la présente loi.

Art. 48 Conservation, archivage et destruction des données

1 Les services spécialisés CSP peuvent enregistrer les auditions visées à l'art. 35, al. 2, let. d, et 3, et conserver les enregistrements sur des supports appropriés.

2 Ils conservent les données aussi longtemps que la personne concernée exerce l'activité sensible, mais dix ans au plus.

3 L'archivage des données est régi par les dispositions de la législation relative à l'archivage.

4 Lorsque la procédure est classée ou que les services spécialisés CSP apprennent qu'une personne contrôlée n'occupe pas la fonction prévue ou a refusé d'exécuter le mandat prévu, ces derniers détruisent l'ensemble des données et dossiers relatifs à la procédure dans les trois mois.

Section 6 Dispositions édictées par le Conseil fédéral

Art. 49

Le Conseil fédéral règle:

a. les modalités de la procédure du contrôle de sécurité relatif aux personnes;

b. l'organisation des services spécialisés CSP;

c. les modalités de délivrance des certificats internationaux de sécurité;

d. les responsabilités en matière de protection des données traitées dans le système d'information visé à l'art. 46 et la sécurité des données;

e. les modalités du contrôle périodique réalisé par un organe indépendant du traitement des données personnelles.

Chapitre 4 Procédure de sécurité relative aux entreprises

Section 1 Dispositions générales

Art. 50 But de la procédure

La procédure de sécurité relative aux entreprises vise à préserver la sécurité de l'information lors de l'exécution de mandats publics par des entreprises, des parties d'entre elles ou des sous-contractants (entreprises), dans la mesure où ces mandats impliquent l'exercice d'une activité sensible (mandats sensibles).

Art. 51 Entreprises concernées

1 Les entreprises suivantes peuvent être soumises à la procédure de sécurité:

a. entreprises appelées à exécuter un mandat sensible pour le compte d'une autorité ou d'une organisation soumise à la présente loi;

b. entreprises dont le siège est en Suisse et qui soumissionnent pour des mandats dont l'exécution requiert un certificat international de sécurité au sens de l'art. 67.

2 La procédure ne peut être menée sans le consentement de l'entreprise concernée.

3 Les entreprises visées à l'al. 1, let. b, supportent les coûts de la procédure.

Art. 52 Classement de la procédure

1 La procédure de sécurité est classée dans les cas suivants:

a. l'entreprise concernée revient sur son consentement ou ne collabore pas à la procédure;

b. l'entreprise concernée retire son offre;

c. l'entreprise concernée n'entre plus en considération pour l'exécution du mandat.

2 Le service spécialisé chargé de mener la procédure de sécurité relative aux entreprises (service spécialisé PSE) notifie le classement de la procédure à l'entreprise et à l'autorité ou l'organisation qui attribue le mandat (adjudicateur).

Section 2 Ouverture de la procédure

Art. 53 Demande d'ouverture de la procédure

1 Lorsque les autorités et organisations soumises à la présente loi envisagent d'attribuer un mandat sensible, elles adressent au service spécialisé PSE une demande d'ouverture de la procédure.

2 Les autorités soumises à la présente loi désignent les services compétents pour demander l'ouverture de la procédure.

3 Les autorités étrangères ou organisations internationales doivent déposer elles-mêmes une demande pour les entreprises visées à l'art. 51, al. 1, let. b.

Art. 54 Examen de la demande

1 Le service spécialisé PSE examine la demande et ouvre la procédure.

2 Il peut renoncer, en accord avec l'adjudicateur, à ouvrir une procédure lorsque d'autres mesures permettent de ramener le risque pour la sécurité à un niveau acceptable. Il recommande les mesures à prendre.

Art. 55 Définition des exigences en matière de sécurité

Le service spécialisé PSE fixe, en accord avec l'adjudicateur, les exigences en matière de sécurité de l'information pour la procédure d'adjudication et la phase d'exécution du mandat.

Section 3 Évaluation des entreprises

Art. 56 Qualification

1 L'adjudicateur indique au service spécialisé PSE quelles entreprises entrent en considération pour l'exécution du mandat sensible.

2 Le service spécialisé PSE évalue si les entreprises concernées présentent les qualifications requises sous l'angle de la sécurité pour exécuter le mandat sensible ou s'il existe un risque pour la sécurité.

3 Il réalise l'évaluation sans aucune instruction.

Art. 57 Collecte des données

1 Pour évaluer la qualification d'une entreprise, le service spécialisé PSE peut collecter des données auprès des sources suivantes:

a. l'entreprise concernée;

b. le SRC;

c. toute source publique d'information.

2 Il peut demander à des services étrangers ou internationaux de lui transmettre des données. La demande est adressée par l'intermédiaire du SRC.

