Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Secrétariat général du DDPS SG-DDPS
Digitalisation et cybersécurité DDPS

8 novembre 2023

Droit d'exécution de la loi sur la sécurité de l'information

Rapport sur les résultats de la procédure de consultation

Table des matières

1 Contexte

Le 24 août 2022, le Conseil fédéral a chargé le DDPS de consulter les cantons, les partis politiques, les associations faîtières des communes, des villes, des régions de montagne et du secteur de l'économie qui œuvrent au niveau national ainsi que les autres milieux intéressés sur les dispositions d'exécution de la nouvelle loi sur la sécurité de l'information (LSI). La consultation a pris fin le 24 novembre 2022.

Le droit d'exécution de la LSI comprend trois nouvelles ordonnances et une ordonnance révisée.

- *Ordonnance sur la sécurité de l'information (OSI ; nouveau)* – L'OSI règle la gestion de la sécurité de l'information, la protection des informations classifiées, la sécurité informatique et les mesures relatives à la sécurité personnelle et physique pour l'administration fédérale et l'armée. Elle fixe les tâches, les compétences et les responsabilités en la matière. La principale modification réside dans l'introduction d'un système de management de la sécurité de l'information (SMSI) dans toutes les unités administratives.
- *Ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP ; nouveau)* – L'OCSP compile les dispositions d'exécution sur les différents contrôles de sécurité relatifs aux personnes (CSP). Le nombre de ces contrôles doit être réduit, selon la LSI, au strict minimum requis pour identifier les risques majeurs pour la Confédération.
- *Ordonnance sur la procédure de sécurité relative aux entreprises (OPSEnt ; nouveau)* – L'OPSEnt règle les modalités de la procédure de sécurité relative aux entreprises introduite par la LSI. Cette procédure peut être appliquée à tous les mandats sensibles confiés par la Confédération à des entreprises du secteur privé.
- *Ordonnance sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération (OIAM ; modification)* – La révision partielle de l'OIAM étend le champ d'application de l'ordonnance aux unités administratives de l'administration fédérale décentralisée, dans la mesure où celles-ci ont accès aux systèmes informatiques de l'administration fédérale centrale.

Les cantons ont été priés de se prononcer, lors de la consultation, sur les quatre questions ci-après.

1. La mise en œuvre des ordonnances est-elle compréhensible pour les cantons *(chap. 3.1.1)* ?
2. Comment les cantons envisagent-ils la mise en œuvre des ordonnances *(chap. 3.1.1)* ?
3. À quelles conséquences financières s'attendent les cantons *(chap. 3.1.2)* ?
4. Les cantons devront désigner un service faisant office d'interlocuteur pour les questions relatives à la sécurité de l'information. Quel est cet interlocuteur dans votre canton ?

2 Résultats de la procédure de consultation

	Destinataires	**Nombre de parties consultées**	**Nombre des avis et des commentaires** *(y c. lettre de renonciation expresse à donner un avis)*
1	Cantons	26	27* *(*FR : 2)*
2	Partis politiques	11	2
3	Associations faîtières des communes, villes et régions de montagne	3	0
4	Associations faîtières de l'économie	8	2
5	Autres organisations intéressées	14	2
6	Parties consultées non invitées à titre individuel		3
	Total	**62**	**36**

Appréciation globale	**Nombre**	**Parties consultées**
Oui : adoption sans réserve	12	AI, BS, BE, FR, GL, GR, SH, SO, SG, SZ, TI, VS
Oui, mais : approbation de principe assortie de demandes de modification ou ambiguïtés	22	AG, AR, BL, FR (SITel), GE, JU, LU, NE, NW, OW, TG, UR, VD, ZG, ZH, PS, UDC, asut, MPC, APC, Swissgrid, X. D.
Non, mais : rejet de principe assorti de demandes de modification ou ambiguïtés	0	
Non : rejet	1	USAM
Aucun commentaire : partie consultée ayant expressément renoncé à donner un avis	1	Union patronale suisse

3 Avis sur le droit d'exécution et sur le rapport explicatif

Diverses questions et remarques que le rapport n'aborde pas ont surgi lors de la consultation. Les annonces de fautes d'orthographe ou d'amélioration dans la traduction n'y figurent pas.

