Loi fédérale 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, 173, al. 1, let. a et b, et al. 2, de la Constitution fédérale[1],

vu le message du Conseil fédéral du …[2],

arrête:

Chapitre 1 Dispositions générales

Art. 1 But

[1] La présente loi vise à garantir la sécurité du traitement des informations et de l'engagement des moyens technologiques de l'information et de la communication (moyens TIC).

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

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

b. la sécurité intérieure et extérieure de la Suisse;

c. les intérêts de 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 fédérales quant à la protection des informations.

Art. 2 Autorités et organisations concernées

[1] La présente loi s'applique:

a. à l'Assemblée fédérale;

b. au Conseil fédéral;

c. aux tribunaux fédéraux;

RO …

1 RS **101**

2 FF ...

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

e. à la Banque nationale suisse.

[2] Elle s'applique également aux organisations suivantes:

a. les services du Parlement;

b. l'administration fédérale;

c. les administrations des tribunaux fédéraux;

d. l'armée;

e. les organisations de droit public ou privé qui exercent des activités sensibles lors de l'accomplissement de tâches administratives au sens de l'art. 2, al. 4, de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration[3];

f. les autorités et services cantonaux qui exercent des activités sensibles sur mandat de la Confédération et sous sa surveillance.

[3] Sont des activités sensibles:

a. le traitement d'informations classifiées «CONFIDENTIEL» ou «SECRET» et l'utilisation de matériel classifié pareillement (art. 14, al. 2 et 3);

b. l'administration, l'exploitation, la maintenance et le contrôle de moyens TIC appartenant aux catégories de sécurité «protection élevée» ou «protection très élevée» (art. 21, al. 2 et 3);

c. 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 (art. 31).

Art. 3 Rapport avec la législation spéciale

[1] La loi fédérale du 17 décembre 2004 sur le principe de la transparence dans l'administration[4] demeure réservée.

[2] Lorsque les informations doivent être protégées en vertu d'autres lois fédérales, les dispositions de la présente loi s'appliquent à titre complémentaire.

[3] L'application de la présente loi aux organisations de droit public ou privé exploitant des infrastructures indispensables au fonctionnement de la société, de l'économie et de l'Etat (infrastructures critiques) se fonde sur la législation spéciale.

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

Chapitre 2 Mesures générales de la sécurité de l'information

Section 1 Principes

Art. 4 Sécurité de l'information

[1] Les autorités et organisations concernées s'assurent que le besoin de protection des informations dont elles ont la responsabilité est évalué en fonction d'une atteinte éventuelle aux intérêts au sens de l'art. 1, al. 2.

[2] Elles s'assurent, pour répondre à ce besoin de protection, que ces informations:

a. ne sont accessibles qu'aux personnes et organisations autorisées (confidentialité);

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

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

d. sont traitées de manière traçable (traçabilité).

[3] Elles s'assurent que les moyens TIC qu'elles utilisent pour remplir leurs tâches légales sont protégés contre les abus et les dérangements.

[4] Pour ce faire, elles adoptent une approche fondée sur le risque et tiennent compte des principes de la proportionnalité, de l'efficience économique et de la simplicité d'emploi pour les utilisateurs.

Art. 5 Responsabilité de conduite des autorités

[1] Dans leur domaine de compétence, les autorités concernées s'assurent que la sécurité de l'information:

a. est organisée, mise en oeuvre et contrôlée en fonction de l'état d'avancement des connaissances et de la technologie;

b. est coordonnée entre les domaines spécialisés.

[2] Elles fixent les tâches des services concernés.

[3] Elles déterminent également:

a. leurs objectifs quant à la sécurité de l'information;

b. les principes pour le traitement des risques;

c. les conséquences en cas de violation des prescriptions.

[4] Elles s'assurent que les cadres et le personnel reçoivent régulièrement des informations adaptées aux divers échelons de responsabilité.

Art. 6 Gestion des risques

[1] Les autorités et organisations concernées s'assurent que les risques en matière de sécurité de l'information sont constamment identifiés, évalués, jugés et contrôlés dans leur domaine de compétence ainsi que dans le cadre de leur collaboration avec des tiers.

[2] A cette fin, elles s'assurent que les mesures nécessaires sont prises aux niveaux de l'organisation, du personnel et des constructions, de même que sur le plan technique, pour écarter les risques identifiés ou les réduire dans une proportion supportable.

[3] Elles s'assurent que les risques identifiés qui doivent être supportés sont annoncés et acceptés.

[4] La gestion des risques propre au domaine de la sécurité de l'information doit être intégrée au processus global de gestion des risques.

Art. 7 Exigences et mesures de sécurité

[1] Lorsqu'elles fixent les exigences et les mesures de sécurité, les autorités et organisations concernées s'inspirent des exigences et mesures standard selon l'art. 88.

[2] Les mesures de sécurité sont déterminées en fonction de l'état d'avancement des connaissances et de la technologie.

Art. 8 Collaboration avec les tiers

[1] Les autorités et organisations concernées s'assurent, dans leur collaboration avec les tiers, que les exigences et mesures au sens de la présente loi sont fixées dans les accords et contrats correspondants.

[2] Elles contrôlent l'application des mesures.

Art. 9 Procédure en cas de violation de la sécurité de l'information

Les autorités et organisation concernées s'assurent que les violations de la sécurité de l'information sont décelées à temps, leurs causes clarifiées et leurs éventuelles conséquences limitées à leur strict minimum.

Art. 10 Plans préventifs

Les autorités concernées s'assurent que des plans préventifs sont élaborés et dûment exercés dans l'éventualité de violations graves de la sécurité de l'information susceptibles d'entraver l'accomplissement de leurs tâches essentielles.

Art. 11 Contrôles

[1] Les autorités et organisations concernées s'assurent que le respect des prescriptions de la présente loi est régulièrement contrôlé.

[2] Les autorités concernées chargent périodiquement un service indépendant de vérifier l'efficacité des mesures prises dans leur domaine de compétence.

Section 2 Classification des informations

Art. 12 Principes de classification

[1] Les autorités et organisations concernées s'assurent que les informations remplissant les critères définis à l'art. 14 sont classifiées en conséquence.

[2] La classification doit se limiter au minimum requis.

[3] Elle doit être limitée dans le temps lorsqu'il est possible de prévoir qu'elle ne sera nécessaire que pour une période donnée.

[4] Chaque classification doit être contrôlée périodiquement.

Art. 13 Compétences

[1] Les autorités concernées désignent les personnes ou services compétents pour classifier les informations (auteur de la classification).

[2] Les classifications ne peuvent être modifiées ou supprimées que par l'auteur de la classification ou par le service qui lui est supérieur.

Art. 14 Echelons de classification

[1] Sont classifiées «INTERNE» les informations dont la prise de connaissance par des personnes non autorisées peut nuire aux intérêts au sens de l'art. 1, al. 2, let. a à d.

[2] Sont classifiées «CONFIDENTIEL» les informations dont la prise de connaissance par des personnes non autorisées peut nuire considérablement aux intérêts au sens de l'art. 1, al. 2, let. a à d.

[3] Sont classifiées «SECRET» les informations dont la prise de connaissance par des personnes non autorisées peut nuire gravement aux intérêts au sens de l'art. 1, al. 2, let. a à d.

Art. 15 Accès aux informations classifiées

[1] Seules peuvent accéder aux informations classifiées de la Confédération les personnes offrant toutes les garanties pour un traitement correct des informations et qui:

a. ont besoin des informations en question pour l'accomplissement de leurs tâches légales, ou

b. se voient conférer par contrat une autorisation d'accès et ont besoin des informations en question pour l'accomplissement des tâches qui leurs sont confiées.

