



Septembre 2013

Loi sur le renseignement (LRens)

Rapport sur les résultats de la procédure de consultation

Sommaire

1. Objet du projet en consultation
2. Déroulement de la procédure de consultation
3. Participants à la procédure
4. Appréciation générale du projet
5. Réponses concernant les divers articles
6. Autres remarques
7. Résumé des réponses au questionnaire

1. Objet du projet en consultation

Le projet de loi sur le renseignement (LRens) a pour but de créer une base légale formelle uniforme pour le Service de renseignement de la Confédération (SRC) réglant les activités, le mandat et le contrôle de ce service.

En 2009, le Conseil fédéral a chargé le DDPS de lui présenter, d'ici fin 2013, un message portant sur un projet de loi globale sur le service de renseignement (ACF du 27 novembre 2009). Le mandat du Conseil fédéral était formulé comme suit:

*« Le Conseil fédéral charge le DDPS
...de présenter, d'ici fin 2013 au plus tard, un message avec un projet pour une nouvelle loi sur le service de renseignement créant la base légale pour les tâches, les droits, les obligations et les systèmes d'information des services de renseignement civils de la Suisse. Les parties controversées du message du 15 juin 2007 relatif à la modification de la LMSI ainsi que les dispositions en vigueur doivent nouvellement être réglés dans le projet de loi. »*

En avril 2012, le projet LRens a fait l'objet d'une première consultation des offices et – compte tenu de la nécessité ressentie – d'une deuxième consultation des offices en octobre 2012.

Les principaux éléments du projet sont les suivants:

Codification

Les dispositions relatives au service de renseignement intérieur et au service de renseignement extérieur, contenues jusqu'à présent dans deux lois distinctes, doivent être regroupées dans une seule loi.

Nouvelle orientation de la recherche d'informations

Concernant la recherche d'informations, le projet de loi ne distingue plus en priorité – comme auparavant - entre les menaces émanant de l'intérieur du pays et celles de l'étranger, mais entre l'extrémisme violent en lien avec la Suisse et les autres champs de menaces et tâches. Le nouveau concept prévoit qu'en matière d'extrémisme violent, les mesures de recherche d'informations soumises à autorisation et impliquant des ingérences particulièrement importantes dans les droits fondamentaux ne soient pas applicables; en outre, ce concept précise que les données relatives à l'extrémisme violent doivent être gérées sur la base de critères particulièrement stricts. Les données ayant trait à l'extrémisme violent présentent souvent des liens plus étroits avec la Suisse que les données d'autres champs d'activité du SRC. Elles sont souvent aussi plus délicates car plus proches de pures activités politiques qui, dans notre pays, conformément à l'art. 3, al. 5, ne peuvent pas être surveillées à des fins de renseignement

Introduction de nouvelles mesures de recherche d'informations

Les moyens spéciaux de recherche d'informations, tels que proposés dans le projet d'origine LMSI II et renvoyés par le Parlement pour être réexaminés, ont été remaniés et adaptés aux nouvelles circonstances. Le projet de loi les prévoit maintenant comme mesures de recherche soumises à autorisation en Suisse.

Pour que ces mesures puissent être mises en œuvre, elles doivent au préalable être approuvées par le président de la cour compétente du Tribunal administratif fédéral, avoir fait l'objet d'un examen quant à leurs aspects politiques par une instance supérieure et avoir reçu l'aval du chef du DDPS.

Ces nouvelles mesures sont proposées car les instruments actuellement à disposition du SRC (art. 14 LMSI) ne lui permettent plus d'assurer ses tâches de prévention dans le domaine de la sûreté intérieure. Des acteurs de plus en plus agressifs et des formes de menaces de plus en plus complexes menacent, elles, la sécurité intérieure et extérieure de la Suisse et requièrent l'introduction de mesures de recherche plus efficaces. Le Conseil fédéral avait déjà constaté cette nécessité dans le projet d'origine de la LMSI II.

Extension des mesures de recherche non soumises à autorisation

Les mesures de recherche non soumises à autorisation ont aussi été modérément élargies. En font notamment explicitement partie la possibilité de procéder à un signalement préventif de personnes pour la recherche de leur lieu de séjour et de véhicules à des fins de localisation.

Gestion et traitement différencié des données

Le projet de loi prévoit que les renseignements recherchés ou communiqués au SRC soient enregistrés dans des systèmes d'information intégrés spécialisés en fonction de leur thématique, de leur source et de leur sensibilité. S'agissant des divers types de données, des prescriptions peuvent ainsi être fixées pour leur traitement et leur protection (délais de contrôle et de conservation des données, accès différencié aux données par le personnel du SRC, etc.). Par ailleurs, avant que le SRC transmette des données, il doit obligatoirement et dans chaque cas s'assurer que leur traitement ait été effectué conformément à la loi et que leur transmission soit licite.

2. Déroulement de la procédure de consultation

Le Conseil fédéral a envoyé le projet de la nouvelle loi sur le renseignement en consultation le 8 mars 2013 et cette procédure a duré jusqu'au 30 juin 2013. Ont été invités à s'exprimer sur le projet 72 participants, notamment les cantons, les partis politiques, les associations faitières des communes, des villes et des régions de montagne, les associations faitières de l'économie œuvrant au niveau national ainsi que d'autres milieux concernés par le projet dans le cas d'espèce.

3. Participants à la procédure

68 participants ont envoyé leur réponse, 8 ont explicitement renoncé à donner leur avis.

Cantons

Tous les cantons se sont exprimés, de même que la Conférence des commandants des polices cantonales (CCPCS), la Conférence législative intercantonale (CLI, (AG, AI, BL, BS, BE, JU, LU, SG, SO, TI, VD, ZH), l'organe de contrôle pour la protection de l'Etat du canton de Bâle-Ville (OCPE-BS) et le service de surveillance de la protection des données du canton de Thurgovie (SPD-TG). (30)

Partis politiques représentés à l'Assemblée fédérale

Se sont prononcés le Parti bourgeois-démocratique (PBD), le Parti démocrate-chrétien (PDC), les Libéraux-Radicaux (PLR), les Verts (PES), le Parti vert libéral (pvl), le Parti Pirate Suisse (PPS), le Parti socialiste suisse (PS) et l'Union démocratique du centre (UDC). (8)

Associations faitières de l'économie œuvrant au niveau national

Ont donné leur avis économesuisse, l'Union suisse des arts et métiers (USAM) et l'Association suisse des banquiers (SwissBanking). (3)

Autres milieux concernés par le projet dans le cas d'espèce

Ont donné leur avis le Tribunal fédéral (TF), le Tribunal administratif fédéral (TAF), Amnesty International (AIInt), les Juristes démocrates de Suisse (JDS), le Groupe pour une Suisse sans armée (GSsA), la Conférence des autorités de poursuite pénale de Suisse (CAPS), la Conférence des directrices et des directeurs de la sécurité des villes suisses (CDSVS), la Société suisse des officiers (SSO), l'Association suisse des officiers de renseignements (ASOR) et la Fédération suisse des fonctionnaires de police (FSFP). (10)

Prises de position d'organisations qui n'avaient pas été officiellement invitées à se prononcer

Se sont exprimé l'Association suisse des télécommunications (asut), Action pour une Suisse indépendante et neutre (ASIN), le Chaos Computer Club Zurich (CCCZH), le Centre Patronal (CP), la Chambre vaudoise des arts et métiers (CVAM), la Digitale Gesellschaft (DigGes), la Délégation des finances des Chambres fédérales (DéFin), droitsfondamentaux.ch, l'Association des commissaires suisses à la protection des données (privatim), le Comité référendaire LMSI (Référendum LMSI), la Fédération suisse des communautés Israélites (FSCI), l'Association économique suisse de la bureautique, de l'informatique, de la télématique et de l'organisation (Swico), l'Association pour la sphère privée (Swiss Privacy Foundation, SPF), Swisscom, l'Université de Genève ainsi que deux particuliers (PP1/PP2). (17)

Renoncement à une prise de position

Ont explicitement renoncé à se prononcer le Tribunal pénal fédéral, l'Union patronale suisse, l'Association des Communes suisses, l'Union syndicale suisse, La Croix-Rouge suisse, l'Union des villes suisses, la Conférence des directrices et directeurs des départements cantonaux de justice et police et la Société suisse des employés de commerce. (8)

4. Appréciation générale du projet

La *CCPCS, AR, BE, BL, BS, GE, GL, GR, JU, LU, NE, NW, SO, SZ, TI, UR, VD et ZH*, le *SPD-TG* et la *CAPS* saluent la création d'une base légale formelle et uniforme pour régler les activités de renseignement en faveur de la sécurité intérieure de la Suisse. Ces milieux estiment que le projet est une base permettant d'augmenter la sécurité juridique des citoyens et citoyennes dans un domaine particulièrement sensible, Cela dit, ce projet représente dans l'ensemble, quant au fond et à la forme, une base apte à mettre en œuvre des activités de renseignement.

La *CCPCS, AR, BE, GR, NW, SO* et *UR* considèrent comme judicieuse la différenciation de principe figurant dans la loi entre l'extrémisme violent en lien avec la Suisse, d'une part, et les autres champs d'activité et tâches, d'autre part.

La *CCPCS, AR, GR* et *SZ* estiment que les mesures proposées répondent à une nécessité urgente pour protéger la population d'actes de violence et qu'en plus, elles tiennent suffisamment compte des changements intervenus au niveau des risques et des menaces modernes.

AI soutient le projet et part du principe que la mise en œuvre des mesures pour la recherche d'informations répondra toujours de manière stricte aux règles de l'Etat de droit. Il attend également que les limites des ressources et des moyens techniques dont dispose *AI* soient prises en considération.

BS est d'avis que le projet répond par principe à une base légale tenant compte de la norme de la légalité ancrée dans le droit constitutionnel. Plus l'ingérence dans les droits constitutionnels de la personne concernée est importante, plus les exigences légales relatives à la forme d'ingérence visée doivent être élevées. Le projet est d'une haute densité normative et répond ainsi aux conditions ayant trait aux droits fondamentaux.

FR approuve en principe les propositions faites dans le projet.

GE met en évidence comme éléments positifs l'étroite collaboration entre la Confédération et les cantons, le soutien sous forme de moyens techniques et de formations, la possibilité de conférer des identités d'emprunt et l'introduction de la surveillance des communications. En revanche, il fait état de son insatisfaction surtout par rapport à la conservation des données limitée à une année, l'accord de la Confédération requis pour établir des contacts avec des partenaires étrangers, la procédure d'autorisation requise pour des mesures de recherche et les règles d'accès aux données de la Confédération.

GR considère que le mécanisme de contrôle pour les nouvelles mesures de recherche soumises à autorisation est approprié en vue d'assurer la légalité et la proportionnalité de l'activité du SRC. Du point de vue des dispositions en matière de protection des données, la densité normative du projet pour les procédures de traitement de données comportant un potentiel de danger aussi élevé parvient également à convaincre. La gestion et la saisie

différenciées des données contribuent à protéger les personnes concernées d'atteintes à leurs droits fondamentaux constitutionnels et de droit international public.

LU constate que les points critiqués dans des projets antérieurs ont maintenant été améliorés et que les règles y ont gagné en qualité du point de vue de l'Etat de droit. Il salue en particulier les instruments instaurés pour la garantie de la qualité, la coordination politique et le contrôle du SRC, les dispositions différenciées pour la protection des données et la procédure d'autorisation à plusieurs niveaux.

NE se demande si de par les mesures et les contrôles prévus, le SRC est encore apte à accomplir ses tâches.

SH est favorable au projet. Il estime qu'il présente une considération soignée des biens juridiques dans un champ de tension existant entre le maintien de la sûreté intérieure et extérieure et la protection des libertés personnelles.

Pour *TI*, le projet se fonde sur cinq nouveautés fondamentales:

- une base légale uniforme pour le SRC;
- la nouvelle orientation pour la recherche d'informations, sans différenciation entre menaces intérieures et extérieures;
- l'introduction de nouvelles mesures de recherche pour les domaines du terrorisme, de l'espionnage, de la prolifération, d'attaques contre des infrastructures sensibles ou pour la sauvegarde d'autres intérêts essentiels de la Suisse:
- un système différencié de gestion des données;
- un système de surveillance à plusieurs niveaux.

ZH rappelle que la loi concerne un domaine politique et juridique délicats, ainsi qu'un champ de tension agissant entre la sécurité et la liberté, respectivement la protection des droits fondamentaux des citoyens. Il s'agit donc, dit-il, d'éviter que les mécanismes d'autorisation et de contrôle prévus dans le projet soient recadrés au cours des travaux législatifs.

Le *SPD-TG* déplore que ce projet prévoit de doter les organes de la politique de sécurité de moyens de recherche de très grande envergure, ce qui signifie que le but visé jusqu'à présent par le service de renseignement intérieur (sauvegarde des bases démocratiques et d'Etat de droit de la Suisse, et surtout la protection des libertés individuelles de sa population) ne soit plus assuré. Compte tenu de ces libertés, il s'agit de renoncer aux ingérences allant trop loin quant aux droits personnels de nos propres citoyens.

Le *PDB* est en principe favorable à la loi sur le renseignement. S'il estime d'un côté que l'actualisation de la recherche d'informations est positive, il exprime aussi de l'autre les inquiétudes suivantes:

Le discours entre le besoin accru de sécurité de la population, d'une part, et le besoin de protection de la sphère privée (bien que les particuliers, via Internet, révèlent aujourd'hui volontairement bien plus de leur vie privée que cela n'a jamais été le cas), d'autre part, a visiblement aussi laissé des traces dans ce projet. C'est avec une extrême minutie qu'à l'échelon de la loi sont réglées les définitions, les tâches et les limites exactes. Or, à notre époque fébrile, alors que la technologie progresse très rapidement et que les menaces évoluent constamment, le SRC se freine lui-même dans ses activités en devant appliquer des règles trop étroites et des procédures trop pesantes.

Pour le *PDC*, il est évident qu'au vu de la situation de la menace qui se modifie continuellement, l'Etat a besoin d'instruments efficaces pour se protéger lui-même et sa population, une obligation faisant partie de ses tâches essentielles. Le *PDC* part de l'idée

que l'élément crucial dans l'ensemble du projet est que la compétence du service de renseignement n'aille pas au-delà de celle de l'autorité de poursuite pénale. Le PDC admet certes que la sphère privée des citoyens et citoyennes puisse être touchée en fonction de la nécessité, mais uniquement dans une proportion aussi faible que possible.

Le *PLR* est satisfait de la direction prise par ce projet et il est favorable à une base légale uniforme pour le SRC et à la nouvelle orientation de la recherche d'informations. Il l'est également en ce qui concerne les nouvelles mesures de recherche, le renforcement de la gestion et le traitement des données, le triple contrôle des activités du SRC ainsi que l'introduction de nouveaux moyens de surveillance en raison de l'évolution de la technologie.

La protection de la sphère privée reste cependant un élément fondamental pour le *PLR*. Il ne faut pas oublier que les moyens du SRC, en particulier les nouvelles mesures de recherche d'informations, permettent une forte ingérence dans la sphère privée. Elle doit donc faire l'objet de règles strictes et toujours respecter le principe de proportionnalité. Le double contrôle est un minimum indispensable pour garantir l'Etat de droit. Le risque d'abus semble avoir été maîtrisé avec justesse. Il s'agit aussi de veiller à une collaboration optimale et à un équilibre entre la Confédération et les cantons en matière d'exécution et de contrôle des mesures de surveillance.

Les Verts refusent le projet en raison des ingérences supplémentaires qu'il prévoit d'instaurer dans les libertés individuelles.

En général, rien ne s'oppose à la création d'une nouvelle loi sur le service de renseignement. Il est vrai toutefois que *Les Verts* avaient auparavant déjà, et dès le début, manifesté une attitude critique face à la LMSI en raison de certaines compétences qu'elle conférerait à l'Etat pour sa protection. Il est donc évident que cette attitude se manifeste à plus forte raison que le projet *LRens* prévoit d'élargir ces compétences-là.

Le fait que la tâche de l'Etat est de garantir – de manière préventive et substantielle – la sécurité de la population suisse est incontestable. Cette tâche, prescrite par la Constitution fédérale, ne doit cependant pas heurter de manière inadmissible les droits fondamentaux des citoyens. Les moyens à engager doivent donc toujours être proportionnels.

Concernant les menaces concrètes indiquées, des éléments constitutifs d'infraction existent aujourd'hui déjà dans le CP; en cas de soupçon, les autorités de poursuite pénale doivent intervenir d'office en ayant la faculté de demander des mesures de contrainte fondées sur le droit de procédure ou de les faire approuver auprès du Tribunal des mesures de contrainte compétent.

Les Verts renvoient par ailleurs à la prise de position de « droitsfondamentaux.ch ».

L'avis émis par le *pvl* sur le projet est en principe positif. Dans certains domaines il considère toutefois qu'il va trop loin. Il reconnaît que le service du renseignement, pour lutter contre le terrorisme, la prolifération et les attaques contre des infrastructures sensibles a dans des cas particuliers besoin de nouvelles mesures de recherche d'informations qui peuvent aussi toucher le domaine privé. Dans ce contexte, il salue toutefois explicitement le fait que de telles mesures soient soumises à une procédure d'autorisation comportant plusieurs échelons et que le Tribunal administratif fédéral soit impliqué.

Le *PPS* oppose un refus catégorique au projet. Il est déçu par ce projet puisque aucune leçon n'a été tirée du rejet de la LMSI II. Le projet suspend les droits fondamentaux sans soupçon initial et sans examen approfondi.

Le *PS* salue la création pour le service de renseignement d'une base légale qui réponde à notre époque.

Le projet présenté accroît d'une part les compétences du service de renseignement, ce qui, du point de vue de la politique de sécurité, peut se justifier. D'autre part, il renforce les droits d'accès des personnes concernées et augmente la surveillance politique et d'Etat de droit

sur ce service en introduisant un système d'autorisation et de surveillance à trois niveaux. Les contrôles internes indépendants sont aussi renforcés, les demandes d'autorisation obligatoires par des tribunaux sont élargies et le législateur veille à ce que les instances politiques puissent assumer leurs responsabilités.

Pour le *PS*, le développement des droits d'accès et des systèmes d'autorisation et de surveillance revêtent une grande importance. Des compétences supplémentaires peuvent être accordée au service de renseignement seulement si un cadre d'Etat de droit et politique fort soit institué pour ses activités et si la protection indispensable des droits fondamentaux est assurée.

C'est pourquoi le *PS* exige que la haute surveillance politique et d'Etat de droit sur le service de renseignement soit encore renforcée et développée pour certaines parties du projet.

L'*UDC* est pour l'essentiel favorable au projet et estime que la Suisse est tributaire d'un service de renseignement performant comme élément de son dispositif de sécurité. Le fait de devoir peser avec soin soit la nécessité de protéger les intérêts des citoyens soit d'épier inutilement des personnes intègres est largement prise en compte dans le projet soumis.

L'*UDC* salue le fait que la loi sur le renseignement crée une base légale formelle uniforme et que le législateur complète les mesures de recherche d'informations en vigueur jusqu'à présent.

Alnt s'inquiète du fait que toutes les recommandations formulées par le professeur Biaggini dans son expertise de 2009 relative à la constitutionnalité du projet LMSI II n'aient pas été prises en compte dans le projet LRens.

L'*ASIN* rejette intégralement ce projet. La loi ne prend suffisamment en considération ni la protection des libertés, ni la sphère privée des citoyens et cette loi heurte en outre les droits de liberté fondamentaux du peuple suisse.

Le *CCCZH* rejette également l'ensemble du projet et n'y trouve aucun élément positif.

Il considère que la nouvelle codification légale pour le service de renseignement civil, représenté par le SRC, est une farce à l'état pur et constitue un danger pour l'ordre libéral de la Suisse. Etant donné qu'actuellement déjà, le SRC est incapable de se repérer dans les dispositions légales en vigueur, le *CCCZH* estime qu'il n'existe aucune raison de le doter de compétences supplémentaires. Le *CCCZH* recommande tout au plus de procéder à une restructuration de la LMSI (la LFRC par contre doit être abrogée dans les meilleurs délais).

Le *CP* et la *CVAM* estiment que la création d'une base légale formelle pour le service de renseignement est judicieuse mais ils souhaitent que la question de la constitutionnalité soit réglée correctement et que l'on réexamine la différenciation entre l'extrémisme violent et le terrorisme ou qu'on la motive pour le moins avec sérieux.