3.1 Avis généraux

Il ressort de la consultation qu'une large majorité des parties (**AG, AI, AR, BL, BS, BE, FR, GE, GL, GR, LU, NE, NW, OW, SH, SZ, SO, SG, TI, TG, UR, VD, VS, ZG, ZH, PS, UDC, asut, APC, Swissgrid**) approuvent en principe le droit d'exécution de la LSI. Outre quelques adaptations souhaitées, il reste plusieurs points d'ombre en ce qui concerne la mise en œuvre et la validité de certaines dispositions pour les cantons. Seule l'**Union suisse des arts et métiers (USAM)** rejette l'ensemble du projet au prétexte qu'il dépasserait le cadre de la base légale et que les coûts qu'il générerait ne seraient pas précisés.

L'**UDC** salue l'amélioration sensible de la comparaison avec le droit d'autres pays, rendue possible par la nouvelle LSI, afin d'améliorer la collaboration internationale dans le domaine de la sécurité de l'information. Elle considère toutefois que les données personnelles saisies et enregistrées par la Confédération devraient impérativement être conservées en Suisse, tout au moins celles tombant dans la catégorie de classification la plus élevée. Enfin, elle estime que la voie officielle doit être impérativement choisie pour l'échange de données. L'**UDC** souhaite que les coûts liés à la mise en œuvre des mesures et les pourcentages supplémentaires de postes soient indiqués de manière transparente. Elle demande que les mesures prévues permettent de réaliser des économies et d'améliorer la protection des données.

Le **PS** est en principe d'accord avec les dispositions d'exécution de la LSI. Il considère toutefois que la collecte des données dans le cadre des CSP va beaucoup trop loin et la rejette. Il estime notamment qu'il est inacceptable que des données sur la sphère intime et sur la sexualité ainsi que sur les idées ou activités religieuses, politiques, syndicales et idéologiques puissent être prélevées et traitées.

NW acte que la LSI et les ordonnances correspondantes n'ont généralement qu'une incidence indirecte sur les cantons lorsqu'ils accèdent ou traitent les données de la Confédération. Et d'ajouter qu'il s'agirait de retenir que, d'un point de vue actuel, certaines dispositions importantes pour les cantons ne seraient pas définitivement réglées et que cela concernerait surtout la révision de la LSI et l'ordonnance relative à l'obligation de signaler les cyberattaques contre les infrastructures critiques (chap. 5 LSI). Il soutient néanmoins les adaptations générales qui, selon lui, allaient dans le bon sens dès lors qu'elles tenaient compte de l'environnement interconnecté et numérisé ainsi que de l'échange croissant de données selon le principe « once only » qui en découle. La sécurité de l'information, en tant que tâche commune à responsabilité interconnectée qui détermine des objectifs communs et suit une procédure coordonnée dans le respect de standards minimaux, est considérée comme importante.

NW et **OW** constatent que la notion de canton dans le droit d'exécution est redéfinie et comprend des collectivités, des institutions et des fondations publiques. Ils soulignent qu'une terminologie cohérente, qui s'inscrive dans la définition visée à l'art. 3 Cst., serait la bienvenue. Ils estiment aussi que les autres collectivités devraient être mentionnées séparément.

L'**asut** apprécie le cadre régulateur solide mis en place pour la sécurité de l'information ; selon elle, ce cadre s'adapte à l'avancée actuelle des technologies et aux risques qui y sont liés. Elle estime que les ordonnances sont suffisamment souples et précises pour signaler clairement les responsabilités de chaque partie prenante, même face à de nouveaux développements technologiques. L'**asut** salue également l'approche de l'administration fédérale, qui entend procéder, à l'avenir, à moins de classification afin de réduire autant que possible la bureaucratie.

3.1.1 Appréciation de la faisabilité et de l'intelligibilité

La consultation a révélé que les dispositions d'exécution de la LSI et de son application sont, en principe, intelligibles pour la majorité des cantons (**AG, AI, AR, BL, BS, BE, GE, GL, GR, LU, NE, NW, OW, SG, SH, SO, SZ, TI, TG, UR, VD, VS, ZG et ZH**). Quant aux effets, il reste encore quelques incertitudes. Ces incertitudes concernent non seulement le financement, mais aussi les degrés d'équivalence dans le domaine de la sécurité de l'information ainsi que les conditions et prescriptions minimales applicables, bien qu'encore en suspens. Pour certaines parties consultées (**FR (SITel)**, **JU et VD**), la charge liée à la mise en œuvre est difficile à évaluer en raison de ces incertitudes.

Divers cantons prévoient leur propre législation sur la sécurité de l'information (**AG, BE, FR**) ou examinent dans quelle mesure et sous quelle forme les dispositions nécessaires et les bases existantes doivent ou peuvent être respectivement formulées ou adaptées (**NW, SH, UR** et **ZH**).