[2] Demeurent réservées les limitations d'accès réglées par les conventions de droit international public au sens de l'art. 90.

Art. 16 Traitement des informations classifiées

[1] Les informations classifiées doivent être protégées de la prise de connaissance par des personnes non autorisées pendant toute la durée où elles sont jugées dignes de protection.

[2] Elles doivent indiquer l'auteur de la classification.

[3] Le traitement d'informations classifiées émanant de l'étranger est régi sur la base de la convention correspondante de droit international public au sens de l'art. 90.

Art. 17 Communication d'informations classifiées dans le cadre de procédures spéciales

[1] Le droit de procédure applicable au cas d'espèce régit la communication d'informations classifiées au sein de l'Assemblée fédérale et des services du Parlement, et auprès des tribunaux et des ministères publics.

[2] Avant toute décision relative à la publication d'une information au sens de l'al. 1, l'organe parlementaire ou le tribunal compétent peut consulter l'auteur de la classification.

Art. 18 Mesures provisoires de protection

[1] Les autorités et organisations concernées s'assurent que l'auteur de la classification est informé lorsque:

a. des informations classifiées sont menacées, utilisées abusivement ou perdues;

b. des informations ont manifestement été incorrectement classifiées ou n'ont pas été classifiées des suites d'une erreur.

[2] Elles prennent les mesures nécessaires à la protection provisoire des informations.

Section 3 Sécurité lors de l'utilisation des moyens TIC

Art. 19 Procédure de sécurité

[1] Les autorités concernées fixent une procédure garantissant la sécurité de l'information lors de l'utilisation de moyens TIC (procédure de sécurité).

[2] Sont responsables de l'exécution de la procédure de sécurité les autorités et organisations concernées qui, pour l'accomplissement de leurs tâches légales, mandatent l'exploitation de moyens TIC ou exploitent elles-mêmes de tels moyens.

[3] La procédure doit être répétée en cas de modification des risques.

Art. 20 Analyse du besoin de protection et évaluation des risques

[1] Les autorités et organisations concernées s'assurent que les besoins liés à la sécurité de l'information sont évalués lors de la planification de l'engagement de moyens TIC.

[2] Les autorités et organisations concernées qui ont l'intention d'engager de nouvelles technologies veillent à évaluer les risques qui peuvent en résulter pour la sécurité de l'information. Elles communiquent les résultats de l'évaluation au service spécialisé de la Confédération en matière de sécurité de l'information.

Art. 21 Catégories de sécurité des moyens TIC

[1] La catégorie de sécurité «protection de base» s'applique aux moyens TIC dans la mesure où ils ne nécessitent pas d'être attribués à une catégorie supérieure.

[2] La catégorie de sécurité «protection élevée» s'applique aux moyens TIC:

a. devant servir à traiter des informations dont la violation de la confidentialité, de la disponibilité, de l'intégrité ou de la traçabilité peut nuire considérablement aux intérêts au sens de l'art. 1, al. 2, ou

b. dont le dérangement ou l'usage abusif ou indu peut nuire considérablement aux intérêts au sens de l'art. 1, al. 2.

[3] La catégorie de sécurité «protection très élevée» s'applique aux moyens TIC:

a. devant servir à traiter des informations dont la violation de la confidentialité, de la disponibilité, de l'intégrité ou de la traçabilité peut nuire gravement aux intérêts au sens de l'art. 1, al. 2, ou

b. dont le dérangement ou l'usage abusif ou indu peut nuire gravement aux intérêts au sens de l'art. 1, al. 2.

Art. 22 Exigences de sécurité pour la catégorie de sécurité «protection de base»

[1] Les autorités concernées fixent les exigences minimales pour les moyens TIC de la catégorie de sécurité «protection de base».

[2] Tous les moyens TIC doivent répondre à ces exigences minimales.

Art. 23 Concept de sécurité de l'information

[1] Les autorités et organisations concernées s'assurent qu'une analyse du risque est menée et qu'un concept de sécurité de l'information est établi pour les moyens TIC des catégories de sécurité «protection élevée» et «protection très élevée».

[2] Le concept de sécurité de l'information doit être examiné par le préposé à la sécurité de l'information compétent et approuvé par l'autorité ou l'organisation concernée.

[3] Il doit être régulièrement actualisé.

Art. 24 Contrôles de conformité et d'efficacité

[1] Le déroulement correct de la procédure de sécurité et l'application des mesures décidées doivent être contrôlés avant tout engagement d'un moyen TIC.

[2] L'efficacité des mesures appliquées doit être contrôlée avant tout engagement d'un moyen TIC de la catégorie «protection très élevée».

Art. 25 Autorisation relative à la sécurité

[1] Après avoir exécuté la procédure de sécurité, les autorités et organisations concernées autorisent l'engagement du moyen TIC quant à la sécurité de l'information.

[2] En délivrant l'autorisation relative à la sécurité, l'autorité ou l'organisation accepte les risques résiduels.

Art. 26 Inventaire des moyens TIC

Les autorités et organisations concernées s'assurent que leurs moyens TIC sont inventoriés.

Art. 27 Sécurité durant l'exploitation

Les autorités et organisations concernées exploitant des moyens TIC s'assurent que la sécurité de l'information est garantie durant leur exploitation.

Section 4 Mesures relatives aux personnes

Art. 28 Exigences relatives aux personnes lors du traitement d'informations et de l'utilisation de moyens TIC de la Confédération

Les autorités et organisations concernées s'assurent que les personnes devant traiter des informations ou utiliser des moyens TIC de la Confédération dans le cadre de leurs tâches ou d'un mandat:

a. sont choisies avec soin;

b. reçoivent une instruction et un perfectionnement conforme à leur niveau de responsabilité;

c. sont tenues, au besoin, au maintien du secret.

Art. 29 Délivrance restrictive d'autorisations

[1] Les autorités et organisations concernées s'assurent de ne délivrer que les autorisations de traiter des informations, d'utiliser des moyens TIC et d'accéder aux locaux dont les personnes concernées ont besoin pour l'accomplissement de leurs tâches.

[2] Les autorisations doivent être retirées à l'expiration de l'engagement, du contrat ou après l'accomplissement d'une tâche. Elles peuvent être bloquées ou retirées sans

préavis lorsque des indices concrets donnent lieu de penser que la sécurité de l'information est menacée.

[3] Les autorités et organisations concernées veillent au contrôle régulier des autorisations.

Section 5 Protection physique des informations et des moyens TIC

Art. 30 Principes

[1] Les autorités et organisations concernées veillent à la protection physique adéquate, dans leurs locaux, de leurs informations et moyens TIC contre les accès non autorisés, les détériorations et les dérangements.

[2] Elles s'assurent que les informations et moyens TIC sont protégés adéquatement dans les domaines accessibles au public.

Art. 31 Zones de sécurité

[1] Les autorités et organisations concernées peuvent désigner, comme zones de sécurité, des domaines où:

a. des informations classifiées «CONFIDENTIEL» ou «SECRET» sont souvent traitées, ou

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

[2] Elles s'assurent que seules les personnes identifiées et autorisées peuvent accéder aux zones de sécurité.

[3] Dans la mesure où la garantie de la sécurité de l'information l'exige, les autorités et organisations concernées sont habilitées, dans les zones de sécurité:

a. à recourir à des méthodes de vérification biométriques;

b. à interdire l'accès de certains objets, en particulier les appareils de prises de vue et de son;

c. à surveiller les domaines sensibles avec des appareils de prises de vue;

d. à procéder à des fouilles corporelles;

e. à procéder inopinément à des contrôles dans les locaux, même en l'absence des employés.