La *DigGes* est horrifiée par ce projet. L'article sur l'objet et le but de la loi mentionne certes avec justesse qu'elle vise à « contribuer à préserver les fondements de la démocratie et de l'Etat de droit en Suisse », mais il conviendrait alors d'abord de garantir qu'elle n'édulcore pas elle-même ces fondements. La *DigGes* exige donc le respect des principes suivants:

- Justification de la proportionnalité.
- Protection des droits de l'homme aussi en ce qui concerne ceux à l'étranger.
- Protection de la libre formation d'opinion et de son expression.
- Utilisation restreinte de l'utilisation d'informations obtenues par des moyens du renseignement.
- Respect des limites fixées aux ingérences dans la sphère privée en vue d'une poursuite pénale.

- Empêchement d'infliger des sanctions indirectes en cas d'expression d'une opinion politique critique.
- Protection des droits de l'homme en faveur des requérants d'asile.
- Protection des données lors d'altercations entre des entreprises et des personnes qui les critiquent.
- Surveillance uniquement en cas d'indices de soupçon d'un délit.
- Loyauté des procédures d'autorisation.
- Droit d'accès aux données et droit de les faire corriger.
- Droit d'être informé sur des mesures de surveillance effectuées. Droit d'être informé en cas de transmission de données personnelles à l'étranger.
- Les exceptions aux deux principes mentionnés ci-devant doivent être rares et leur nombre doit être publié.
- Contrôle indépendant des principes mentionnés et rapport public.
- Règles détaillées sur le type, la recherche et l'utilisation ultérieure des informations.
- Information publique détaillée sur les mesures prises et les informations récoltées.

économiesuisse salue le principe de création d'une base légale formelle uniforme pour le SRC. Une recherche moderne d'informations au service de la sécurité de la Suisse est aussi dans l'intérêt de l'économie de la place suisse. Mais il faut également prendre en compte les intérêts légitimes des particuliers et des entreprises. Dans cette optique, les nouvelles mesures de recherche d'informations vont trop loin. Des compétences, si bien intentionnées fussent-elles, peuvent être sujettes à des abus et causer des préjudices importants. Les charges des mesures ne peuvent pas non plus simplement être répercutées sur des tiers ou des intermédiaires (non impliqués). Il convient par conséquent de fixer des limites étroites aux autorités et de décrire leurs compétences en détail. Le projet soumis comporte trop de descriptions générales et vagues. Une sécurité absolue ne peut pas être assurée, un risque existera toujours. En cas de doute, il faut opter pour la liberté et contre de vastes compétences d'ingérence.

droitsfondamentaux.ch, les *JDS* et la *SPF* rejettent intégralement ce projet et n'y trouvent aucun élément positif. Ce projet est une liste de vœux pieux de la protection de l'Etat qui doit être transformée en dispositions légales. Le projet de loi ignore complètement ou fait alors peu de cas des éclatantes faiblesses de la protection de l'Etat, ainsi que des réserves émises par le Parlement.

Le droit pénal et les codes de procédures pénales offrent aujourd'hui déjà suffisamment de moyens qui vont très loin, aussi pour des investigations préventives. Les ingérences dans la sphère privée prévues dans la LRens sont disproportionnées. Les nouvelles mesures de contrainte que le SRC devrait se voir autoriser de mettre en œuvre sont l'élément crucial du projet, même si dans ce projet elles peuvent facilement être rendues méconnaissables.

Le *GSsA* rejette la totalité du projet. Ce projet, dit le *GSsA*, occulte pour ainsi dire complètement le rejet de la LMSI II et les conditions qui y étaient liées et que le Parlement avait formulées à l'attention du Conseil fédéral. Par ailleurs, le *GSsA* critique sur le fond que l'ancien service de renseignement civil, après sa fusion avec le service de renseignement de l'armée et sa nouvelle constitution en SRC, soit intégré au DDPS et non pas à un département « civil ».

Pour des investigations préventives, le code de procédure pénale et le droit pénal en vigueur offrent aujourd'hui déjà suffisamment de moyens qui vont très loin.

Les ingérences dans la sphère privée envisagées dans la LRens sont disproportionnées et le danger de nouveaux fichiers foisonnants de données tous azimut est élevé. De toute façon, des ingérences dans la sphère privée de personnes engagées politiquement n'est pas seulement un danger pour la démocratie, mais aussi un énorme gaspillage des ressources de l'Etat.

Le GSsA craint aussi que la protection de l'Etat, sans surveillance effective et sans transparence, ne s'oriente pas en fonction des menaces réelles pour le pays, mais en fonction des préférences politiques de ses collaborateurs. Il n'y a pas d'indications permettant de penser qu'à l'heure actuelle, il en irait différemment qu'à l'époque du scandale des fiches.

PP1 retient avec intérêt que le projet comporte une vaste série de garanties importantes pour le contrôle des activités des organes du SRC et pour la protection d'impacts excessifs, à savoir: principe de la proportionnalité; sauvegarde de l'espace de vie privé et de la sphère privée; implication d'une instance juridique indépendante pour des mesures d'ingérence lourdes de conséquences; responsabilité personnelle et politique des mandataires de mesures de surveillance; protection des personnes détentrices de secrets professionnels dévolus par la loi; création (ultérieure) de transparence; dispositions sur la garantie de la protection des données; haute surveillance parlementaire; protection juridique et responsabilité de l'Etat pour des actions illicites des organes de la Confédération ou des cantons, conformément aux lois ad hoc en matière de responsabilités.

Le *Référendum LMSI* peut parfaitement renoncer à un fichage et à la surveillance des communications téléphoniques et par courriel. A l'avenir aussi, le SRC recherchera et traitera des informations sur les activités politiques et l'exercice de la liberté d'opinion, de réunion ou d'association à moins de dissoudre ce service ou de limiter massivement son acharnement à vouloir collecter des données. La LRens contient toutes les échappatoires de la LMSI. Si des mesures supplémentaires de recherche soumises à autorisation devaient être accordées au SRC, l'avalanche insensée de données sans valeur s'accroîtrait massivement. La manière la plus simple d'éviter cela à l'avenir et de supprimer le service de renseignement intérieur. Dans cet esprit, le *Référendum LMSI* recommande au Parlement de maintenir les dispositions transitoires qui abrogent la LMSI et de supprimer purement et simplement le reste du projet.

L'*USAM* refuse le projet, estimant que ce ne sont pas les activités de renseignement qui dérangent, mais la protection insuffisante de la sphère privée des citoyens. La manière d'aborder la gestion des données et l'imprécision de la différenciation entre celles concernant la Suisse et celles relatives à l'étranger, est particulièrement problématique. Savoir quelles sont les délimitations entre ces catégories et quelle est l'importance de cette différenciation pour le droit de protection de la sphère privée, telle est la question qui doit être posée. Sont également problématiques les investigations sans soupçon, les mesures de contrainte et le fait que le SRC soit perçu comme une « Police de la Confédération ».

Un service de renseignement fort se caractérise par les éléments suivants: la défense contre des dangers à l'intérieur du pays et à l'étranger, le monitoring de tendances géostratégiques, y compris les relations d'échange dans le cadre des flux globaux de production et de financement, et l'élucidation d'importantes interrelations concernant la politique de sécurité pouvant exercer une influence sur la Suisse. D'ailleurs, c'est sur cette toile de fond, que l'*USAM* est favorable à un service de renseignement bien organisé et efficace sur le plan opérationnel.

Simultanément, il faut absolument tenir compte des besoins de protection de la population, qui n'a pas seulement un droit d'être protégée en cas de menace pour sa sécurité, mais aussi du droit inaltérable de protection de sa sphère privée. Ce droit inclut la souveraineté sur des informations et données personnelles ainsi que la protection d'ingérences excessives de l'Etat.

La *FSCI* espère que le projet sera approuvé si possible sans modifications ou pour le moins sans être atténué. La *FSCI* serait par ailleurs favorable au fait que les mesures de recherche soumises à autorisation soient aussi applicables à l'extrémisme violent. La projet est

considéré comme équilibré et ne remet pas en question le droit à la sphère privée et les libertés personnelles.

La SSO et l'ASOR approuvent la nouvelle base légale uniforme pour le SRC, y compris la nouvelle orientation de la recherche d'informations et les mesures prévues à cet effet, les dispositions légales différenciées pour la saisie, le traitement et l'enregistrement des données ainsi que le système de contrôle proposé.

Les instruments contenus dans le projet sont nécessaires pour lutter contre les menaces actuelles et pour détecter à temps de futures menaces. La procédure proposée pour garantir l'équilibre entre la sauvegarde des droits individuels et l'intérêt public pour la protection de la sûreté intérieure et extérieure de notre pays semble appropriée.

La différenciation entre activités terroristes et extrémisme violent est considérée comme non applicable dans la pratique. Par ailleurs, les dangers résultants pour l'Etat et les citoyens de ces deux activités interdites sont d'une gravité comparable. L'exclusion de l'extrémisme violent des mesures de recherche d'informations soumises à autorisation est de ce fait rejetée.

La possibilité du Conseil fédéral – en informant simultanément la Délégation des Chambres fédérales compétente – de pouvoir faire intervenir le SRC pour la sauvegarde d'intérêts essentiels de la Suisse est par contre explicitement approuvée.

La Swico approuve dans l'ensemble la création d'une base légale formelle uniforme pour l'activité de renseignement et les systèmes d'information y relatifs, mais elle se défend contre un élargissement dans l'esprit d'une surveillance totale.

SwissBanking parvient à la conclusion que le projet semble très équilibré en ce qui concerne le champ de tension entre les intérêts de sécurité de notre pays et de sa population et les intérêts des personnes touchées par les ingérences dans leurs droits fondamentaux. La création d'une base légale globale permet d'imposer des réglementations et des mécanismes de protection éprouvés pour tous les domaines partiels du service de renseignement qui s'enchevêtrent.

Swisscom rejoint entièrement la prise de position et les propositions de son association professionnelle, l'asut.

La FSFP soutient cette solution politique minimale. En ce moment, la Suisse n'a qu'une loi sur le renseignement extrêmement tempérée (LMSI). On peut dire sans hésiter que comparée à d'autres Etats, la protection de la sphère privée est un principe fondamental très respecté en Suisse. Cependant, il faut être conscients que la situation actuelle de la menace n'est plus du tout la même qu'il y a encore quelques années.

5. Réponses concernant les divers articles

Article 1

Alinéa 1:

Le CCCZH considère qu'il est absurde que le SRC puisse interagir avec n'importe quel particulier ou avec l'étranger (al. 1, let. b). Il ne veut pas que le SRC puisse entretenir des contacts avec des criminels qui pourraient lui être utiles ou des pays qui ne respectent ni lois ni morale.

Alinéa 2:

Pour le PS, il est clair que ce sont les activités de renseignement fixées à l'al. 2 qui ont la priorité. Des activités supplémentaires, qui ne correspondent pas aux tâches ordinaires d'un

service de renseignement, ne devraient être réalisées qu'à titre exceptionnel sur décision du Conseil fédéral et n'être effectuées que dans le cadre de limites temporelles et géographiques étroitement définies en fonction de cas spécifiques (art. 62).

Concernant les let. a et b, le *CCCZH*, se demande dans quelle mesure le SRC ne contribue pas lui-même à inciter à l'insécurité et à l'illégalité en se jouant des lois et en s'ingérant de manière illicite dans la sphère privée de personnes.

Selon la *SSO* et l'*ASOR*, la détection précoce d'indices de menaces ou une mise en alerte avant qu'un potentiel de risque ne se développe en menace concrète est critique. Ces deux organisations proposent de compléter l'objectif et le but de la présente loi tels que stipulés à l'art. 1, al.2, avec les let. a et e suivantes:

a. contribuer au maintien de l'indépendance et de la sécurité de la Suisse face aux menaces extérieures;

Les lettres a à c deviennent les lettres b à d.

e. entreprendre à temps l'adaptation des instruments de politique de sécurité de la Confédération, notamment l'armée, au développement de la menace;

La lettre d devient la lettre f.

Alinéa 3:

Pour le *PS*, les éléments suivants n'ont pas été éclaircis dans le rapport sur l'avant-projet: que signifie « soutien de la politique extérieure de la Suisse » ? Et que veut dire « protection de la place industrielle, économique et financière de la Suisse » ? Le message devrait donner des précisions à ce sujet.

Pour le *CCCZH*, cet alinéa ouvre la voie à l'espionnage industriel et économique, ce qui pourrait mettre en danger la neutralité de la Suisse.

La *SSO* et l'*ASOR* saluent la possibilité donnée au Conseil fédéral de faire intervenir le SRC pour sauvegarder d'autres intérêts essentiels de la Suisse en informant l'organe compétent des Chambres fédérales. Ces deux organismes suggèrent toutefois de préciser que ces intérêts doivent relever de la compétence constitutionnelle de la Confédération, à moins qu'une demande ait été déposée par un ou par plusieurs cantons pour lancer une intervention du SRC en vue de la sauvegarde d'autres intérêts essentiels de la Suisse relevant de la compétence constitutionnelle des cantons.

Selon *PP1*, l'attribution des domaines d'activités et des compétences est peu claire car la liste des tâches fixées à l'art. 4 n'est pas en exacte concordance avec l'art. 1, al. 2 et 3. Par ailleurs, l'art. 17, al. 2, contient une liste de faits qui découlent de l'art. 4 et qui décrivent les « menaces concrètes pour la sûreté intérieure ou extérieure » de la Suisse. A ce sujet, il faut remarquer que les domaines d'activités du SRC selon l'al. 2, let a, et l'al. 3, sont difficiles à délimiter, ce qui pourrait entraîner certains risques d'activités et de prises d'influence du SRC dans le débat démocratique ayant trait à la politique intérieure.

PP1 recommande par conséquent de concentrer les al. 2 et 3 plus explicitement sur les domaines d'activités essentiels du SRC.

Al. 2: Tâches décrites dans la *LRens* qui doivent être réalisées par les organes du SRC sans mandat supplémentaire, axé sans équivoque – et strictement limité – à la protection de la population suisse (év. en y incluant les Suisses de l'étranger), la liberté du peuple et l'assurance de la sécurité et de l'indépendance du pays conformément au libellé de l'art. 2, al. 1, Cst; il s'agit des tâches qui sont définies à l'art. 4, al. 1, let. a; et al. 3: Sauvegarde « d'autres intérêts essentiels de la Suisse », tels que des intérêts internationaux ayant trait à

la sécurité, le soutien de la politique extérieure et la protection de la place industrielle, économique et financière de la Suisse sur la base de mandats clairement définis, conférés par le Conseil fédéral dans le cadre de sa responsabilité politique soit par l'attribution d'un mandat général dans la législation d'exécution selon l'art. 72, tel que la promulgation de la « Liste d'observation » selon l'art. 63; ou par l'attribution d'un mandat ponctuel, à déterminer de cas en cas selon la procédure fixée à l'art. 62.

L'USAM suggère d'utiliser à l'al. 3, en principe déjà formulé avec suffisamment de précision, le terme plus usuel et encore plus précis de « place économique suisse ». Il ne ressort en effet pas de l'énumération en quoi consistent les différences respectives et si l'énumération ne prend en considération que les besoins de protection de ces éléments.

Article 2

Le CCCZH attire l'attention sur le rapport problématique qui existe entre la let. b et c. A la let. b, il manque l'engagement de ne rechercher directement ou indirectement (par des intermédiaires) des informations que par voie légale.

La SSO et l'ASOR trouvent que la formulation de cet article n'est pas heureuse. Il peut en effet être interprété en ce sens que la loi ne concerne que les acteurs explicitement mentionnés. Ils proposent donc d'obliger aussi les autres autorités de la Confédération, qui ne sont pas directement chargées de l'exécution de la loi, de collaborer pour autant qu'elles disposent d'informations pertinentes en matière de renseignement:

Art. 2 *Autorités et personnes concernées*

La présente loi s'applique aux autorités et personnes suivantes:

- a. *[inchangé]*
- b. *autorités de la Confédération et des cantons et autres personnes morales de droit public ou privé pour autant qu'elles accomplissent des tâches de souveraineté et qu'elles disposent d'informations pertinentes en matière de renseignement;*
- c. *personnes physiques ou morales, pour autant qu'elles soient tenues par la présente loi à transmettre des informations pertinentes en matière de renseignement ou qu'elles les transmettent volontairement.*

Article 3

GE déplore le délai d'une année car il est notoire que les investigations sur des faits importants nécessitent plus de temps.

Il manque au PPS la règle du principe de proportionnalité.

Pour le CCCZH, les al. 1 et 4 démontrent clairement que l'ingérence dans la sphère privée de personnes doit être érigée en norme.

Le SSO et l'ASOR trouvent que la formulation des al. 1 à 5 est excellente.

Alinéa 3:

Selon le PPS, c'est une instance indépendante qui devrait toujours procéder à l'évaluation de ces critères.

La *DigGes* relève un conflit possible entre les let. a et b et souhaite la création d'une instance responsable face au Parlement qui édicte des lignes directrices contraignantes pour gérer ce conflit (sinon, dans la pratique, la let. b n'aurait aucun effet).

Alinéa 4:

Selon l'*Université de Genève*, cette disposition enfreint l'art. 4, al. 4, LPD. Comme elle lèse gravement l'autodétermination sur les données personnelle, une base légale précise est recommandée. L'al. 4 ne peut pas être formulé de manière aussi ouverte: il ne doit pas seulement mentionner la recherche de données, mais également leur traitement et cela sous réserve de l'art. 29 et la prise en compte de l'art. 22.

Alinéa 5:

Le *PPS* attire l'attention sur le fait qu'en général, des organisations extrémistes ont aussi un bras politique modéré.

Le *CCCZH* n'accorde aucune confiance au contenu de cet alinéa.

Une interdiction de principe ne suffit pas à la *DigGes* sans la garantie que de telles exceptions sont autorisées de manière objective et indépendante par un juge.

Alinéa 6:

AG confirme l'importance du principe énoncé à l'al. 6.

Avec cet alinéa, selon le *CCCZH*, le SRC peut déjà observer lors de leur préparation toutes les activités qui lui paraissent relever de l'extrémisme violent ou du terrorisme.

De l'avis de la SSO et de l'ASOR, les exceptions sont trop restrictives. Ils proposent la formulation suivante:

⁶ *Il peut exceptionnellement rechercher des informations relatives à une organisation ou à une personne et les saisir avec une référence nominale s'il dispose d'indices fondés qu'elle met en danger la sécurité intérieure ou extérieure de la Suisse en exerçant ses droits selon l'al. 5.*

Eventuellement complété par:

...en particulier pour préparer ou exécuter des activités terroristes, d'espionnage ou d'extrémisme violent interdites.

L'al. 6 ss règle les compétences de recherche d'informations du SRC dans un domaine délicat du droit politique et sensible au niveau des droits démocratiques des citoyens (activités politiques et exercice de la liberté d'opinion, de réunion et d'association). De l'avis de *PP1*, il faut éviter ici de créer pour le SRC une compétence de recherche d'informations par une disposition d'exception formulée de manière générale car elle offre aux responsables de ce service une marge de manœuvre considérable pour des décisions discrétionnaires. Il s'agirait bien plus, au cas par cas, de demander l'aval du Conseil fédéral ou de sa Délégation pour la sécurité.

L'al. 8 devrait être remplacé par un nouvel al. 7, qui décrit cette procédure d'autorisation. L'actuel al. 7 concernant l'effacement des informations saisies dans ce domaine devrait être ajouté comme al. 8 à la fin de l'art. 3.

Alinéa 7:

De l'avis de *PP2*, l'effacement des données ne devrait empêcher ni la personne concernée d'y avoir accès ni les tribunaux de traiter un recours.

Pour le *PPS*, cet alinéa est le seul élément progressiste dans ce projet. Néanmoins, des investigations préliminaires approfondies devraient empêcher la saisie de telles données. Le *PPS* se demande comment le SRC peut garantir que toutes les données soient effacées dans l'ensemble de ses banques de données et que des Etats tiers procèdent également à leur effacement.

La *DigGes* considère que ce principe est juste en soi mais demande des mesures d'accompagnement supplémentaires, par exemple l'effacement de copies dans d'autres banques de données, la rectification d'informations comportant des erreurs qui ont aussi été transmises à d'autres autorités ou le constat de l'illicéité de la recherche d'informations par un tribunal. Par ailleurs, des mécanismes qui génèrent un effet formateur pour le SRC devraient être introduits.