Pour **BL**, une incertitude surgit pour des communes et d'autres organisations quant à savoir comment des institutions ou entreprises de droit public installés dans les cantons sont aussi raccordés aux systèmes d'information de la Confédération. Le droit d'exécution avec état au 24 août 2022 n'établirait pas clairement qui doit veiller à ce que les mesures de sécurité soient respectées par ces organisations. Il pense qu'il est possible que les cantons ne le soient pas pour les communes. Pour lui, un concept établi dans le cadre proposé serait dès lors bien plus efficace si tous ceux qui veulent être raccordés aux moyens d'information de la Confédération devaient remplir les conditions fixées par cette dernière. Cette solution clarifierait et simplifierait beaucoup plus les choses, et les mesures de sécurité pourraient être efficacement mises en œuvre.

AR se demande si la Constitution fédérale oblige les cantons à assurer une sécurité générale de l'information – en dehors des exigences relatives à la sécurité des données qui doivent être respectées dans le cadre de la protection des données personnelles, de la personnalité et de la sphère privée. Parallèlement, il lui semble évident que la protection des données personnelles tirerait aussi profit d'un accroissement de la sécurité générale de l'information.

FR (SITel) propose d'uniformiser les exigences techniques hétérogènes de la Confédération lors de l'établissement des directives qui font encore défaut. Actuellement, la Confédération aurait par exemple trois « public key infrastructures » (PKI). Selon le canton **FR**, il lui serait difficile de savoir quelle sécurité garantir au juste si la Confédération impose des exigences ambiguës. Et d'ajouter que si l'Administration numérique suisse (ANS) devait n'avoir qu'une seule fonction, elle devrait servir d'organe fédérateur en rapport avec les systèmes d'information et, dès lors aussi, avec le domaine de la sécurité de l'information. **FR** souhaite que l'ANS s'implique davantage dans les matières qui touchent les cantons et leurs systèmes d'information. Sans organe fédérateur, le paysage informationnel du canton serait ingérable, d'autant plus pour les cantons ne disposant pas des mêmes budgets que la Confédération.

JU et **VD** souhaitent des dispositions d'ordonnance en rapport avec les effets et les attentes vis-à-vis des cantons.

SG synchronise autant que possible les exigences de sécurité dans le canton avec celles de la Confédération sur la protection de base. Une harmonisation dans ce sens du SMSI cantonal est en cours. Une analyse d'impact montrerait quelles mesures concrètes doivent ensuite être appliquées dans des projets. Les droits d'accès doivent être attribués, dans le respect des directives de la Confédération, aux acteurs des offices qui en ont besoin pour remplir leur mandat légal.

Pour **TI**, l'obligation de soumettre le personnel des unités administratives et de la justice du canton ainsi que d'autres organes externes assumant des tâches selon la réglementation du droit fédéral à des CSP n'est pas claire. Selon lui, l'impossibilité de consulter la liste exhaustive des fonctions soumises à contrôle soulève des questions sur le plan de la mise en œuvre.

VS appliquerait une politique de la sécurité de l'information et des directives-cadres qui fixeraient les objectifs, les principes généraux et l'organisation de la sécurité de l'information, lesquels s'appliqueraient à toutes les autorités cantonales. Les communes et les institutions cantonales ne seraient par contre pas concernées par les lignes directrices en vigueur. Toutefois, tous les accès à la Confédération par le truchement des cantons seraient gérés et sécurisés par l'administration cantonale. Le canton propose aux communes qui le désirent un soutien subsidiaire dans le domaine de la cybersécurité et offrira, dès 2023, la solution de sensibilisation eCyAd mise au point par la Confédération dans le cadre de la deuxième stratégie de protection de la Suisse contre les cyberrisques.

Pour **ZG**, les exigences sont compréhensibles, mais n'établissent pas suffisamment les obligations des cantons. De plus, il estime que l'approche fédéraliste suivie, selon laquelle les directives fédérales ne sont applicables que si les réglementations cantonales ne suffisent pas à répondre aux exigences de sécurité de la Confédération, complique le tout.