Art. 58 Évaluation du risque pour la sécurité

1 Il existe un risque pour la sécurité lorsque des indices concrets fondés sur les données collectées laissent supposer avec une probabilité élevée que l'entreprise exécutera le mandat sensible de manière inadéquate ou contraire aux prescriptions.

2 La probabilité d'une exécution inadéquate ou contraire aux prescriptions du mandat sensible peut être jugée élevée dans les cas suivants notamment:

a. l'entreprise manque d'intégrité ou de loyauté;

b. l'entreprise est contrôlée par des États étrangers ou des organisations étrangères de droit public ou privé ou se trouve sous leur influence, lorsque ce contrôle ou cette influence sont incompatibles avec les intérêts définis à l'art. 1, al. 2;

c. un service spécialisé CSP a rendu une déclaration de risque pour un membre du personnel de l'entreprise et cette personne est indispensable pour l'exécution du mandat.

3 L'évaluation doit se fonder sur des faits concernant la situation de l'entreprise, indépendamment de toute faute commise.

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

1 Le service spécialisé PSE communique son évaluation à l'adjudicateur et la notifie formellement à l'entreprise.

2 Si le service spécialisé PSE conclut que l'exécution du mandat sensible par l'entreprise concernée pose un risque pour la sécurité, l'adjudicateur exclut l'entreprise de la procédure d'adjudication.

3 Si toutes les entreprises qui entrent en considération posent un risque pour la sécurité, l'adjudicateur peut néanmoins confier le mandat à l'une d'entre elles. Le service spécialisé PSE classe la procédure. L'adjudicateur applique par analogie les mesures visées aux art. 60, 61, 64 et 65.

Section 4 Plan de sécurité

Art. 60 Adjudication et plan de sécurité

1 L'adjudicateur indique au service spécialisé PSE quelle est l'entreprise adjudicataire.

2 L'entreprise établit un plan de sécurité en suivant les directives du service spécialisé PSE.

3 Le plan de sécurité est soumis au contrôle du service spécialisé PSE. Ce dernier peut collecter les données nécessaires par écrit ou inspecter les locaux de l'entreprise.

Art. 61 Contrôles de sécurité relatifs aux personnes

1 Les collaborateurs de l'entreprise qui sont appelés à exercer une activité sensible sont soumis à un contrôle de sécurité.

2 L'instance décisionnelle au sens de l'art. 42, al. 2, est le service spécialisé PSE. Si la procédure de sécurité relative aux entreprises est classée conformément à l'art. 59, al. 3, parce qu'aucune entreprise ne présente les qualifications requises pour exécuter le mandat, l'adjudicateur prend la décision.

Section 5 Déclaration de sécurité relative aux entreprises

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

1 Le service spécialisé PSE rend formellement une déclaration de sécurité lorsque l'entreprise apporte la preuve qu'elle a mis en œuvre le plan de sécurité.

2 Il refuse à l'entreprise la déclaration de sécurité et classe la procédure si l'entreprise ne met pas en œuvre le plan de sécurité. Il rend formellement une décision en conséquence.

3 Les décisions visées aux al. 1 et 2 sont communiquées à l'adjudicateur.

4 L'adjudicateur est lié par la décision du service spécialisé PSE, sous réserve de l'art. 59, al. 3.

5 La déclaration de sécurité est valable cinq ans.

Art. 63 Exécution d'un mandat sensible

L'adjudicateur ne peut laisser une entreprise exécuter un mandat sensible qu'une fois que celle-ci a obtenu une déclaration de sécurité.

Art. 64 Obligations de l'entreprise

1 Les entreprises qui ont obtenu une déclaration de sécurité doivent constamment appliquer les mesures prévues par le plan de sécurité.

2 Elles informent immédiatement le service spécialisé PSE et l'adjudicateur de tout changement et de tout incident dans le domaine de la sécurité.

Art. 65 Contrôles et mesures de protection

1 Le service spécialisé PSE peut procéder aux contrôles suivants:

a. inspecter inopinément les locaux où le mandat sensible est exécuté;

b. consulter les documents relatifs au mandat.

2 Lorsque des indices concrets donnent à penser que la sécurité de l'information est menacée dans une entreprise, il peut prendre immédiatement les mesures de protection qui s'imposent, notamment mettre les documents et le matériel en lieu sûr.

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

Les entreprises qui ont obtenu une déclaration de sécurité sont réputées qualifiées en cas d'adjudication d'autres mandats sensibles. Le service spécialisé PSE examine la nécessité d'adapter le plan de sécurité.

Art. 67 Certificat international de sécurité

Le service spécialisé PSE établit à la demande de l'entreprise un certificat international de sécurité.

