Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapport explicatif concernant la modification de la loi fédérale sur les systèmes d'information de l'armée

du 20 mai 2020

Condensé

Le Département fédéral de la défense, de la protection de la population et des sports (DDPS) exploite plusieurs systèmes d'information, en particulier de l'armée, dans lesquels des données personnelles sont traitées. Cette modification de la loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée (LSIA) crée les bases légales voulues par la législation sur la protection des données afin de pouvoir disposer des données personnelles nécessaires à l'accomplissement des tâches dans le futur.

Contexte

Les exigences du DDPS liées au traitement des données personnelles par ses systèmes d'information en vue de l'accomplissement optimal de ses tâches ont évolué, en particulier aussi en raison du développement de l'armée (DEVA). Afin de pouvoir traiter légalement des données personnelles conformément à ces nouvelles exigences, le droit de la protection des données requiert l'existence d'une base légale. Actuellement, le LSIA ne contient pas encore ces bases légales requises par le droit de la protection des données. Il est donc nécessaire d'adapter les dispositions relatives aux systèmes d'information déjà réglés par la LSIA et d'en édicter pour les nouveaux systèmes d'information nécessaires.

Contenu du projet

Le projet prévoit d'adapter les dispositions générales de la LSIA et celles relatives aux systèmes d'information déjà réglés par la LSIA ainsi que d'édicter des dispositions pour des nouveaux systèmes d'information dans la LSIA.

Ces modifications concernent notamment (a.) le traitement de nouvelles données personnelles ou à des fins nouvelles, (b.) la collecte ou la communication de données personnelles auprès respectivement envers d'autres services, personnes ou systèmes d'information, (c.) le regroupement des systèmes d'information, (d.) la nouvelle réglementation des organes responsables des systèmes d'information, (e.) le changement des noms des systèmes d'information, (f.) la simplification de la transmission des données par des accès en ligne, par des interfaces et par des portails électroniques ainsi que (g.) la nouvelle réglementation de la durée de conservation des données.

Table des matières

Rapport explicatif

1 Contexte

1.1 Mesures nécessaires et buts

Le Groupement Défense et les unités administratives qui lui sont subordonnées détiennent et exploitent plusieurs systèmes d'information de l'armée. Le traitement de *données personnelles sensibles et de profils de la personnalité* que ces systèmes renferment est régi par la loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée (LSIA)[1]. Celle-ci contient aussi des dispositions concernant divers systèmes d'information exploités par d'autres unités du Département fédéral de la défense, de la protection de la population et des sports (DDPS) et le traitement qui y est fait des données personnelles.

Le processus global de *développement de l'armée* (DEVA) a nécessité une adaptation fondamentale des structures, de l'organisation et des processus au sein de l'armée et du Groupement Défense (et des unités administratives qui lui sont subordonnées). Les exigences liées au traitement des données personnelles – notamment ces données sensibles – par les systèmes d'information du Groupement Défense et de ces unités en vue de l'accomplissement de leurs tâches ont évolué: certains besoins ont disparu ou changé et d'autres sont apparus. Il en va de même pour les systèmes d'information du DDPS que n'exploite pas le Groupement Défense.

Actuellement, la LSIA ne tient pas compte des nouvelles exigences liées au traitement des données personnelles dans les systèmes d'information du DDPS. Les bases légales en matière de protection des données (cf. art. 17 de la loi fédérale du 19 juin 1992 sur la protection des données [LPD][2]), indispensables pour garantir à l'avenir l'accomplissement des tâches au DDPS, en particulier à l'armée et au Groupement Défense, font défaut. Une révision de la LSIA s'impose donc.

1.2 Solution proposée

Pour prendre en compte l'évolution des besoins du DDPS et les exigences de la législation sur la protection de données en regard du traitement des données personnelles par les systèmes d'information, les dispositions de la LSIA relatives à ces systèmes seront adaptées et de nouvelles dispositions édictées pour les nouveaux systèmes d'information dont la nécessité est reconnue et qui traitent aussi des données personnelles sensibles et des profils de la personnalité.

1.3 Programme de la législature et la stratégie du Conseil fédéral

L'adaptation des bases légales pour les systèmes d'information de l'armée et du DDPS n'est pas mentionnée explicitement dans l'arrêté fédéral du 14 juin 2016 sur

1 RS **510.91**
2 RS **235.1**

le programme de la législature 2015 à 2019[3] et dans le message du 29 janvier 2020 sur le programme de la législature 2019 à 2023[4]. Étant donné que cette adaptation est une condition à l'accomplissement optimal des taches légales incombant au DDPS – ainsi qu'au Groupement Défense et à l'armée en particulier –, elle vise à atteindre d'autres mesures et objectifs cités dans ce programme et ce message (tel l'objectif: «La Suisse connaît les menaces [intérieures et extérieures] qui pèsent sur sa sécurité et dispose des instruments nécessaires pour y parer efficacement»[5]). L'adaptation proposée et l'optimisation de l'environnement des systèmes d'information qu'elle suscite contribuent aussi à atteindre l'objectif fixé par le Conseil fédéral pour 2020, à fournir des prestations étatiques efficaces, autant que possible sous forme numérique (cf. Objectifs du Conseil fédéral 2020, volume I, objectif 2, p. 11 ss; voir aussi le message sur le programme de la législature 2019 à 2023, objectif 2[6]).

1.4 Questions sur la mise en œuvre

Sous réserve de son adoption par les Chambres fédérales, la solution proposée devrait entrer dans les faits à partir du 1er août 2022.

Le projet doit trouver sa concrétisation dans les dispositions d'exécution d'une ordonnance. Les lignes directrices qu'elles contiendront seront reprises du présent rapport. Le Conseil fédéral et le DDPS élaboreront ces dispositions de telle sorte qu'elles soient approuvées et entrent en vigueur à la date prévue, soit le 1er août 2022.

1.5 Classement d'interventions parlementaires

Le présent projet n'entraîne pas le classement d'interventions parlementaires.

2 Grandes lignes du projet

Le projet prévoit d'adapter les dispositions relatives à plusieurs systèmes d'information déjà réglés par la LSIA ou d'en établir pour les nouveaux. Ces adaptations sont les suivantes:

- étendre l'objet et le champ d'application de la LSIA aux systèmes d'information du DDPS, y compris la modification du titre et d'autres modifications rendues ainsi nécessaires dans d'autres dispositions;
- créer une base légale pour l'utilisation et le traitement du numéro d'assuré AVS dans les systèmes d'information du DDPS ne relevant pas de l'armée;
- intégrer dans le réseau des systèmes d'information ceux réglés par les dispositions d'exécution relatives à la LSIA;

3 FF **2016** 4999
4 FF **2020** 1709
5 FF **2016** 4999, 5006 (arrêté fédéral sur le programme de la législature 2015 à 2019, objectif 16); FF **2020** 1709, 1790 s. et 1829 s. (message sur le programme de la législature 2019 à 2023, objectif 15)
6 FF **2020** 1709, 1767 s. et 1821