[4] Elles sont, en outre, habilitées à exploiter, en vertu de l'art. 34, al. 1[ter], de la loi du 30 avril 1997 sur les télécommunications[5], une installation perturbatrice dans les zones de sécurité traitant souvent des informations classifiées «SECRET» ou exploitant des moyens TIC de la catégorie de sécurité «protection très élevée».

5 RS **784.10**

[5] Demeurent réservées les dispositions particulières relatives aux zones de sécurité établies conformément aux traités internationaux visés à l'art. 90, ainsi que celles relatives aux zones de protection des installations au sens de la législation sur la protection des ouvrages militaires.

Chapitre 3 Contrôle de sécurité relatif aux personnes

Section 1 But du contrôle, personnes assujetties au contrôle et degrés de contrôle

Art. 32 But du contrôle

Le contrôle de sécurité relatif aux personnes vise à déterminer s'il existe un risque pour la sécurité lorsqu'une personne doit exercer une activité sensible dans le cadre de sa fonction ou d'un mandat.

Art. 33 Liste des fonctions liées à des activités sensibles

Les autorités concernées édictent, pour leur domaine de compétence, une liste des fonctions dont l'accomplissement des tâches exige l'exercice d'une activité sensible.

Art. 34 Personnes assujetties au contrôle

[1] Font l'objet d'un contrôle de sécurité les personnes:

a. devant exercer une fonction figurant sur une liste établie conformément à l'art. 33;

b. devant exécuter, pour une des autorités ou organisations concernées, un mandat exigeant l'exercice d'une activité sensible;

c. assujetties à un contrôle de sécurité sur la base d'une convention de droit international public au sens de l'art. 90.

[2] Lorsqu'une autorité étrangère ou internationale confie une activité sensible à une personne, cette dernière fait l'objet d'un contrôle de sécurité si la Suisse a conclu avec le pays concerné ou l'organisation internationale une convention de droit international public au sens de l'art. 90.

[3] Les personnes exerçant ou devant exercer une fonction qui devrait figurer sur une liste établie conformément à l'art. 33, mais qui n'y figurent pas encore, peuvent, sur approbation de l'autorité concernée, faire l'objet d'un contrôle de sécurité. La liste des fonctions doit être adaptée à la première occasion.

[4] En qualité de membres des autorités, ne sont pas assujettis à un contrôle de sécurité:

a. les membres de l'Assemblée fédérale;

b. les membres du Conseil fédéral et le chancelier de la Confédération;

c. les juges des tribunaux fédéraux;

d. le procureur de la Confédération;

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

f. les membres des gouvernements et des tribunaux cantonaux.

Art. 35 Degrés de contrôle

Les autorités concernées attribuent aux activités sensibles l'un des degrés de contrôle suivants:

a. contrôle de sécurité de base: applicable aux activités sensibles dont l'exercice inadéquat ou contraire aux prescriptions peut nuire considérablement aux intérêts visés à l'art. 1, al. 2.

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

Section 2 Procédure

Art. 36 Services requérants

Les autorités concernées désignent les services qui ont la compétence d'ouvrir la procédure du contrôle de sécurité (services requérants).

Art. 37 Consentement

[1] Le contrôle de sécurité ne peut être réalisé sans le consentement de la personne concernée.

[2] Les contrôles de sécurité pour des fonctions de l'armée ou de la protection civile peuvent être réalisés sans le consentement des personnes concernées.

Art. 38 Moment du contrôle de sécurité

[1] Pour les personnes visées à l'art. 34, al. 1, let. a., la procédure du contrôle de sécurité doit être ouverte avant l'attribution de la fonction concernée.

[2] Pour les personnes visées à l'art. 34, al. 1, let. a, qui sont proposées au Conseil fédéral pour nomination, le contrôle de sécurité doit être achevé avant que la personne puisse être proposée pour nomination.

[3] Pour les personnes visées à l'art. 34, al. 1, let. b, le contrôle de sécurité doit être achevé avant de pouvoir exercer l'activité sensible concernée.

[4] Le moment du contrôle de sécurité pour les personnes faisant l'objet d'un contrôle de sécurité en vertu de conventions de droit international public au sens de l'art. 90 dépend des dispositions des conventions correspondantes.

Art. 39 Collecte des données

[1] Les services spécialisés chargés d'évaluer le risque pour la sécurité dans le cadre des contrôles de sécurité relatifs aux personnes (services spécialisés CSP) peuvent, en vue d'un contrôle de sécurité de base, collecter des données:

a. du casier judiciaire;

b. auprès des autorités de poursuite pénale et des tribunaux compétents sur des procédures pénales en cours, classées ou suspendues, et sur les dossiers des tribunaux et de l'instruction y afférents;

c. auprès des organes de sécurité de la Confédération, du Service de renseignement de la Confédération, des organes de l'armée et d'autres organes de la Confédération, dans la mesure où ceux-ci traitent des données nécessaires à l'évaluation du risque pour la sécurité;

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

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

f. des dossiers établis par des contrôles de sécurité antérieurs;

g. auprès de sources d'information publiques.

[2] En vue d'un contrôle de sécurité élargi, les services spécialisés CSP peuvent, en sus, collecter des données concernant la personne:

a. auprès des autorités fiscales fédérales et cantonales;

b. auprès des services tenant le registre du contrôle des habitants;

c. auprès des établissements financiers et des banques entretenant des relations d'affaires avec la personne concernée; ou

d. en auditionnant la personne concernée.

[3] Les services spécialisés CSP peuvent demander à des services étrangers des données au sens des al. 1 et 2.

[4] Pour l'évaluation du risque pour la sécurité, les services spécialisés CSP doivent pouvoir disposer de données suffisantes sur une période suffisamment longue.

[5] En présence d'un indice donnant à penser qu'un fait peut menacer la sécurité ou en cas de manque de données suffisantes sur une période suffisamment longue, les services spécialisés CSP peuvent interroger la personne concernée. Ils peuvent également, avec le consentement de cette dernière, interroger des tiers, ceux-ci n'étant pas tenus de fournir des renseignements.

[6] Les données des tiers indissociablement liées à celles de la personne faisant l'objet du contrôle peuvent être traitées pour autant qu'elles s'avèrent indispensables à l'évaluation du risque pour la sécurité. Les services spécialisés CSP informent les tiers concernés du traitement de leurs données.

Art. 40 Prise en charge des coûts

[1] Les autorités et organisations de droit public, auprès desquelles des données peuvent être collectées ou qui sont tenues de participer à la procédure, prêtent leur concours gratuitement.

[2] Lorsque la participation de tierces personnes représente une charge considérable, elles sont indemnisées.

Art. 41 Suspension de la procédure

[1] Les services spécialisés CSP suspendent la procédure lorsque:

a. la personne concernée revient sur son consentement ou ne participe pas à la procédure;

b. pour toute autre raison, la personne concernée n'entre plus en considération pour la fonction prévue ou pour l'exécution du mandat.

[2] Ils notifient la suspension de la procédure à la personne concernée et au service requérant. La personne concernée est alors réputée non contrôlée.

[3] La suspension de la procédure entraîne la destruction de toutes les données et de tous les dossiers collectés.

Section 3 Evaluation du risque pour la sécurité

Art. 42 Risque pour la sécurité

[1] Il existe un risque pour la sécurité lorsque, sur la base des données collectées, des signes concrets donnent à penser que, selon une probabilité élevée, la personne contrôlée exercera 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, en particulier, être élevée lorsque des indices donnent à penser que la personne à contrôler:

a. manque d'intégrité ou de fiabilité,

b. pourrait être victime de chantage ou corrompue, ou

c. ne dispose pas de toutes les capacités requises de jugement et de décision.