Art. 68 Révocation de la déclaration de sécurité

[1] Le service spécialisé PSE révoque la déclaration de sécurité dans les cas suivants:

a. l'entreprise n'a pas rempli ses obligations au sens de l'art. 64;

b. une répétition de la procédure a permis d'identifier un risque pour la sécurité.

[2] Il notifie sa décision à l'entreprise et à l'adjudicateur.

[3] En cas de révocation de la déclaration de sécurité, l'adjudicateur retire immédiatement le mandat à l'entreprise, sous réserve de l'art. 59, al. 3. L'entreprise n'a droit à aucune indemnisation.

Section 6 Répétition de la procédure et voies de droit

Art. 69 Répétition de la procédure

La procédure de sécurité est répétée dans les cas suivants:

a. la déclaration de sécurité de l'entreprise échoit alors que l'entreprise exécute un mandat sensible;

b. des changements importants sont intervenus au sein de l'entreprise et des indices concrets donnent à penser que ces changements ont fait apparaître de nouveaux risques pour la sécurité.

Art. 70 Voies de droit

[1] L'entreprise a 30 jours à compter de la notification de la décision du service spécialisé PSE pour utiliser les voies de droit suivantes:

a. consulter le dossier du contrôle;

b. demander la rectification des données erronées ou la destruction des données obsolètes;

c. demander que l'on ajoute à une donnée la mention de son caractère litigieux;

d. faire recours devant le Tribunal administratif fédéral.

[2] Les restrictions à la communication de renseignements sont régies par l'art. 9 LPD[17].

17 RS **235.1**

Section 7 Traitement des données personnelles

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

1 Le service spécialisé PSE exploite un système d'information pour réaliser et gérer les procédures de sécurité relatives aux entreprises.

2 Les données sensibles et les profils de la personnalité au sens de l'art. 3, let. c et d, LPD[18] peuvent être traités dans le système d'information dans la mesure où ils sont nécessaires à l'exécution de la procédure.

3 Le système d'information contient les données suivantes:

a. les données visées aux art. 57 et 60, al. 3;

b. le résultat de l'évaluation visée à l'art. 56, al. 2;

c. le résultat des contrôles de sécurité relatifs aux personnes visés à l'art. 61, al. 1;

d. la décision du service spécialisé PSE visée à l'art. 61, al. 2;

e. la raison sociale des entreprises qui ont obtenu une déclaration de sécurité;

f. les mesures de protection visées à l'art. 65;

g. les données et les dossiers relatifs aux procédures de recours.

4 Le service spécialisé PSE est responsable de la sécurité du système d'information et de la licéité du traitement des données personnelles.

Art. 72 Consultation et communication des données

1 Les organes suivants peuvent consulter en ligne les données ci-après:

a. les adjudicateurs: les données visées à l'art. 71, al. 3, let. b et d à g;

b. les entreprises qui sont habilitées par le Conseil fédéral, en vertu de l'art. 32, al. 1, let. a, à ouvrir des procédures de contrôle de sécurité relatifs aux personnes dans leur domaine de compétence: les données visées à l'art. 71, al. 3, let. d.

2 Le service spécialisé PSE peut au surplus communiquer les données visées à l'art. 71, al. 3, let. b à d, à d'autres services de la Confédération dans la mesure où ces données sont nécessaires à la sécurité de l'information.

Art. 73 Conservation, archivage et destruction des données

1 Le service spécialisé PSE conserve les données aussi longtemps que l'entreprise concernée dispose d'une déclaration de sécurité, mais dix ans au plus.

2 L'archivage des données est régi par les dispositions de la législation relative à l'archivage.

18 RS **235.1**

3 Lorsque la procédure est classée, le service spécialisé PSE détruit l'ensemble des données et dossiers relatifs à la procédure dans les trois mois.

Section 8 Dispositions édictées par le Conseil fédéral

Art. 74

Le Conseil fédéral règle:

a. les modalités de la procédure de sécurité relative aux entreprises;

b. l'application aux sous-contractants de la procédure de sécurité relative aux entreprises;

c. l'organisation du service spécialisé PSE;

d. les mesures nécessaires pour garantir la sécurité des données du système visé à l'art. 71;

e. les modalités du contrôle périodique réalisé par un organe indépendant du traitement des données personnelles.

Chapitre 5 Infrastructures critiques

Art. 75 Tâches de la Confédération

1 La Confédération apporte un soutien aux exploitants d'infrastructures critiques pour garantir que les interruptions de réseau et de système et que les utilisations abusives soient rares, de courte durée, maîtrisables et peu dommageables.

2 Le soutien apporté par la Confédération en matière de sécurité de l'information prend les formes suivantes:

a. identification et évaluation précoces des menaces, dangers, vulnérabilités et failles de sécurité;

b. identification des incidents;

c. maintien et rétablissement de la sécurité de l'information après un incident;

d. suivi des incidents.