ZG déclare que la responsabilité principale vis-à-vis de la sécurité lors du traitement d'informations classifiées de la Confédération incombe aux organes cantonaux qui traitent ces données ou ont accès aux moyens informatiques de la Confédération (notamment : office des affaires militaires et de la protection civile, organisation d'urgence, police zougoise, association pour des mesures concernant le marché du travail). Ces organes auraient défini les processus, compétences et mesures nécessaires permettant de garantir le niveau de sécurité exigé par la Confédération. À ce propos, les prescriptions de la Confédération ont été appliquées uniquement lorsque celles des cantons et leurs mesures étaient insuffisantes au regard des exigences de sécurité de la Confédération. Le personnel des organes est responsable du respect des directives lors de la manipulation des informations classifiées et des moyens informatiques. Le bon comportement envers de telles informations et de tels moyens exige que les autorités fédérales établissent des directives à l'intention de ces organes.

3.1.2 Évaluation des conséquences financières

La consultation a très largement montré les conséquences financières de la mise en œuvre de la LSI.

Pour **AG, AI, BL, BS, GL** et **VS**, la mise en œuvre de la LSI n'implique ni changement conséquent ni surcroît de coûts. **BL** attend seulement un surcoût limité dans le domaine de la conformité et un gel temporaire des ressources en personnel. **VS** accorde une attention particulière à d'éventuelles modifications en lien avec des fonctions exigeant un CSP.

Plusieurs cantons (**AR, FR [SITel], GE**, **JU, SG, SH, SZ, TG, UR** et **ZG**) n'ont pas pu évaluer correctement les conséquences financières lors de la consultation.

NE estime les coûts entre 500 000 et 3 millions de francs pour la mise en œuvre d'un SMSI et le renforcement de la sécurité. Des adaptations techniques supplémentaires pourraient se chiffrer à plusieurs millions.

NW estime les surcoûts annuels à quelque 100 000 francs.

OW estime les coûts annuels à 50 000 francs.

SZ établit à 425 pour cent supplémentaire de postes et s'attend à des investissements dans le SMSI et les systèmes de sécurité qui auraient aussi à voir indirectement avec la mise en œuvre des ordonnances. Les charges financières supplémentaires en lien avec la nouvelle LSI sont estimées, pour la première année, à un montant global de 300 000 francs pour le personnel et les investissements.

TI et **ZG** s'attendent, en plus des coûts de personnel comme ceux consacrés aux formations et aux CSP, à des coûts liés à la concrétisation des mesures de sécurité techniques.

ZH s'attend à un surcoût estimé entre 10 000 et 50 000 francs pour chaque accréditation de sécurité des moyens informatiques et pour chaque contrôle régulier de la sécurité effectué au cours de leur cycle de vie. Concernant les autres coûts, il ne lui serait actuellement pas possible de fournir des estimations définitives.

3.2 Avis sur l'ordonnance sur la sécurité de l'information (OSI)

3.2.1 Remarques générales

L'uniformisation dans le cadre de la nouvelle OSI du SMSI pour toutes les unités administratives est saluée (**UDC**). La centralisation donne à l'**UDC** l'espoir de réaliser des économies et de garantir une utilisation et un entretien efficient. Il s'agirait donc d'introduire le plus rapidement possible le même SMSI dans tous les offices.

GE souligne la complexité et le caractère coûteux de la mise en œuvre de l'ordonnance.

3.2.2 Avis sur les articles de l'OSI

Art. 2 Champ d'application

Al. 6 – La consultation a révélé que, pour plusieurs cantons (**AG, BL et ZH**), l'équivalence de leurs propres lois avec la LSI est difficile à démontrer.

AG souhaite que soit présentée la façon dont les cantons pourraient se prévaloir contre un accès refusé par la Confédération, sans quoi la disposition d'exception (art. 3, al. 2, LSI) n'aurait pas de sens.

Art. 6 Gestion des bases juridiques et des engagements contractuels

NE n'arrive pas à savoir si les cantons doivent également consulter le service spécialisé de la Confédération pour la sécurité de l'information lorsqu'ils établissent leurs propres bases légales pour atteindre un niveau semblable de sécurité ou lorsqu'ils mettent en œuvre par exemple les recommandations techniques.

Art. 9 Autorisation et exceptions

Al. 2 – **LU** souhaite que soit précisé à qui le service spécialisé de la Confédération pour la sécurité de l'information et les départements peuvent déléguer l'octroi d'exceptions.

Al. 4, let. b – **LU** se demande si les unités administratives, les départements et le service spécialisé de la Confédération pour la sécurité de l'information sont, dans tous les cas, informés lorsque la possibilité d'autoriser des exceptions est déléguée, afin de pouvoir mentionner ces autorisations dans leur liste également. Pour garantir le flux d'information, il recommande l'établissement d'une obligation de communiquer et d'informer pour les services auxquels la possibilité d'autoriser des exceptions a été déléguée.