[3] Le risque pour la sécurité doit être motivé par des faits concrets concernant la situation personnelle de la personne contrôlée, indépendamment de toute faute commise.

[4] Les services spécialisés CSP ne sont soumis à aucune directive en ce qui concerne l'évaluation du risque pour la sécurité.

Art. 43 Résultat de l'évaluation

[1] Les services spécialisés CSP établissent l'une des déclarations suivantes:

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

b. déclaration de sécurité assortie de réserves: un risque pour la sécurité existe, mais peut être suffisamment réduit sous conditions; l'autorité de contrôle recommande des conditions adéquates;

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

d. déclaration de constatation: il n'y a pas de données suffisantes sur une période suffisamment longue pour évaluer le risque pour la sécurité.

[2] Avant d'établir une déclaration selon l'al. 1, let. b à d, les services spécialisés CSP donnent à la personne contrôlée l'occasion d'exprimer son avis.

Art. 44 Communication de l'évaluation

[1] Les services spécialisés CSP communiquent par écrit leur déclaration à la personne concernée ainsi qu'à l'instance compétente pour la décision de confier l'activité sensible (instance de décision).

[2] En ce qui concerne les personnes nommées par le Conseil fédéral, les services spécialisés CSP communiquent leur déclaration au département requérant, à l'intention du Conseil fédéral.

[3] Ils peuvent informer l'instance de décision concerné des résultats de l'évaluation lorsque la personne contrôlée:

a. est assujettie au contrôle de sécurité en relation avec une autre activité sensible au sens de la présente loi;

b. est assujettie à un contrôle de fiabilité au sens d'une autre loi fédérale;

c. est assujettie, comme militaire, à un examen de dangerosité en vertu de l'art. 113 de la loi fédérale du 3 février 1995 sur l'armée et l'administration militaire[6] (LAAM).

[4] Ils peuvent aussi informer l'instance chargée de statuer sur la remise ou le retrait de l'arme militaire (selon l'art. 113 LAAM) des résultats de l'évaluation.

Art. 45 Communication de constatations avant la clôture du contrôle de sécurité

Si les services spécialisés CSP disposent, avant la clôture de l'évaluation, d'éléments concrets attestant qu'un risque pour la sécurité pourrait exister et si l'affaire est urgente, ils peuvent informer par écrit les instances ou services visés à l'art. 44 et la personne concernée des constatations faites jusque-là.

6 RS **510.10**

Section 4 Conséquences de l'évaluation

Art. 46 Exercice d'une activité sensible

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

[2] L'instance de décision décide, après avoir pris connaissance des résultats de l'évaluation, si la personne contrôlée peut exercer l'activité sensible en question.

[3] Elle peut soumettre l'exercice de cette activité à conditions.

Art. 47 Devoir de communication

L'instance de décision informe par écrit le service spécialisé CSP compétent lorsqu'elle:

a. confie une activité sensible à une personne pour laquelle une déclaration au sens de l'art. 43, al. 1, let. c ou d, a été établie, ou

b. déroge aux conditions recommandées par le service spécialisé CSP en confiant l'activité sensible.

Art. 48 Utilisation d'une déclaration pour d'autres activités

Il est possible de renoncer à procéder à un contrôle lorsqu'une déclaration de sécurité de valeur au moins équivalente a déjà été établie en faveur de la personne concernée suite à un contrôle pour:

a. une autre activité sensible au sens de la présente loi;

b. une activité au sens d'autres lois fédérales dont l'exercice nécessite un contrôle de fiabilité.

Art. 49 Certificat de sécurité à usage international

Le service spécialisé CSP compétent délivre sur demande un certificat de sécurité à usage international lorsqu'il a établi une déclaration de sécurité en faveur de la personne concernée.

Art. 50 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] Lorsque le service requérant ou l'instance de décision a des raisons d'estimer que de nouveaux risques sont apparus depuis le dernier contrôle, il peut en tout temps demander au service spécialisé CSP compétent que le contrôle de sécurité soit répété, avec motivation écrite.

Art. 51 Voies de droit

[1] Dans un délai de dix jours à compter de la remise d'une déclaration au sens de l'art. 43, al. 1, la personne concernée peut:

a. consulter les documents du contrôle;

b. exiger la rectification de données erronées;

c. exiger la suppression des données obsolètes dans les dossiers des services spécialisés CSP ;

d. exiger l'inscription d'une remarque attestant sa contestation.

[2] L'art. 9 de la loi fédérale du 19 juin 1992 sur la protection des donnée[7] (LPD) est applicable aux restrictions imposées à la communication de renseignements.

[3] Dans un délai de 30 jours à compter de la remise de la déclaration, la personne concernée peut exiger du service spécialisé CSP compétent qu'il émette une décision sur les résultats de son contrôle.

Section 5 Traitement de données personnelles

Art. 52 Système d'information sur le contrôle de sécurité relatif aux personnes

[1] Les services spécialisés CSP engagent un système d'information pour réaliser et gérer les contrôles de sécurité relatif aux personnes.

[2] Chaque service spécialisé CSP est responsable du traitement correct, opportun et adapté des données personnelles qu'il traite dans le système d'information.

[3] Les données personnelles et les profils de la personnalité au sens de l'art. 3, let. c et d, LPD[8], peuvent être traités dans le système d'information lorsque l'évaluation du risque pour la sécurité l'exige.

[4] Le système d'information contient les données suivantes:

a. les données d'identité des personnes devant être contrôlées ou qui ont été contrôlées;

b. les données au sens de l'art. 39 collectées pour le contrôle de sécurité;

c. l'évaluation du risque pour la sécurité;

d. les résultats de l'évaluation selon l'art. 43, al. 1, avec l'identité, l'adresse, le numéro d'assuré AVS, le degré du contrôle, la date et l'échéance;

e. la décision de l'instance de décision;

f. les données et les dossiers d'éventuelles procédures de recours;

g. les listes et statistiques contenant des données au sens des let. a à f.

7 RS **235.1**
8 RS **235.1**

[5] Le traitement des données au sens de l'al. 4 en dehors du système d'information doit être signalé dans ledit système.

Art. 53 Communication des données

[1] Les organes ci-après peuvent consulter en ligne les données suivantes:

a. les services spécialisés CSP: toutes les données au sens de l'art. 52, al. 4;

b. les services requérants au sens de l'art. 36: les données au sens de l'art. 52, al. 4, let. b, qui sont collectées d'office lors de l'ouverture de la procédure de contrôle, ainsi que les données au sens de l'art. 52, al. 4, let. a, d et e;

c. les instances de décision au sens de l'art. 44, al. 1: les données au sens de l'art. 52, al. 4, let. a, d et e;

d. les préposés à la sécurité de l'information au sens de l'art. 84 pour l'exécution de leurs tâches de contrôle: les données au sens de l'art. 52, al. 4, let. a, d et e;

e. les services de la Confédération et des cantons auprès desquels des données au sens de l'art. 39 sont collectées, en tant que mandat de livraison desdites données: les données au sens de l'art. 52, al. 4, let. a.

[2] Les organes ci-après peuvent consulter, par l'intermédiaire d'une interface, les données au sens de l'art. 52, al. 4, let. d, aux fins suivantes:

a. le service spécialisé PSE au sens de l'art. 59 par l'intermédiaire d'une interface liée au système d'information au sens de l'art. 77, pour mener la procédure de sécurité relative aux entreprises.

b. l'Etat-major de l'armée, par l'intermédiaire d'une interface liée au système d'information selon les art. 156 à 161 de la loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée[9] (LSIA), pour traiter les demandes de visite à l'étranger impliquant l'accès à des informations classifiées;

c. l'Etat-major de conduite de l'armée:

1. par l'intermédiaire d'une interface liée au système d'information selon les art. 162 à 167 LSIA, pour contrôler l'accès aux zones de sécurité au sens de l'art. 31 ou aux installations au sens de la législation sur la protection des ouvrages militaires;

2. par l'intermédiaire d'une interface liée au système d'information selon les art. 12 à 17 LSIA, pour accomplir ses tâches légales au sens de l'art. 13 LSIA;

3. par l'intermédiaire d'une interface liée au système d'information selon les art. 18 à 23 LSIA, pour effectuer le recrutement des conscrits et du personnel pour la promotion de la paix.