- communiquer les données personnelles aux fournisseurs externes de prestations informatiques chargés des tâches de maintenance, d'entretien et de programmation;
- intégrer le Système d'information sur le recrutement (SIR) et la banque de données cliniques du Service psycho-pédagogique de l'armée (banque de données SPP) dans le Système d'information sur le personnel de l'armée et de la protection civile (SIPA);
- créer une base légale pour le traitement d'autres données personnelles dans divers systèmes d'information (SIPA, Système d'information sur l'évaluation du détachement de reconnaissance de l'armée [EDRA], Système d'information sur les autorisations de conduire militaires [SIAC]);
- préciser la base légale pour le traitement des données personnelles dans le Système d'information du Centre de dommages du DDPS (CEDO);
- créer une base légale permettant d'acquérir des données personnelles traitées dans les systèmes d'information ou lors de l'engagement de moyens de surveillance par d'autres services, personnes ou systèmes d'information, de les communiquer à ces derniers, voire de les traiter à d'autres fins;
- désigner le Groupement Défense comme exploitant de divers systèmes d'information (SIPA, Systèmes d'information sur les patients [SIPAT], Système d'information de la médecine aéronautique [MEDIS FA], Système d'information du domaine social [SISOC], Système d'information et d'intervention du Service sanitaire coordonné [SII SSC]), ce qui permet de définir les unités administratives subordonnées – détentrices des données et organes fédéraux responsables de la protection des données – dans les dispositions d'exécution au niveau de l'ordonnance;
- renommer certains systèmes d'information (EDRA, SISOC, SIAC, Système de journal et de rapport de la Sécurité militaire [JORASYS], CEDO, Système d'information stratégique de la logistique [SISLOG]);
- créer une base légale permettant l'utilisation de certaines données du Système d'information pour l'administration des prestations (MIL Office) afin d'empêcher tout abus dans le domaine des allocations pour perte de gain, ainsi que leur communication à la centrale de compensation;
- régler l'utilisation d'un portail électronique pour la transmission volontaire aux commandements militaires compétents des données personnelles traitées dans MIL Office (p. ex. des demandes de congé documentées);
- prolonger la durée de conservation des données personnelles (Systèmes d'information pour les simulateurs [SISIM], Système d'information pour la gestion de l'instruction [Learning Management System, LMS DDPS], SIAC) ou la réglementer pour MEDIS FA, JORASYS;
- permettre de consulter des données accessibles en ligne ou automatiquement par une interface (Système d'information du contrôle de sécurité relatif aux personnes [SICSP], JORASYS);

– établir une réglementation pour le Système d'information sur la protection préventive de l'armée (SIPPA; sert au Service de protection préventive de l'armée [SPPA] pour l'accomplissement de ses tâches et pour la tenue d'un journal et la gestion de ses engagements) et pour le Système d'information *Master Data Management* (MDM; vise l'administration et la préparation de données de base communes et formelles de partenaires commerciaux pour divers processus d'affaires concernant le DDPS);
– apporter des modifications formelles, d'ordre linguistique ou en rapport avec la technique législative (dispositions générales, SIPA, Système d'information médicale de l'armée [MEDISA], Système d'information sur le personnel du Groupement Défense [SIP DEF], SII SSC, MIL Office, Système d'information pour la gestion des compétences [SIGC], Système d'information et de conduite du soldat [SICS], SIAC, JORASYS, Système d'information pour la gestion intégrée des ressources [PSN]).

3 Explication relatives aux dispositions

Titre

La LSIA règle déjà le traitement des données personnelles dans divers systèmes d'information qu'exploitent d'autres unités administratives du DDPS que celles du Groupement Défense. Le titre de l'acte, qui se limite aux systèmes d'information de l'armée, doit donc être élargi à l'ensemble du département.

Préambule

Les dispositions mentionnées dans le préambule (art. 40, al. 2, et art. 60, al. 1, Cst.[7]) constituent la base légale de la réglementation des systèmes d'information de l'armée. Le projet vise à étendre cette base aux systèmes d'information autres que militaires du DDPS déjà régis par la LSIA (faute d'une norme de compétence explicite en faveur de la Confédération), conformément à la pratique visée à l'art. 173, al. 2, Cst.

Art. 1, al. 1, phrase introductive, let. b, c, d, et al. 2

Le champ d'application est trop limitatif. Il faut ajouter à la liste des systèmes d'information de l'armée déjà régis par la LSIA ceux du DDPS qui n'ont pas de caractère militaire (cf. art. 1, al. 1, phrase introductive). Puisque les données personnelles contenues dans ces derniers ne sont pas seulement traitées en vu de l'accomplissement de tâches en lien avec les affaires militaires, mais aussi de celles en rapport avec le DDPS, il est nécessaire de compléter l'art. 1, al. 1, let. d. De plus, des données personnelles en rapport avec la protection civile sont traitées dans divers systèmes d'information régis par la LSIA. C'est pourquoi il est prévu de

7 RS **101**

mentionner aussi dans l'art. 1, al. 1, let. b, c et d, les membres de la protection civile et les personnes remplissant des tâches relevant de cette dernière.

Par ailleurs, les dispositions de la LSIA sur les divers systèmes d'information ne prévoient pas uniquement le traitement de données personnelles sensibles et de profils de la personnalité (au sens des art. 3, let. c et d, LPD), mais aussi d'autres données (telles celles réglées dans les art. 128, let. b, 143c, let. a, 167c, al. 1, let. a, 179c, al. 1, let. a, et 179i, let. a, LSIA). Ceci est pris en compte dans la phrase introductive de l'art. 1, al. 1, par l'adjonction de la mention autres données personnelles (hormis les données personnelles sensibles et les profils de la personnalité).

L'art. 1, al. 2, indique que seul le traitement de données par le service de renseignement (réglé dans d'autres actes) est exclu du champ d'application, et non le traitement de donnée concernant ce service et son personnel.

Art. 2, al. 1, phrase introductive et let. a

Puisque le champ d'application général de la LSIA doit être étendu aux systèmes d'information autres que militaires du DDPS (cf. les explications relatives à l'art. 1, al. 1, phrase introductive), ses dispositions générales, en particulier l'art. 2 (Principes du traitement des données), doivent s'appliquer par analogie auxdits systèmes. C'est ce que souligne la phrase introductive de l'art. 2, al. 1. Cette extension crée notamment la base légale nécessaire à l'utilisation du numéro d'assuré AVS dans les systèmes d'information autres que militaires du DDPS selon l'art. 50a, al. 1, de la loi du 20 décembre 1946 sur l'assurance-vieillesse et survivants[8]. Dans le cadre de l'accomplissement des tâches légales, de nombreux points de contact existent entre les unités administratives du DDPS n'appartenant pas au Groupement Défense et entre l'armée et l'administration militaire, d'où l'exploitation de divers systèmes d'information (p. ex. LMS DDPS, système de gestion des identités [ICAM]) dans l'ensemble du DDPS. Le recours aux numéros d'assuré AVS pour identifier les personnes s'impose donc aussi dans les domaines autres que militaires afin de garantir que les activités administratives et l'accomplissement des tâches soient optimaux et efficaces.