Les exigences relatives au degré de la preuve que l'autorité doit apporter sont renforcées (« s'il s'avère que... »). Etant donné qu'il est fréquent qu'un délai d'une année ne suffise pas à élucider suffisamment un fait, une exigence plus modeste s'impose. La *SSO* et l'*ASOR* proposent de formuler cet alinéa comme suit:

⁷ *Il efface immédiatement, mais au plus tard après une année, les données personnelles saisies s'il s'avère que les présomptions sont infondées.*

Alinéa 8:

Pour le *PS*, cet alinéa va trop loin. Il propose de remplacer « permettent d'apprécier » par la formulation plus restrictive de « sont nécessaires pour apprécier »:

⁸ *... lorsque ces informations sont nécessaires pour apprécier la menace...* ».

droitsfondamentaux.ch, *Les Verts*, les *JDS* et la *SPF* attirent l'attention sur le fait que régulièrement, le SRC ne s'en est pas tenu aux limites de l'al. 5, qui interdit la recherche et le traitement d'informations sur les activités politiques et l'exercice de la liberté d'opinion, de réunion ou d'association.

Il s'agit soit de supprimer définitivement l'al. 8 soit de soumettre à une décision judiciaire la liste d'observation et la liste des groupements qui doivent être considérés comme extrémistes violents, ainsi que chaque ingérence dans les domaines mentionnés à l'al. 5.

Il serait encore plus utile qu'à l'avenir, ces listes soient publiques ou que les groupements et le nombre des personnes surveillées soient pour le moins indiqués dans le rapport annuel du SRC. La *DigGes* est également de cet avis. .

La *SSO* et l'*ASOR* aimeraient éviter la référence à une disposition qui figure plus avant dans le projet:

⁸ *Il peut au surplus rechercher des informations sur une organisation ou une personne et les enregistrer avec référence nominale lorsqu'il existe une présomption justifiée qu'elle menace la sûreté intérieure ou extérieure de la Suisse.*

Article 4

GE estime que la liste des domaines d'activités du SRC est adéquate. La mention des attaques visant les infrastructures sensible complète en particulier de façon appropriée l'éventail des tâches du SRC.

SG préconise que les éléments dont dispose le SRC sur d'éventuels actes punissables soient par principe transmis au Parquet et que ce principe soit inscrit dans la loi. Si les autorités pénales sont tenues d'informer le service de renseignement, cette règle doit être valable réciproquement. Comment les autorités de poursuite pénale auraient-elles connaissance que le SRC détient des données pertinentes de preuves dont elles pourraient

- selon l'art. 55 - demander la transmission dans le cadre de procédures pénales? Voilà qui n'est pas clair.

La *CAPS* considère que le catalogue des tâches est suffisamment bien décrit, mais constate que l'al. 1, let d, donne l'impression d'être une clause ayant une portée beaucoup trop générale.

Pour le *PBD*, la limite aux substances radioactives définie sous chiffre 4 est trop étroite. Compte tenu de l'imprévisibilité de certaines menaces, le Conseil fédéral, doit aussi pouvoir confier un mandat ultérieurement en se fondant sur les dispositions de la let. d.

Le *PLR* trouve la différenciation entre le terrorisme et l'extrémisme violent adéquate. Les récents événements ont montré que la guerre électronique et les dangers pouvant émaner des moyens informatiques doivent être pris très au sérieux. Le SRC doit donc disposer de moyens pour prévoir ces menaces et y faire face. Le *PLR* propose de compléter le chiffre 5 ou d'ajouter un nouveau chiffre 6 à sa suite:

« Les attaques informatiques ou préparatifs visant à pénétrer, affaiblir, détruire ou détourner les systèmes civils, militaires ou d'organismes internationaux présents en Suisse ou directement liés aux intérêts de la Suisse ».

Le *PPS* aimerait que l'al. 1, let. a, chiffre 5 soit formulé de manière exhaustive. Le *PPS* et *DigGes* souhaitent que l'al. 7 soit supprimé, puisque le même thème est repris à l'art. 5.

La recherche d'informations dans le domaine des biens à double usage (dual use) est un but légitime, mais ouvre au SRC un champ d'action très étendu. *PP1* considère que cela comporte un certain risque que soient enregistrées dans les banques de données du SRC des informations précieuses sur les activités industrielles relatives à « la place économique et industrielle de la Suisse », données appartenant à la sphère privée et juridiquement protégée des entreprises concernées. Ces données pourraient devenir un gage attrayant pour la collaboration avec des services de renseignement étrangers ou représenter une cible de choix pour des tentatives d'accès de la part de services de renseignement étrangers.

La législation d'exécution doit donc formuler l'activité du SRC dans ce domaine de manière plus concrète. Pour ce faire, le législateur peut s'inspirer des lois fédérales sur le matériel de guerre et sur le contrôle des biens. Pour les informations rassemblées dans le domaine de la prolifération, il s'agit de prévoir à l'art. 5 des mesures de protection et de sécurité particulières.

La séparation des pouvoirs est une condition fondamentale pour un ordre démocratique. C'est pourquoi *l'ASIN* exige que le Conseil fédéral présente des situations concrètes permettant d'entreprendre des activités de renseignement. Le fait d'inclure le Tribunal administratif fédéral en lui présentant une demande d'autorisation (art. 25) est une erreur. Par ailleurs, le Conseil fédéral doit définir de manière exhaustive les faits concrets pour toute activité de renseignement, ce qui en règlera aussi sans équivoque la responsabilité. Le présent projet de loi ne respecte pas le principe de la séparation des pouvoirs.

Le *CCCZH* se demande quelle est la différence entre « terrorisme » et « extrémisme violent ». De plus, il est évident que le chiffre 4 est volontiers mis en relation avec le chiffre 1. On peut aussi se poser la question si le rôle du SRC pour assurer la sécurité du Forum économique mondial n'est pas en contradiction avec l'art. 3, al. 5.

La *DigGes* craint que la formulation peu claire du chiffre 5 soit sujette à interprétations diverses afin de pouvoir par la suite élargir les mesures de recherche.

La SSO et l'ASOR estiment que cette formulation exclut les besoins généraux de renseignement. La phrase d'introduction de l'art. 4, al. 1, let. a, doit être la suivante:

a. *déceler à temps et empêcher les menaces pour la sûreté intérieure ou extérieure de la Suisse émanant en particulier:*

L'al. 7 doit être formulé de sorte à ce qu'il soit clair qu'il s'agit ici de toutes les obligations du SRC liées à l'accomplissement de ses tâches :

⁷ *Dans le cadre de l'accomplissement de ses tâches, il protège ses collaborateurs, ses installations, ses sources et les données qu'il a traitées.*

La Swico voit dans ce catalogue vaste et ouvert de tâches une autorisation quasiment illimitée pour la recherche et le traitement de données, raison pour laquelle il doit être ramené aux tâches et activités essentielles et absolument indispensables du SRC.

Article 5

La DigGes souhaite qu'il soit précisé que les mesures de protection et de sécurité ne servent qu'à assurer le mandat légal du SRC et qu'elles ne doivent cacher à la population ni le type ni le volume des activités du SRC ou couvrir des faits répréhensibles.

Pour *droitsfondamentaux.ch*, *Les Verts*, les *JDS* et la *SPF*, ces dispositions ne doivent pas figurer dans une loi. Pour un service qui travaille dans un domaine aussi sensible, elles devraient aller de soi. Des dispositions de ce type peuvent être fixées dans une ordonnance ou même dans un règlement. Selon l'art. 34, al. 1^{er}, LTC, le Conseil fédéral définit les conditions dans lesquelles la police et les autorités d'exécution des peines peuvent mettre en place, en service ou exploiter une installation perturbatrice afin de garantir la sécurité publique. Cette norme peut éventuellement être complétée par « autorités de protection de l'Etat ». C'est tout au plus l'al. 2 de cet article qui fait sens (tout comme l'art. 4, al. 7, d'ailleurs).

Compte tenu des explications relatives à cette disposition, le CCCZH se demande si, aujourd'hui, les délimitations entre le service de renseignement civil et le service de renseignement militaire ne sont pas déjà assez floues. Il se demande aussi quelle peut bien être la catégorie de personnes peut avoir accès à des fiches personnelles sensibles puisque apparemment, des tiers peuvent être mandatés pour effectuer des contrôles de sécurité et que des membres de l'armée vont et viennent librement au SRC. Le cercle des personnes qui ont potentiellement accès à des données personnelles sensibles semble trop important, et le SRC ne peut pas non plus exclure que des « collaborateurs frustrés » s'approprient d'importants fichiers de données.

Le SRC continue à planifier l'engagement d'installations de télécommunication perturbatrices. Le CCCZH est d'avis qu'il faut interdire au SRC l'utilisation de tels appareils, car cette réglementation pourrait être évoquée pour effectuer des « entretiens » dans des lieux où la communication entre personnes doit être perturbée de manière ciblée.

Pour *PP1*, par analogie avec l'art. 42, al. 2, seuls les collaborateurs y ayant dûment été autorisés selon les règles de la sécurité de l'information doivent avoir accès au réseau exploité par le SRC. Cette disposition doit être fixée dans la législation d'exécution.

Article 6

Le CCCZH pense que le fait d'armer un service de renseignement civil est erroné et il se demande dans quelles circonstances en lien avec les activités du SRC le port d'une arme

peut s'avérer absolument indispensable. Il manque aussi au *CCCZH* une indication générale sur le type d'arme envisagé. Régler cette question par voie d'ordonnance lui paraît délicat, car en définitive, tout peut être légitimé, en particulier à l'étranger.

Article 7

Alinéa 2:

Le *PPS* et la *DigGes* estiment qu'avec les moyens techniques à disposition aujourd'hui, il n'y a plus de problème pour transmettre des mandats écrits sans aucun délai et éventuellement d'en confirmer l'envoi par téléphone. Rédiger les mandats par écrit permet aussi d'en assurer l'exécution précise et le contrôle. Cet alinéa doit donc être supprimé.

Le *PBD*, par contre, aimerait qu'un délai exact soit fixé lorsqu'il s'agit de confirmer ultérieurement par écrit des mandats qui ont été conférés oralement.

Article 8

GE salue ces règles.

La *CCPCS*, *AR*, *BE*, *SG*, *SO*, *SZ*, *TG*, *UR* et *ZG* attirent l'attention sur le fait que les corps de police, pour pouvoir procéder à l'appréciation des situations exceptionnelles du point de vue de la police de sûreté, sont tributaires d'informations détaillées sur les événements particuliers. Cette nécessité concerne aussi des événements d'importance cantonale et locale (actions « Reclaim the street » à Zurich, actions autour de la Reithalle à Berne, etc.). Des représentants des services cantonaux d'exécution participent régulièrement aux appréciations de la situation et contribuent, par leurs connaissances, à une présentation globale de la situation sans devoir pour autant faire part de données personnelles sensibles, d'informations sur des opérations ou d'autres renseignements qui ne sont pas nécessaires à la maîtrise de l'événement. Comme il s'agit néanmoins d'informations classifiées, une autorisation légale pour l'utilisation des informations provenant d'activités du renseignement sur mandat de la Confédération serait judicieuse. L'art. 48 mentionne certes le système de présentation électronique de la situation (PES), mais l'utilisation d'informations provenant du renseignement pour diriger et mettre en œuvre des mesures de police de sûreté (des cantons) devrait déjà être décrite au chapitre 2 de la loi, raison pour laquelle l'art. 8 devrait être complété dans ce sens.

Article 9

Le *CCCZH* voit dans la collaboration du SRC avec l'armée l'autorisation de facto d'échanger des données avec les services de renseignement de l'armée, ce qui rendrait floue la délimitation entre sécurité civile et sécurité militaire. Le *CCCZH* craint aussi que l'art. 9 serve au SRC de « porte d'entrée » pour pouvoir rechercher des informations par toutes sortes de voies, car les réglementations qui régissent le SRA sont un peu moins strictes.

Alinéa 2:

PP1 craint, lors de l'attribution de mandats, un éventuel conflit de compétences avec les organes supérieurs des services de l'armée concernés.

Article 10

PP1 est d'avis que par analogie avec l'art. 9, al. 3, le Conseil fédéral devrait être habilité et chargé d'édicter des dispositions supplémentaires pour le domaine sensible de la collaboration avec des services de renseignement et des autorités de sécurité étrangers. Leur contrôle devrait être ajouté au plan de contrôle de l'autorité indépendante de surveillance stipulé à l'art. 66 ss.

Alinéa 1:

Lettre e:

SZ et ZG exigent qu'à l'encontre de la règle prévue à l'art. 61, les contrats de droit international ne soient pas seulement conclus par le Conseil fédéral, mais qu'ils soient aussi approuvés par le Parlement, ce qui permet de garantir un débat politique suffisant sur les données qui doivent être échangées.

Le *PPS* veut que des informations ne soient échangées qu'avec des Etats qui respectent les droits de l'homme et des données personnelles uniquement avec des Etats qui, selon l'appréciation du Préposé fédéral à la protection des données et à la transparence, remplissent certains standards minimums concernant la protection des données.

Le *CCCZH* manifeste de l'inquiétude face à la collaboration légale du SRC avec des services de renseignement étrangers.

La *DigGes* aimerait que cette disposition soit complétée par le renvoi à un article qui doit être ajouté et qui règle que:

- les données mises à disposition par l'intermédiaire de systèmes internationaux d'information soient aussi utilisées par les autorités d'autres pays en conformité avec les dispositions légales suisses;
- le respect de l'application de ce principe puisse être contrôlé par un service indépendant;
- les personnes concernées puissent faire valoir au niveau international leurs droits à la protection de leurs données;
- les personnes concernées soient informées de la transmission de données personnelles à l'étranger;
- quels genres de données et dans quelles conditions elles peuvent être saisies dans de tels systèmes d'information.

Un article de ce type pourrait être ajouté de manière appropriée à la suite de l'art. 56.

Alinéa 2:

Le *pvl* est critique face à la compétence créée par cette disposition. Il demande au Conseil fédéral de soumettre l'engagement de collaborateurs à l'étranger à une analyse des coûts-efficacité et le cas échéant d'y renoncer.

Alinéa 3:

BS souhaite que la licéité de la transmission de données par une autorité cantonale à une autorité de sûreté étrangère soit fixée dans la loi, de même que les conditions qui doivent être respectées dans ce cas.

GE attire l'attention sur le fait que cette disposition crée une limite qui pourrait s'avérer problématique. En particulier pour *GE*: en tant que canton à la frontière, il est amené à traiter de nombreuses questions concernant des frontaliers. De plus, il aimerait encore développer l'échange préventif d'informations avec les services compétents des pays voisins, une pratique actuellement indispensable. Cet aspect important est totalement éliminé par la limite imposée.

PP1 propose d'examiner quels sont les moyens que la Confédération pourrait utiliser pour faire respecter cette disposition.

Chapitre 3. Recherche d'informations (art. 11 à 38)

AG estime que l'extension des mesures de recherche d'informations non soumises à autorisation, par exemple, l'engagement de drones, est judicieuse. Du point de vue de la

police, les nouvelles possibilités qu'offrent les mesures de recherche d'informations soumises à autorisation doivent être saluées.

Compte tenu que ces dernières doivent être autorisées par le Tribunal administratif fédéral et avoir ensuite l'aval du chef du DDPS, un examen juridique et politique de l'admissibilité de ces mesures est assuré dans chaque cas.

AG et *privatim* se posent des questions par rapport aux réseaux sociaux, mais aussi aux exploitants de moteurs de recherche tels que Google ou aux entreprises de ventes en ligne comme Amazon, car ces services disposent de quantités astronomiques d'informations sur les caractéristiques personnelles, le lieu de séjour, le matériel informatique, les contacts, etc. de leurs utilisateurs, et aussi de profils fantômes de personnes qui ne font pas partie de leurs utilisateurs dûment enregistrés. Ces données pourraient être d'un grand intérêt pour les services de renseignement.

Il n'est pas clair si de telles mesures sont réellement envisagées et dans l'affirmative, si les dispositions contenues dans le projet sont suffisamment précises à leur sujet. La question se pose par rapport à des serveurs en Suisse et à l'étranger. Compte tenu de la complexité de la situation juridique, des biens juridiques en jeu et de la masse des informations qui peuvent être collectées, des explications sur cette thématique s'imposent dans le message.

SG relève que pour des raisons incompréhensibles, les mesures de recherche d'informations prévues dans le projet ne sont pas coordonnées avec celles du CPP. Si des informations sur des actes punissables devaient être transmises aux autorités de poursuite pénale, des problèmes pourraient en résulter si l'accusé, au cours de la procédure pénale, pouvait objecter que des preuves ont été apportées à l'aide de mesures qui ne sont pas prévues dans le CPP.

Sections 1 à 3 (art. 11 à 21)

GE estime que les cantons doivent bénéficier des mêmes privilèges que le SRC et il approuve de ce fait les propositions de la CCPCS.

Article 11

PP1 propose que soit examiné, et le cas échéant réglé dans la législation d'exécution, si les médias sociaux (Facebook, Twitter, XING, etc.), s'ils devenaient librement accessibles aux organes du SRC sur la base d'une inscription, peuvent être qualifiés de « médias accessibles au public ». Il reste la question de savoir si, d'un point de vue politico-juridique, la libre évaluation par le SRC des informations ainsi collectées doit être autorisée indéfiniment.

Par ailleurs, concernant le libre accès aux prises de vues de « Google Earth », « Google Maps » ou « Street View », qui sont par exemple déjà utilisés par les autorités fiscales, *PP1* se demande dans quelles conditions, quantités et à quelles fins le SRC peut utiliser systématiquement de telles informations pour ses buts et il conclut qu'un événement dûment justifié pour le moins par des réflexions politico-juridiques ou relevant de la raison d'Etat devrait être requis.

Lettre b:

Le *CCCZH* voit dans cette disposition un passe-droit pour l'obtention de toutes formes de données et aussi pour l'utilisation de recueils de données qui n'ont pas été recherchés par des voies légales. Des particuliers pourraient être recrutés pour élaborer de tels recueils.

De l'avis de *PP2*, des données obtenues illégalement par des particuliers ne peuvent pas être exploitées.

Article 12

Alinéa 1:

La *CCPCS*, *AR*, *BE*, *SG*, *SO*, *TG* et *ZG* indiquent que dans le CPP et les récentes lois cantonales sur la police, les observations sont soumises à des conditions et des limites particulières (étant donné que les observations représentent une restriction aux droits fondamentaux, même si elle n'est que modeste selon le TF lorsqu'il s'agit d'observations dans l'espace public). Compte tenu de cette évolution, il faut sans doute que les observations à des fins de renseignement obéissent aussi à certaines exigences. Par analogie aux dispositions qui régissent la police (qui est également engagée dans le cadre de la lutte contre les dangers), une action dépassant une certaine durée devrait aussi être autorisée par un service supérieur. Au SRC, ce service devrait obligatoirement se situer à l'échelon des chefs de domaines.

BE aimerait par ailleurs instaurer une règle analogue pour les autorités d'exécution cantonales.

La *CCPCS*, *AR*, *SG*, *SO*, *SZ*, *TG* et *ZG* suggèrent de fixer l'engagement de moyens techniques pour l'observation (relevés, localisation) dans la loi.

Le *PLR* considère que la question des drones doit être traitée séparément, compte tenu des possibilités mais aussi des dangers que comporte cette technologie.

Pour le *pvl*, l'engagement d'aéronefs et de satellites doit être intégré dans la catégorie des mesures de recherche d'informations soumises à autorisation.

PP2 aimerait que les observations d'une durée supérieure à 30 jours soient soumises à autorisation et qu'elles soient obligatoirement communiquées aux personnes concernées. L'engagement de drones, s'ils visent une personne déterminée, doit également être soumis à autorisation.

Le *PPS* attire l'attention sur le fait que le terme « aéronefs » peut englober toute la gamme des avions de combat aux drones sans pilote. Il s'agit ici de faire une différence entre la Suisse et l'étranger, car l'engagement – de drones, par exemple, à l'étranger –, peut être appropriée alors qu'elle ne l'est pas en Suisse, les enlèvements relevant de la compétence des cantons.

Selon le *CCCZH*, l'engagement de moyens au sol doit suffire et le contribuable ne pas être obligé de financer des « jouets » pour le SRC.

Alinéa 2:

De l'avis de *PP2*, la notion de « sphère privée protégée » devrait être précisée.

Pour le *PPS*, la deuxième phrase devrait être supprimée: les moyens dont l'utilisation ne permet pas de protéger la sphère privée ne conviennent pas pour des observations.

En général, le *CCCZH* demande de renoncer à toute observation dans le domaine de la sphère privée, car le SRC pourrait interpréter la différence entre sphère privée protégée et non protégée selon sa propre conception juridique.

Article 13

Le *PPS* considère que des règles plus strictes sont de mise dans ce domaine. L'engagement d'informateurs devrait aussi être mentionné à l'art. 22.

Compte tenu de l'importance des informations collectées par le SRC pour la sécurité de la Suisse, *PP1* suggère d'examiner s'il ne fallait pas fixer une obligation légale de garder le secret particulièrement sévère pour les collaborateurs du SRC et leurs sources.