Art. 12 Gestion des incidents

Al. 7, let. a – **LU** souhaite que soient précisées les informations qui doivent être communiquées, sans quoi cela soulèverait des problèmes, surtout du point de vue du droit sur la protection des données.

Art. 16 Principes

L'article est intelligible pour **AG**. Cependant, il estime que les charges auxquelles l'article se réfère ne peuvent pas être estimées.

TG et **ZH** soulignent un manque de clarté en ce qui concerne la compétence et la procédure en cas de demande de consultation d'informations classifiées de la Confédération au canton. **TG**

souhaite qu'il soit expliqué, à l'al. 3, que les lois cantonales sur la transparence ne s'appliqueraient pas.

Art. 17 Auteurs de la classification

Pour **AG**, il n'est pas évident de savoir dans quelle mesure cette disposition serait pertinente pour les cantons puisqu'ils ne sont pas considérés comme auteurs de la classification.

Art. 18 à 20 Échelons de classification INTERNE, CONFIDENTIEL et SECRET

Ces dispositions sont intelligibles pour **AG**. Il estime cependant qu'il n'est pas évident de savoir si et dans quelle mesure il existe des problèmes de concordance et des difficultés entre les échelons de classification des cantons et ceux de la Confédération.

GE demande que le critère de la divulgation de l'identité des personnes exposées soit biffé de l'échelon CONFIDENTIEL visé à l'art. 19, let. c, pour être reporté au seul échelon SECRET, à l'art. 20, let. c. Il considère aussi que l'aspect des préjudices envers les sources elles-mêmes en cas d'accès à leur identité n'est pas pris en compte, ce qui pose problème et pourrait aussi nuire à l'État.

Concernant l'art. 18, let. c, **VD** souligne que les conséquences d'une atteinte psychologique peuvent être plus graves que celles provoquées par des lésions corporelles. Or la let. c ne mentionne que les lésions corporelles.

VD demande une adaptation des dispositions sur les échelons de classification. Selon ce canton, outre les intérêts de la Confédération, ceux des entreprises et des particuliers devraient aussi être protégés par la loi en cas d'attaque contre la sécurité informatique des systèmes de la Confédération.

Art. 21 Directives relatives au traitement

Étant donné que, selon l'art. 21 OSI, les directives générales et abstraites s'appliqueraient uniquement aux services visés à l'art. 2, al. 1 à 3, **AG** estime qu'on ne sait pas clairement quelles directives s'appliquent pour les cantons et qui les édicte.

Art. 22 Mesures de sécurité liées à l'engagement

Pour **AG**, la raison pour laquelle cette disposition doit être mise en œuvre par les cantons n'est pas claire.

X. D. demande d'ajouter le chef du Renseignement militaire (RM) et du Service de protection préventive de l'armée à l'al. 1.

Art. 23 Accréditation de sécurité des moyens informatiques

Pour **AG**, la raison pour laquelle cette disposition doit être mise en œuvre par les cantons n'est pas claire.

Art. 24 Protection en cas de menace des informations classifiées

Pour **AG**, cette disposition est intelligible et applicable. Les charges liées à cette mise en œuvre devraient être moindres.

Art. 25 Contrôle du besoin de protection et personnes autorisées

AG est d'avis que cette disposition n'est pas pertinente pour les cantons, car ceux-ci ne disposeraient pas d'auteurs de la classification au sens de l'art. 17 OSI.

Art. 26 Archivage

Pour **AG**, cette disposition est intelligible et applicable. Par contre, les charges liées à sa mise en œuvre ne peuvent pas être estimées.

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

Pour **AG**, cette disposition est intelligible et applicable. Par contre, les charges liées à son application ne peuvent pas être estimées.

Art. 29 Mesures de sécurité

Étant donné que, selon l'art. 29 1 OSI, les directives générales et abstraites s'appliqueraient uniquement aux organes visés à l'art. 2, al. 1 à 3, OSI, **AG** estime qu'on ne sait pas clairement quelles consignes minimales en fonction des catégories de sécurité s'appliquent pour les cantons et qui les édicte.

Pour **AG**, cette disposition est intelligible et applicable, pour autant qu'elle s'applique aux cantons. Il considère que l'applicabilité dépendrait des directives encore en suspens sur les consignes minimales.

Art. 30 Sécurité de l'exploitation

Pour **AG**, cette disposition est intelligible et applicable. Par contre, les charges liées à sa mise en œuvre ne peuvent pas être estimées.