L'art. 2, al. 1, let. a, sera abrogé car la nécessité d'avoir une base légale pour le traitement de données personnelles et pour leur accessibilité en ligne figure déjà dans les art. 17 et 19, al. 3, LPD (qui s'applique ici aussi en vertu de l'art. 1, al. 3, LSIA). Il fonde aussi son contenu sur celui de l'actuel art. 1, al. 1, LSIA et ne s'applique plus au traitement des données personnelles qui seront mentionnées dans ce même art. 1, al. 1 (cf. les explications déjà données à ce sujet), et ne peuvent être qualifiées de sensibles ou assimilées aux profils de la personnalité. Le traitement de ces données ou leur accessibilité en ligne ne requiert pas de base légale dans une loi; une disposition dans une ordonnance du Conseil fédéral suffit (cf. art. 17 et 19, al. 3, LPD, art. 186, al. 1, let. b, LSIA).

8 RS **831.10**

Art. 3

Puisque le champ d'application général de la LSIA sera étendu aux systèmes d'information autres que militaires du DDPS, il est possible d'envisager d'autres prestataires que la Base d'aide au commandement pour ces systèmes en particulier. L'art. 3 doit donc être abrogé. Les exploitants techniques d'un système d'information donné peuvent, par exemple, être désignés dans un règlement de traitement (cf. art. 36, al. 4, LPD, en relation avec l'art. 21 de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données[9]).

Art. 4, al. 1

Puisque le champ d'application général de la LSIA doit être étendu aux systèmes d'information autres que militaires du DDPS, ces systèmes doivent pouvoir être intégrés au réseau des systèmes d'information réglé par l'art. 4. La réglementation contenue dans les dispositions d'exécution de la LSIA (cf. l'art. 2, al. 2, de l'ordonnance du 16 décembre 2009 sur les systèmes d'information de l'armée [OSIAr][10]) prévoit l'intégration dans le réseau visé à l'art. 4 LSIA des systèmes d'information réglés dans ces dispositions d'exécution.

Art. 6

L'art. 6 LSIA fixe le niveau de la réglementation (loi formelle ou traité international sujet au référendum) nécessaire pour la base légale sur laquelle fonder le traitement de données personnelles sensibles et de profils de la personnalité (cf. le champ d'application visé à l'art. 1, al. 1) dans le cadre de la coopération internationale. Pour ne pas étendre cette exigence – lors du processus prévu d'élargissement du champ d'application de la LSIA – aux données personnelles qui ne sont pas sensibles, l'art. 6 doit être adapté. Pour le traitement de ce genre de données dans le cadre de la coopération internationale réglée par l'art. 6, les dispositions d'exécution edictées par le Conseil fédéral pour la LSIA ou un accord international conclu par le Conseil fédéral doivent suffire comme base légale. Vu les art. 17, al. 2, et 19, al. 3, LPD, la limitation à ce niveau de la réglementation s'avère indiquée, alors que le traitement de données personnelles sensibles et de profils de la personnalité doit d'être réglementé dans une loi au sens formel.

Art. 7, al. 2, première phrase

Les fournisseurs de prestations informatiques internes à la Confédération dépendent, pour des raisons de coûts et d'efficacité, de prestataires externes à leur unité administrative ou à l'administration fédérale. Il peut ainsi arriver que ceux-ci, en vue de l'exécution de tâches de maintenance, d'entretien ou de programmation, doivent divulguer des données personnelles qui ne sont pas généralement accessibles pour pouvoir maintenir en fonction les systèmes d'information ou limiter les périodes d'interruption. Par souci de clarté, il est nécessaire de préciser dans l'art. 7, al. 2,

9 RS **235.11**
10 RS **510.911**

première phrase, que ces prestataires externes comptent aussi parmi les personnes autorisées à traiter des données dans le respect des conditions mentionnées.

Art. 8

La disposition doit être simplifiée et adaptée au déroulement chronologique de la conservation et de l'archivage des données. On mentionnera d'abord la proposition d'archivage, et ensuite seulement la destruction des données (la notion d'effacement étant désormais caduque).

Art. 11

La question de savoir quelles données personnelles doivent être traitées par un système d'information, dans quel but et sous quelle forme, et quelle doit être leur durée de conservation, doit être réglée dans les dispositions particulières. L'art. 11 peut donc être abrogé.

Art. 13, let. n, o et p, 14, al. 1, let. a^{bis}, c^{bis} et n, 2, phrase introductive, et 4, 15, al. 1, phrase introductive et 4, 16, al. 1, phrase introductive, let. b^{bis}, et 1ter, 17, al. 4ter, 4^{quater} et 5 (SIPA)

La réglementation en vigueur du SIPA doit être adaptée aux réalités et besoins actuels, voire étoffée.

Les changements principaux concernent l'intégration dans le SIPA de deux systèmes d'information, le SIR (cf. art. 18 ss) et la banque de données SPP (cf. art. 36 ss). À ce sujet, il est indispensable d'adapter et de compléter les dispositions du SIPA comme indiqué ci-après.

- Pour l'intégration du SIR, il faut adapter trois dispositions: les art. 14, al. 1, let. a^{bis}, 16, al. 1, phrase introductive et let. b^{bis}, et 17, al. 4ter. Dans la première, on s'appuie sur l'art. 20. Dans la deuxième, on s'appuie sur l'art. 22, al. 1, qui donne l'accès au personnel compétent pour les tâches visées à l'art. 14, al. 1, let. a^{bis}. Dans la troisième, on s'appuie sur l'art. 23, qui fixe un délai d'une semaine. Les autres dispositions du SIR sont déjà reprises, en termes de contenu, dans celles du SIPA.
- Pour l'intégration de la banque de données SPP, il faut adapter les art. 13, let. o (correspond à l'art. 37, let. a), 14, al. 4 (art. 38), 15, al. 4 (art. 39), 16, al. 1ter (art. 40, al. 1, les données à communiquer selon l'art. 40, al. 2 sont régies par l'art. 14, al. 1, et peuvent être collectées selon l'art. 15, al. 1, let. d auprès du SPP puis communiquées aux autorités et commandement militaires visés à l'art. 16, al. 1, let. a et b), et 17, al. 4^{quater} (art. 41).

En outre, le complément prévu à la fin de la phrase introductive de l'art. 16, al. 1, limite la communication de données selon le principe de proportionnalité appliqué au traitement des données (cf. art. 4, al. 2, LPD) sous l'angle de l'intégration du SIR et de la banque de données SPP, et dès lors des données sanitaires versées entre autres dans le SIPA. Il s'impose d'éviter que n'importe qui puisse consulter

l'ensemble des données (telles les données sanitaires collectées lors du recrutement visées à l'art. 14, al. 1, let. a^{bis}), d'où la limitation aux données nécessaires.

Les modifications apportées aux art. 13, let. n, et 14, al. 1, let. n, permettent de traiter les données du SIPA en rapport avec l'examen et le contrôle des indemnités de formation. Les données du SIPA seront, selon l'art. 13, let. p, accessibles pour donner des réponses anonymisées aux questions sur des statistiques du DDPS. De plus, les données sur les instructions suivies et les autorisations obtenues pour l'utilisation de systèmes militaires doivent aussi être versées dans le SIPA (cf. art. 14, al. 1, let. c^{bis}) pour assurer notamment une répartition, une planification et une administration optimales des effectifs du personnel de l'armée. La modification apportée à l'art. 17, al. 5, et l'ajout de la précision au plus indiquent que l'effacement des autres données du SIPA que celles visées aux alinéas précédents de l'art. 17 est aussi possible avant l'échéance de cinq ans (p. ex. effacement par classe d'âge) et qu'un délai de conservation de cinq ans n'est pas obligatoire.