9 RS **510.91**

[3] Le service spécialisé CSP compétent peut aussi communiquer électroniquement des données au sens de l'art. 52, al. 4, let. d, à d'autres organisations de la Confédération lorsque ces données sont nécessaires pour contrôler l'accès aux zones de sécurité au sens de l'art. 31.

[4] Les services spécialisés CSP peuvent communiquer aux autorités et organisations concernées les listes et statistiques au sens de l'al. 1, let. g, dont elles ont besoin pour exécuter leurs tâches de contrôle conformément à la présente loi. Les listes et statistiques ne peuvent contenir que des données personnelles émanant du domaine de compétence des autorités et organisations concernées.

Art. 54 Conservation et destruction des données

[1] Les services spécialisés CSP peuvent enregistrer, au moyen d'appareils techniques, les auditions au sens de l'art. 39, al. 2, let. d, et al. 5, et les conserver sur des supports de données appropriés.

[2] Ils conservent les données dix ans au plus ou aussi longtemps que la personne concernée exerce sa fonction ou remplit son mandat.

[3] Lorsqu'une personne contrôlée n'occupe pas la fonction prévue ou refuse de remplir le mandat prévu, les données et dossiers sont détruits.

[4] Les services spécialisés CSP détruisent aussi dans les meilleurs délais les données:

b. qui ne correspondent pas au but visé,

c. dont le traitement n'est pas autorisé pour d'autres raisons, ou

c. qui sont inexactes.

[5] Pour les données conservées en dehors du système d'information, les services spécialisés CSP détruisent simultanément les remarques concernant leur traitement au sens de l'art. 52, al. 5.

[6] Demeure réservé l'archivage des données selon les dispositions de la législation fédérale relative à l'archivage.

Section 6 Dispositions complémentaires édictées par le Conseil fédéral

Art. 55

Le Conseil fédéral édicte des dispositions complémentaires concernant:

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

b. l'organisation des services spécialisés CSP;

c. la responsabilité de la protection des données en lien avec le système d'information au sens de l'art. 52;

c. la sécurité des données;

d. le contrôle indépendant, réalisé périodiquement, du traitement correct des données personnelles.

Chapitre 4 Procédure de sécurité relative aux entreprises

Section 1 Dispositions générales

Art. 56 But de la procédure

La procédure de sécurité relative aux entreprises vise à préserver la sécurité de l'information lors de l'adjudication de mandats publics à des entreprises ou parties d'entreprises (entreprises), dans la mesure où ces mandats s'étendent à l'exercice d'une activité sensible (mandats sensibles).

Art. 57 Entreprises assujetties

[1] Font l'objet d'une procédure de sécurité les entreprises:

a. qui sont chargées d'un mandat sensible par une autorité ou une organisation concernée;

b. dont le siège est en Suisse, qui soumissionnent pour des mandats d'une autorité étrangère ou d'une organisation internationale et dont l'exécution exige un certificat de sécurité pour entreprises selon l'art. 73.

[2] La procédure ne peut pas 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. 58 Suspension de la procédure

[1] La procédure de sécurité est suspendue lorsque l'entreprise concernée:

a. revient sur son consentement ou ne participe pas à la procédure;

b. retire son offre;

c. n'obtient pas l'adjudication; ou

d. n'entre plus en considération pour l'exécution du mandat pour une autre raison.

[2] Lorsque la procédure est suspendue, les données et dossiers qui lui sont liés sont détruits.

Section 2 Ouverture de la procédure; exigences de sécurité

Art. 59 Demande d'ouverture de la procédure

[1] Les autorités et organisations concernées demandent au service spécialisé chargée de mener la procédure de sécurité relative aux entreprises (service spécialisé PSE) d'ouvrir cette dernière lorsqu'elles ont l'intention de confier un mandat sensible.

[2] Les autorités concernées désignent les services compétents pour demander l'ouverture de la procédure.

[3] Concernant les mandats d'autorités étrangères ou d'organisations internationales, les demandes d'ouverture d'une procédure sont déposées par les autorités étrangères ou les organisations internationales compétentes.

Art. 60 Examen de la demande

[1] Lorsque les conditions sont réunies pour mener une procédure de sécurité, le service spécialisé PSE en ouvre une.

[2] Ce dernier peut renoncer à en ouvrir une lorsque le risque pour la sécurité peut être suffisamment réduit par d'autres mesures. Il propose les mesures adéquates.

Art. 61 Exigences de sécurité

Après l'ouverture de la procédure, le service spécialisé PSE fixe, en accord avec l'autorité ou l'organisation émettrice du mandat (l'adjudicateur), les exigences relatives à la sécurité de l'information lors de la procédure d'adjudication et de la phase d'exécution du mandat.

Section 3 Qualification des entreprises concernant la sécurité de l'information

Art. 62 Evaluation de la qualification

[1] L'adjudicateur désigne au service spécialisé PSE les entreprises entrant en considération pour l'exécution du mandat sensible.

[2] Le service spécialisé PSE examine si ces entreprises sont qualifiées à exécuter ledit mandat ou s'il existe un risque pour la sécurité.

[3] Le service spécialisé PSE n'est soumis à aucune directive en ce qui concerne l'évaluation de la qualification des entreprises.

Art. 63 Collecte des données

[1] Pour juger de la qualification d'une entreprise, le service spécialisé PSE peut collecter des données:

a. auprès de l'entreprise;

b. auprès du Service de renseignement de la Confédération;

c. à partir de sources publiques d'information.

[2] Il peut demander à des services étrangers des données correspondant à celles visées à l'al. 1.

Art. 64 Risque pour la sécurité

[1] Il existe un risque pour la sécurité lorsque, sur la base des données collectées, des signes concrets donnent à penser que, selon une probabilité élevée, 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, en particulier, être élevée lorsque:

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

b. l'entreprise est contrôlée par des Etats étrangers ou des organisations étrangères de droit public ou privé, ou se trouve sous leur influence, et que ce contrôle ou cette influence sont incompatibles avec les intérêts selon l'art. 43, al. 1, let. c;

c. une déclaration de risque est établie en vertu de l'art. 43, al. 1, let. c, pour les personnes de l'entreprise jugées indispensables dans l'exécution du mandat sensible.

[3] Le risque pour la sécurité doit être justifié par des faits concrets concernant la situation et les relations de l'entreprise, indépendamment de toute faute commise.

Art. 65 Notification de l'évaluation et exclusion de la procédure d'adjudication

[1] Le service spécialisé PSE fait part de son évaluation à l'adjudicateur et la notifie à l'entreprise par une décision.

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

Section 4 Concept de sécurité; déclaration de sécurité pour les entreprises

Art. 66 Concept de sécurité

[1] L'adjudicateur désigne au service spécialisé PSE l'entreprise qui a obtenu l'adjudication.

[2] Le service spécialisé PSE établit un concept de sécurité pour l'entreprise.

[3] A cet effet, il peut collecter les données nécessaires par écrit ou en visitant les lieux.