Art. 34 Mesures physiques de protection

Étant donné que, selon l'art. 34, al. 1, OSI, les directives générales et abstraites s'appliqueraient uniquement aux organes visés à l'art. 2, al. 1 à 3, **AG** estime qu'on ne sait pas clairement quelles mesures minimales indispensables pour protéger physiquement les informations et les moyens informatiques s'appliquent pour les cantons et qui les édicte. Pour **AG**, cette disposition est intelligible et applicable, pour autant qu'elle s'applique aux cantons. Selon lui, l'applicabilité dépendrait des exigences minimales encore en suspens.

Art. 35 Zones de sécurité

GE indique que les directives générales et abstraites sur les zones de sécurité pourraient amener une modification des locaux afin que l'échelon SECRET continue d'être respecté.

X. D. demande un aménagement de la réglementation permettant de contrôler l'utilisation malveillante d'ondes électromagnétiques aux alentours des zones de sécurité.

Art. 44 Généralités

X. D. demande un examen de la base légale concernant l'échange de données et, le cas échéant, une précision de l'article de l'OSI.

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

3.3.1 Remarques générales sur l'OIAM

VD relève avec intérêt que cette nouvelle version de l'ordonnance permet désormais la mise en réseau avec un IAM cantonal, et indique qu'il évaluera le cas échéant cette nouvelle possibilité. Il indique que la révision de l'ordonnance concerne surtout des aspects techniques de systèmes servant à administrer des données d'identification, et que ceux-ci pourraient avoir des effets sur la

gestion des identités du portail IAM du canton ou d'autres bases de données, notamment dans la perspective de l'obligation d'administrer des accréditations et des accès aux systèmes d'information de la Confédération. Cela concernerait en l'occurrence des « tiers » qui utiliseraient aussi ces systèmes d'identification.

Concernant le contrôle des personnes, l'**UDC** salue l'extension du champ d'application aux unités administratives de l'administration fédérale décentralisée. Il s'agirait toutefois, selon elle, d'assurer un suivi critique des conséquences sur la protection des données, dues notamment au traitement élargi des données biométriques.

VS relève avec intérêt que cette nouvelle version de l'ordonnance permet désormais la mise en réseau avec un IAM cantonal, et indique qu'elle évaluera le cas échéant cette nouvelle possibilité.

3.3.2 Avis sur les articles de l'OIAM

Art. 13 Base centralisée des identités pour la distribution des données

Al. 4 – **GE** demande si la notion de « système concerné » se rapporte au système source ou à un autre système d'information interne à l'administration fédérale.

Art. 18 Exigences concernant la sécurité de l'information

Al. 2 – **GE** demande que soit précisé par qui et dans quel cadre les exigences minimales sont définies.

Art. 21 Conditions pour le raccordement de systèmes IAM externes

Let. c – **GE** souligne que son système IAM contient des données personnelles que les systèmes d'information rendus disponibles par la Confédération n'utiliseraient pas. **GE** demande donc si, dans son système IAM, seuls les sous-ensembles de personnes qui auraient accès aux systèmes informatiques de la Confédération pouvaient être connectés au système IAM de celle-ci.

Annexe

Let. e : Données techniques – Concernant la catégorie de données « 7. Mots de passe », **GE** demande que l'obligation de chiffrer ou de hacher les données en cas de besoin soit précisée.

3.4 Avis sur l'ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP)

3.4.1 Remarques générales sur l'OCSP

L'**UDC** souhaite souligner l'aspect positif de la réduction d'au moins 30 % des CSP. Elle estime compréhensible le remplacement qui en découle des anciennes ordonnances.

VD indique que l'OCSP aura des répercussions sur les organes responsables des CSP au niveau cantonal. Et d'ajouter qu'il ne faut pas oublier que la vaste collecte de données prévue et le traitement de données personnelles sensibles exigeraient une surveillance stricte qui soit compatible avec la législation sur la protection des données.

X. D. indique que l'OCSP est extrêmement problématique au regard des droits fondamentaux et des droits constitutionnels. Il estime dès lors que l'ordonnance doit, une fois encore, être soumise à examen.