La modification apportée à l'art. 14, al. 2, est secondaire, d'ordre linguistique et relève de la technique législative. Le lien avec le SIPA est déjà établi dans l'al. 1, et il est donc inutile de répéter l'abréviation du système d'information dans l'art. 14, al. 2.

Art. 18 à 23 (système d'information SIR)

Vu l'intégration du SIR dans le SIPA et le traitement de ses données dans ce dernier (cf. art. 14, al. 1, let. a^{bis}), les dispositions en vigueur relatives au SIR peuvent être abrogées.

Art. 24, 27, phrase introductive, 28, al. 1, phrase introductive, let. c, et al. 3, phrase introductive (système d'information MEDISA)

Comme pour les autres systèmes d'information du Groupement Défense mentionnés dans la LSIA, seul ce dernier (au sens d'une unité administrative supérieure selon l'annexe 1 de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration, OLOGA[11]) est mentionné comme exploitant du MEDISA (cf. art. 24 et phrases introductives des art. 27 et 28, al. 1 et 3). L'unité administrative subordonnée détenant les données et qui est l'organe fédéral responsable de leur protection doit être précisée dans des dispositions d'exécution au niveau de l'ordonnance (cf. art. 2*a* et annexe 1 OSIAr).

La modification apportée à l'art. 28, al. 1, let. c, est d'ordre purement formel et relève de la technique législative (utilisation de l'abréviation SPP introduite précédemment dans l'art. 14, al. 4).

Art. 30 et 33, phrase introductive (système d'information SIPAT)

Cf. les remarques concernant l'art. 24, hormis celle concernant l'art. 28, al. 1, let. c.

11 RS **172.010.1**

Art. 36 à 41 (banque de données SPP)

L'intégration de la banque de données SPP et le traitement de son contenu dans le SIPA (cf. art. 14, al. 4) permet d'abroger les dispositions relatives au SIR.

Art. 42, 45, phrase introductive, 46, al. 1, phrase introductive, et 2, et 47, al. 1 et 3 (système d'information MEDIS FA)

Cf. les remarques concernant l'art. 24, hormis celle concernant l'art. 28, al. 1, let. c. L'art. 47, al. 1, doit être abrogé puisque, selon l'art. 8 et la loi fédérale du 26 juin 1998 sur l'archivage[12] (loi sur l'archivage; LAr), les Archives fédérales traitent les documents qui ne sont plus systématiquement utiles. L'art. 2, al. 3, autorise encore le traitement non électronique des données du MEDIS FA. La nouvelle teneur de l'art. 47, al. 3, garantit aussi que les données des personnes traitées ou suivies par l'institut après la fin de la durée de conservation visée à l'art. 47, al. 2, peuvent être consultées et conservées durant dix ans après l'arrêt du traitement ou du suivi.

Titre précédant l'art. 48, art. 48, 49, phrase introductive, let. a et b, 50, 51, phrase introductive, 52, al. 1, et 53, al. 2 (système d'information EDRA)

Outre les données des membres du détachement de l'armée subordonné aux forces spéciales (CFS) et du personnel d'aide à l'engagement (conduite, logistique, aide au commandement), celles des candidats à évaluer et des membres du détachement spécial de la police militaire (qui fait partie du CFS) doivent aussi être traitées. Le nom donné au système d'information, son abréviation et certaines dispositions citant les cercles de personnes concernées (art. 49, let. a et b, et 53, al. 2) seront adaptés de manière à inclure toutes les personnes susmentionnées.

Titre précédant l'art. 54, art. 54 à 58 (système d'information SISOC)

Cf. les remarques concernant l'art. 24, hormis celle concernant l'art. 28, al. 1, let. c.

Le nouveau nom du système d'information («système d'information pour l'assistance sociale» remplaçant «système d'information du domaine social») doit être repris dans l'art. 54 tout comme dans le titre qui précède cet article.

Le but fixé à l'art. 55 doit inclure les membres de la protection civile et le personnel du Service de la Croix-Rouge, les personnes engagées dans le service de promotion de la paix, les membres de la Justice militaire ainsi que les parents des personnes citées à l'art. 55, car ces personnes aussi bénéficient du soutien du Service social de l'armée, conformément à l'ordonnance du 30 novembre 2018 sur le Fonds social pour la défense et le protection de la population[13].

Pour fonder ses décisions, le Service social de l'armée a besoin, en plus des données visées à l'art. 56, de celles relatives à la gestion des cas, des notes sur la conduite d'entretiens et des documents personnels nécessaires à l'évaluation de prestations de

12 SR **152.1**
13 RS **611.021**

conseil et de soutien (notamment financier). Une modification en conséquence de l'art. 56 s'impose. Le SIPA sera aussi être mentionné dans l'art. 57 comme source de données. La collecte de données à partir du SIPA dans le but de planifier des entretiens se limite à l'identité et au numéro d'assuré AVS. En outre, dans l'optique du versement d'une somme à partir du Fonds social pour la défense et la protection de la population, il s'agit de vérifier dans le SIPA si le bénéficiaire y a droit (encore astreint au service militaire) ou non (déjà libéré des obligations militaires).

Les militaires incorporés à l'état-major spécialisé du Service social de l'armée, qui contribuent également à atteindre le but de l'art. 55 LSIA et à accomplir les tâches de ce service et qui, pour ce faire, ont besoin d'accéder aux données du SISOC, doivent aussi être mentionnés explicitement à l'art. 58, let. b, car ils ne font pas partie du personnel du service, mais des éléments de milice de l'armée. Par ailleurs, le service spécialisé Diversité dans l'Armée suisse et l'Aumônerie de l'armée introduits dans l'art. 58 par les let. c et d, qui proposent aussi un appui social aux militaires, doivent pouvoir accéder aux seules données du SISOC concernant leurs clients.

Art. 63, al. 2, et 65, al. 2 (système d'information SIP DEF)

Le Système d'information sur le personnel de la Confédération (BV PLUS) a été remplacé par le Système d'information pour la gestion des données du personnel (IGDP), traité dans les art. 30 à 38 de l'ordonnance du 22 novembre 2017 concernant la protection de données personnelles du personnel de la Confédération (OPDC)[14]. De ce fait, dans l'art. 63, al. 2, l'IGDP remplace le BV PLUS comme source de données. Dans l'art. 65, al. 2, la notion d'effacement est remplacée par celle de destruction.

Art. 72 et 73, phrase introductive (système d'information SII SSC)

Cf. les remarques concernant l'art. 24, hormis celle concernant l'art. 28, al. 1, let. c. Après adaptation, l'art. 72 ne mentionnera plus le SSC. Celui-ci doit donc être explicité dans la phrase introductive de l'art. 73.