3 La Confédération gère un service national d'alerte et un service d'assistance pour la mise en place de mesures techniques de sécurité à titre préventif ou après un incident.

4 Elle veille à ce que le s exploitants d'infrastructures critiques puissent échanger des informations en toute sécurité, entre elles et avec les services compétents de la Confédération.

5 Le Conseil fédéral désigne les services fédéraux chargés d'accomplir ces tâches.

Art. 76 Traitement des données personnelles

1 Les services visés à l'art. 75, al. 5, peuvent traiter des ressources d'adressage au sens de l'art. 3, let. f, de la loi du 30 avril 1997 sur les télécommunications[19] et les données personnelles qui s'y rapportent dans la mesure où elles en ont besoin pour accomplir leurs tâches.

2 Ils peuvent également traiter les données visées à l'al. 1 lorsque ces dernières comportent des informations concernant:

a. des opinions religieuses, philosophiques ou politiques; le traitement des données n'est admissible que dans la mesure où elles sont nécessaires à l'évaluation de menaces et dangers concrets en matière de sécurité de l'information;

b. des poursuites ou sanctions pénales ou administratives.

3 Les données personnelles peuvent être traitées à l'insu de la personne concernée.

4 En cas de soupçon fondé d'usurpation d'identité ou d'utilisation abusive de ressources d'adressage, les services visés à l'art. 75, al. 5, informent la personne concernée. Les art. 18*a*, al. 4, let. b, et 18*b* LPD[20] sont réservés.

Art. 77 Coopération sur le plan national

1 Les services visés à l'art. 75, al. 5, peuvent communiquer aux exploitants d'infrastructures critiques des données personnelles au sens de l'art 76 dans la mesure où elles sont utiles à la sécurité de l'information.

2 Ils peuvent communiquer aux fournisseurs et exploitants de services informatiques et de communication des données personnelles au sens de l'art. 76 dans la mesure où elles sont nécessaires à la sécurité de l'information d'infrastructures critiques.

3 Les exploitants d'infrastructures critiques de même que les fournisseurs et les exploitants de services informatiques et de communication peuvent communiquer aux services visés à l'art. 75, al. 5, des données liées à des incidents, y compris des données personnelles. Les services visés à l'art. 75, al. 5, ne peuvent transmettre ces données à des fins de poursuite pénale qu'avec l'autorisation expresse du fournisseur des données.

Art. 78 Coopération internationale

1 Les services visés à l'art. 75, al. 5, peuvent échanger avec des services étrangers ou internationaux chargés de la protection d'infrastructures critiques des données au sens de l'art. 76 lorsqu'elles sont nécessaires pour accomplir des tâches correspondant à celles définies à l'art. 75.

2 L'échange de données au sens de l'al. 1 n'est autorisé que si les services étrangers ou internationaux garantissent que les données seront utilisées exclusivement aux fins prévues à l'al. 1.

19 RS **784.10**
20 RS **235.1**

3 Si les données sont nécessaires à l'exécution d'une procédure à l'étranger, les dispositions régissant l'assistance administrative et l'entraide judiciaire sont applicables.

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

1 Les services visés à l'art. 75, al. 5, exploitent un système d'information permettant d'échanger en toute sécurité des informations avec les exploitants des infrastructures critiques.

2 Le système contient les informations suivantes:

a. description et évaluation des menaces et dangers;

b. consignes sur l'identification et la résolution techniques des incidents;

c. analyses des incidents et recommandations pour la sécurité;

d. analyses des vulnérabilités que présentent les moyens informatiques;

e. correspondance.

3 Les informations visées à l'al. 2 peuvent contenir des données personnelles au sens de l'art. 76.

Art. 80 Conservation et archivage des données

1 Les services visés à l'art. 75, al. 5, conservent les données personnelles aussi longtemps que celles-ci sont utiles pour prévenir des dangers ou pour identifier des incidents, mais cinq ans au plus.

2 L'archivage des données est régi par les dispositions de la législation relative à l'archivage.

Art. 81 Dispositions édictées par le Conseil fédéral

Le Conseil fédéral règle:

a. la répartition des tâches, la collaboration et les échanges entre les services visés à l'art. 75, al. 5, et le SRC;

b. les modalités de la communication d'informations aux exploitants d'infrastructures critiques, à des tiers et aux services étrangers et internationaux;

c. les responsabilités en matière de protection des données traitées dans le système d'information visé à l'art. 79 et la sécurité des données;

d. les modalités du contrôle périodique réalisé par un organe indépendant du traitement des données personnelles dans le système d'information visé à l'art. 79.