Art. 67 Contrôles de sécurité relatif aux personnes

[1] Les personnes de l'entreprise qui sont appelées à exercer une activité sensible sont assujetties au contrôle de sécurité.

[2] La décision, en vertu de l'art. 46, al. 2, incombe au service spécialisé PSE.

Art. 68 Déclaration de sécurité pour les entreprises

[1] Le service spécialisé PSE établit, sous la forme d'une décision, une déclaration de sécurité pour les entreprises lorsque l'entreprise apporte la preuve qu'elle a appliqué le concept de sécurité.

[2] Il refuse à l'entreprise la déclaration de sécurité et suspend la procédure si l'entreprise n'applique pas le concept de sécurité. Il émet une décision en conséquence.

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

[4] La durée de validité de la déclaration de sécurité est de cinq ans.

Section 5 Conséquences de la déclaration de sécurité pour les entreprises

Art. 69 Exécution d'un mandat sensible

L'adjudicateur est lié à la décision du service spécialisé PSE. Il ne peut confier le mandat sensible qu'après l'établissement de la déclaration de sécurité pour les entreprises.

Art. 70 Obligations de l'entreprise

[1] Les entreprises au bénéfice d'une déclaration de sécurité appliquent constamment les mesures prévues par le concept de sécurité.

[2] Elles informent immédiatement le service spécialisé PSE et l'adjudicateur de tout changement et incident en lien avec la sécurité.

Art. 71 Contrôles et mesures de protection

[1] Le service spécialisé PSE est habilité à:

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

b. consulter les documents relatifs au mandat.

[2] Lorsque des indices 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 et, notamment, mettre les documents et matériels en lieu sûr.

Art. 72 Procédure simplifiée en cas d'adjudication d'autres mandats sensibles

[1] En cas d'adjudication d'autres mandats sensibles, les entreprises au bénéfice d'une déclaration de sécurité sont réputées qualifiées au sens de l'art. 62.

[2] Lorsqu'une telle entreprise obtient l'adjudication, le service spécialisé PSE examine la nécessité d'une adaptation du concept de sécurité.

Art. 73 Certificat de sécurité pour entreprises à usage international

Le service spécialisé PSE établit, sur demande de l'entreprise, un certificat de sécurité pour entreprises à usage international.

Section 6 Révocation de la déclaration de sécurité, répétition de la procédure de sécurité et voies de droit

Art. 74 Révocation de la déclaration de sécurité pour les entreprises

[1] Le service spécialisé PSE révoque la déclaration de sécurité lorsque:

a. l'entreprise n'a pas rempli ses obligations au sens de l'art. 70;

b. un risque pour la sécurité est identifié dans le cadre d'une répétition de la procédure.

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

Art. 75 Répétition de la procédure

La procédure de sécurité est répétée lorsque:

a. un mandat sensible est pendant à l'échéance de la déclaration de sécurité;

b. des motifs concrets donnent à penser que de nouveaux risques pour la sécurité sont apparus suite à des changements importants au sein de l'entreprise.

Art. 76 Voies de droit

[1] Suite à la notification des décisions du service spécialisé PSE, les organes de l'entreprise ont dix jours pour:

a. consulter les documents;

b. exiger la rectification des données erronées;

c. exiger la suppression des données obsolètes dans les dossiers du service spécialisé PSE;

d. exiger l'inscription d'une remarque témoignant de sa contestation.

[2] L'art. 9 de la loi fédérale du 19 juin 1992 sur la protection des données[10] (LPD) est applicable aux restrictions imposées à la communication des renseignements.

[3] Les décisions du service spécialisé PSE peuvent faire l'objet d'un recours devant le Tribunal administratif fédéral.

Section 7 Traitement des données personnelles

Art. 77 Système d'information sur la procédure de sécurité relative aux entreprises

[1] Le service spécialisé PSE engage un système d'information pour mener la procédure de sécurité et les contrôles de sécurité relatifs aux personnes qui en dépendent.

[2] Le système d'information permet de traiter des données personnelles sensibles et des profils de la personnalité au sens de l'art. 3, let. c et d, LPD[11], lorsque cela s'avère nécessaire pour mener à bien la procédure de sécurité relative aux entreprises.

[3] Le système d'information contient les données suivantes:

a. les données collectées conformément aux art. 63 et 66, al. 3, en vue de la procédure de sécurité;

b. les résultats de l'évaluation selon l'art. 62, al. 2;

c. les résultats des contrôles de sécurité relatifs aux personnes selon l'art. 67, al. 1, nécessaires à la procédure de sécurité relative aux entreprises;

d. la décision du service spécialisé PSE selon l'art. 67, al. 2;

e. le nom des entreprises au bénéfice d'une déclaration de sécurité, date d'émission comprise;

f. les mesures pour d'éventuels contrôles selon l'art. 71;

g. les données et dossiers d'éventuelles procédures de recours.

[4] Le service spécialisé PSE est responsable de la sécurité du système d'information et du traitement correct, opportun et adapté des données personnelles.

Art. 78 Communication des données

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

a. les adjudicateurs au sens de l'art. 61: les données au sens de l'art. 77, al. 3, let. b et d à g;

b. les entreprises qui sont habilitées par le Conseil fédéral, en vertu de l'art. 36, à ouvrir des procédures de contrôle de sécurité relatifs aux personnes dans

10 RS **235.1**
11 RS **235.1**

leur domaine de compétence: les données au sens de l'art. 77, al. 3, let. c et d.

Art. 79 Conservation et destruction des données

[1] Le service spécialisé PSE conserve les données dix ans au plus ou aussi longtemps que l'entreprise concernée est au bénéfice d'une déclaration de sécurité.

[2] Il détruit immédiatement les données:

a. qui ne correspondent pas au but visé;

b. dont le traitement n'est pas autorisé pour d'autres raisons; ou

c. qui sont inexactes.

[3] Demeure réservé l'archivage des données selon les dispositions de la législation fédérale relative à l'archivage.

Section 8 Dispositions complémentaires édictées par le Conseil fédéral

Art. 80

Le Conseil fédéral édicte des dispositions complémentaires concernant:

a. la procédure de sécurité relative aux entreprises;

b. le traitement des données, le système d'information et la sécurité des données;

c. l'organisation du service spécialisé PSE.

Chapitre 5 Sécurité de l'information dans les infrastructures critiques

Art. 81 Tâches de la Confédération

[1] Dans le domaine de la sécurité de l'information, la Confédération prête son concours aux personnes exploitant des infrastructures critiques, notamment lors:

a. de l'identification et de l'évaluation précoces de menaces et de dangers;

b. de la détection d'incidents;

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

d. du suivi des incidents.

[2] Elle gère un service national d'alerte précoce et un service d'assistance pour la prise de mesures préventives et réactives dans le domaine de la sécurité technique de l'information.

[3] Elle s'assure que les personnes exploitant des infrastructures critiques puissent, en toute sécurité, échanger entre elles et avec les services compétents de la Confédération des informations sur les menaces, les risques et les incidents.

Art. 82 Traitement de données personnelles

[1] Afin de prévenir les dangers et dans la mesure où cela est nécessaire à l'exécution de leurs tâches, les services compétents selon l'art. 81 sont habilités à traiter des données personnelles, notamment des ressources d'adressage dans le domaine des télécommunications, et à les communiquer aux autorités et organisations concernées et aux services compétents des cantons, ainsi qu'aux tiers. Le traitement peut s'effectuer sans que les personnes concernées s'en apperçoivent.

[2] L'al. 1 s'applique aussi aux données personnelles sensibles liées à des poursuites ou à des sanctions administratives ou pénales.