Art. 85, al. 2, 86, let. a, a^{bis} et h, 87, let. a, et 88 (système d'information MIL Office)

Afin d'empêcher tout abus dans le cadre du versement des allocations pour perte de gain, la modification des art. 85, al. 2, et 88 (nouvelle let. d) crée une base légale permettant de communiquer à la Centrale de compensation les données du MIL Office sur les décomptes de soldes et de frais ainsi que sur les absences et les services commandés en même temps que d'autres données (identité, adresse, coordonnées, incorporation, grade, fonction et instruction).

L'adaptation de l'art. 87, let. a, crée une base légale permettant à la personne concernée d'utiliser un portail électronique pour transmettre volontairement des données personnelles (telles des demandes de congé assorties d'annexes) au

14 RS **172.220.111.4**

commandement militaire compétent. Cette possibilité raccourcit et simplifie les processus en lien avec l'administration et l'organisation des écoles et des cours (cf. le but du MIL Office visé à l'art. 85 LSIA).

L'adaptation de l'art. 86 (nouvelle teneur de la let. a et ajout de la let. h; l'actuelle let. a devient la let. a^{bis}) reprend ce qui est dit en ce qui concerne les données personnelles (qui ne sont pas sensibles) déjà mentionnées dans les dispositions d'exécution (cf. annexe 16, ch. 1, 5 et 12, OSIAr).

Art. 94 (système d'information SIGC)

Comme dans de nombreuses autres dispositions de la LSIA réglant la communication de données propres à un système d'information, par souci d'uniformité, l'art. 94 ne limite plus cette communication à des personnes uniquement, mais aussi à des services.

Art. 103, phrase introductive et let. a et c (système d'information et de conduite des Forces terrestres, SIC FT)

Le SIC FT ne sera plus engagé pour conduire des actions, mais pour suivre la situation, et servir au commandement des Opérations et à la Base d'aide au commandement dans l'exécution de leurs tâches. D'où la nécessité d'apporter ces précisions à l'art. 103, let. a et c. La modification apportée à la phrase introductive est purement grammaticale.

Art. 109, let. a, et 110, let. a (système d'information et de conduite des Forces aériennes, SIC FA)

Le SIC FA ne sera plus engagé pour conduire des actions, mais pour suivre la situation. D'où la nécessité d'apporter cette précision à l'art. 109, let. a. L'appartenance religieuse n'étant pas traitée par le SIC FA, cette précision peut par ailleurs être biffée à l'art. 110, let. a.

Art. 119 (Système d'information et de conduite du soldat SICS)

La notion d'effacement est remplacée par celle de destruction (cf. explications relatives à l'art. 8).

Art. 121, 123, let. c, 124, al. 2, let. c, et 125, al. 2 (systèmes d'information pour les simulateurs)

Les données des personnes s'entraînant régulièrement sur simulateurs doivent (si possible) être disponibles et conservées durant toute leur période passée à l'armée, qui dépasse généralement cinq ans. La modification de l'art. 125, al. 2, fait ainsi passer la date actuelle de conservation des données de cinq à dix ans. Il est aussi prévu, dans les diverses dispositions (art. 121, 123, let. c, 124, al. 2, let. c, et 125, al. 2), que les données de civils ou de tiers (tels les membres d'organisation

d'intervention d'urgence) s'entraînant sur simulateurs (mais qui ne participent pas à un engagement de durée déterminée de l'armée) puissent être traitées et également collectées par leurs supérieurs civils ou leur être communiquées.

Art. 131 (système d'information LMS DDPS)

L'expérience montre que, souvent, les militaires et les employés du DDPS participent à des activités hors du service une dizaine d'années après la fin de leur obligation de servir dans l'armée ou de leurs rapports de travail, voire continuent un engagement auprès de l'administration fédérale. Pour connaître les capacités acquises par ces personnes dans le LMS et qui sont nécessaires aux activités hors du service ou à un réengagement auprès de la Confédération (p. ex. les conducteurs de véhicules à moteur engagés en dehors du service dans les domaines du transport de marchandises dangereuses ou de la sécurité de l'arrimage, ou encore les officiers fédéraux de tir dans le domaine des prescriptions générales de sécurité) et permettre ainsi de contrôler l'instruction (cf. art. 127, let. d, LSIA) ainsi que d'assurer la gestion des compétences (cf. art. 127, let. g, LSIA), il faut pouvoir conserver les données durant dix ans après la libération des obligations militaires ou la fin des rapports de travail. Ces personnes ne seront ainsi pas obligées de suivre une nouvelle fois les formations ou présenter les certificats de capacités dans la branche correspondante.

Titre précédent l'art. 138, art. 138, 139, phrase introductive, let. a, c, e et f, 140, phrase introductive, let. b, 141, phrase introductive, let. b, c, d et e, 142, al. 1, et 143 (système d'information SIAC)

L'Office de la circulation routière et de la navigation de l'armée (OCRNA) est notamment chargé de l'établissement, de l'administration et du retrait

- des autorisations de conduire militaires pour les conducteurs de véhicules et de bateau (cf. art. 32 et 38 de l'ordonnance du 11 février 2004 sur la circulation militaire, OCM[15], et art. 4 et 14 de l'ordonnance du 1er mars 2006 concernant la navigation militaire, ONM[16]);
- des permis des experts de la circulation militaire (ou des experts aux examens) qui organisent les examens pour les conducteurs de véhicules et de bateau (cf. art. 29 OCM et art. 4 ONM);
- des permis de conduire fédéraux (art. 3 et 11 de l'ordonnance du 1er mars 2006 concernant la navigation civile de l'administration fédérale[17]).

Les données personnelles nécessaires à l'accomplissement de ces tâches doivent être traitées dans le système d'information de l'OCRNA. Aussi, l'appellation trop limitative de système d'information sur les autorisations de conduire militaires (abrégé SIAC) doit être comprise dans un sens plus général et modifiée en système d'information sur la circulation routière et la navigation de l'armée (abrégé SI

15 RS **510.710**
16 RS **510.755**
17 RS **747.201.2**

OCRNA). Les groupes de personnes ainsi que les autorisations de conduire et les permis préalablement cités – dans la mesure où ils n'ont pas encore été mentionnés – doivent venir compléter l'art. 139, let. a et c, et la disposition portant sur les données personnelles à traiter (art. 140, let. b). De plus, l'IGDP (cf. art. 30 à 38 OPDC), en tant que nouvelle source de données, notamment pour ce qui concerne les permis de conduire fédéraux, doit être mentionné dans l'art. 141, let. d.

Par ailleurs, dans l'art. 139, l'actuelle let. f doit être abrogée, car plus aucune donnée n'est désormais traitée dans le cadre fixé par cet article.

Les registres signalés comme sources de données à l'art. 141, let. b, et comme destinataires de données à l'art. 142, al. 1, let. b (registre des autorisations de conduire et registre des mesures administratives), ont été remplacés par le système d'information relatif à l'admission à la circulation (SIAC; cf. l'ordonnance du 30 novembre 2018 sur le système d'information relatif à la circulation[18]).