PP1 est également d'avis que les informateurs qui recherchent ou qui communiquent des informations au SRC devraient, pour leur propre sécurité mais aussi comme condition pour que le SRC exerce ses activités avoir l'obligation de respecter une stricte confidentialité sur leurs contacts avec le SRC, comme le prévoient les dispositions de l'art. 17, al. 3 pour les services de la Confédération et des cantons assujettis à l'obligation de renseigner.

La *DigGes* estime que puisque les règles en la matière ayant fait défaut jusqu'à ce jour, il est dorénavant absolument nécessaire de garantir que:

- cette mesure – fût-elle prise ou non - ne doit l'être qu'en cas de menaces graves;
- le respect de l'application du principe de proportionnalité doit pouvoir être contrôlé par une autorité indépendante;
- le public soit informé de l'ampleur et des buts de la mesure.

Dans ce domaine, la loi doit impérativement prescrire un examen par un juge, en particulier pour l'octroi de l'exonération fiscale et à l'assujettissement à l'AVS.

Alinéa 1:

Lettre b :

Ces prestations, selon *PP2*, ne peuvent pas inclure des activités qui seraient interdites au SRC.

Alinéa 2:

Le *PPS* aimerait que les moyens engagés ici soient spécialement inscrits au budget et il estime que le SRC doit verser les contributions à l'AVS sous forme anonyme.

Des indemnisations peuvent se justifier, mais elles devraient selon le *PS* rester une exception, être modestes et en aucun cas être versées dans l'intention d'exercer une influence (corruption). Ces indemnisations devraient aussi être examinées chaque année par la DélCdG. Le *PS* propose une formulation plus restrictive:

² *Le SRC, à titre exceptionnel et dans des cas dûment justifiés, peut indemniser ses informateurs pour leur activité. ...*

droitsfondamentaux.ch, Les Verts, les JDS et la SPF pensent qu'il existe un risque que des sources, dans une optique de modèle d'entreprise, puissent vendre aux SRC des informations inventées de toute pièce ou pour le moins des dramatisations contraires aux faits. Si l'indemnisation est maintenue, elle doit être soumise à l'autorisation d'un juge, les montants pour le moins être assujettis à l'AVS et à l'impôt et la DélCdG être informée chaque année des versements effectués à ce titre.

GE considère que les al. 3 et 4 sont parfaitement justifiés.

Article 14

NE est d'avis que cette mesure devrait aussi pouvoir être mise en œuvre par les cantons.

Le *PPS* exige que cette disposition soit supprimée, car elle représente une atteinte grave aux droits de la personne des individus concernés. Pour le même raison, la *DigGes* demande que des règles identiques à celles de l'art. 13 soient fixées ici.

Afin d'empêcher tout abus par le SRC et par conséquent un débordement des signalements, *droitsfondamentaux.ch, Les Verts, les JDS et la SPF* demandent une réduction de la liste des menaces qui permettent de déterminer le lieu de séjour. Tous les signalements doivent de plus être soumis à l'autorisation d'un juge

PP1 part du principe que cette énumération concerne des situations d'options possibles et il est d'avis qu'un signalement émis par le SRC en vue de sauvegarder des intérêts essentiels de la Suisse doit dépendre du respect de la procédure prévue à l'art. 62.

PP2 demande que des mesures soient prises afin de ne pas créer l'impression, lors de la consultation du registre, que la personne faisant l'objet d'un signalement est soupçonnée d'avoir commis un délit ou un crime.

Section 2: Couverture et identité d'emprunt:

GE salue la possibilité de doter les collaborateurs de couvertures et d'identités d'emprunt.

Les art. 15 et 16 prévoient l'engagement sous couverture de collaborateurs des autorités d'exécution cantonales mandatées par la Confédération. La CCPCS, AR, SG, SO, SZ, ZG et ZH suggèrent de fixer comme condition pour ces cas l'approbation du supérieur hiérarchique cantonal du collaborateur concerné puisque ce dernier sera exposé à un risque non négligeable, ce qui est inadmissible sans l'aval du directeur responsable (commandant de police) de ce collaborateur.

Article 15

Concernant l'approbation du supérieur hiérarchique cantonal, ZG propose d'ajouter ce qui suit :

« ¹L'engagement d'un collaborateur d'une autorité d'exécution cantonale ne peut intervenir sans l'approbation du chef de cette autorité. »

Le PPS aimerait que seuls les collaborateurs du SRC puissent être dotés d'identités d'emprunt, et non pas les collaborateurs des autorités d'exécution cantonales.

Article 16

En raison de l'atteinte grave portée aux droits de la personne, le PPS exige que les identités d'emprunt soient soumises à autorisation et que leur nombre soit publié dans un rapport.

droitsfondamentaux.ch, *Les Verts*, les *JDS* et la *SPF* se demandent pourquoi, après quelques mois (juillet 2012), une extension de ces dispositions s'impose (par ex. prolongation après 5 ans pour 3 années supplémentaires, utilisation lors de chaque « menace concrète de la sûreté intérieure et extérieure de la Suisse » dans l'esprit de l'art. 4, al. 1, identités d'emprunt jusqu'à 12 mois pour des opérations précises). Avec une identité d'emprunt dans le cadre d'opérations précises, les sources peuvent en particulier devenir rapidement incontrôlables. Avant de réfléchir à une extension, le SRC doit d'abord rendre des comptes au Parlement sur la pratique adoptée jusqu'à présent.

Alinéa 2:

La CCPCS, AR, SZ, UR et ZG saluent le fait que la durée ne soit pas limitée de manière absolue. Mais la formulation à ce sujet n'est pas assez claire: malgré la notion intitulée « au besoin », cette disposition peut être interprétée en ce sens que les identités d'emprunt doivent être levées après huit ans au maximum. La formulation de l'al. 2 doit être adaptée en conséquence.

Section 3: Droit d'obtenir des renseignements et obligation de fournir des renseignements (art. 17 à 21):

La *CCPCS*, *AR*, *BE*, *SG*, *SO*, *SZ*, *TG*, *UR* et *ZG* attirent l'attention sur le fait que le projet, comme déjà relevé, ne mentionne explicitement que dans un nombre restreint de normes de délégation les services d'exécution des cantons comme instances autorisées. Ce fait est particulièrement critique en ce qui concerne l'art. 17 ss relatifs à l'obligation des autorités et des particuliers de renseigner et de communiquer des informations. L'obtention de renseignement auprès d'autres autorités fait partie du travail quotidien des collaborateurs des services d'exécution cantonaux. Ces dernières années, ces collaborateurs ont de plus en plus souvent été interrogés par ces services sur les bases légales pour la transmission des données demandées. Une norme de compétence explicite doit de ce fait être ajoutée dans la loi.

Article 17

Le *PPS* veut que l'obligation de renseigner soit autorisée par un service indépendant et que les informations transmises soient également évaluées par un tel service.

Le *CCCZH* considère que l'effet déstabilisateur émanant du SRC sur la collectivité publique est plus important que celui qui émane des graves menaces indiquées dans le rapport sur l'avant-projet.

droitsfondamentaux.ch, *Les Verts*, les *JDS* et la *SPF* estiment que cet article comporte un automatisme qui entraînera une accumulation de données non pertinentes n'ayant aucune utilité. Ce fait a été démontré à plusieurs reprises dans le passé.

Alinéa 1:

Pour nombre de cantons, la demande motivée ne semble pas être axée sur la pratique. La *CCPCS*, *AR*, *BE*, *SG*, *SO*, *SZ*, *TG*, *UR* et *ZG* souhaitent un complément en ce sens que le motif de la demande d'information ne doit être fourni qu'ultérieurement, faute de quoi il existe le risque que la mesure soit déjouée. Par ailleurs, le motif ne doit pas répondre à des exigences trop élevées puisque souvent, les services d'exécution cantonaux ne disposent pas de connaissances globales sur le cas et que la transmission d'informations sur des menaces concrètes pour la sûreté intérieure ou extérieure de la Suisse à des autorités tierces peut s'avérer très délicate.

SwissBanking veut qu'il soit précisé que les banques cantonales ne sont pas considérées comme services des cantons au sens de l'art. 17, al. 1 et qu'elles ne sont pas concernées par l'obligation de renseigner ou qu'elles en sont exemptées.

Alinéa 2:

Le *PPS* demande qu'il soit renvoyé ici aux tâches fixées à l'art. 4, car les let. a, d et e s'en écartent par l'emploi de termes imprécis.

droitsfondamentaux.ch, *Les Verts*, les *JDS* et la *SPF* veulent supprimer la let. e: étant donné que la notion « approuvent des actes de violence » couvre pratiquement tout ce qui peut être dit lors d'une discussion particulièrement animée.

Alinéa 3:

AG trouve qu'il est important que les services concernés aient l'obligation de garder le secret sur les demandes de renseignement et la transmission d'informations à l'égard de tiers, mais qu'il convient de préciser explicitement que l'information des services supérieurs et des organes de surveillance sont exemptés de cette règle.

Le *PPS* veut que le nombre de demandes soit documenté dans un rapport annuel.

Article 18

Alinéa 1:

La *CCPCS*, le *PLR*, *AR*, *BE*, *SG*, *SO*, *SZ*, *TG* et *UR* demandent que les autorités de l'aide sociale et les autorités fiscales soient ajoutées au catalogue des autorités tenues de fournir et de communiquer des renseignements.

La *CCPCS*, *BE*, *SO* et *TG* saluent le fait que les autorités de surveillance des marchés financiers et les autorités qui reçoivent les communications en matière de blanchiment d'argent aient été ajoutées au catalogue des autorités tenues de fournir et de communiquer des renseignements. Ces dernières jouent en effet un rôle important dans la lutte contre le terrorisme.

TG propose de remplacer « les autorités de police, les autorités d'exécution des peines et les autorités pénales » par « les autorités de police, autres autorités pénales et d'exécution des peines »: selon le *CPP*, la police fait en effet partie des autorités pénales.

Le *PPS* aimerait que les obligations de renseigner et de fournir des informations soient autorisées et évaluées par un service cantonal et un service national indépendants. La coopération « d'autorités compétentes pour l'exploitation de systèmes informatiques » doit être réglée séparément.

Le *CCCZH* se demande pourquoi il s'agit de faciliter au *SRC* l'accès à des données de l'*ODM* et aimerait, concernant les obligations de renseigner, que les mains du *SRC* soient liées compte tenu de l'énorme potentiel d'abus que comporte cette règle.

La *DigGes* estime qu'il est nécessaire de préciser à la let. i que l'obligation de renseigner ne s'étend qu'au seul domaine de l'exploitation des systèmes informatiques et non à toutes les informations enregistrées dans ces systèmes.

Selon *droitsfondamentaux.ch*, *Les Verts*, les *JDS* et la *SPF*, cette disposition entraîne également un automatisme qui ne ferait qu'aboutir à une énorme quantité de données non pertinentes dont on ne tirerait en fin de compte aucun bénéfice. Grâce à la let. i, le *SRC* obtient un accès illimité à toutes les affaires, procédures et données d'autorités communales, cantonales et nationales.

Alinéa 2:

Le *PPS* veut que le nombre de demandes soit documenté dans un rapport annuel.

L'obligation générale de garder le secret sur les demandes et les renseignements communiqués est considérée comme disproportionnée par la *DigGes*. Elle ne devrait être ordonnée que dans des cas précis et dans des situations concrètes et n'être accordée que pour une durée limitée. De plus, elle devrait être autorisée par un juge. Le cas échéant, la loi pourrait prévoir une obligation de garder le secret qui est automatiquement supprimée après deux semaines si la décision d'un juge n'a pas été obtenue dans ce délai.

Alinéa 3:

droitsfondamentaux.ch, *Les Verts*, les *JDS* et la *SPF* considèrent que cette disposition est un passe-droit supplémentaire pour favoriser des dénonciations de par la loi. Il est à craindre que les autorités mises ainsi sous pression livrent des données personnelles en vrac sans exercer leur sens critique, raison pour laquelle cette disposition doit être supprimée.

Alinéa 4:

Si cette liste n'est pas publique, elle doit, selon le *PPS*, au moins être examinée par une autorité indépendante.

La liste non publique prévue viole le principe de la transparence (*DigGes*).

Article 19

Alinéa 2:

Le *TAF* fait remarquer que contrairement aux dispositions de la LMSI II, il n'est pas précisé si sa décision est définitive. Il n'est donc pas clair s'il s'agit d'un cas d'application de l'art. 36a LTAF (dans ce cas, la décision n'est pas sujette à recours) ou d'une décision concernant la sûreté intérieure ou extérieure (décision contre laquelle il n'est pas non plus possible de recourir).

Etant donné que le tribunal doit statuer le plus rapidement possible dans le cadre d'une procédure sommaire, qui doit encore être précisée dans les dispositions d'exécution, le *TAF* souhaite que ce point soit précisé dans la loi et dans le message.

Article 20

PP1 est d'avis que les tiers ou les organisations qui fournissent des informations devraient être tenues à la confidentialité (de manière analogue aux art. 17 et 18). Des mesures de protection des sources devraient aussi être prises en leur faveur (à l'exemple des art. 13 et 31).

Article 21

La *DigGes* suggère de préciser ici qu'il s'agit en premier lieu de transports commerciaux de personnes. Cette règle devrait toutefois être soumise à l'autorisation d'un juge. Le texte de loi devrait aussi être complété par une énumération détaillée des catégories d'infrastructures de sécurité concernées, faute de quoi cet article – très élastique – peut donner lieu à des interprétations diverses.

La loi doit également fixer que l'autorisation d'un juge doit être obtenue avant de demander des informations. Les personnes dont la sphère privée sera sûrement ou selon toute vraisemblance touchée doivent pour le moins être informées ultérieurement de cette mesure. Le juge doit en particulier examiner si les données demandées concernent ou sont liées à des événements politiques ou religieux, s'il s'agit éventuellement d'autoriser l'accès aux enregistrements sous certaines conditions ou de ne pas l'autoriser du tout. Les organisateurs des événements concernés doivent au moins être informés ultérieurement de cette mesure.

Le *CCCZH* aimerait mettre le holà au catalogue débordant des souhaits du SRC.

Alinéa 1:

Le *PPS* demande que chaque obligation de fournir des renseignements soit confirmée par un service indépendant et que les particuliers soient indemnisés pour leur débours. Par ailleurs, les droits de la personne de tiers ne doivent pas être touchés et les enregistrements d'événements à caractère politique doivent être interdits.

droitsfondamentaux.ch, *Les Verts*, les *JDS* et la *SPF* demandent que cette disposition soit supprimée.

PP1 fait remarquer que dans ce cas aussi, face à la personne ou l'organisation approchée pour fournir des renseignements, le SRC doit être en mesure de démontrer ou de rendre crédible la menace concrète particulière justifiant cette mesure. Par analogie à l'art. 17, al. 3, et l'art. 18, al. 2, les personnes qui fournissent des informations doivent être tenues de garder le secret, le cas échéant signifiée sous la menace de la peine prévue selon l'art. 292 CPP. Des mesures pour la protection des sources au sens des art. 13, al. 3 à 5 et 31 devraient également être ordonnées.

Lettre b:

La *Swico* critique l'absence de l'effet suspensif (art. 71, al. 3) de la décision sujette à recours, sans lequel un recours interjeté par les exploitants dont il est question est nul et non avenu.

PP2 craint que la remise et l'évaluation de matériel provenant de particuliers puisse être utilisé pour contourner la LRens. Les systèmes de surveillance vidéo doivent être installés sur des bases légales et le SRC ne peut traiter que du matériel qu'il aurait aussi eu le droit de rechercher lui-même. Cette disposition doit être précisée dans ce sens.

Alinéa 2:

Le *PSS* demande que les conditions plus strictes du CPP soient aussi applicables au SRC.

La *DigGes* exige que les renseignements selon l'art. 14, al. 4 LSCPT soient exclus, sinon la possibilité de communication anonyme par Internet serait compromise. De telles ingérences dans les droits fondamentaux ne devraient être exceptionnellement autorisées que dans le cadre de mesures de recherche d'informations soumises à autorisation.

droitsfondamentaux.ch, *Les Verts*, les *JDS* et la *SPF* estiment qu'il ne devrait en principe pas être possible, lors d'actes punissables commis via Internet, de porter atteinte au secret de la correspondance par télécommunication sans l'autorisation d'un juge.

Section 4: Mesures de recherche soumises à autorisation (Art. 22 à 38):

Le *CCPCS*, *AR*, *BE*, *FR*, *SO*, *TG* et *ZG* estiment que les mesures de recherche d'informations que le législateur prévoit nouvellement sont aussi nécessaires qu'utiles. Aux yeux des organes d'exécution cantonaux, il conviendrait de clarifier d'une part les compétences pour ordonner de telles mesures, et d'autre part de déterminer quelle sera la participation des cantons concernant la mise en œuvre des mesures ordonnées par le SRC.

Le projet de loi – se fondant sur les évolutions géopolitiques et technologiques récentes – tente, par le biais de mesures de surveillance secrètes, mais aussi par des mesures de défense, de permettre d'identifier des menaces en temps utile et de pouvoir aussi y parer. Pour *BS*, cela constituerait la reconnaissance de l'affirmation, fréquemment avancée, que des instruments pertinents déjà disponibles dans le cadre de procédures pénales seraient inopérants parce qu'une quelconque suspicion à caractère urgent d'un acte prohibé serait souvent identifiée trop tard et qu'en matière de procédure pénale, il ne s'agit pas au premier chef de mesures visant à limiter ou éviter des dommages, mais de l'identification du ou des auteur(s) de l'infraction et de le(s) poursuivre pénalement.

GE est d'avis que la procédure d'autorisation à plusieurs échelons ainsi que la procédure d'urgence surprennent de par leur lourdeur, qui nuit à l'efficacité. Par conséquent, il conviendrait de remanier le projet de loi dans le but de simplifier les diverses procédures.

SO fait dépendre son adhésion aux nouvelles mesures de recherche d'informations soumises à autorisation de trois conditions – qui figurent actuellement dans le projet de loi – et qui lui semblent essentielles, à savoir:

- une appréciation différenciée des diverses menaces et champs de tâches du SRC;
- des normes très détaillées concernant les processus de traitement des données;
- la procédure d'autorisation à plusieurs échelons.

UR relève qu'il ne sera guère possible aux services d'exécution de petite taille d'appliquer des mesures de recherche d'informations soumises à autorisation et ordonnées par le SRC.

Le CCPCS, TG et ZG souhaitent compléter les dispositions des art. 22 ss en ce sens que les autorités cantonales d'exécution bénéficient du droit d'ordonner des mesures de recherche d'informations soumises à autorisation.

VD donne son aval à l'introduction de mesures soumises à autorisation à condition toutefois qu'elles ne soient mises en œuvre que dans des cas particuliers et exceptionnels. Ce canton salue le fait que ces mesures ne seraient pas appliquées à des représentants de partis politiques reconnus, même si leurs idées pourraient parfois être teintées d'extrémisme.

Les mesures de recherche d'informations actuelles se fondent essentiellement sur des informations provenant de sources publiques, sur la collecte de renseignements et sur l'observation de lieux publics. Mais ce type de recherche ne correspond plus guère à la réalité actuelle. C'est pourquoi le PDC est d'accord que le législateur autorise de nouvelles mesures de recherche d'informations en Suisse dans les domaines du terrorisme, du service de renseignement prohibé (espionnage), de la prolifération, des attaques d'infrastructures sensibles ainsi que pour la préservation d'autres intérêts essentiels de la Suisse.

La loi doit cependant être complétée en ce sens que des missions de recherche d'informations soumises à autorisation soient également possibles dans des cas d'extrémisme violent. En effet, aujourd'hui, ni la police ni le service de renseignement de la Confédération n'ont la faculté d'exercer une surveillance à titre préventif ou après une escalade de la violence dans des cas d'extrémisme violent ni de surveiller des appels téléphoniques ou des échanges de courriels.

Ces mesures constituent incontestablement une ingérence dans les droits fondamentaux de la personne. Le PDC salue dès lors le fait que ces mesures soient soumises à une double obligation d'autorisation, soit par le Tribunal administratif fédéral et par le chef du DDPS ainsi qu'à de strictes consignes en matière de protection des données.

L'UDC salue l'introduction de mesures de recherche d'informations soumises à autorisation. Les processus essentiels pour apprécier des menaces ne se situent pas dans l'espace public et ce n'est que dans des cas rares que l'on ferait sans doute usage de ces nouvelles mesures. De prime abord, on s'étonne que ce ne soit pas le Tribunal pénal fédéral qui soit déclaré compétent pour ladite autorisation, puisque c'est lui qui, en vertu de sa spécialisation, se prêterait particulièrement bien pour ce type d'affaires. Mais après réflexion, il s'agit finalement au premier chef d'un acte administratif d'une autorité fédérale. Cela rend alors plausible le choix du Tribunal administratif fédéral pour le déclarer compétent.