3.4.2 Avis sur les articles de l'OCSP

Art. 2 Champ d'application

Swissgrid demande la prise en compte de la LApEl dans le champ d'application puisque cette loi constitue une base légale en soi. « *La présente ordonnance s'applique, sous réserve des art. 84, al. 3, LSI et 2, al. 2 à 5, de l'ordonnance sur la sécurité de l'information du... pour les autorités et organisations concernées visées aux art. 2 LSI et 20a LApEl. »*

Art. 3 Attribution

Al. 3 – **Swissgrid** demande l'ajout du complément ci-après, car **elle** ne fait pas partie de l'administration fédérale :

« La liste de l'annexe 6 s'applique aux fonctions visées à l'art. 20a, al. 1, LApEl. Pour les demandes au sens de l'art. 4, les contrôles de l'actualité au sens de l'art. 6 et les demandes de contrôles extraordinaires selon l'art. 7, l'autorité compétente est la Commission de l'électricité visée à l'art. 21 LApEl, au lieu du département. »

Art. 5 Publication, conservation et communication

Swissgrid apprécierait que la liste de fonctions concernée ne soit pas publiée dans le Recueil systématique en raison de sa confidentialité et par souci de protection, tant pour **elle-même** que pour son personnel.

Art. 8 Contrôles du personnel et des tiers

Al. 1 – **AG** souhaite que soit dressée la liste des fonctions des employés cantonaux soumis à contrôle, conformément à l'art. 29, al. 1, let. b, LSI, et que soit définie la procédure de dépôt de demande au DDPS.

Les fonctions en **VS** qui exigent un CSP seraient connues et les contrôles seraient déjà effectués depuis plusieurs années. **VS** constate toutefois que le DDPS, selon le commentaire relatif à l'art. 8 du rapport explicatif, a été chargé d'unifier les pratiques. Cela pourrait signifier une extension des contrôles dans le canton, et donc entraîner des coûts financiers non négligeables.

Art. 11 Contrôle de loyauté selon la LPers

Al. 1, let. c, et 2 – Le **MPC**, en qualité d'autorité de poursuite pénale, demande un complément à la base sur laquelle repose le contrôle de sécurité de base et un CSP élargi pour son personnel (interne et externe) en raison d'un risque de préjudice majeur ou grave.

Art. 14 Contrôles de loyauté selon la LApEl

Swissgrid approuve le texte et remercie d'avoir pris en compte les données correspondantes.

Art. 15 Services qui demandent le contrôle et instances décisionnelles

Al. 4 – **Swissgrid** salue la disposition précisant que la société nationale du réseau de transport est à la fois le service qui demande le contrôle et l'instance décisionnelle.

Art. 19 Collecte des données

X. D. exprime une forte réprobation envers cet article. Il estime qu'il devrait être réduit à 5 ou 6 articles plus petits et qu'en matière de légistique, il n'est pas digne de la qualité rédactionnelle des lois et ordonnances du droit suisse.

Al. 2, let. c – **Swissgrid** demande de reprendre la société nationale du réseau de transport dans un nouveau ch. 8, une audition étant systématiquement effectuée lors d'un CSP élargi, ceci en raison d'expériences tirées des CSP faits sur la base du droit privé.

Art. 26*f* **Répétition ordinaire ou extraordinaire du contrôle**

NE se demande combien de temps dure la validité d'un CSP et si sa répétition motivée par un risque pour la sécurité complète ou remplace l'évaluation précédente.

Art. 30 **Certificat international de sécurité**

X. D. propose d'étendre le champ d'application de cet article et de définir l'octroi d'office pour diverses fonctions du SRC, du RM et de l'AS-Rens afin de réduire la charge administrative liée au nombre de demandes de certificat.

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

AG ne prévoit actuellement pas de transférer à l'avenir les CSP à la Confédération. Il estime que les exigences pourraient toutefois être remplies et le montant des émoluments adapté.

GE indique que le montant des frais, par exemple pour la police ou l'Office cantonal des systèmes d'information et du numérique, pourrait être considérable.

GE examine l'opportunité de créer une base pour le CSP visant à assurer sa propre sécurité de l'information.

NE se demande si les motifs de sécurité invocables sont ceux définis par les bases légales cantonales ou ceux de l'OCSP.

Art. 38 **Dispositions transitoires**

Al. 4 – **Swissgrid** demande que l'alinéa soit adapté comme suit : « *Les contrôles de sécurité que la société nationale du réseau de transport a reçus ~~sur la base du droit privé~~ avant et jusqu'à un an après l'entrée en vigueur de la présente ordonnance ~~et avant l'échéance du délai fixé à l'al. 5~~ restent applicables comme suit dans le cadre des délais fixés pour les répétitions visées aux art. 26 et 27 : […]* »

Al. 5 – **Swissgrid** demande que l'alinéa soit supprimé.