À l'art. 143, al. 1, la conservation des données du SI OCRNA est prolongée jusqu'à 80 ans après leur saisie. Cette mesure est nécessaire dès lors que les autorisations de conduire militaires conservent leur validité dans le cadre des activités militaires hors du service, même lorsque leurs détenteurs ont quitté l'armée, conformément à l'art. 33 OCM notamment. Elle l'est aussi du fait que de nombreux experts de la circulation militaire ne sont plus forcément astreints au service militaire. C'est pourquoi l'OCRNA doit aussi pouvoir exercer ses tâches d'administration et de contrôle après la libération des obligations militaires de la personne concernée et disposer des données personnelles nécessaires à ces fins. Cela se justifie aussi par le fait que le SIP DEF est indiqué à l'art. 141, let. c, comme autre source de données permettant notamment d'accéder – autrement que par le SIPA – aux dernières données relatives aux permis des experts de la circulation militaire qui ne sont plus astreints au service militaire. Contrairement à l'al. 1, les données du SI OCRNA portant sur les mesures administratives civiles seront conservées, selon l'al. 2, aussi longtemps qu'elles le seront dans le SIAC. Concernant les examens de contrôle visés à l'al. 3, seuls importent à l'OCRNA le moment où les derniers ont été effectués et leurs résultats, ainsi que la durée de validité de ces résultats (afin de savoir quand les prochains examens de contrôle devront être effectués). Les données des examens de contrôle précédents ne doivent pas être conservées.

D'autres modifications touchent l'art. 141, let. e, et 142, al. 1, let. a (par souci d'uniformité, services et personnes au lieu de personnes et services, comme dans de nombreux autres dispositions de la LSIA).

Art. 147, al. 2, let. d, et 148, al. 1, let. c, ch. 2bis, et d (système d'information SICSP)

Les bases légales permettant d'accéder en ligne aux données des diverses banques [sic] de l'office central des armes visés à l'art. 32a, al.1, de la loi du 20 juin 1997 sur les armes (LArm)[19] (plate-forme d'information sur les armes ARMADA) existent déjà. Elles se trouvent dans l'art. 32c, al. 8, en relation avec l'art. 61, al. 2, let. e, et dans l'art. 61, al. 6, en relation avec l'annexe 3 de l'ordonnance du 2 juillet 2008 sur

18 RS **741.58**
19 RS **514.54**

les armes[20]. La possibilité d'un accès en ligne doit aussi être intégrée dans l'al. 2, let. d. Il a été décidé de renoncer à énumérer les diverses bases de données accessibles de l'office central dans l'al. 2, let. d, car la phrase introductive lie l'accès en ligne aux dispositions légales correspondantes, rendant automatiques les adaptations des droits d'accès au niveau de l'ordonnance sans toucher à la LSIA, même lorsque cela concerne le SICSP.

De même, la Société nationale du réseau de transport est mentionnée à l'art. 148, al. 1, let. c, ch. 2bis car, selon l'art. 20a entré en vigueur début 2018 de la loi du 23 mars 2007 sur l'approvisionnement en électricité (LApEl)[21], même les personnes chargées de certaines tâches au sein de cette société doivent être soumises au contrôle de sécurité. L'accès en ligne au SICSP de cette société facilite la communication des résultats des contrôles, comme le prévoit l'art. 20a, al. 3, LApEl. La société pourrait elle-même accéder en ligne aux données du SICSP dans la mesure où seules les données nécessaires à l'accomplissement de ses tâches seraient accessibles selon le principe de proportionnalité impliqué par l'art. 1, al. 3, LSIA, en relation avec l'art. 4, al. 2, LPD.

La précision apportée à l'art. 148, al. 1, let. d, garantit l'accès en ligne des données du SICSP – et donc des contrôles de sécurité relatifs aux personnes – aux seuls services fédéraux chargés de tâches de sécurité dont l'activité doit se fonder sur de telles données. De plus, l'accès est limité aux données qui ne sont pas préjudiciables à la personne concernée.

Titre précédent l'art. 167a, art. 167a, 167b, let. a et b, 167d, 167e, al. 1, 2, let. b et c, et 167f (système d'information)

Le nom JORASYS est adapté aux structures créées dans le cadre du DEVA (*Police militaire* remplace *Sécurité militaire*).

L'art. 167d, let. e, reprend les dispositions de l'actuel 167d, al. 2, LSIA où la nouvelle abréviation SI OCRNA inclut le SIAC (cf. à ce sujet les art. 138 ss et les explications correspondantes). De plus, la phrase introductive de l'art. 167d, let. e, précise qu'il est possible de collecter manuellement (généralement par une interface réseau fournie par les opérateurs du système ou par un logiciel spécifique) ces données en ligne à partir des systèmes d'information visés à l'art. 167d, let. e (notamment ceux visés aux ch. 2 à 7 et 9), ou par une interface permettant une transmission automatique des données. De ce fait, le processus de collecte de données personnelles qui sont nécessaires à l'accomplissement de tâches quotidiennes et doivent rester disponibles dans leur dernière mise à jour est accéléré et simplifié. Dans le détail, les systèmes d'information énumérés à l'art. 167d, let. e, donnent accès aux données suivantes.

20 RS **514.541**
21 RS **734.7**

(Ajouté) **Système d'information**	**Données**
RIPOL	Données sur les infractions non élucidées (p. ex. les objets déclarés volés) (art. 3, let. h, 6, al. 1, let. o, 7, al. 1, et annexe 1, ch. 2 des tableaux, de l'ordonnance du 26 octobre 2016 RIPOL[22])
SIAC	Données sur les véhicules et leur admission à la circulation, sur les conducteurs et leur autorisation de conduire, sur les détenteurs et les assureurs (art. 89e, let. a, de la loi fédérale du 19 décembre 1958 sur la circulation routière[23])
Banques de données visées à l'art. 32a LArm	Accès en ligne aux banques de données de l'office central des armes visées à l'art. 32a LArm pour voir si une personne a l'interdiction d'acquérir une arme ou si une arme lui a été retirée (art. 32a à 32c LArm)
Consultation en ligne des registres d'armes cantonaux	Accès en ligne aux registres cantonaux sur les possesseurs d'une arme à feu (données sur l'acquisition et la possession d'armes à feu) (art. 32a, al. 2 et 3, et 32b, al. 6, LArm)
SIPA	Données militaires comme l'incorporation, le grade, la fonction et les services effectués (art. 167c, al. 1, let. d)
SIP DEF	Données comme la fonction, l'instruction, l'engagement dans l'armée, le statut militaire, la carrière professionnelle, les connaissances linguistiques (art. 62, let. b à e et g, LSIA)
SI IDD	Données comme l'incorporation, le grade, la fonction, l'instruction, la qualification et l'équipement dans l'armée ou la protection civile (art. 176, let. a, LSIA)

L'art. 100 de la loi du 3 février 1995 sur l'armée (LAAM)[24] mentionnant plusieurs tâches que les membres de la Police militaire doivent accomplir, il faut adapter la notion de tâche dans l'art. 167e, al. 1, let. b. Par souci de simplification et de clarté, la notion actuelle de personnes chargées d'évaluer la situation militaire sur le plan de la sécurité et d'assurer l'autoprotection de l'armée (art. 100, al. 1, let. a et e, LAAM et 11 de l'ordonnance du 21 novembre 2018 sur la sécurité militaire, OSM[25]) est également remplacée par celle de personnel du SPPA dans l'art. 167e, al. 1, let. c.