Chapitre 6 Organisation et exécution
Section 1 Organisation

Art. 82 Préposés à la sécurité de l'information

1 Les autorités et organisations suivantes désignent, chacune dans son domaine de compétence, un préposé à la sécurité de l'information et un suppléant:

a. le Conseil fédéral;

b. la Délégation administrative de l'Assemblée fédérale;

c. les tribunaux fédéraux;

d. le Ministère public de la Confédération;

e. la Banque nationale suisse;

f. les départements et la Chancellerie fédérale.

2 Les préposés à la sécurité de l'information accomplissent les tâches suivantes:

a. conseiller et aider dans leur domaine les services compétents dans l'accomplissement des tâches et l'exécution des obligations qui leur incombent en vertu de la présente loi;

b. diriger, sur mandat de l'autorité ou de l'organisation à laquelle ils sont subordonnés, l'organisation spécialisée chargée de la sécurité de l'information et la gestion des risques;

c. vérifier, sur mandat de l'autorité ou de l'organisation à laquelle ils sont subordonnés, le respect des prescriptions relatives à la sécurité de l'information, en rendre compte et proposer les mesures qui s'imposent;

d. signaler, sur une base volontaire, les incidents dans le domaine de la sécurité de l'information au service spécialisé de la Confédération pour la sécurité de l'information et aux services visés à l'art. 75, al. 5.

3 Aucune tâche susceptible d'entrer en conflit avec l'une des tâches visées à l'al. 2 ne peut être confiée aux préposés à la sécurité de l'information.

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

1 La Conférence des préposés à la sécurité de l'information se compose des préposés à la sécurité de l'information au sens de l'art. 82, al. 1, de deux représentants des cantons et du Préposé fédéral à la protection des données et à la transparence.

2 Elle accomplit les tâches suivantes:

a. promouvoir l'exécution uniforme de la présente loi;

b. contribuer à la normalisation des exigences et mesures visées à l'art. 86;

c. conseiller 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;

d. veiller à l'échange d'informations, notamment sur la gestion des risques et sur les problèmes et les incidents dans le domaine de la sécurité de l'information;

e. assurer la coordination avec les autres services qui accomplissent des tâches dans le domaine de la sécurité de l'information.

3 Elle édicte son règlement interne.

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

1 Le service spécialisé de la Confédération pour la sécurité de l'information:

a. conseille et soutient les autorités soumises à la présente loi, leurs préposés à la sécurité de l'information et les cantons dans l'exécution de la présente loi;

b. peut recommander des mesures si la sécurité de l'information de la Confédération est menacée;

c. peut mener des contrôles à la demande des autorités soumises à la présente loi;

d. peut évaluer, à la demande des autorités soumises à la présente loi, les risques liés à l'utilisation de nouvelles technologies;

e. peut examiner, à la demande des autorités et organisations soumises à la présente loi, l'adéquation de leurs processus, moyens, installations, objets et prestations par rapport aux exigences en matière de sécurité de l'information;

f. peut gérer et coordonner, à la demande des autorités soumises à la présente loi, les questions liées à la sécurité de l'information lorsque des projets importants impliquent plusieurs autorités;

g. sert d'interlocuteur pour les contacts spécialisés avec des services nationaux, étrangers ou internationaux;

h. rend compte chaque année au Conseil fédéral de la situation en matière de sécurité de l'information au sein de la Confédération.

2 Le préposé du Conseil fédéral à la sécurité de l'information dirige le service spécialisé de la Confédération pour la sécurité de l'information.

3 Le Conseil fédéral règle l'organisation du service spécialisé de la Confédération pour la sécurité de l'information. Il peut le charger d'autres tâches pour le compte de l'administration fédérale ou de l'armée.

Section 2 Exécution

Art. 85 Dispositions d'exécution

1 Les autorités soumises à la présente loi édictent les dispositions d'exécution de la présente loi. Le Conseil fédéral peut charger la Chancellerie fédérale d'édicter des dispositions d'exécution pour les affaires du Conseil fédéral.

2 Les compétences que la présente loi donne à l'Assemblée fédérale sont exercées par la Délégation administrative de l'Assemblée fédérale.

3 Les dispositions d'exécution du Conseil fédéral s'appliquent par analogie aux autorités soumises à la présente loi si elles n'édictent pas leurs propres dispositions d'exécution.

Art. 86 Exigences et mesures standard

1 Le Conseil fédéral fixe des exigences standard en matière de sécurité et définit des mesures standard en matière d'organisation, de personnel et de construction, de même que sur le plan technique, pour assurer la sécurité de l'information; il suit à cet effet l'avancement des connaissances et de la technique.

2 Il peut déléguer cette tâche.

3 Les exigences et mesures standard du Conseil fédéral ont valeur de recommandations, sauf si les autorités soumises à la présente loi les déclarent obligatoires.