[3] Les exploitants de moyens TIC ainsi que les fournisseurs de services TIC peuvent communiquer des données personnelles, visées à l'al. 1, liées à un incident, aux services compétents selon l'art. 81 sans que les personnes concernées s'en aperçoivent. Ces données ne peuvent pas être utilisées dans le cadre d'une procédure judiciaire.

Art. 83 Dispositions complémentaires édictées par le Conseil fédéral

Le Conseil fédéral édicte des dispositions complémentaires concernant:

a. la répartition des tâches et la collaboration entre les services assumant les tâches selon l'art. 81 et le Service de renseignement de la Confédération;

b. l'échange d'informations émanant du Service de renseignement de la Confédération entre les services visés à la let. a et leur communication à des personnes exploitant des infrastructures critiques;

c. le traitement des données par les services assumant les tâches visées à l'art. 81, ainsi que la sécurité des données.

Chapitre 6 Organisation et exécution

Section 1 Organisation

Art. 84 Préposés à la sécurité de l'information

[1] Dans leur domaine de compétence, les autorités et organisations ci-après désignent un préposé à la sécurité de l'information et une suppléance:

a. le Conseil fédéral;

b. la délégation administrative des services du Parlement;

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 ont pour tâches:

a. de conseiller et d'aider dans leur domaine les services compétents dans l'accomplissement de leurs tâches et de leurs obligations au titre de la présente loi;

b. de diriger, sur mandat de leur autorité ou de leur organisation, l'organisation spécialisée de la sécurité de l'information et la gestion des risques.

c. de vérifier régulièrement le respect des prescriptions relatives à la sécurité de l'information, de faire rapport à ce sujet et de proposer à leur autorité les mesures qui s'imposent;

d. de signaler, sur une base volontaire, les incidents relatifs à la sécurité de l'information au service spécialisé de la Confédération en matière de sécurité de l'information et à la Conférence des préposés à la sécurité de l'information, ainsi qu'aux services assumant les tâches visées à l'art. 81.

[3] Les préposés à la sécurité de l'information ne sont investis d'aucune tâche pouvant entrer en conflit avec l'une de celles énumérées à l'al. 2.

Art. 85 Conférence des préposés à la sécurité de l'information

[1] Les préposés à la sécurité de l'information, selon l'art. 84, al. 1, sont réunis en une conférence.

[2] La conférence a pour tâches:

a. de promouvoir l'exécution uniforme de la présente loi par toutes les autorités;

b. de conseiller le service spécialisé de la Confédération en matière de sécurité de l'information sur tous les aspects de la coordination de l'exécution et sur tous les points d'importance stratégique;

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

d. d'assurer la coordination avec le Préposé fédéral à la protection des données et à la transparence, et avec les autres services assumant des tâches dans le domaine de la sécurité de l'information.

[3] La conférence édicte son règlement interne.

Art. 86 Service spécialisé de la Confédération en matière de sécurité de l'information

[1] Le service spécialisé de la Confédération en matière de sécurité de l'information a pour tâches:

a. de conseiller et d'aider les autorités concernées et leurs préposés à la sécurité de l'information dans l'exécution de la présente loi, notamment dans la gestion de la sécurité de l'information et dans la gestion des risques;

b. de recommander des mesures d'urgence en cas de menace sur la sécurité de l'information de la Confédération;

c. de mener des contrôles et des inspections sur mandat des autorités concernées;

d. d'évaluer, sur mandat des autorités concernées, les risques auxquels peut être confrontée la sécurité de l'information lors de la mise en service de nouvelles technologies;

e. d'examiner, sur demande des autorités et organisations concernées, l'adéquation de certains processus, moyens, installations, objets et prestations avec les aspects liés à la sécurité.

f. de gérer et coordonner, sur demande des autorités concernées, les aspects liés à la sécurité de l'information dans le cadre de projets transversaux importants;

g. de servir d'interlocuteur pour les contacts spécialisés avec des services nationaux, étrangers ou internationaux œuvrant dans le domaine de la sécurité de l'information;

h. de rendre compte annuellement au Conseil fédéral de la situation en matière de sécurité de l'information au sein de la Confédération.

[2] La préposé du Conseil fédéral à la sécurité de l'information dirige aussi le service spécialisé de la Confédération en matière de sécurité de l'information.

[3] Le Conseil fédéral règle l'organisation du service spécialisé de la Confédération en matière de sécurité de l'information.

Section 2 Exécution

Art. 87 Dispositions d'exécution

[1] Les autorités concernées édictent les dispositions portant exécution de la présente loi. Le Conseil fédéral peut charger la Chancellerie fédérale d'édicter des dispositions d'exécution relatives à ses affaires.

[2] Les compétences que la présente loi attribue aux autorités concernées sont assumées par la Délégation administrative de l'Assemblée fédérale au nom de cette dernière.

[3] Les dispositions d'exécution du Conseil fédéral s'appliquent par analogie aux autorités concernées dans la mesure où ces dernières n'édictent pas de dispositions au sens de l'al. 1 pour leur domaine de compétence.

[4] Le Conseil fédéral détermine, par voie d'ordonnance, les organisations au sens de l'art. 2, al. 2, let. e, devant appliquer, en tout ou en partie, la présente loi.

Art. 88 Exigences et mesures standard

[1] Le Conseil fédéral fixe des exigences et mesures standard relatives à la sécurité de l'information au niveau de l'organisation, du personnel et des constructions, de même que sur le plan technique, en fonction de l'état d'avancement des connaissances et de la technologie.

[2] Il peut déléguer cette tâche au service spécialisé de la Confédération en matière de sécurité de l'information ou à d'autres services compétents.

[3] Les exigences et mesures standard du Conseil fédéral ont une valeur de recommandation, sauf si elles ont été déclarées obligatoires par les autorités concernées.

Art. 89 Cantons

[1] Dans la mesure où des autorités et services cantonaux exercent, sur mandat et sous la surveillance de la Confédération, des activités sensibles, les cantons veillent à appliquer les mesures en se fondant sur la présente loi.

[2] Le Conseil fédéral règle:

a. les contrôles de sécurité relatifs aux personnes, pour les organes cantonaux;

b. le contrôle des mesures appliquées selon l'al. 1.

[2] Chaque canton désigne un service comme interlocuteur pour les autorités fédérales en matière de sécurité de l'information.

Art. 90 Conventions de droit international public

Le Conseil fédéral est habilité à conclure des conventions de droit international public en matière de sécurité de l'information, portant sur:

a. l'échange d'informations sur des menaces, des points faibles 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 réciproque des contrôles de sécurité relatifs aux personnes et des procédures de sécurité relatives aux entreprises;

d. la reconnaissance réciproque des déclarations de sécurité;

e. les contrôles mutuels.

Art. 91 Evaluation

[1] Le Conseil fédéral s'assure que l'exécution, l'opportunité, l'efficacité et le caractère économique de la présente loi sont contrôlés périodiquement.

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

Chapitre 7 Dispositions finales

Art. 92 Modification d’autres actes législatifs

La modification d’autres actes législatifs est réglée en annexe.

Art. 93 Dispositions transitoires

[1] Les déclarations de sécurité relatives aux personnes et aux entreprises fondées sur le droit en vigueur restent valables jusqu’à leur échéance.

[2] Le Conseil fédéral définit les délais transitoires pour les adaptations:

a. aux prescriptions de classification;

b. aux prescriptions de sécurité relatives à l'engagement des moyens TIC.

Art. 94 Référendum et entrée en vigueur

[1] La présente loi est sujette au référendum facultatif.

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

Annexe
(Art. 92)

Modification d'autres actes législatifs

1. Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure[12]

Art. 2, al. 4, let. c

Abrogée

Art. 19 à 21

Abrogés

2. Loi fédérale du 26 juin 1998 sur l'archivage[13]

Art. 6, al. 2

[2] Avant leur remise aux Archives fédérales, les documents classifiés doivent être déclassifiés conformément aux dispositions de la législation sur la sécurité de l'information.