22 SR **361.0**
23 SR **741.01**
24 RS **510.10**
25 RS **513.61**

L'art. 167e, al. 2, let. c, ne cite plus spécifiquement l'organe responsable de la sécurité des informations et des objets (tel le domaine Sécurité des informations et des objets, qui dépend administrativement du Secrétariat général du DDPS), mais englobe, dans une notion générale, tous les services chargés de la sécurité des informations et des objets (dont ceux du Groupement Défense) comme bénéficiaires possibles de données. De plus, considérant qu'il est aussi nécessaire que suffisant de conserver des données dix ans après la fin des activités de la police militaire relatives à un cas donné, l'art. 167f est adapté en conséquence.

(Chapitre 5) / Section 6 (art. 167g à 167l, système d'information SIPPA)

Les art. 167g à 167l nouvellement introduits créent une base légale pour le SIPPA permettant au SPPA d'accomplir ses tâches, de tenir son journal et de diriger son engagement. Ce service doit notamment évaluer la situation en termes de sécurité, et protéger l'armée d'actes illicites, par exemple l'espionnage et le sabotage (art. 100, al. 1, let. a et e, LAAM, et 11 OSM). Pour ce faire, il a besoin de saisir les personnes pouvant représenter une menace et les détails à propos de cette menace.

Ce service devant aussi traiter dans le SIPPA des données personnelles sensibles, la base légale doit figurer dans la loi, conformément à l'art. 17, al. 2, LPD. Les données portent sur l'appartenance ethnique et religieuse, l'orientation politique et idéologique, les caractéristiques médicales et biométriques (identification de personnes ou détection de maladies psychiques touchant à la sécurité de l'armée). Les profils de la personnalité portent sur le lieu de séjour et les profils de déplacement, les moyens de locomotion et de communication avec leur utilisation et leur positionnement, les déplacements.

Les personnes visées à l'art. 167i, let. j, ne constituent pas une menace pour l'armée mais ont un rapport direct avec une personne pouvant constituer une menace pour l'armée. Elles peuvent permettre d'identifier ou d'approcher cette menace pour la réduire ou la neutraliser.

Aux sources indiquées à l'art. 167j, let. a à f, s'ajoutent – par un accès en ligne permanent – les systèmes d'information visés à l'art. 167j, let. g, afin que le SPPA dispose rapidement et aisément des données qui lui sont nécessaires.

Art. 168, 169, phrase introductive, let. d et e, 170, phrase introductive, let. a et a^{bis}, 171, phrase introductive, let. i, 172 et 173 (système d'information SI CEDO)

Le Secrétariat général du DDPS travaille avec l'application qui succède à celle utilisée depuis fin 2003 sous le nom de SI SIN. La désignation technique de la nouvelle application est SI CEDO, pour système d'information) et centre de dommages du DDPS.

L'art. 169, let. d et e, mentionne deux nouveaux buts visés par le SI CEDO.

- Le Centre de dommages DDPS règle les accidents et les sinistres impliquant des véhicules de la Confédération, conformément à l'art. 21 de l'ordonnance du 23 février 2005 concernant les véhicules automobiles de la Confédération et leurs conducteurs[26]. Pour cette raison on lui confie, en vertu de l'art. 5, al. 1, let. b, de l'ordonnance du 20 novembre 1959 sur l'assurance des véhicules[27], l'établissement des attestations d'assurance à l'intention des services cantonaux chargés de l'immatriculation des véhicules (services des automobiles). Désormais, cette procédure peut être traitée sur l'application SI CEDO et ainsi s'ajouter aux buts indiqués (let. d).
- Le règlement des sinistres concerne aussi les véhicules à moteur des députés, conformément à l'art. 4, al. 2, de l'ordonnance de l'Assemblée fédérale du 18 mars 1988 relative à la loi sur les moyens alloués aux parlementaires[28]. Il s'effectue en recourant à l'application SI CEDO, il faut donc l'indiquer dans les buts (let. e).

La base légale du Système d'information du Centre de dommages du DDPS, rendue nécessaire pour des raisons liées à la législation sur la protection des données, permettait déjà de traiter des données concernant des sinistres. Pour répondre aux impératifs actuels de protection, il est nécessaire de préciser ces données dans l'art. 170, let. a, et de citer expressément dans la loi le traitement des données personnelles sensibles des personnes impliquées dans les sinistres – comme celles concernant la situation financière ainsi que les procédures pénales, civiles, disciplinaires et administratives. En outre, le traitement (réduit à son minimum) de données de tiers est également indiqué (cf. art. 170, let. a^{bis}).

Lors du règlement des sinistres, les assurances privées échangent entre elles les données les plus diverses, par exemple pour clarifier la question de la responsabilité au regard des dossiers ou pour établir le montant des créances récursoires. Le fait que le CEDO agisse comme n'importe quel assureur pour collecter des données auprès d'autres assurances n'était jusqu'à présent qu'implicite dans la loi, dans la mesure où ces données devaient être collectées par l'intermédiaire des personnes concernées ou des personnes de contact. Désormais, les assurances sont mentionnées à l'art. 171, let. i.

Le règlement des sinistres exige, dans bien des cas, que certaines données soient communiquées à des tiers, lesquels n'agissent pas toujours formellement sur mandat du Secrétariat général ou du CEDO, d'où la suppression de cette limitation inutile (art. 172, al. 2).

26 RS **514.31**
27 RS **741.31**
28 RS **171.211**

Titre précédent l'art. 174, art. 174, 175, phrase introductive, 176, phrase introductive et let. c, 177, phrase introductive, 178 et 179 (système d'information SISLOG)

La désignation et l'abréviation du système d'information sont adaptées selon sa nouvelle structure et le but principal qu'il vise en tant qu'interface de données. Le système d'information stratégique de la logistique (SISLOG) devient donc le Système d'information concernant l'interface des données de la défense (SI IDD). Le SI IDD ne sera pas seulement utilisé par la Base logistique de l'armée, mais par le Groupement Défense dans son ensemble.

Les données visées à l'art. 176, let. c, qui sont échangées entre les systèmes d'information de l'armée par le truchement du SI IDD, conformément à l'art. 175, let. c, incluent les données au sens de l'art. 1, al. 1.

L'art. 178 différencie plus nettement les services et personnes auxquelles les données personnelles traitées par le SI IDD doivent être communiquées. Ainsi, ces données susceptibles d'être échangées avec d'autres systèmes d'information de l'armée pourront être communiquées uniquement aux services ou personnes compétents. Seules les données personnelles visées à l'art. 176, al. a et b, pourront être communiquées aux commandements militaires et aux unités administratives de la Confédération et des cantons.

Art. 179b, let. d, 179c, al. 4, 179d, let. e, et 179e, al. 2, let. e (système d'information PSN)

En remplacement des deux articles abrogés, on renvoie à l'art. 179c, al. 4, de la loi du 24 mars 2000 sur le personnel de la Confédération[29] uniquement sous sa forme abrégée et à ses dispositions d'exécution (cf. art. 8 ss et 19 ss OPDC, dossier de candidature et dossier du personnel).

Le BV PLUS étant remplacé par l'IGPD, que règlent les art. 30 à 38 OPDC, il en va de même pour son appellation dans les art. 179d, let. e, et 179e, al. 2, let. e.