Art. 87 Cantons

1 Les cantons veillent au contrôle périodique de la mise en œuvre et de l'efficacité des mesures prévues par la présente loi dans les cas visés à l'art. 3.

2 Ils informent le service spécialisé de la Confédération pour la sécurité de l'information des résultats des contrôles visés à l'al. 1.

3 Ils désignent le service qui est l'interlocuteur des autorités soumises à la présente loi en matière de sécurité de l'information.

4 Le Conseil fédéral définit les cas dans lesquels les cantons peuvent recourir aux prestations des services spécialisés visés par la présente loi afin d'assurer leur propre sécurité de l'information. Ces prestations sont soumises à des émoluments. Leur montant est fixé par le Conseil fédéral.

Art. 88 Traités internationaux

Le Conseil fédéral peut conclure des traités internationaux en matière de sécurité de l'information portant sur les objets suivants:

a. l'échange d'informations sur des menaces, des vulnérabilités et des incidents dans le domaine de la sécurité de l'information, en particulier dans les infrastructures critiques;

b. l'échange d'informations classifiées;

c. l'exécution des contrôles de sécurité relatifs aux personnes et des procédures de sécurité relatives aux entreprises;

d. la reconnaissance des déclarations de sécurité;

e. l'exécution de contrôles.

Art. 89 Évaluation

[1] Le Conseil fédéral veille à ce que l'exécution, l'adéquation, l'efficacité et l'économicité de la présente loi soient contrôlés périodiquement.

[2] Il en rend compte régulièrement aux commissions compétentes de l'Assemblée fédérale.

Chapitre 7 Dispositions finales

Art. 90 Modification d'autres actes

La modification d'autres actes est réglée en annexe.

Art. 91 Dispositions transitoires

[1] Les informations classifiées selon l'ancien droit sont adaptées aux règles de classification du nouveau droit dès qu'elles sont traitées après l'entrée en vigueur de la présente loi.

[2] Les moyens informatiques doivent être classés dans un délai de deux ans à compter de son entrée en vigueur. Les mesures techniques visant à assurer la sécurité de l'information doivent être mises en place dans un délai de six ans à compter de l'entrée en vigueur de la présente loi.

[3] Les déclarations relatives à la sécurité des personnes et les déclarations relatives à la sécurité des entreprises rendues selon l'ancien droit sont valables cinq ans à compter de leur établissement.

Art. 92 Référendum et entrée en vigueur

[1] La présente loi est sujette au référendum.

[2] Le Conseil fédéral fixe la date de l'entrée en vigueur.

Annexe
(art. 90)

Modification d'autres actes

Les actes mentionnés ci-après sont modifiés comme suit:

1. Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure[21]

Art. 2, al. 4, let. c

Abrogée

Section 4 (art. 19 à 21)

Abrogée

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

7 Le système d'information peut être consulté en ligne par les services de fedpol chargés de l'exécution de la présente loi, par les autorités de police des cantons, par l'Observatoire suisse du hooliganisme (observatoire), par les autorités douanières et par les services spécialisés chargés de réaliser les contrôles de sécurité relatifs aux personnes au sens de l'art. 32, al. 2, de la loi du … sur la sécurité de l'information[22].
…

2. Loi fédérale du 25 septembre 2015 sur le renseignement[23]

Art. 51, al. 4, let. d

4 Les personnes suivantes ont accès en ligne aux données ci-après du système:

d. les collaborateurs des services spécialisés chargés de réaliser les contrôles de sécurité relatifs aux personnes au sens de l'art. 32, al. 2, de la loi du … sur la sécurité de l'information[24]: les données visées à l'al. 3, let. a, en vue d'exécuter les contrôles de sécurité relatif aux personnes, les contrôles de loyauté et l'évaluation du potentiel de violence.

21 RS **120**
22 RS …; FF **2017** 2765 2907
23 FF **2015** 6597
24 RS …; FF **2017** 2765 2907

3. Loi fédérale du 24 mars 2000 sur le personnel de la Confédération[25]

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

L'employeur peut 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 ses intérêts.

Art. 20b Contrôle de loyauté

1 Les employeurs au sens de l'art. 3, al. 1, let. a, b, e et f, peuvent faire contrôler la loyauté des candidats à un poste et de leurs employés dans les cas suivants:

a. les personnes concernées sont régulièrement appelées à représenter la Suisse à l'étranger dans le cadre de leur fonction et pourraient porter à ce titre une atteinte considérable à l'image de la Confédération;

b. les personnes concernées sont appelées à exercer dans le cadre de leur fonction des compétences décisionnelles ou des tâches de surveillance dans d'importantes affaires financières ou fiscales et pourraient porter à ce titre une atteinte considérable aux intérêts financiers de la Confédération.