3. Loi fédérale du 24 mars 2000 sur le personnel de la Confédération[14]

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

Dans la mesure où la défense des intérêts de l'employeur l'exige, ce dernier peut exiger des personnes postulant un emploi ou de ses employés qu'ils présentent un extrait du casier judiciaire et du registre des poursuites.

Art. 20b Contrôle de fiabilité

[1] Le Conseil fédéral peut faire contrôler la fiabilité des personnes postulant un emploi et des employés lorsque, dans le cadre de leur fonction, ils doivent:

a. régulièrement représenter la Suisse à l'étranger et pourraient, alors, porter une atteinte considérable à l'image de la Confédération;

12 RS **120**
13 RS **152.1**
14 RS **172.220.1**

b. assumer des compétences décisionnelles ou des tâches de surveillance dans d'importantes affaires financières ou fiscales et pourraient, alors, porter une atteinte considérable aux intérêts financiers de la Confédération.

[2] Le Conseil fédéral détermine quelles fonctions doivent être soumises à contrôle. Il limite ce contrôle à ce qui est strictement nécessaire pour la défense des intérêts de la Confédération.

[3] Les dispositions relatives au contrôle de sécurité relatif aux personnes de la loi fédérale du ... sur la sécurité de l'information[15] s'appliquent par analogie à la procédure de contrôle.

[4] Lorsque les personnes postulant un emploi et les employés selon l'al. 1 font simultanément l'objet d'un contrôle de sécurité au sens de la loi fédérale sur la sécurité de l'information, les deux procédures sont combinées.

4. Code pénal suisse du 21 décembre 1937[16]

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 de la loi fédérale du ... sur la sécurité de l'information[17] et des contrôles de fiabilité au sens de la législation spéciale;

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

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

i. les services spécialisés chargés des contrôles de sécurité relatifs aux personnes selon la loi fédérale sur la sécurité de l'information;

[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 chargés des contrôles de sécurité relatifs aux personnes selon la loi fédérale sur la sécurité de l'information;

15 RS ...
16 RS **311.0**
17 RS ...

5. Loi fédérale du 13 juin 2008 sur les systèmes d'information de la police de la Confédération[18]

Art. 15, al. 4, let. f

[4] Dans l'accomplissement de leurs tâches, les autorités suivantes peuvent consulter en ligne les données du système informatisé:

f. les services spécialisés chargés des contrôles de sécurité relatifs aux personnes selon la loi fédérale du ... sur la sécurité de l'information[19], dans le cadre d'un contrôle de sécurité relatif aux personnes, d'un contrôle de fiabilité ou d'une évaluation du potentiel de violence, en vue d'évaluer le risque pour la sécurité;

Art. 17, al. 4, let. l

[4] Ont automatiquement accès en ligne à ces données:

l. les services spécialisés chargés des contrôles de sécurité relatifs aux personnes selon la loi fédérale du ... sur la sécurité de l'information[20], dans le cadre d'un contrôle de sécurité relatif aux personnes, d'un contrôle de fiabilité ou d'une évaluation du potentiel de violence, en vue d'évaluer le risque pour la sécurité;

6. Loi fédérale du 3 février 1995 sur l'armée et l'administration militaire[21]

Art. 14 Contrôle de fiabilité

[1] La fiabilité des militaires peut être contrôlée lorsque, dans le cadre de leur fonction, ils doivent:

a. régulièrement représenter la Suisse à l'étranger et pourraient, alors, porter une atteinte considérable à l'image de la Confédération;

b. assumer des compétences décisionnelles ou des tâches de surveil-lance dans d'importantes affaires financières ou fiscales et pourraient, alors, porter une atteinte considérable aux intérêts financiers de la Confédération.

[2] Le Conseil fédéral désigne les fonctions devant être soumises à contrôle. Il limite ce contrôle à ce qui est strictement nécessaire pour la défense des intérêts de la Confédération.

18 RS **361**
19 RS ...
20 RS ...
21 RS **510.10**

[3] Les dispositions relatives au contrôle de sécurité relatif aux personnes de la loi fédérale du ... sur la sécurité de l'information[22] s'appliquent par analogie à la procédure de contrôle.

[4] Lorsque les militaires selon l'al. 1 font simultanément l'objet d'un contrôle de sécurité au sens de la loi fédérale sur la sécurité de l'information, les deux procédures sont combinées.

Art. 113, al. 5

[5] Les dispositions relatives au contrôle de sécurité de base selon l'art. 35, let. a, de la loi fédérale du ... sur la sécurité de l'information[23] s'appliquent par analogie à la procédure. Si un contrôle de sécurité de base doit être effectué pour d'autres motifs, les deux procédures sont combinées.

Art. 150, al. 4

Abrogé

7. Loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée[24]

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

Abrogées

8. Loi du 21 mars 2003 sur l'énergie nucléaire[25]

Art. 5

[3] Des mesures de sûreté doivent être prises pour empêcher des tiers d'attenter à la sécurité des installations et des matières nucléaires ou que des matières nucléaires ne puissent être dérobées. Ces mesures doivent, autant que possible, être classifiées et traitées conformément aux dispositions de la loi fédérale du ... sur la sécurité de l'information[26].

22 RS ...
23 RS **...**
24 RS **510.91**
25 RS **732.1**
26 RS **...**

Art. 24 Contrôle de fiabilité

[1] En vue d'une évaluation du risque pour la sécurité, les personnes appelées à exercer des fonctions importantes pour la sécurité nucléaire et pour la sûreté des installations nucléaires sont assujetties à un contrôle de fiabilité.

[2] Le Conseil fédéral désigne les groupes de personnes devant être contrôlés.

[3] Les dispositions relatives au contrôle de sécurité relatif aux personnes de la loi fédérale du ... sur la sécurité de l'information[27] s'appliquent par analogie à la procédure de contrôle.

[4] Les données du contrôle peuvent être communiquées au propriétaire de l'installation nucléaire et à l'autorité de surveillance.

9. Loi du 23 mars 2007 sur l'approvisionnement en électricité[28]

Titre précédant l'art. 25

Chapitre 6 Obligation de renseigner, secret de fonction et d'affaires, contrôle de fiabilité, taxe de surveillance

Art 26a Contrôle de fiabilité

[1] En vue d'une évaluation du risque pour la sécurité, les membres du personnel de la société nationale du réseau de transport appelés à exercer des tâches importantes pour la sécurité du réseau de transport à l'échelon de la Suisse et pour la fiabilité et la performance de son exploitation sont assujettis à un contrôle de fiabilité.

[2] Le Conseil fédéral désigne les groupes de personnes devant être contrôlés. Il limite ce contrôle à ce qui est strictement nécessaire.

[3] Les dispositions relatives au contrôle de sécurité relatif aux personnes de la loi fédérale du ... sur la sécurité de l'information[29] s'appliquent par analogie à la procédure de contrôle.

[4] Les données du contrôle peuvent être communiquées à la direction de la société nationale du réseau de transport, à l'office fédéral et à ElCom.

27 RS **...**
28 RS **734.7**
29 RS ...

10. Loi du 3 décembre 2003 sur la Banque nationale[30]

Art. 16, titre et al. 5

Confidentialité et sécurité de l'information

[5] Dans son domaine, la Banque nationale applique la loi fédérale du … sur la sécurité de l'information[31]. Au demeurant la loi fédérale du 19 juin 1992 sur la protection des données[32] est applicable.

30 RS **951.11**
31 RS ...
32 RS **235.1**