Alnt fait remarquer que les personnes sans fonction publique ne devraient pas s'accommoder du fait que les organes étatiques puissent enregistrer leurs faits et gestes en mots, images et sons. Pouvoir se mouvoir par principe sans surveillance étatique dans l'espace public est une exigence garantie par le droit fondamental. Les mesures de recherche d'informations soumises à autorisation, qui prévoient la collecte et le traitement de données dans l'espace non-public pèsent davantage que celui prévu pour les données dans l'espace publique. Ces mesures constitueraient par conséquent des ingérences graves au sens de

l'art. 13 Cst. et de l'art. 8 CEDH. *Alnt* demande dès lors de radier purement et simplement du projet de loi les mesures de recherche d'informations soumises à autorisation.

En résumé, l'*asut* expose ce qui suit:

L'extension des mesures de recherche d'informations soumises à autorisation en vertu des dispositions des art. 22 et suivants constitue une nouveauté cruciale. Cela étant, un élément central de cette disposition touche les mesures de surveillance dans le domaine du trafic des télécommunications. Outre les surveillances en matière pénales, les fournisseurs de services de télécommunication (FST) devront être contraints – et c'est nouveau – d'exécuter des ordres de surveillance ordonnés par le SRC.

Pour l'*asut*, il est primordial que les charges administratives pour l'exécution de ces ordres de surveillance supplémentaires demeurent dans un cadre raisonnable et défendable. Il convient aussi de relever que la Confédération n'indemnise pas les FST à prix coûtant pour la surveillance de télécommunications ainsi ordonnée, mais ne leur versent qu'une indemnité appropriée qui est loin de compenser les coûts de ces opérations. Dans le cadre de la révision, de la LSCPT, le Conseil fédéral veut d'ailleurs tenir à ce concept.

Aux termes du rapport sur l'avant-projet, il faudrait s'attendre à un très faible nombre de surveillances supplémentaires du SRC. Le rapport estime à dix par année les cas qui nécessiteraient une autorisation. Cela représenterait effectivement un nombre infime de cas comparé au nombre de surveillances effectuées dans le domaine de la poursuite pénale.

Mais il n'y a pas seulement le nombre de cas qui compte, car il importe que le législateur, dans la LRens, ne définisse pas des mesures et de procédures allant au-delà de la LSCPT. En ce qui concerne les possibilités de surveillances, la LRens devrait donc s'en tenir intégralement aux dispositions de la LSCPT ou se référer à cette dernière. D'ailleurs, on ne verrait pas pourquoi une dérogation à ce principe se justifierait. Sinon on courrait le risque que le SCR, se fondant sur un libellé qui s'écarterait des dispositions de la LSCPT, pose d'autres exigences, voire des exigences allant bien plus loin encore au service de la surveillance du trafic postal et des télécommunications et, partant, aux FST. Il faudrait en effet éviter que les obligations des FST en matière de surveillance du trafic des télécommunications soient élargies par le biais du SRC.

C'est sur cette toile de fond que l'*asut* demande que le législateur renonce dans la LRens d'instaurer une description autonome des possibles mesures de surveillance du trafic des télécommunications et de supprimer purement et simplement l'art. 22, al. 1, let. a à d. En lieu et place de cette disposition, il y aura lieu de se référer explicitement et exclusivement aux mesures de recherche d'informations et mesures de surveillance prévues par la LSCPT. Dans la 4^e section du projet de loi, il convient ensuite d'apporter une autre observation encore, à savoir que les mesures de surveillance dans le domaine du trafic des télécommunications interviennent par le biais du service Surveillance de la correspondance par poste et télécommunication (SCPT) et en vertu des consignes et des processus figurant dans la LSCPT.

Enfin, l'*asut* fait encore remarquer que la mesure de recherche d'information prévue à la lettre g est très « ouverte » et, partant, formulée de manière beaucoup trop vague pour être claire. La formulation « s'introduire dans des systèmes et des réseaux informatiques » pourrait permettre l'interprétation que l'on veuille s'introduire dans de vastes systèmes de courriels, dans de vastes systèmes Cloud ou dans des systèmes de transports entiers liés à Internet. Mais les possibilités d'ingérence du SRC dans de tels systèmes et réseaux iraient alors beaucoup trop loin. Voilà pourquoi il convient, selon l'*asut*, de préciser cette disposition en ce sens que les possibilités d'ingérence aux termes des chiffres 1 et 2 ne pourront se restreindre qu'au domaine purement privé (c'est-à-dire à des systèmes et des réseaux informatiques « d'utilisateurs finaux »). Par ailleurs, il convient encore de garantir et de statuer que ces mesures ne lèseront aucun client tiers. Les FST ne pourraient en effet pas fournir d'explications satisfaisantes pour de telles perturbations dans leurs prestations de services.

Pour le CCCZH, c'est ici que se manifeste l'acharnement de surveillance que le SRC veut exercer. La plupart du temps, les cénacles qui devraient donner leur aval se laisseraient de toute façon convaincre et ne seraient pas en mesure d'apprécier la nécessité de telles mesures, faute de connaissances suffisantes du cas.

Le CP et la CVAM ne peuvent pas s'imaginer qu'un service de renseignement puisse accomplir les tâches qui lui sont dévolues sans disposer des moyens spécifiques du renseignement. Tous deux sont dès lors convaincus que tous les Etats ont recours à de tels moyens. Voilà pourquoi il n'y a pas d'objection à formuler à l'encontre de la réglementation de leur application dans la loi. D'ailleurs, le contrôle tant judiciaire que politique auxquelles ces mesures sont soumises, offrirait suffisamment de protection contre d'éventuels abus.

Le CP et la CVAM comprennent et saluent l'intention de ne plus faire de distinctions entre les menaces venant de l'intérieur ou de l'extérieur. En revanche, la différenciation que le législateur voudrait faire entre l'extrémisme violent et le restant des menaces semble plutôt sujette à caution. Dans le domaine de l'extrémisme violent, la seule justification de cette distinction semble être l'intention de vouloir protéger la sphère privée plus strictement, afin de ne pas faire resurgir l'ancienne polémique de l'affaire des fiches. Pour le CP et à la CVAM cette motivation ne tient pas vraiment debout, à plus forte raison que la distinction entre l'extrémisme violent et le terrorisme est toujours plus ténue.

économiesuisse constate que les descriptions ne concordent pas avec les bases légales dans le domaine de la police, mais qu'elles vont plus loin. Or, à son avis, c'est une erreur, car tant les compétences que la manière de procéder devrait être aménagée de manière identiques aux dispositions en la matière figurant dans la LSCPT.

Les frais générés lors de la surveillance de tiers devraient leur être remboursés intégralement et même les coûts de mise en œuvre. Mais l'Etat se doit aussi de prendre intégralement à sa charge les suites dues à d'éventuels préjudices. Cela comprend en particulier les coûts subséquents à une panne ou à un ralentissement de systèmes informatiques. Certes, en cas de danger de retard, cette mesure pourrait paraître nécessaire, par exemple pour protéger des infrastructures sensibles. Mais on ne doit pas oublier que des erreurs d'appréciation peuvent toujours se produire.

PP1 fait remarquer que les mesures en vertu de l'art. 22, al.1, let. g, ch. 1 font courir le risque que le fonctionnement de ces systèmes informatique ou réseaux soit détruit ou que les données soient modifiées, voire supprimées, etc. Pour de tels risques, tout comme pour tous les autres cas dans lesquels l'activité d'organes du SRC cause des préjudices à des tiers, le SRC devrait être doté de normes particulières de responsabilité de la Confédération. En outre, PP1 déplore dans le rapport sur l'avant-projet l'absence d'une justification pour que le SRC n'ait pas à demander d'autorisation en cas de recherche d'informations en vue de lutter contre l'extrémisme violent.

La formulation du passage « sauvegarder les intérêts essentiels de la Suisse », selon l'art. 1, al. 3 est très générale et ne décrit pas de manière exhaustive la justification des cas d'application des mesures de recherche sujettes à autorisation; celles-ci s'ingèrent profondément dans le droit tant apprécié des personnes concernées et il importe dans ces cas que le Conseil fédéral ait préalablement donné son aval en vertu des dispositions de l'art. 62. Le seul fait qu'une organisation figure dans la « liste d'observation » prévue à l'art. 63 ne devrait pas suffire au SRC pour qu'il puisse ordonner une mesure de recherche d'informations soumise à autorisation.

Il convient aussi de rappeler qu'en cas de procédure d'autorisation chez les deux instances décisionnelles, ce sont des personnes individuelles qui prennent la décision de l'exécution de la procédure et que ces personnes sont tributaires des documents que le SRC leur soumet. En d'autres termes, une vérification intégrale sûre à cent pour cent de la demande d'autorisation n'est donc pas garantie, mais vu la nécessité de garder la confidentialité de la procédure, il n'est sans doute pas possible non plus de faire une demande d'autorisation

mieux qualifiée encore. En pratique, vu le principe du secret professionnel, il n'y a guère que des tiers qui pourront interjeter recours auprès du Tribunal administratif fédéral.

Lorsque des tiers sont soumis à une procédure de recherche d'informations soumise à autorisation en vertu des dispositions de l'art. 24, il faudrait garantir que tous les documents et toutes les informations recueillis dans cette procédure et qui n'ont aucun lien avec cette mesure soient séparés et qu'ils soient détruits immédiatement. D'ailleurs une disposition similaire figure à l'art. 33, al. 6 concernant l'exploration radio.

PP1 s'étonne que dans la procédure d'autorisation selon l'art. 25, al.1, le législateur ne demande pas que la demande adressée au TAF doit contenir des indications sur l'existence d'une situation concrète de menace justifiant cette mesure de recherche d'informations soumise à autorisation.

PP1 constate avec satisfaction que les documents sur la procédure d'autorisation sont exclus de l'accès aux documents officiels conformément à l'amendement prévu à l'art. 3, al. 1, lettre a, ch. 7 (nouveau) LTrans.

De l'avis de *PP1*, l'art. 29 devrait être complété d'une disposition en vertu de laquelle il serait précisé que lorsque des tiers en particulier ont été impliqués dans une mesure de recherche d'informations et que le report de les en informer a été autorisé sur la base de l'art. 29, al. 3, cette information devra intervenir immédiatement dès que tombent les motifs justifiant le report ou la renonciation à cette communication. A cette fin, il conviendrait de vérifier une fois par année si les données enregistrées séparément en vertu des dispositions de l'art. 53 relatives à des mesures de recherche d'informations soumise à autorisation répondent encore à la nécessité de l'obligation d'informer, comme le dispose, par exemple, le contrôle de qualité prévu à l'art. 40, al. 4.

De l'avis de *PP2*, le projet de loi ne doit pas introduire de mesures préventives de surveillance. D'ailleurs, le législateur s'y était refusé déjà lors de la révision de la LMSI. Dans les commentaires, on ne justifie pas pourquoi, soudain, ces mesures seraient indispensables bien qu'elles doivent être mises en œuvre rarement. De fait, en dépit de toutes les garanties théoriques, le risque d'un abus reste tout de même assez important. Les personnes concernées par ces mesures ne seraient de toute manière guère informées, car il est patent qu'il n'est guère possible de vérifier si la renonciation à informer les intéressés se justifie réellement. La notion de la menace concrète est très difficile à apprécier et dépend assurément aussi des influences qui, suivant les circonstances, pourraient ou non être communiquées par le SRC.

Le CP, ainsi que le rappelle *PP2*, contient une liste des délits dont les actes dits de préparation sont punissables. Dans un Etat démocratique, il ne faudrait reprocher au citoyen que des actes répréhensibles fixés d'avance et qui pourraient engendrer une mesure de surveillance. Du reste, de telles mesures ne devraient s'appliquer qu'aux personnes qui se voient aussi reprocher un délit, sinon on laisserait le champ libre à une surveillance intégrale et permanente. A propos, on pourrait mettre en doute les compétences cantonales en la matière, car les autorités cantonales pourraient alors appliquer des dispositions dérogeant à la législation fédérale.

La *privatim* se demande quant à elle si, somme toute, on peut parler de proportionnalité lorsqu'il s'agit de légaliser un logiciel gouvernemental dans le domaine de la prévention, où l'ingérence dans les droits de liberté des citoyens et citoyennes est si grande. On peut difficilement s'imaginer quelle situation de soupçons pourrait justifier l'utilisation de tels instruments qui n'auraient pas déjà été mis en œuvre par des procédures préalables en matière de poursuites pénales. Et si toutefois il fallait quand même répondre par l'affirmative à la nécessité du déploiement de tels instruments, il conviendra alors de s'assurer que les citoyens et citoyennes disposent d'une sécurité du droit et que le domaine crucial des droits fondamentaux ne soient pas touché par de telles missions.

Cela devient tout à fait clair au constat que le législateur autorise que l'on s'introduise dans des systèmes et des réseaux informatiques. Et comme en vertu de l'art. 24 on peut aussi s'imaginer des mesures de recherche d'informations à l'encontre de tiers, mêmes des

personnes n'ayant pas la moindre intention terroriste pourraient se voir exposer à une attaque cybernétique de la part de l'Etat. Par conséquent, il importe que non seulement les exigences posées aux bases légales soient élevées mais qu'elles le soient également dans la procédure d'approbation. A ce titre, si les réglementations sont formulées de manière suffisamment concrète, on peut en revanche déplorer que le rapport sur l'avant-projet reste encore très vague à ce sujet.

Il est donc absolument indispensable d'un point de vue relevant de l'Etat de droit que la demande faite au Tribunal administratif fédéral, contienne des indications détaillées ayant pour objectif la mesure de recherche d'informations ainsi que celles concernant les personnes visées. Outre ces éléments, il faudrait qu'elle comprenne également des indications précisant aussi exactement que possible quelles sont les informations qu'il s'agit d'obtenir en pénétrant dans d'autres réseaux informatiques. Ou encore à quelles informations il s'agit de rendre l'accès impossible, de le rendre plus difficile, voire de le détruire purement et simplement.

Référendum LMSI rejette catégoriquement une surveillance préventive sans présomption.

L'*USAM* remarque de manière critique que désormais, tout ce qui était permis avec l'aval du Tribunal aux autorités de poursuite pénale en cas d'une présomption fondée devrait dorénavant aussi être permis au SRC. Mais ici, les compétences du SRC sont élargies sans pour autant les lier absolument à la décision d'un juge.

S'agissant de la surveillance du trafic des télécommunications, l'*USAM* fait valoir que les Cours constitutionnelles des Etats européens qui avaient dû se prononcer sur la « conservation préventive de données » les avaient jusqu'à ce jour toutes jugées contraires à la Constitution. Mais il y a plus grave encore puisque par la révision de la LSCPT, il est question de prolonger l'obligation de conserver les données de fichiers comptables et de communications de six à douze mois. Par ailleurs, le Tribunal fédéral permet aussi l'accès aux données qui sont bien plus anciennes que la période de six mois, telle que le fixe le législateur.

Désormais – et c'est nouveau – des exploitants de structures de sécurités pourraient être obligés de remettre des enregistrements aux autorités. Mais ce faisant, on saisirait en même temps un nombre incontrôlable de tiers « innocents », qui pourtant ne disposeraient d'aucun moyen de droit pour se défendre.

C'est dire que quelques-unes des mesures de surveillance s'ingèrent beaucoup trop fortement dans la sphère intime des personnes pour en conférer le pouvoir à un service de renseignement agissant clandestinement et à titre préventif.

La révision de la LSCPT devra permettre également aux autorités de poursuites pénales de pénétrer dans des systèmes et des réseaux informatiques mais seulement pour intercepter et canaliser le contenu de la communication et les données marginales du trafic de télécommunications dans une forme non cryptée. Mais le projet LRens prévoit que le SRC peut pénétrer dans un système informatique et s'y procurer et utiliser toutes les informations qui y figurent, Théoriquement, on pourrait donc aussi manipuler les données. Pour installer des chevaux de Troie par Internet dans un ordinateur, le SRC devrait alors coopérer avec le service Internet du fournisseur de la personne-cible. Il est incompréhensible et même dangereux que le législateur autorise une telle attaque cybernétique.

Contrairement aux perquisitions pratiquées par les autorités de poursuite pénale, les perquisitions de locaux pratiquées par les collaborateurs du SRC sont secrètes. Les personnes concernées par ces perquisitions n'ont pas la possibilité de demander des mises sous scellés ou d'être présentes lors du tri de documents confisqués.

Voilà pourquoi l'*USAM* rejette catégoriquement ces mesures de recherches d'information et en donne les raisons suivantes: c'est parce qu'il convient par principe de distinguer les tâches de la police de celles d'un service de renseignement et qu'il ne faut pas combiner comme il est prévu dans le projet de loi les activités de la protection de l'Etat avec la procédure pénale. L'*USAM* rejette également la procédure à deux niveaux, parce qu'il n'est

pas réaliste de voir ici le Conseil fédéral comme une barrière, alors que le SRC est justement l'un de ses moyens.

SwissBanking salue en particulier le fait que, par rapport à l'ordre juridique en vigueur, l'on ait étendu l'instrument en matière de mesures de recherche d'informations soumises à autorisation. Conférer au SRC des compétences en matière de surveillance du trafic postal et des télécommunications, permettre des mesures techniques de surveillances générales, mais aussi mentionner explicitement la permission de pénétrer dans des systèmes et des réseaux informatiques semblent répondre à une nécessité d'actualité. Vu l'agressivité accrue constatée au cours de ces dernières années de la part d'acteurs étatiques et de leurs sbires en vue de se procurer des informations financières et, partant, de mettre en danger les intérêts économiques de la Suisse par des attaques de notre place financière, la réponse résolue d'être actifs dans le domaine du service de renseignement prohibé à titre préventif et non pas seulement après coup lors d'une poursuite pénale, s'impose d'urgence.

Swisscom souhaite qu'une correction soit faite au niveau de l'obligation de la Confédération d'indemniser les charges supplémentaires des fournisseurs de services de télécommunications; pour *Swisscom*, cette indemnisation est tout à fait insuffisante. . En effet, aux termes du rapport du Conseil fédéral sur l'avant-projet, les mesures de surveillance dans le domaine du renseignement fournissent une contribution substantielle à la sécurité de la Suisse et, partant, à la collectivité helvétique. *Swisscom* ne voit donc pas pourquoi la Confédération ne devrait pas en assumer le coût.

Article 22

SG demande quel est l'esprit des dérogations dans le libellé des dispositions de procédure pénale quant à la surveillance des télécommunications.

Les Verts déplorent que le Conseil fédéral ne puisse en aucune manière rendre plausible pourquoi les dix cas prédits par année ne peuvent pas être subsumés parmi les pouvoirs d'enquête conférés jusqu'à présent à la police judiciaire.

La *DigGes* estime que les principes fondamentaux de l'Etat de droit sont bafoués de la manière la plus éclatante:

- Tant que les mesures proposées ne sont pas strictement indispensables pour que soit maintenu l'ordre démocratique de la Suisse, la proposition d'une telle extension doit être rejetée déjà pour des raisons découlant de la convention des droits de l'homme.
- Mais s'il s'avérait que de telles mesures répondent réellement à une nécessité, alors les personnes concernées devraient être informées tout au moins après coup qu'elles ont fait l'objet d'une surveillance. Il conviendrait aussi de leur communiquer les mesures concrètes qui avaient été ordonnées à leur encontre. Au cas où les mesures ordonnées auraient été injustifiées, il conviendrait que la Confédération leur alloue alors une indemnité.

Pour *droitsfondamentaux.ch*, *Les Verts*, les JDS et la *SPF*, il est exagéré que le SRC puisse maintenant, avec des compétences encore plus étendues, tout faire à l'instar de ce qui est permis aux autorités de poursuite pénale lors d'une présomption fondée avec l'aval du Tribunal. Il convient de rappeler que toutes les Cours constitutionnelles des Etats européens qui avaient dû se prononcer sur la « conservation préventive de données » les avaient jusqu'à ce jour toutes jugées contraires à la Constitution.

S'il convenait d'engager une discussion, ce sont les restrictions imposées aux autorités de poursuite pénale qu'il faudrait aborder et sûrement pas l'extension des droits du SRC.