2 Ils limitent le contrôle au strict nécessaire.

3 Les services spécialisés chargés de réaliser les contrôles de sécurité relatifs aux personnes au sens de l'art. 32, al. 2, de la loi du … sur la sécurité de l'information (LSI)[26] réalisent le contrôle. Les dispositions de cette loi relatives au contrôle de sécurité s'appliquent par analogie.

4 Lorsque les candidats à un poste et les employés sont soumis simultanément à un contrôle de sécurité au sens de la LSI, les deux procédures sont combinées.

4. Code de procédure civile[27]

Art. 166, al. 1, let. c

1 Tout tiers peut refuser de collaborer:

c. à l'établissement de faits qui lui ont été confiés en sa qualité officielle de fonctionnaire au sens de l'art. 110, al. 3, CP ou de membre d'une autorité, ou dont il a eu connaissance dans l'exercice de ses fonctions ou de son activité auxiliaire pour un fonctionnaire ou une autorité; il doit collaborer s'il est soumis à une obligation de dénoncer ou si l'autorité dont il relève l'y a habilité;

25 RS **172.220.1**
26 RS …; FF **2017** 2765 2907
27 RS **272**

5. Loi fédérale du 4 décembre 1947 de procédure civile fédérale[28]

Art. 42, al. 3

3 Les fonctionnaires et leurs auxiliaires ne sont tenus de témoigner sur des faits dont ils ont eu connaissance dans l'exercice de leurs fonctions ou de leur activité auxiliaire que dans les limites du droit administratif fédéral ou cantonal.

6. Code pénal[29]

Art. 320 Violation du secret de fonction

1. Quiconque révèle un secret à lui confié en sa qualité de membre d'une autorité ou de fonctionnaire, ou dont il a eu connaissance à raison de sa charge ou de son emploi ou en tant qu'auxiliaire d'une autorité ou d'un fonctionnaire, est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

La révélation demeure punissable alors même que la charge ou l'emploi ou l'activité auxiliaire a pris fin.

2. La révélation n'est pas punissable si elle est faite avec le consentement écrit de l'autorité supérieure.

Art. 365, al. 2, let. d

2 Le casier sert les autorités fédérales et cantonales dans l'accomplissement des tâches suivantes:

d. évaluation du risque pour la sécurité dans le cadre des contrôles de sécurité relatifs aux personnes au sens de la loi du … sur la sécurité de l'information (LSI)[30] et des contrôles de loyauté au sens de la législation spéciale;

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

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

i. les services spécialisés chargés de réaliser les contrôles de sécurité relatifs aux personnes au sens de l'art. 32, al. 2, LSI[31] (services spécialisés CSP);

28 RS **273**
29 RS **311.0**
30 RS …; FF **2017** 2765 2907
31 RS …; FF **2017** 2765 2907

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

b. les services spécialisés CSP;

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

7. Code de procédure pénale[32]

Art. 170, al. 1

[1] Les fonctionnaires au sens de l'art. 110, al. 3, CP[33] ainsi que leurs auxiliaires et les membres des autorités ainsi que leurs auxiliaires peuvent refuser de témoigner sur les secrets qui leur ont été confiés en leur qualité officielle ou dont ils ont eu connaissance dans l'exercice de leur fonction, de leur charge ou de leur activité auxiliaire.

8. Code pénal militaire du 13 juin 1927[34]

Art. 77 Violation du secret de service

1. Quiconque révèle un secret à lui confié en sa qualité de militaire ou de fonctionnaire, ou dont il a eu connaissance à raison de sa situation militaire ou de sa fonction ou en tant qu'auxiliaire d'un tel détenteur de secret, est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

L'infraction est punie disciplinairement si elle est de peu de gravité.

2. La révélation demeure punissable alors même que la situation militaire ou la fonction ou l'activité auxiliaire a pris fin.

9. Procédure pénale militaire du 23 mars 1979[35]

Art. 77, al. 2

[2] Les fonctionnaires et leurs auxiliaires ne peuvent être entendus comme témoins sur un secret de fonction (art. 320 CP[36]) ou astreints à produire des documents officiels qu'avec le consentement de l'autorité supérieure. Au surplus, les prescriptions du droit administratif fédéral et cantonal sont applicables.