Annexe 6 **Fonctions visées à l'art. 20*a*, al. 1, LApEl**

Swissgrid propose, pour la distinction des fonctions selon les diverses activités, leur différenciation selon leurs types.

Annexe 7 **Collecte et traitement des données**

Il ressort de la consultation que, pour diverses parties (**GE, TG, UR, PS, APC, USAM et X. D.**), l'annexe concernant le traitement de données sensibles va trop loin.

Le **SP** demande que le mot « notamment » dans l'annexe 7 OCSP soit biffé sans remplacement. La compétence de l'État doit être mentionnée explicitement et clairement définie. Toute liste non exhaustive est rejetée.

3.5 Avis sur l'ordonnance sur la procédure de sécurité relative aux entreprises (OPSEnt)

3.5.1 Remarques générales sur l'OPSEnt

Pour l'**UDC**, l'OPSEnt est nécessaire et considère que remplacement de l'ordonnance concernant la sauvegarde du secret se fait attendre.

AG souhaite voir une possibilité de bénéficier de prestations dans la réalisation des procédures de sécurité relatives aux entreprises qui soit analogue à celle de l'OCSP.

UR déclare qu'aucune mise en œuvre de l'OPSEnt n'est nécessaire pour les cantons.

L'**USAM** déclare que la mise en œuvre par voie d'ordonnance a un effet de régulation plus intense que celui prévu dans la loi. En outre, il considère que des données ont manqué sur les coûts de régulation et les coûts supplémentaires incidents pour les cantons.

3.5.2 Avis sur les articles de l'OPSEnt

Art. 2 Entreprises concernées

VD demande de préciser les relations entre l'art. 2, al. 1, selon lequel l'ordonnance s'applique uniquement aux entreprises dont le siège est en Suisse, et l'art. 6, dans lequel les modalités pour l'engagement de la procédure auprès d'entreprises étrangères sont réglées.

Art. 14 Contenu et contrôle du plan de sécurité

VD demande que le plan de sécurité soit adapté en cas de développements techniques ou d'évolution des risques.

Art. 17 Information de la part de l'entreprise

GE demande des précisions, à savoir : l'al. 1, let. a, doit préciser que cela s'applique aussi aux filiales ; l'al. 1, let. e, doit être complété par « en Suisse ou ailleurs » ; à l'al. 2, il importe d'ajouter, en lien avec les incidents dans le domaine de la sécurité, les violations de la protection des données au sens de la nLPD.

4 Annexe – Parties consultées et demandes de modification

Abréviation	Parties consultées	Demandes de modification et ambiguïtés Ordonnances / Rapport explicatif				
		OSI	OIAM	OCSP	OPSEnt	Rap. expl. P. gén.[1]
Cantons						
ZH	Zurich	x				x
BE	Berne					
LU	Lucerne	x				
UR	Uri			x		
SZ	Schwyz					
OW	Obwald					x
NW	Nidwald					x
GL	Glaris					
ZG	Zoug					x
FR	Fribourg					
FR (SITel)	Fribourg, Office fédéral de l'informatique et de la télécommunication	x				
SO	Soleure					
BS	Bâle-Ville					
BL	Bâle-Campagne	x				x
SH	Schaffhouse					
AR	Appenzell Rhodes-Extérieures	x				
AI	Appenzell Rhodes-Intérieures					
SG	Saint-Gall					
GR	Grisons					
AG	Argovie	x		x	x	
TG	Thurgovie	x		x		
TI	Tessin					
VD	Vaud	x	x	x		
VS	Valais					
NE	Neuchâtel	x		x		

[1] P. gén. = partie générale

Abréviation	Parties consultées	Demandes de modification et ambiguïtés Ordonnances / Rapport explicatif				
		OSI	OIAM	OCSP	OPSEnt	Rap. expl. P. gén.[1]
GE	Genève	x	x	x	x	
JU	Jura	x				
Partis politiques						
UDC	Union démocratique du centre					
PS	Parti socialiste suisse			x		
Associations faîtières de l'économie œuvrant au niveau national						
USAM	Union suisse des arts et métiers			x		
	Union patronale suisse					
Autres organisations intéressées						
APC	Association du personnel de la Confédération			x		
	Swissgrid SA			x		
Parties consultées non invitées à titre individuel						
asut	Association suisse des télécommunications				x	
MPC	Ministère public de la Confédération			x		
X. D.	Xavier Dufour	x		x		