Ces protagonistes rejettent catégoriquement l'introduction de ces mesures de recherche d'informations soumises à autorisation pour plusieurs raisons, notamment celle qui

commande de séparer par principe les données des organes de la police et celles du service de renseignement. Mais il y en a encore une autre: le projet de loi prévoit de combiner des activités déployées pour la protection de l'Etat avec une procédure pénale; cela est inacceptable et c'est pour cette raison aussi que l'on doit rejeter cette disposition.

La *Swico* pense que le danger d'un abus de chevaux de Troie étatiques est énorme. De plus, il est très improbable que la procédure d'autorisation puisse exercer une véritable fonction de « filtrage ». De telles ingérences dans la communication privée de tiers ne peuvent en aucun cas se justifier.

PP2 et *Swisscom* se plaignent que la terminologie utilisée dans la LRens s'écarte sans fondement de celle figurant dans le code de procédure pénale. Pourtant, une concordance dans la terminologie s'avère d'autant plus cruciale que ces deux actes législatifs se réfèrent aux dispositions de la LSCPT.

Alinéa 1:

Lettre g:

BS est d'avis qu'il convient d'indiquer dans le message que ces mesures de recherche impliquent de graves ingérences dans les droits fondamentaux. Il convient dès lors de hausser les exigences posées à l'obligation de motiver la demande relative à ces mesures. Enfin, il y a également lieu de fixer des critères d'examen particulièrement sévères dans le contexte de la procédure d'autorisation. Par ailleurs, il convient de faire remarquer que la plupart des cantons ne seront guère à même d'exécuter intégralement ou partiellement les mandats du SRC en la matière avec leur propre personnel ou leurs propres moyens techniques.

TI souhaite que le message du Conseil fédéral précise que les graves ingérences dans les droits fondamentaux découlant de cette mesure de recherche ne puissent intervenir qu'en cas de motifs sérieux et importants. Mais *TI* reconnaît, il est vrai, que cet instrument instauré pour obtenir de telles informations s'avère crucial pour lutter contre les formes de criminalité modernes et que dans cet esprit-là, il ne faudrait pas que sa mise en œuvre soit empêchée par un excès de formalisme.

ZH déclare qu'en dépit de l'autorisation nécessaire octroyée par le Tribunal administratif fédéral et par le chef du DDPS, il ne peut pas donner son aval à la compétence que prévoit de conférer au SRC la lettre g de cet article pour manipuler des ordinateurs et d'y copier des données qui y sont enregistrées. Le législateur donnerait ainsi au SRC davantage de droit hors procédure pénale qu'à la police et au procureur général dans le cadre d'une enquête.

Le *SPD-TG* estime que cette disposition est problématique du point de vue de la protection des données. Le déploiement de chevaux de Troie par l'Etat de droit est extrêmement préoccupant, parce que l'on ne peut plus ainsi garantir la stricte séparation d'une écoute et de la sphère digitale privée.

A l'heure qu'il est, il est même possible de doter les chevaux de Troie d'une fonction de télécommande, grâce à laquelle on peut télécharger ultérieurement n'importe quel logiciel malveillant et l'activer. Ainsi, un cheval de Troie n'est pas seulement capable de fouiller des données existantes dans une mémoire, mais il est aussi apte à manipuler n'importe quelle donnée personnelle, voire d'infiltrer d'autres données encore dans un système informatique ainsi que d'avoir accès à un microphone, à une caméra ou au clavier d'un ordinateur, à une tablette ou à un téléphone portable.

Cet espace juridique se soustrait de cette manière à toute restriction et à tout contrôle. Lorsqu'on introduit un cheval de Troie dans un système tiers, il n'a forcément pas la capacité de faire la distinction entre les données appartenant à la sphère privée de la personne concernée et qui doivent être protégées et celles qui doivent être surveillées de par la loi.

Lorsque des chevaux de Troie entrent en fonction, cela conduit finalement au fait qu'il n'y a plus aucun contrôle sur la surveillance et que cette surveillance globale se traduit finalement par une ingérence extrêmement massive dans les droits fondamentaux des personnes concernées.

Le déploiement de chevaux de Troie rendrait dès les dispositions des articles suivants complètement illusoires, à savoir: art. 3, al. 5; art. 1, al. 2, let. a; art. 3, al. 2, let. b; art. 3, al. 7, art.10, al. 1, let. e; art. 20, al. 3; art. 24, al. 2; art. 28; art. 34, al. 2.

Le *SPD-TG* recommande donc instamment de renoncer à l'art. 22, al. 1, let. g.

Le *PDC* se pose la question de la mise en œuvre pratique de cette mesure: que se passerait-il s'il s'avérait que l'ordinateur visé se trouve à l'étranger ?

Le *PS* salue le catalogue restrictif et exhaustif des actes soumis à autorisation et il considère que la procédure à plusieurs niveaux par le biais du Tribunal administratif fédéral et par le chef du DDPS est adéquate. De cette manière, tant une vérification judiciaire que politique est garantie.

Ce nonobstant, l'art. 22, al. 1, let. g, ch. 2 soulève néanmoins des questions. Aux termes de cette disposition, à la suite d'une demande fondée, le SRC pourrait se voir autorisé non seulement à épier les informations contenues dans des systèmes et réseaux informatiques tiers, mais encore d'en perturber activement l'accès. Pour le *PS*, il est décisif que de tels actes soient effectivement restreints à des cas dans lesquels ces systèmes et réseaux informatiques sont utilisés pour « des attaques visant des infrastructures critiques », tel que le précise le libellé de ce chiffre-là. Dans sa loi sur le service de renseignement, la Suisse ne devrait pas éveiller un soupçon d'impression qu'elle pourrait déjà à la moindre suspicion détruire des systèmes informatiques étrangers. De tels actes ne devraient dès lors se limiter effectivement qu'à des cas où une attaque est démontrée. Voilà pourquoi le *PS* propose que soit précisé le chiffre 2 de telle manière:

² [...] à condition que ces systèmes et réseaux informatiques soient utilisés de toute évidence dans des attaques visant des infrastructures critiques;

Le *PPS* demande que cette disposition soit radiée.

Lettre h :

Le *PPS* demande une précision de cette disposition, étant donné qu'elle est rédigée d'une manière extrêmement vague.

Alinéa 2:

Le parti Pirate demande que la personne visée soit informée lorsque la suspicion s'avère infondée.

Article 23

Selon l'*asut*, dans le mécanisme décisionnel, il convient de distinguer entre deux questions, à savoir si dans un cas concret, des mesures de surveillance peuvent en soi être ordonnées et quelles mesures de surveillance concrètes pourraient être appliquées ou quels actes seraient somme toute possibles et devraient être mis à disposition par les fournisseurs de services de télécommunications.

En effet, le mécanisme décisionnel présente les mêmes faiblesses que celles déjà constatées dans la LSCPT.

Les autorités mentionnées examinent seulement d'une manière générale si, dans un cas concret, une surveillance du trafic de télécommunications d'une personne à surveiller entre vraiment en ligne de compte et cela à la suite de considérations de politique de sécurité. Pourtant, d'un point de vue du droit administratif, ces autorités n'examineraient pas si un SCPT peut être obligé ou non d'exécuter une mesure de surveillance tout à fait déterminée

– et au besoin même d'exécuter une toute nouvelle technique de mesure de surveillance. Cette dernière devrait cependant tout au moins être examinée par une autorité administrative, par exemple par le service SCPT à la demande d'un fournisseur de services de télécommunications sollicité. Mais, aux termes de l'art. 13, al. 1, let. a, modifié du projet de la LSCPT, c'est précisément le service SCPT qui ne pourra pas le faire. A l'égard des fournisseurs de services de télécommunications, il devra imposer l'exécution de la surveillance autorisée, même si les genres de surveillances en la matière ne font pas du tout partie du cahier des charges des FST. Cela étant, il y a donc un grand risque que l'on demande continuellement aux FST l'extension de leur sollicitation, alors que les coûts générés seraient unilatéralement à leur charge. Par ailleurs, il convient de faire remarquer l'incohérence suivante: aux termes de la LRens, le Tribunal administratif fédéral est mis à contribution deux fois, mais chaque fois dans un contexte complètement différent. En effet, dans un premier rôle, il doit procéder à une vérification en matière de politique sécuritaire, à savoir si une mesure de surveillance est indiquée ou non dans un cas et répond aussi au principe de la proportionnalité. Mais là, le TAF n'examinerait pas si les FST doivent effectivement mettre en œuvre ou non une mesure concrète. Le service SCPT auprès duquel cet examen devrait en toute logique se faire, ne peut pas non plus le faire, comme il a été exposé plus haut. Or, si cette mesure avalisée et ordonnée par le Tribunal administratif fédéral aux FST pour être exécutée en « aveugle » s'avérait pour ces fournisseurs de services de télécommunications être intolérable, voire illicite sous des aspects de droit administratif, il ne resterait alors à ces FST qu'une unique et seule voie: interjeter recours au Tribunal administratif fédéral. Cela dit, il est extrêmement peu probable que ce tribunal soit disposé ensuite à remettre en doute, en se fondant sur d'autres critères, une mesure qu'il aurait lui-même avalisée.

Il y a aussi une question qui reste floue, à savoir si cette procédure de recours doit maintenant intervenir selon les règles des dispositions de l'art. 71 LRens ou, au contraire, selon les normes de la LSCPT (jusqu'à présent, l'OSCPT prévoyait une telle possibilité de recours, alors que maintenant, une réglementation analogue aux dispositions de l'art. 71 serait prévue mais qui n'est pas identique à l'esprit des dispositions contenue dans le projet de la LSCPT à l'art. 42.

Au fond et en principe, il y aurait lieu de résoudre les problèmes soulevés par ce mécanisme décisionnel entaché de vices en commun avec la révision de la LSCPT.

Le PPS demande que les services compétents saisissent le nombre et le genre de ces mesures soumises à autorisation et les publient chaque année.

Alnt apprécie d'une manière positive le commandement de la proportionnalité, l'obligation d'autorisation à deux niveaux (par le Tribunal administratif fédéral et par le chef du DDPS) de cette mesure, ainsi que l'exigence supplémentaire quant à la gravité de la menace et à la condition que la recherche d'informations serait sinon restée vaine, vouée à l'échec ou aurait demandé des efforts disproportionnés. En définitive, c'est bien aux autorités qui appliquent la loi qu'il revient d'apprécier les cas de demande de recherche d'informations soumises à autorisation et c'est finalement cette grande marge de manœuvre dans l'appréciation qui est problématique du point de vue du droit fondamental.

Quant à la sauvegarde d'autres intérêts essentiels de la Suisse (qui, selon le projet de loi, justifient la grave ingérence dans les droits fondamentaux), il manque la définition des biens à protéger, telle que le professeur Biaggini l'avait suggérée dans son expertise dans laquelle il avait insisté sur ce fait.

Alnt est en outre d'avis que le droit fondamental est bafoué et elle dénonce la procédure d'urgence qui permettrait ainsi une surveillance sans autorisation du Tribunal. En plus, il n'est pas clair du tout à partir de quand court le délai de trois jours et surtout quand, somme toute, on est en présence d'un cas d'urgence.

Alinéa 1:

Lettre a:

SZ, UR et ZG déconseillent fortement de vouloir exclure expressément des mesures de recherche d'informations soumises à autorisation les missions devant être déployées en cas d'extrémisme violent. Pour des raisons politiques, on pourrait encore s'accommoder de cette renonciation, mais pas du point de vue de la police ou du service de renseignement. C'est justement dans ce contexte que la recherche d'informations s'avère extrêmement difficile. Un comportement conspiratif pouvant guère mener à des sources d'informations utilisables rend pratiquement impossible une large acquisition de renseignements exploitables à temps. Par ailleurs, on sait que les mouvements d'extrémisme de droite sont en réseau sur le plan international. La radicalisation de divers groupements de l'extrême droite et de l'extrême gauche ainsi que des associations islamistes radicales comportent un très sérieux potentiel de violence. S'il faut l'identifier à temps et l'empêcher au moyen de mesures préventives, alors des instruments de recherche d'informations soumis à autorisation devraient être mis en place de toute urgence.

Il convient donc de modifier l'art. 23, al.1, let. a, comme suit:

« il existe une menace concrète au sens de l'art. 17, al. 2, let. a à e, ou si d'autres intérêts essentiels de la Suisse le commandent (art. 62); ».

Pour la CCCZH, les « intérêts essentiels du pays » sont uniquement un autre terme pour « espionnage économique et industriel ».

Lettre c:

Le PPS voit dans cette condition une justification de simplifier les mesures soumises à autorisation.

Alinéa 2:

L'Université de Genève mentionne de nombreuses raisons qui, en matière de compétences, militent en faveur de donner la préférence au Tribunal fédéral pénal: ce tribunal a déjà acquis de l'expérience dans ce domaine et c'est pourquoi il conviendrait d'en tirer profit sans oublier que l'on gagnerait ainsi une certaine cohérence pour garantir l'application des mesures de contraintes. Ces mesures visent d'ailleurs fréquemment l'élucidation de machinations dans un contexte pénal. Enfin, le Tribunal fédéral pénal intervient occasionnellement dans des procédures administratives. Ces réflexions s'appliqueraient du reste aussi à l'art. 71.

Le CCCZH se méfie que ces mesures doivent être autorisées par le Conseil fédéral.

Alinéa 3:

PP2 souhaite que l'on apporte à la réglementation la précision que le chef du DDPS doit personnellement donner son aval et qu'il ne peut déléguer cette compétence à autrui.

Pour le CCCZH, cette approche « top down » implique la collaboration d'autres services fédéraux et les mettrait ainsi dans le pétrin.

Article 24

Alnt, le PPS et le CCCZH voient dans cette disposition une base pour que le SRC s'introduise dans la sphère privée de tiers (notamment de membres de la famille, d'employeurs, de collaborateurs) qui ne se sont rendus coupables d'aucune infraction.

Alnt attire l'attention que des mesures prises à l'encontre de tiers contreviennent au principe du perturbateur applicable en droit de police, mais cette organisation reconnaît aussi que des réglementations relatives aux découvertes par hasard et aux secrets professionnels de

tiers au moyen d'une adaptation au code de procédure pénal sont défendables du point de vue du droit fondamental.

Le *PPS*, lui, propose de radier cet article, qui est tout simplement inacceptable.

Alinéa 2:

SwissBanking demande que l'on exclue expressément les obligations de secret professionnel des prestataires de services financiers du champ d'application des mesures de recherche d'informations à l'égard de tiers. Le renvoi figurant à l'art. 24, al. 2 au code de procédure pénal ne suffit pas.

Article 25 ss

SZ ressent la procédure d'autorisation comme étant une procédure très lourde. Dans la pratique, il faut partir de l'idée que le chef du DDPS a déjà été mis au courant par le SRC bien avant que celui-ci ait fait la demande de mesure de recherche d'informations. Si la demande en question ne correspond pas à une opinion politique concordante, ni à celle de la Délégation pour la sécurité, la procédure d'autorisation devrait prendre fin déjà à ce stade-là. Cela n'a aucun sens de faire décider le Tribunal administratif fédéral si la volonté politique de mettre ensuite cette mesure en œuvre fait complètement défaut. C'est dans cet esprit qu'il convient de faire préalablement une vérification au niveau politique avant de lancer la procédure d'autorisation auprès du Tribunal administratif fédéral et de le décharger d'un travail autant supplémentaire qu'inutile.

Pour la *CAPS*, la procédure d'autorisation est adéquate.

Les Verts critiquent le mélange d'appréciation judiciaire et politique et le fait que le législateur ne prévoie pas que le SRC ne doive pas mettre le dossier à disposition du Tribunal administratif fédéral lors de sa demande.

Le *TAF* souhaite qu'il soit précisé dans les dispositions relatives à la procédure d'autorisation s'il s'agit, pour les délais, de jours ouvrables ou des jours civils.

Par ailleurs, jusqu'à ce jour, la *LTAF* ne connaît aucune procédure d'autorisation telle que la prévoit le projet de la *LRens*. Le professeur Biaggini a d'ailleurs déjà soulevé des questions relatives à la constitutionnalité de ces réglementations de procédure auxquelles le présent projet de loi ne répond pas. Il serait donc souhaitable de compléter les explications à ce sujet.

Pour la *DigGes*, il manque ici la garantie d'une représentation efficace des intérêts à la protection de la sphère privée. Par ailleurs, elle demande que soient publiés des statistiques qui démontreraient tout au moins le nombre de demandes, le nombre des demandes ayant été autorisées intégralement ou partiellement et toutes celles qui n'ont pas été autorisées, le nombre des demandes retirées et, enfin, la moyenne des heures de travail que les juges ont consacrées pour apprécier ces demandes.

Pour *droitsfondamentaux.ch*, *les Verts*, les *JDS* et la *SPF*, la réglementation proposée est contraire à la séparation des pouvoirs. Le Tribunal fédéral est l'instance des voies de droit du Tribunal administratif fédéral et non pas le Conseil fédéral. Par ailleurs, pour des mesures de recherche d'informations soumise à autorisation à l'encontre d'une organisation, d'un tiers ou d'un groupement de personnes figurant dans la liste d'observation, le Conseil fédéral serait alors tant le mandant que l'organe donnant son aval. On risque aussi qu'un juge – admettant que le Conseil fédéral examine très soigneusement les demandes de mesures avant de les soumettre –, les autorisera toutes d'emblée et vice-versa. En tout cas, la réglementation prévue en la matière n'offre aucune protection efficace contre des autorisations disproportionnées de telles mesures.

D'une manière générale, il faudrait mettre la barrière plus haute pour les mesures de recherche d'informations soumises à autorisation demandées par le SRC qui ne suscitent aucun soupçon que pour des mesures comparables d'après le code de procédure pénale: l'art. 197, al. 3, CPP dispose que les mesures de contrainte qui portent atteinte aux droits fondamentaux des personnes qui n'ont pas le statut de prévenu sont appliquées avec une retenue particulière. *droitsfondamentaux.ch*, *les Verts*, les JDS et la *SPF* proposent une réglementation analogue au triage procédé par les juges de documents mis sous scellés de personnes qui sont soumises à un secret professionnel. De fait, seules devraient être remises au SRC des données en rapport avec le but de la mesure ayant fait l'objet d'une demande d'autorisation.

Article 25

Alinéa 1:

Lettre d:

NE souhaite que le SRC soit discret dans la dénomination d'autres services pour ne pas exposer par exemple des groupes d'observation ou des commandos d'intervention.

Etant donné que ni le texte de loi ni les commentaires ne donnent des précisions à propos des obligations des cantons relatives à l'ampleur des mesures de recherche d'informations soumises à autorisation, *SO* et *TG* souhaitent que l'on éclaircisse ici si ces mesures de recherche d'informations soumises à autorisation ne seront par principe mises en œuvre que par le SRC ou si elles pourront aussi être accomplies par les autorités d'exécution cantonales. *SO* est en effet tout à fait ouvert à une telle possibilité, mais il estime qu'une indemnisation supplémentaire pour des mesures de recherche d'informations particulièrement coûteuses se justifiera alors. *TG* souhaite obtenir une précision pour savoir si, par principe, seul le SRC exécutera des mesures de recherche d'informations soumises à autorisation (car sinon, il conviendra que la Confédération fournisse une compensation financière aux cantons.).

Le *PPS* souhaite qu'un service indépendant se charge de la représentation de la personne concernée dans la procédure.

Article 27

Le *CCCZH* croit que le SRC pourrait dans tous les cas fouiner de son propre chef dans la sphère privée de personnes grâce à la réglementation sur l'urgence et se procurer ainsi des données pouvant fonder d'autres soupçons encore. L'obtention après coup de l'autorisation est tout à fait inutile puisque le SRC se serait alors déjà emparé des informations et que le Conseil fédéral ne pourrait pas contrôler si les données obtenues de manière illégale ne seraient pas, en fin de compte, quand même enregistrées dans des registres non-officiels.

Article 28

Alinéa 2:

PP2 fait remarquer que les données obtenues dans le contexte de la procédure d'urgence ne devraient pas seulement être détruites mais ne pourraient pas non plus être utilisées à défaut d'autorisation après coup.

Article 29

Alinéa 2:

L'*UDC* salue le principe de l'obligation d'informer prévue dans le projet de loi, mais souhaite apporter un amendement à la lettre d du deuxième alinéa en ce sens que le chef du DDPS

devrait avoir la possibilité de déroger à l'obligation d'informer aussi lorsque la personne concernée n'a pas d'intérêt à une telle communication.

Le *PPS* s'oppose à cet article et souhaite biffer l'al. 2, parce que d'un point de vue constitutionnel, il n'y a aucune raison de ne pas informer les personnes surveillées dans le cadre d'une telle procédure.