32 RS **312.0**
33 RS **311.0**
34 RS **321.0**
35 RS **322.1**
36 RS **311.0**

10. Loi fédérale du 13 juin 2008 sur les systèmes d'information de la police de la Confédération[37]

Art. 15, al. 4, let. f

Abrogée

Art. 17, al. 4, phrase introductive et let. l

4 Ont accès en ligne à ces données:

l. les services spécialisés chargés des contrôles de sécurité relatifs à des personnes au sens de l'art. 32, al. 2, de la loi du … sur la sécurité de l'information (LSI)[38], afin d'évaluer le risque pour la sécurité dans le cadre d'un contrôle de sécurité relatif aux personnes, d'un contrôle de loyauté ou d'une évaluation du potentiel de violence;

11. Loi du 3 février 1995 sur l'armée[39]

Art. 14 Contrôle de loyauté

1 La loyauté des militaires peut être contrôlée dans les cas suivants:

a. ils sont régulièrement appelés à représenter la Suisse à l'étranger dans le cadre de leur fonction et pourraient porter à ce titre une atteinte considérable à l'image de la Confédération;

b. ils sont appelés à exercer dans le cadre de leur fonction des compétences décisionnelles ou des tâches de surveillance dans d'importantes affaires financières ou fiscales et pourraient porter à ce titre une atteinte considérable aux intérêts financiers de la Confédération.

2 Le Conseil fédéral désigne les fonctions soumises au contrôle. Il s'en tient au strict nécessaire.

3 Les services spécialisés chargés des contrôles de sécurité relatifs à des personnes au sens de l'art. 32, al. 2, de la loi du … sur la sécurité de l'information (LSI)[40] réalisent le contrôle. La procédure est régie par les dispositions de cette loi relatives au contrôle de sécurité, qui s'appliquent par analogie.

4 Lorsque les militaires sont soumis simultanément à un contrôle de sécurité au sens de la LSI, les deux procédures sont combinées.

37 RS **361**
38 RS …; FF **2017** 2765 2907
39 RS **510.10**
40 RS …; FF **2017** 2765 2907

Art. 113, al. 6

6 La procédure est régie par les dispositions relatives au contrôle de sécurité de base au sens de l'art. 31, let. a, LSI[41], qui s'appliquent par analogie. Si un contrôle de sécurité de base doit être réalisé simultanément pour d'autres motifs, les deux procédures sont combinées.

Art. 150, al. 4

Abrogé

12. Loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée[42]

Art. 14, al. 1, let. i

1 Le SIPA contient les données ci-après sur les conscrits, les personnes astreintes au service militaire, ainsi que les civils pris en charge par la troupe ou qui participent à un engagement de l'armée de durée déterminée:

i. les données relatives au contrôle de loyauté au sens de l'art. 14 de la loi du 3 février 1995 sur l'armée (LAAM)[43], y compris la décision.

Art. 17, al. 1, let. a

Les données du SIPA relatives à des infractions, des décisions ou des mesures pénales peuvent être conservées si elles ont fondé:

a. une décision de non-recrutement, d'exclusion ou de dégradation au sens de la LAAM[44];

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

Abrogées

13. Loi du 21 mars 2003 sur l'énergie nucléaire[45]

Art. 5, al. 3 et 3bis

3 Des mesures de sûreté doivent être prises pour empêcher des tiers d'attenter à la sécurité des installations et des matières nucléaires et pour empêcher que des matières nucléaires puissent être dérobées.

41 RS …; FF **2017** 2765 2907
42 RS **510.91**
43 RS **510.10**
44 RS **510.10**
45 RS **732.1**

3bis La classification et le traitement des informations sont régis par les dispositions de la législation sur la sécurité de l'information au sein de la Confédération.

14. Loi du 23 mars 2007 sur l'approvisionnement en électricité[46]

Art. 20a Contrôle de loyauté

1 Les membres du personnel de la société nationale du réseau de transport appelés à exercer des tâches essentielles pour la sécurité du réseau de transport à l'échelon de la Suisse et pour la fiabilité et la performance de son exploitation sont soumis à un contrôle de loyauté visant à évaluer le risque pour la sécurité.

2 Le Conseil fédéral désigne les groupes de personnes soumises au contrôle. Il s'en tient au strict nécessaire.

3 Les services spécialisés chargés des contrôles de sécurité relatifs aux personnes au sens de l'art. 32, al. 2, de la loi du … sur la sécurité de l'information[47] réalisent le contrôle. La procédure est régie par les dispositions de cette loi relatives au contrôle de sécurité, qui s'appliquent par analogie.

4 Les résultats du contrôle sont communiqués à la direction de la société nationale du réseau de transport, à l'office et à l'ElCom.

15. Loi du 3 octobre 2003 sur la Banque nationale[48]

Art. 16, titre et al. 5

Confidentialité et sécurité de l'information

5 Au demeurant, la loi fédérale du 19 juin 1992 sur la protection des données[49] et la loi du … sur la sécurité de l'information[50] sont applicables.

46 RS **734.7**
47 RS …; FF **2017** 2765 2907
48 RS **951.11**
49 RS **235.1**
50 RS …; FF **2017** 2765 2907