La modification de l'art. 179b, let. d, est une modification purement formelle qui ne s'impose pour des raisons de technique législative et ne concerne que l'allemand (utilisation de l'abréviation «LArm» précédemment introduite à l'art. 16, al. 3bis).

(Chapitre 6) / Section 5 (art. 179m à 179r, système d'information MDM)

Les art. 179m à 179r (nouveaux) donnent une base légale au MDM exploité par le Secrétariat général du DDPS. Le MDM permet d'administrer et d'utiliser, pour l'ensemble du DDPS, des données homogènes (visées à l'art. 179o) sur les partenaires de ce dernier impliqués ou pouvant l'être dans les processus d'affaires relatifs aux domaines finances, acquisitions, logistique, immobilier et personnel (art. 179n) – communément appelées données de base ou master data. Ces partenaires peuvent être aussi bien des entreprises que des personnes privées. La gestion des données de base prédéfinies est centralisée et assurée uniquement par le

29 RS **172.220.1**

MDM afin d'obtenir une source de données excellente en termes de qualité et de pertinence. En raison des exigences de sécurité et de protection de l'information au sein du DDPS, l'accès au MDM doit se faire par un système d'information qui lui est propre et non par celui que la Confédération (hormis le DDPS) emploie et qui dépend du Département fédéral des finances. Émanant principalement de ce dernier, les données destinées au MDM doivent toutefois être collectées au moyen d'une interface spéciale (art. 179p, let. c); les autres communications de données du MDM au sein du DDPS se font par une procédure d'accès en ligne. Quant à la réglementation concernant la conservation, elle prévoit une durée de 50 ans pour les données de base logistiques impliquant un partenaire (comme celles sur le matériel ou sur la structure des systèmes) en tenant compte du cycle de vie, après la fin des rapports d'affaires avec le partenaire concerné, et pas uniquement les dix ans fixés par la loi du 7 octobre 2005 sur les finances[30] et ses dispositions d'exécution pour les autres données, et de deux ans pour les partenaires potentiels à compter de la date de leur exclusion des rapports d'affaires (art. 179r, al. 1, let. b, et 2).

Art. 181, al. 1, let. a, et 2, phrase introductive (moyens de surveillance)

L'extension du but visé à l'art. 181, al. 1, let. a, permettra d'engager des moyens pour surveiller également des infrastructures de l'armée, de l'administration militaire ou de tiers – tels des biens immobiliers civils de la BLA dans lesquels du matériel de l'armée est entreposé – utilisés à des fins militaires, et de collecter et de traiter les données personnelles nécessaires à cet effet.

L'adaptation de la phrase introductive de l'art. 181, al. 2, précise que l'armée ne met jamais ses moyens de surveillance avec appui aérien et leur personnel *à la disposition* des autorités qui en font la demande, mais leur fournit seulement les prestations obtenues en engageant ces moyens et ce personnel.

Art. 186, al. 3

Cette disposition donne au Conseil fédéral la compétence de conclure des accords internationaux servant de base légale pour le traitement transfrontalier de données personnelles non sensibles (cf. à ce sujet les explications relatives à l'art. 6, let. b).

4 Répercussions

4.1 Conséquences pour la Confédération

Les adaptations proposées dans la LSIA n'ont pas de conséquence pour les finances ou pour le personnel ni d'autre conséquence pour la Confédération. Elles ne créent que les bases légales voulues par la législation sur la protection des données pour légitimer le traitement des données personnelles nécessaires à l'accomplissement des tâches publiques. Les travaux nécessaires, d'ordre technologique (et informatique), s'effectuent dans le cadre des adaptations et des développements des systèmes.

30 RS **611.0**

4.2 Autres conséquences

Les mesures et adaptations du présent rapport n'ont pas d'autre conséquence pour les cantons et les communes, les centres urbains, les agglomérations et les régions de montagne, ni pour l'économie, la société et l'environnement.

5 Aspects juridiques

5.1 Conformité constitutionnelle

Concernant les systèmes d'information de l'armée déjà réglés par la LSIA, comme l'indique le préambule, la Confédération tire entre autres sa compétence de l'art. 60, al. 1, Cst. en regard de la législation militaire ainsi que de l'organisation, de l'instruction et de l'équipement de l'armée, et de l'art. 40, al. 2, Cst. pour ce qui est du traitement des données personnelles des Suisses et des Suissesses de l'étranger. Quant aux systèmes d'information non militaires du DDPS nouvellement introduits dans la LSIA, on peut se fonder sur l'art. 173, al. 2, Cst. faute de normes explicites à ce sujet. De fait, ces systèmes qui ne relèvent pas de l'armée (ainsi que les opérations de traitement des données personnelles qu'ils permettent) servent à assurer des tâches fédérales définies dans d'autres actes législatifs et qui incombent au DDPS. Leur réglementation dépend en fin de compte de l'organisation des unités administratives du DDPS dans la mesure où elles-mêmes ou la Confédération sont compétentes.

5.2 Engagements internationaux de la Suisse

Les modifications proposées sont compatibles avec les engagements de la Suisse relevant du droit international public. Elles n'induisent pour celle-ci aucun nouvel engagement envers un État ou une organisation internationale.

5.3 Forme

Dans le présent cas, il s'agit de dispositions importantes fixant des règles de droit, au sens de l'art. 164 Cst., qui doivent être édictées sous la forme d'une loi. Et le traitement de données personnelles sensibles (au sens de l'art. 17, al. 2, LPD) prévu dans ces dispositions nécessite une base légale.

5.4 Frein aux dépenses

Les modifications proposées ne sont pas assujetties au frein aux dépenses selon l'art. 159, al. 3, let. b, Cst. car elles ne contiennent aucune disposition sur les subventions ni de base pour fixer un crédit d'engagement ou un plafond de dépenses.

5.5 Principes de subsidiarité et d'équivalence fiscale

Les modifications proposées n'ont aucun effet sur les principes de subsidiarité et d'équivalence fiscale.

5.6 Législation sur les subventions

Les modifications proposées ne prévoient pas d'aides financières et d'indemnités au sens de la loi du 5 octobre 1990 sur les subventions[31].

5.7 Délégation des compétences législatives

Les compétences législatives peuvent être déléguées par une loi fédérale dans la mesure où la Cst. n'exclut pas cette possibilité (art. 164, al. 2, Cst.). L'art. 186, al. 3, du présent projet permet au Conseil fédéral de conclure des accords internationaux sur le traitement transfrontalier de données personnelles non sensibles. Le Conseil fédéral est aussi autorisé, en vertu de l'art. 186, al. 1, LSIA, à édicter les dispositions d'exécution nécessaires aux nouveaux systèmes d'information.

5.8 Protection des données

En vertu de la LPD, les organes de la Confédération ne peuvent traiter les données personnelles sensibles et les profils de la personnalité (art. 17, al. 2) et accéder en ligne à des données (l'art. 19, al. 3) que si une loi le prévoit expressément. Afin d'assurer le traitement de données personnelles nécessaire à l'accomplissement de tâches et leur échange, les adaptations prévues dans le présent projet sont requises au regard de la législation sur la protection des données.

31 RS **616.1**