Le *CCCZH* pense que cet article n'a pas le moindre sens, étant donné qu'au cas où le SRC aurait fait fausse route dans sa surveillance, il pourrait toujours faire valoir des motifs en vertu du deuxième alinéa pour ne pas informer la personne concernée.

La *DigGes* pense que le sens de cet article est presque complètement sapé vu les nombreuses exceptions qui y figurent, mais elle considère en revanche que les lettres a et d sont, elles, légitimes. Quant à la lettre b, elle la considère cependant comme inquiétante, étant donné qu'une procédure ordinaire ne pourrait être menacée que si la constatation de faits repose sur une enquête illégale.

L'al. 2 prive la personne concernée de tout droit à se défendre. Voilà pourquoi, selon *droits-fondamentaux.ch*, *Les Verts*, les *JDS* et la *SPF*, il faut explicitement mentionner que les éléments découverts lors de mesures de recherche d'informations soumises à autorisation ne pourront absolument pas être exploitées en procédure pénale, puisque la révélation de ces faits a été obtenue alors que l'on n'était en présence d'aucune suspicion.

PP2 déclare que le devoir d'information devrait être la règle et que le législateur devrait préciser qu'il pourrait exceptionnellement être différé. Par ailleurs, l'information devrait mentionner la faculté d'être soumise à une vérification judiciaire quant à la légitimité de la surveillance. Cette communication devrait également indiquer les voies de recours.

Article 30

Le *CCCZH* demande de faire cesser la libre distribution d'informations relevant du renseignement étant donné que les fichiers seraient sinon soustraits à tout contrôle.

Complétant cette demande, *PP1* propose de prévoir que Confédération réponde des préjudices occasionnés aux tiers, causés par des particuliers agissant au nom du SRC, lorsque ces derniers auraient enfreint les dispositions du SRC ou qu'ils auraient agi de manière contraire à leur obligation de diligence.

Alinéa 2:

BS et la *privatim* peuvent certes comprendre que le SRC doit avoir recours au savoir-faire technique de particuliers dans certaines circonstances, mais ils estiment qu'une telle externalisation recèle un risque accru de violer des droits fondamentaux de la personne, puisque le maniement des données personnelles en question est grandement soustrait au contrôle du SRC. Même si l'al. 2 tient compte de cette problématique, *BS* et la *privatim* recommandent de régler contractuellement avec les personnes mandatées les points tels que l'obligation de garder le secret, les droits de contrôles exercés par le SRC et le PFPDT sur l'utilisation des données, l'interdiction d'exploiter ces données à d'autres fins, les mesures prises pour assurer la sécurité des informations et les sanctions prévues en cas d'infraction.

Le *pvl* suggère que le SRC ait recours à des particuliers avec une extrême réserve dans le domaine de la sûreté intérieure. Comme il s'agit d'un domaine très sensible ayant un impact sur les droits fondamentaux de la personne, il convient de supprimer cet al. 2.

Le *PPS* demande que cet alinéa soit supprimé, sinon le SRC finirait par perdre son savoir-faire et serait alors tributaire pour toujours de prestataires privés.

Article 31

GE qualifie la protection des sources comme étant un élément indispensable.

Alinéa 1:

Pour le *PS*, l'exception ancrée à l'al. 1 a un libellé beaucoup trop étroit, étant donné qu'il peut s'écouler des décennies avant qu'un jugement passe en force. Il propose dès lors de modifier la dernière phrase de l'al. 1 en lui donnant l'extension suivante:

¹ *[...] Les personnes dont une procédure a été engagée pour crimes contre l'humanité ne bénéficient d'aucune protection.*

Alinéa 2:

AG qualifie de positif le fait que le SRC pourra, sous certaines conditions, divulguer l'identité d'un informateur domicilié en Suisse aux autorités de poursuite pénales suisses en vue d'élucider des délits.

ZG demande à ce propos que la notion de « l'infraction grave » soit mieux définie (voir dans ce contexte les expériences faites dans cette problématique dans le cas du « poseur de bombe du Grütli »).

Le *PPS* trouve qu'il est extrêmement hardi de disposer dans un article consacré à la protection des sources que ces dernières peuvent être transmises aux autorités de poursuites pénales. Par conséquent, l'al. 2 doit être supprimé, étant donné que le SRC pourrait alors exercer un chantage sur les informateurs.

PP1 propose de lever la protection des sources aussi pour les personnes poursuivies, recherchées ou condamnées par une Cour pénale internationale pour grave crime contre l'humanité.

De l'avis de *PP2*, l'identité devrait également être révélée lorsqu'elle s'avère nécessaire pour l'instruction d'une procédure pénale.

Alinéa 4:

Les déclarations du *TAF* relatives à l'article 19 s'appliquent ici aussi. Il serait donc cohérent d'adapter les dispositions de l'art. 36a LCA, étant donné qu'elles devraient aussi couvrir ce genre de litiges.

Article 32 ss

Selon *PP2*, rien ne justifie le fait que les ressortissants suisses à l'étranger ne devraient pas bénéficier de la même protection. En matière de recherche d'informations, les dispositions de la section 4 devraient s'appliquer autant à l'intérieur du pays qu'à l'étranger lorsqu'il s'agit de surveiller des ressortissants suisses hors de nos frontières. Par ailleurs, s'agissant de l'exploration du réseau câblé, il conviendrait d'en faire exception lorsque des émetteurs ou des récepteurs se trouvent en Suisse et lorsqu'elle vise des ressortissants résidant à l'étranger. Dans ces cas-là également, il conviendrait d'appliquer les dispositions de la section 4.

Article 32

FR approuve l'application de ces mesures, mais souhaite néanmoins mettre en évidence qu'elles devraient mieux être délimitées et précisées que maintenant.

Le *PLR* est d'accord que le législateur renonce ici à une procédure d'autorisation et qu'il se restreigne à la place à une documentation. Une vérification judiciaire et un contrôle politique seraient certes souhaitables, mais d'une part, la première serait sans effet (et pourrait d'ailleurs être interprétée comme une violation de la souveraineté) et, d'autre part, elle représenterait pour le juge qui donnerait cette autorisation une responsabilité politique, juridique et diplomatique disproportionnée.

La *DigGes* rappelle que la validité des droits de l'homme et, partant, la protection du droit fondamental de la personne ne prend pas fin à nos frontières. Les difficultés accrues – du reste incontestables – dans les missions à l'étranger ne devraient pas conduire à ce que l'on se préoccupe moins de la protection des droits fondamentaux. Si un juge ne peut pas préalablement examiner le cas, cette recherche d'informations devait pour le moins être appréciée par un juge après coup.

L'*USAM* demande qu'il soit précisé expressis verbis dans la loi que les données sur des faits survenant à l'étranger et celles sur ceux survenant en Suisse ne seront pas reliées entre-elles.

Alinéa 2:

Le *PPS* demande la suppression de l'exception prévue à l'art. 22, al.1, let. g, étant donné que le fait de s'introduire dans les réseaux d'ordinateurs dans d'autres Etats pourrait être interprété à juste titre comme un acte de guerre.

La *DigGes* veut que le législateur dispose clairement que le SRC ne peut aucunement procéder à des attaques telles qu'elles sont prévues à l'art. 22, al. 1, let. g, du projet de loi, étant donné qu'à l'étranger, cet acte serait interprété comme un acte de guerre cybernétique et que cela pourrait conduire à une aggravation de la situation.

Le *CCCZH* voit dans les dispositions contenue à l'al. 2, une profession de foi du SRC en faveur d'une guerre cybernétique et d'un « piratage » (hacking) pratiqué sans autorisation par notre Etat. Le législateur ne doit pas conférer de telles compétences au SRC.

PP1 comprend certes que les dispositions de l'art. 22, al. 1, let. g ne peuvent pas être soumises à une procédure d'autorisation qui n'aurait aucun effet à l'étranger. Cependant, vu le paysage informatique d'actualité (que l'on songe par exemple à l'existence du « cloud computing »), il conviendrait d'examiner quand un système d'ordinateurs (et on entend ici sans aucun doute un « serveur ») ou un réseau informatique se trouve en Suisse et quand il se trouve à l'étranger. Il faut aussi partir de l'idée que le trafic de courriels entre des partenaires communiquant en Suisse se déroule par des réseaux et que ceux-ci sont en partie hébergés à l'étranger.

Alinéa 3:

Pour le *PS*, il est décisif que l'essence des droits fondamentaux des personnes concernées soit respectée lorsque le SRC procède à des recherches d'informations à l'étranger.

Alinéa 4:

Le *PS* souhaite que les activités relatives à la recherche d'informations soient parfaitement documentées à l'attention des organes de contrôle et de surveillance.

Alnt salue le fait que les activités du SRC exercées à l'étranger trouvent leurs voies dans la loi. Ce nonobstant, les raisons que le rapport sur l'avant-projet mentionne au sujet de l'exception de l'obligation d'autorisation, de la communication après coup et de la protection du droit ne se justifient pas pour autant. Et ce à plus forte raison qu'il manque une réglementation précisant quand le SRC doit pouvoir agir à l'étranger.

Laisser l'examen des normes de proportionnalité à l'appréciation du SRC se révélerait à coup sûr toujours en faveur des intérêts sécuritaires de notre pays et ne répond dès lors pas au respect des droits fondamentaux des personnes concernées.

Alnt se dit préoccupée du fait que la Suisse, de par ce projet de loi, n'a pas l'intention de se conformer aux règles du droit lorsqu'il s'agit d'agir à l'étranger. Cette organisation demande par conséquent une solution conforme aux droits fondamentaux pour toute activité du SRC à l'étranger. Le projet de loi contrevient aux obligations convenues par le droit international.

Article 33

La SSO et l'ASOR demandent pour l'exploration radio un propre titre de section (étant donné qu'elle est sur un pied d'égalité avec l'exploration du réseau câblé).

Pour le CCCZH, cet article n'a pas la moindre légitimité parce qu'il menace les relations que notre pays entretient avec l'étranger et que le SRC n'a de toute manière rien à faire à l'étranger.

Alinéa 1:

Le PPS se demande comment le SRC va faire la distinction entre des signaux provenant de l'étranger et ceux provenant du pays.

Alinéa 3:

Le PPS souhaite que le législateur détermine les délais dans la loi.

Alinéa 6:

Pour le CCCZH, la formulation « le plus rapidement possible » à cet alinéa est beaucoup trop vague.

Section 7: Exploration du réseau câblé (Art. 34 à 38):

La SSO et l'ASOR saluent le fait que la loi régisse l'exploration du réseau câblé et que celle-ci soit soumise aux règles de la procédure d'autorisation pour les mesures de recherche d'informations soumises à autorisation. Ce faisant, il sera possible d'exclure d'emblée une recherche d'informations pouvant échapper à tout contrôle, tel que cela pourrait se produire à l'étranger.

L'UDC est d'avis que sur le plan international, l'exploration du réseau câblé gagnera en importance et ce parti fait remarquer qu'il conviendrait, du point de vue terminologique, technique et administratif, de coordonner les termes utilisés dans la LRens avec les dispositions révisées de la LSCPT.

Le PPS critique le fait que le projet de loi n'aborde pas le sujet des droits fondamentaux et il craint que l'on se trouve soudain devant une montagne de données dont l'analyse pourrait prendre des années et coûter une fortune sans pour autant apporter une quelconque utilité.

Le pvl rejette tout au moins une surveillance globale des flux de données provenant des réseaux câblés de télécommunications internationales.

Droitsfondamentaux.ch, *Les Verts*, les *JDS* et la *SPF* rejettent purement et simplement l'exploration du réseau câblé, notamment parce qu'ainsi, on violerait le secret des télécommunications qui protège de manière illimitée les usagers de télécommunications.

La *DigGes* rejette par principe l'exploration du réseau câblé vu qu'elle n'apporte aucune utilité prévisible, que la protection des droits fondamentaux de personnes se trouvant à l'étranger n'est pas assurée et que cette exploration pourrait nuire à la renommée de notre pays. La *DigGes* souhaite par ailleurs l'introduction de réglementations relatives à l'information de la population au sujet de l'ampleur des mesures qui seront prises ainsi que la création d'une instance de contrôle analogue à celle prévue en matière d'exploration radio.

Pour le *CCCZH*, les articles concernant l'exploration du réseau câblé sont une sottise (« PRISM schweizerischer Prägung ») et doivent par conséquent être supprimés.

L'*asut* rejette les nouvelles dispositions relatives à l'exploration du réseau câblé, étant donné que ces dernières ne sont pas encore assez élaborées.

L'*asut* s'étonne que le législateur prévoie de créer une base légale pour une vaste mesure de surveillance alors que l'on ne sait pas grand-chose à propos de sa réalisation technique ou organisationnelle, ses charges, sa proportionnalité, son ampleur, son utilité ou son efficacité. Par ailleurs, l'*asut* ne voit pas très clairement comment les consignes légales en la matière devraient pouvoir être mises en œuvre (et en particulier comment en explorant le réseau câblé, il ne sera guère possible d'empêcher la saisie et l'enregistrement de signaux purement indigènes ainsi que des données personnelles).

Tant l'*asut* que *Swisscom* considèrent pour ces motifs qu'il est absolument indispensable d'effectuer préalablement une analyse coût-utilité ainsi qu'une analyse approfondie de la faisabilité, pour ensuite, en se fondant sur ces analyses, formuler dans les dispositions légales un libellé précis dans le domaine de l'exploration des réseaux câblés.

Les Verts, le *plv*, l'*UDC*, mais aussi *droitsfondamentaux.ch*, les *JDS* et la *SPF* sont également d'avis qu'il convient encore d'éclaircir de nombreuses questions avant de créer une base légale. Dès lors, le Conseil fédéral est invité à démontrer clairement dans son message les objectifs, l'utilité, la méthodologie, l'ampleur prévisible de ces mesures, les ressources nécessaires en personnel, la faisabilité technique et les coûts que générera l'exploration du réseau câblé. D'ailleurs, même la valeur ajoutée du renseignement est encore floue à ce sujet.

Article 34

Alinéa 4:

Lettre c:

Le *PPS* voudrait que le législateur fixe les délais dans la loi.

Article 35

Le *plv* salue l'obligation d'obtenir une autorisation.

Article 36

Le *TAF* souhaite que le législateur précise les dispositions relatives à la procédure d'autorisation en indiquant si, pour les délais impartis, il s'agit de jours ouvrables ou de jours civils.

Article 37

Alinéa 3:

Si des données de personnes habitant en Suisse sont saisies ou exploitées et qu'elles concernent la personne elle-même, *DigGes* souhaite compléter la réglementation ordonnant une obligation d'informer ce cercle de personnes également.

Article 38

Alinéa 4:

L'*asut* fait remarquer que l'expérience a démontré que ce genre d'investigations génère des coûts élevés chez les fournisseurs de services de télécommunications, à plus forte raison que des surveillances axées sur des lignes téléphoniques doivent être aménagées de manière beaucoup plus compliquées que l'exploration radio pratiquée aujourd'hui et mentionnée à plusieurs reprises dans le rapport sur l'avant-projet. Les fournisseurs de services de télécommunications devraient donc être indemnisés pleinement pour tous les frais encourus et non pas seulement pour la fourniture de signaux au service exécutant la mesure.

La *Swico* doute fort que les indemnités allouées par la Confédération puissent un tant soit peu couvrir les frais encourus.

Le *PPS* demande que le SRC prenne en charge la totalité des coûts de la mesure sollicitée et qu'il publie également chaque année un rapport sur le budget consacré à cette tâche.

droitsfondamentaux.ch, *Les Verts*, les *JDS* et la *SPF* sont, eux aussi, préoccupés par les énormes coûts que ces mesures engendreront chez les fournisseurs de services de télécommunications et l'indemnisation tout à fait insuffisante à leur égard.

Chapitre 4 Traitement des données et archivage (art. 39 à 59)

L'*UDC* considère que le système prévu est ingénieux et lui donne son aval.

La *Swico* demande de créer un article distinct sur l'enregistrement des données et qui comprenne également une norme obligatoire quant à la durée de l'enregistrement. La *Swico* déclare faire cette proposition parce que toutes les autres dispositions prévues (notamment à l'art. 40, al. 4, à l'art. 52 voire 59) ne contribuent aucunement à clarifier la durée effectivement autorisée de l'enregistrement.

Le *CCCZH* déclare au sujet de ce chapitre que les droits d'accès à ces systèmes sont définis de manière contradictoire à plusieurs endroits (par exemple, à l'article 42, al. 2, let. b). Le législateur doit inscrire les délais de conservation des données dans la loi.

Article 39

Alinéa 1:

AR et *VD* pensent que le libellé de cet alinéa est formulé de manière trop vague et qu'il conviendrait de préciser la catégorie des données ainsi que le but du traitement de ces données au moins au niveau de l'ordonnance.

Pour répondre au critère de la densité normative (s'agissant des processus pour le traitement des données présentant un potentiel de mise en danger comme le sont les systèmes d'information du SRC, cette densité normative est particulièrement élevée), cette

disposition doit faire l'objet d'une concrétisation de toute urgence. Le *PS* propose de tenir bon à l'exigence mentionnée à l'art. 42, al. 2 :

Art. 42, al. 2abis (nouveau)

abis Le Conseil fédéral règle les catégories des données personnelles et profils de la personnalité particulièrement dignes d'être protégés.

Cela étant, le *PS* s'attend à ce que, dans ses dispositions d'exécution, le Conseil fédéral:

- limite les droits des collaborateurs du SRC spécialement chargés de traiter les données contenues dans les différents systèmes d'information;
- limite l'accès en consultation de données inter-systèmes aux seuls collaborateurs du SRC disposant des droits d'accès aux systèmes d'information ad hoc (tout en partant de l'idée qu'il s'agit ici d'un nombre restreint de collaborateurs, sinon il y aura lieu de le préciser dans ladite disposition);
- limite la procédure d'accès en ligne quant au contenu de l'indexation et à des autorités clairement désignées de police, de justice et de la protection de l'Etat.

De l'avis du *PS*, tous ces critères devront être annoncés sans ambages dans le message explicatif du Conseil fédéral.

Alinéa 2:

BS, le *PS* et la *privatim* considèrent cette disposition comme problématique étant donné que le principe fondamental du droit à la protection des données dispose que seules les données correctes peuvent être traitées. Or, d'après les commentaires que fournit le Conseil fédéral, il s'avère qu'il s'agit de désinformation et d'informations erronées.

AR, *BL*, *BS*, *VD* le *PS* et la *privatim* recommandent dès lors l'adaptation suivante:

² *Le SRC peut continuer de traiter des données qui s'avèrent être des désinformations ou des informations erronées, lorsque ce traitement est nécessaire à l'appréciation de la situation ou à l'évaluation d'une source. Il marque ces données comme inexactes.*

Le *PPS* considère qu'il se pose surtout un problème lorsque des données inexactes pourraient aussi être partagées avec des partenaires étrangers et qu'elles pourraient, de ce fait, figurer aussi dans d'autres banques de données.

Le *CCCZH* exige que les données inexactes soient purement et simplement supprimées.

Aux dires de *droitsfondamentaux.ch*, *Les Verts*, les *JDS*, la *SPF* et l'*USAM*, il convient bien entendu de supprimer immédiatement les données inexactes. Si nécessaire, les renseignements obtenus au sujet de la désinformation et les fausses informations pourraient être saisis dans une nouvelle annonce exempte de toute erreur.

Alinéa 3:

droitsfondamentaux.ch, *Les Verts*, les *JDS*, la *SPF* et l'*USAM*, font valoir que le principe conformément à ces dispositions, selon lequel le SRC peut verser ces données dans plusieurs systèmes d'information, est complètement dépourvu de sérieux à plus forte raison qu'il est déclaré qu'avec le transfert, les consignes s'appliqueraient alors à chaque nouveau système d'information. On se retrouverait ainsi dans un contexte que l'on pourrait appeler « une gestion de données chaotiques ou une gestion chaotique de données ». En copiant des données dans un autre système d'information, les attributs de ces informations, tels que les délais pour les révisions périodiques ou la durée de conservation maximale de ces données changeraient. Du reste, dès que la même information existe plusieurs fois, cette information se modifie différemment en fonction des mutations opérées, mais de toute façon, tôt ou tard, on se retrouverait forcément devant une banque de données inconsistantes.

Article 40

AG et VD saluent la mesure prévoyant d'améliorer la vérification périodique de données par le biais du contrôle de qualité.

La *SPD-TG* regrette que le législateur ait abandonné le principe adopté jusqu'à ce jour selon lequel les données relatives à la sûreté intérieure devaient être pertinentes et correctes, principe abandonné à cause de la fusion des données sur la sûreté intérieure avec celles sur la sécurité extérieure dans le nouveau système SAI SRC. Cette nouvelle disposition ne ferait au fond que fixer que le SRC puisse apprécier lui-même la pertinence et l'exactitude des données. A l'égard de l'article 39, al. 2, sensible à l'égard de la politique en matière de droit et du point de vue de la protection des données, la *SPD-TG* recommande que le législateur ordonne que ne puissent être continuées à être traitées dans les nouvelles banques de données regroupées que les données pertinentes et exactes concernant des personnes ayant un lien avec la Suisse et que ces données doivent être supprimées au cas où elles ne répondraient pas à ces deux critères.

Le *CCCZH* reproche que le contrôle de qualité ne soit pas une compétence cruciale du SRC et considère donc ce fait comme problématique.

droitsfondamentaux.ch, *Les Verts*, les *JDS* et la *SPF* estiment quant à eux qu'il n'y pas lieu de se lancer dans une discussion au sujet du contrôle de qualité tant que l'on sera en présence d'une banque de données aussi inconsistante.

Alinéa 3:

Etant donné qu'au sujet de ces données renvoyées, il s'agira sans doute de données transmises en amont par les cantons qui devraient continuer d'être densifiées, il serait alors judicieux d'autoriser les autorités d'exécution cantonales à l'alinéa 3 de continuer de traiter les données renvoyées à leur expéditeur et de pouvoir les archiver dans la banque de données intermédiaires du SRC (*CCPCS*, *AR*, *BE*, *SZ*, *TG*, *ZG*).

Alinéa 4:

Selon *PP2*, s'agissant de la vérification périodique, il convient de fixer un délai pour savoir si les données sont encore nécessaires à l'accomplissement des tâches du SRC. En outre, le législateur devrait prévoir un effacement automatique des données si, à l'expiration du délai imparti, le service compétent n'avait pas encore confirmé qu'il avait encore besoin de ces données.

Alinéa 5:

BS et *TI* saluent la volonté d'ancrer un contrôle de qualité interne dans la loi.

Le *PS* salue expressément le fait que le projet *LRens* inscrive le contrôle de qualité dans ses dispositions, contrôle de qualité introduit avec succès dans divers domaines partiels déjà. Mais le *PS* veut aller plus loin en demandant que soient prévues des règles plus détaillées. A son avis, il ne suffit pas d'introduire un contrôle de qualité qui ne se contente que de vérifier la pertinence et l'exactitude des données personnelles; ici, aussi, selon le *PS*, il convient d'aller plus loin :

Alinéa 5

⁵ *Le service interne de contrôle de la qualité du SRC assume les tâches suivantes:*

- a. *il vérifie la pertinence et l'exactitude des données personnelles saisies dans le système SAI-EXTR SRC (art. 45). Il vérifie le contenu des enregistrements, notamment les indications au sujet des sources, l'appréciation de l'information et la date de l'appréciation globale suivante, puis il confirme la saisie définitive des données. Ce*

n'est que lorsque cette confirmation a été donnée que de nouvelles informations sur la même personne peuvent être saisies;

Le projet LRens devrait être complété de manière explicite pour éliminer les saisies à double :

Alinéa 5

b_{bis} (nouveau) Il vérifie périodiquement toutes les saisies multiples à l'égard de leur utilité.

Article 41

AR, BE, GL, GR, SO, SZ, TG, UR, ZG, ZH et le *CCPCS* expriment leur satisfaction au sujet du fait que les autorités d'exécution cantonales ne pourront plus constituer de propres banques de données en application de la LRens.

Cette disposition déclare d'une part, clairement au sujet des données traitées par les services d'exécution sur mandat de la Confédération qu'il s'agit de données de la Confédération (ce qui crée enfin la clarté souhaitée depuis si longtemps quant à la compétence relative au contrôle de la protection des données auprès des autorités d'exécution cantonales – PFPDT –). D'autre part, le législateur augmente sans conteste la sécurité des données dans le domaine du renseignement.

Les cantons demandent également que des données en amont puissent continuer d'être saisies et dépouillées à bas seuil par les autorités d'exécution cantonales, car on perdrait sinon de précieuses informations pour évaluer la situation et que de ce fait, on pourrait restreindre l'activité opérationnelle des autorités d'exécution cantonales dans ce domaine (domaines qui concerneraient précisément la souveraineté de la Confédération et des cantons). Par ailleurs, il convient de faire en sorte que les autorités d'exécution cantonales puissent s'échanger mutuellement leurs données en amont.

GE regrette que le législateur interdise dorénavant aux cantons de gérer leurs propres banques de données.

VD considère que la disposition relative aux données de la Confédération est très floue et souhaite que le législateur la précise.

La *privatim* ainsi que *BS* et *GR* déclarent que les autorités cantonales ne peuvent pas être considérées comme organes de la Confédération au sens des dispositions de l'art. 2, al.1, let. b, en corrélation avec l'art. 3, let. h, LPD, lorsqu'elles traitent des « données fédérales » à la demande du SRC. Les cantons répondent quant à la forme au droit relatif à la protection des données de leur juridiction. Quant aux normes relatives à la protection des données quant au fond, elles se trouveraient dans la LRens que les autorités d'exécution cantonales doivent appliquer. Voilà pourquoi il convient encore de compléter comme suit l'art. 41 LRens:

« Le traitement d'informations conformément à la présente loi est assujéti au droit sur la protection des données de la Confédération et des cantons ».

BE trouve qu'il serait approprié que la Confédération réponde des actes des organes cantonaux agissant au nom du SRC et pense qu'il serait judicieux d'y apporter la clarté nécessaire en fournissant ici - ou alors plus loin à l'art. 69 - une précision adéquate dans cette disposition légale.

NE se demande comment régler la conservation de données intermédiaires qui ne sont pas encore prêtes pour être intégrées dans la banque de données de la Confédération.

Article 42

La CCPCS, AR, BE, GR, JU, NE, SO, SZ, TG, ZG et ZH demandent un réexamen de principe de la réglementation des droits d'accès des autorités d'exécution cantonales aux systèmes d'information.

Pour GE, il est indispensable d'énumérer tous les systèmes d'information distincts dans la loi afin de garantir la transparence quant à la protection des données et quant à la protection de la sphère privée. GE fait toutefois remarquer que de tels systèmes sont soumis par l'ordre des choses à une évolution technique rapide. Pour pouvoir suivre cette évolution, il convient d'introduire une disposition qui permette au Conseil fédéral de tenir et d'adapter une liste jusqu'à la prochaine révision ordinaire sur la voie de l'ordonnance.

La DigGes pense qu'avec l'architecture proposée comprenant un tel nombre de systèmes d'information, le chaos est programmé d'avance. En effet les données ne sont pas toujours consistantes et « survivront » que trop fréquemment au moment où le législateur aurait pourtant ordonné qu'elles fussent effacées. La seule solution pour y remédier consistera sans doute à restreindre d'emblée massivement la quantité de données qui devraient être obtenues en comparaison avec celles d'aujourd'hui, puis d'introduire un service central chargé de gérer ces données. Les fichiers spécifiques pour les domaines d'application de la loi ne devraient pas contenir des copies de données, mais des références sur les inscriptions figurant dans le système d'information central. Le service central chargé de gérer les données devrait être également responsable de la suppression de données comme l'exige la loi. Par ailleurs, il devrait être « l'antenne responsable » pour assurer le contact avec la population au sujet de l'exercice des droits de la protection des données. Le service central chargé de la gestion des données ne remplace pas le service du contrôle de qualité.

Référendum LMSI rejette la fusion des données provenant de la Suisse et celles provenant de l'étranger dans une seule et même banque de données.

De l'avis de la SSO et de l'ASOR, il conviendrait de définir les systèmes d'information figurant dans la LRens sous une forme abstraite. Ce faisant, il y aurait alors lieu de subdiviser ces systèmes en fonction de leur utilité, des informations qui y sont enregistrées et traitées. Les données devraient également être classées selon leur mérite à être protégées et selon les mesures à prendre pour les protéger, mais aussi en fonction du cercle de personnes qui y ont accès à plusieurs niveaux puis de codifier tout cela dans la loi. En revanche, l'attribution des systèmes d'information actuels aux niveaux formulés de manière générale et abstraite devrait être réglée à l'échelon de l'ordonnance.

Alinéa 1:

Aux yeux du PBD, les noms des systèmes d'informatique devraient tout au plus figurer dans une annexe et non pas dans la loi, car ces systèmes devront s'adapter à l'évolution technologique et changer un jour.

Alinéa 2:

Pour le PS, il est décisif que l'exigence de la densité normative élevée s'applique également aux dispositions de l'ordonnance à concrétiser. Il importe donc beaucoup que le contenu des divers systèmes, le cercle d'utilisateurs et la durée de conservation des données soient réglés soigneusement, à telle enseigne que le principe de la légalité soit observé également dans le cadre de la délégation. Le PS propose dès lors la précision suivante:

2 Le Conseil fédéral règle chaque système d'information du SRC au niveau de l'ordonnance.

Article 43

Le CCCZH déclare que le SRC a l'impudence de se servir du système de stockage des données résiduelles pour tenter de faire l'impasse sur les autres données sensibles qu'il compte mémoriser.

Article 46

UR salue la solution retenue de se servir de l'INDEX SRC en vue de coordonner les données de la Confédération et des cantons et comme plateforme pour le traitement des données à l'échelon cantonal.

BE, GR et SZ font remarquer que les autorités d'exécution cantonales devraient avoir un droit de regard mutuel dans leurs données et dossiers en amont afin d'appréhender le mieux possible les tâches qui leur sont dévolues. Le rapport relatif à l'avant-projet devrait donc être complété dans ce sens.

Article 48

Le CCCZH pense qu'il est absurde de laisser un accès à des particuliers ou à des services étrangers à des données relevant du renseignement, étant donné que ces données échappent alors à toute base légale et que leur destinée ne peut plus être contrôlée.

Article 49

La CCPCS, AR, BE, GR, JU, NE, SO, SZ, TG, ZG et ZH partagent unanimement l'avis qu'il convient que les autorités d'exécution cantonale aient accès au portail ROSO. Comme il s'agit ici de données accessibles d'une manière générale, il devrait s'avérer qu'un tel droit d'accès ne présente pas d'obstacles. Dans le cas contraire, on courrait d'ailleurs le risque de saisies à double.

Cette banque de données est la seule que le CCCZH considère comme légitime, étant donné que ce sont les personnes concernées qui ont mis ces informations à disposition dans la sphère publique. C'est pourquoi il convient de compléter les dispositions en ce sens que le grand public ait accès à cette banque de données. De cette manière, des tiers indépendants pourraient aussi, au sein d'une intelligence collective, se rendre compte des risques qu'encourt notre pays.

Article 50

La CCPCS, AR, BE, GE, JU, NE, TG et ZH pensent qu'il n'est pas judicieux d'exclure l'accès aux autorités d'exécution cantonales, à plus forte raison que les autorités d'exécution de Genève et de Zurich se chargent, sur mandat du SRC, de nombreuses investigations relatives à des personnes transitant par Cointrin ou Kloten. S'agissant de recherches effectuées dans leur propre aéroport, il serait tout de même peu judicieux que les collaborateurs cantonaux soient obligés de se renseigner d'abord plus avant auprès du SRC à Berne alors qu'ils ont justement obtenu préalablement un mandat de sa part.

Le PS estime que cet article mérite d'être éclairci, étant donné que le libellé figurant aux alinéas 1 et 2 ne contient aucune restriction. Aux termes de cet article, mêmes des citoyens intègres ainsi que des contrôles douaniers ne soulevant aucune difficulté pourraient, voire devraient faire l'objet d'un tel enregistrement dans le système. Pourtant, le rapport explique qu'il ne s'agit que de données d'entrées de certaines personnes provenant de certains pays et servant à des fins d'identification précoce d'espionnage et de prolifération. Certes, le 4^{ème}

alinéa de cet article précise que le Conseil fédéral détermine l'ampleur des contrôles douaniers et, partant, de ce système d'information, mais pour prévenir tout malentendu, le PS propose d'amender cet article déjà à l'alinéa 1 et ce de la manière suivante:

¹Le système Quattro P sert à identifier des personnes déterminées qui entrent en Suisse ou qui sortent du territoire suisse et à spécifier les dates de leur entrée et sortie.

Article 52

droitsfondamentaux.ch, Les Verts, les JDS et la SPF font observer que les données provenant de l'exploration du réseau câblé ne devraient pas figurer dans le système de stockage des données résiduelles, mais au contraire dans des systèmes de stockage de données protégés.

Article 53

Alinéa 1:

ZH trouve qu'il faut éclaircir où sont enregistrées des données qui ont été collectées à l'étranger grâce à une mesure soumise à autorisation, mais qui n'en sont pas licites pour autant.

Article 54

La *DigGest* se demande comment cette vérification pourrait bien être réalisée alors qu'elle ne fait pas partie des tâches du service du contrôle de qualité énumérées à l'art.40. D'ailleurs, la *DigGes* s'interroge s'il ne s'agit pas tout simplement d'un vœu pieux ou d'une « tromperie sur l'étiquette ».

Le *PPS* demande qu'avant la transmission de données un service indépendant vérifie les circonstances ainsi que la proportionnalité de cette mesure.

Article 55

AG trouve positif que le service de renseignement de la Confédération soit par principe obligé de soutenir les autorités de poursuite pénale en leur mettant ses renseignements à disposition

Le *PLR* n'accepte pas le data-mining et c'est pourquoi seules des données qui ont été obtenues dans le cadre d'une surveillance et qui ont été demandées au SRC seront transmises (par analogie aux découvertes fortuites de l'art. 278 CPP).

La *DigGes* tient à préciser que la transmission des données personnelles n'est admissible que lorsqu'on doit pouvoir éviter ainsi une menace imminente pour la sûreté intérieure ou extérieure selon l'art. 4, al. 1, let. a. Dans tout autre contexte, on serait en présence d'une violation des droits de l'homme. Par ailleurs, il convient de s'assurer que les autorités ne transmettent en aucun cas les informations obtenues à des entreprises privées.

droitsfondamentaux.ch, Les Verts, les JDS, la SPF et l'USAM sont d'avis que cette disposition contrevient au principe de séparation qui devrait exister entre le service de renseignement et les autorités de police. Les données provenant de mesures de recherche d'informations soumises à autorisation devraient être assujetties aux normes de l'interdiction d'exploitation prescrites à l'art. 277 CCP parce qu'elles proviennent de surveillance non autorisées du point de vue de la procédure pénale et qu'elles ont été obtenues sans qu'il y ait eu préalablement une suspicion (expédition de pêche d'informations).

PP1 est d'avis que le SRC ne doit être ni habilité ni obligé de transmettre de lui-même des informations sur des actes punissables découlant de ses activités de recherche aux autorités de poursuite pénale. Le législateur parle ici de découvertes fortuites au sens de l'art. 278 CCP (pas de droit de dénoncer en vertu de l'art. 301 CPP)

De fait, une transmission de données personnelles ne devrait par principe intervenir qu'à la demande des autorités de poursuite pénale (à l'exception toutefois de la transmission aux organes de police ou aux services de la sûreté pour déjouer une menace concrète au sens des dispositions de l'art. 17, al. 1). Dans cet esprit-là, PP1 propose une vérification, une adaptation et une règle différenciée des dispositions des art. 4, al. 2 et 55, al. 2 à 4.

Alinéa 1:

Le PS propose que les autorités que le Conseil fédéral doit déterminer soient mentionnées directement dans la LRens ou alors que l'on dispose que le Conseil fédéral détermine ces autorités dans une ordonnance. Cet alinéa devrait alors être modifié comme suit:

¹ ...Le Conseil fédéral détermine les autorités concernées dans une ordonnance.

Alinéa 2:

ZH et la CAPS ne voient pas très bien comment les constatations faites pourraient tenir debout en évoquant la protection des sources dans les procédures d'enquêtes et judiciaires.

Par le passé, le SRC a toujours refusé de transmettre des constatations en vue d'une poursuite pénale et pour empêcher de commettre un délit. Le lamentable et désastreux échec du renseignement allemand au sujet des cellules national-socialistes illustre bien en effet qu'il faut empêcher que les constatations du renseignement ne parviennent trop tard, voire jamais aux autorités de poursuite pénale et aux autorités pour empêcher une infraction ou maintenir l'ordre public. Le PS propose dès lors de préciser l'al. 2 comme suit:

² ... le SRC met immédiatement ces données à la disposition des autorités concernées de sa propre initiative en assurant la protection des sources.

Alinéa 3:

ZH et la CAPS souhaitent attirer l'attention sur le fait que les renseignements obtenus lors d'une surveillance d'ordinateur (sauf s'ils concernent des données de communication) ne peuvent pas être utilisés par les autorités de poursuite pénale, étant donné que le CPP ne connaît pas dans ce domaine de mesures comparables.

Ces informations ne peuvent être transmises qu'en respectant les normes de la proportionnalité qui, pour le PPS, ne sont données que si le délit tombe sous le coup de l'art. 4. En cas de doute, on ne devrait pas transmettre ces données.

Article 56

Le PPS renvoie aux observations qu'il a faites à propos de l'art. 10.

Le PS salue les dispositions prévues aux alinéas 1 et 3 et propose de compléter l'al. 2, let. a, comme l'a fait la LMSI, c'est-à-dire dans l'esprit d'un renfort en vue de permettre des poursuites pénales au-delà de nos frontières. Voici la proposition de modification:

a.... tel que prévenir ou élucider un crime ou un délit également punissable en Suisse;

Le CCCZH demande que le SRC ne soit pas autorisé à transmettre des données à l'étranger, étant donné que ces données seraient ensuite privées de tout fondement légal.

La DigGes veut que cette disposition se réfère à un article que le législateur devrait encore créer. De fait, ce nouvel article devrait régler ce qui suit: assurer que les données que le

SRC met à disposition des autorités étrangères soient utilisées par les autorités d'autres Etats seulement si elles répondent aussi aux normes légales de notre pays; assurer que le succès de la mise en œuvre de ce principe puisse être contrôlé par un organe indépendant; facultés des personnes concernées de pouvoir exercer leurs droits de protection des données sur le plan international; information des personnes concernées que leurs données ont été transmises à l'étranger; types de données qui peuvent être enregistrées dans des systèmes d'information internationaux et les conditions y relatives.

droitsfondamentaux.ch, Les Verts, les JDS, la SPF et l'USAM demandent qu'en cas de transmission de données, il conviendra de s'assurer dans tous les cas que les constatations découlant de mesures de recherches soumises à autorisation sont assujetties à l'interdiction d'être exploitées au sens des dispositions de l'art. 277 CPP.

Alinéa 2:

La *DigGes* demande la garantie que les constatations découlant de mesures de recherches soumises à autorisation ne pourront être utilisées que pour écarter d'éventuelles menaces de la sûreté intérieure et extérieure en vertu des dispositions de l'art. 4, al. 1, let. a, et, par conséquent, ne pourront pas être transmises à des Etats qui ne pourraient pas apporter cette garantie.

La *DigGes* fait les propositions suivantes:

Lettre a:

La Suisse ne peut pas contribuer à saper la constitutionnalité d'un Etat dans d'autres pays. C'est pourquoi il convient de supprimer purement et simplement cette disposition

Lettre b:

Cette disposition doit être complétée en ce sens que la transmission des informations doit être autorisée par un tribunal, si elle n'est pas indubitablement dans l'intérêt de la personne concernée.

Lettre e:

Cette disposition doit être complétée en ce sens qu'il devra s'agir ici seulement de pouvoir écarter des menaces de la sûreté intérieure et extérieure en vertu des dispositions de l'art. 4, al.1, let. a.

Alinéa 3:

PP2 demande qu'aucune donnée ne puisse être transmise si ces données ont pour origine une surveillance illégale.

Article 57

Pour le *CCCZH*, cet article est libellé de manière beaucoup trop générale qui permet de transmettre les données à n'importe quel autre service.

Le *PPS* demande que ce soit un service indépendant qui donne son autorisation et que la personne concernée ait été préalablement informée de ce fait.

Alinéa 2:

Lettre b:

La *DigGes* veut que ce texte soit complété de la manière suivante:

« Toute transmission d'informations allant au-delà de l'indication du nom, de l'adresse et des éléments d'adresse de la télécommunication, tels que numéro de téléphone, adresse du courriel, numéro d'IP d'une personne doit avoir été préalablement autorisée par un juge

lorsque cette transmission n'est pas indubitablement dans l'intérêt de la personne concernée. »

Il conviendra également de soumettre au juge en sus de la demande présentée par le SRC la réplique rédigée par un officiel indépendant.

Article 58

Le *PPS* demande la suppression de l'alinéa 7, étant donnée qu'à l'échéance d'un délai si long, seule une réponse standard et sans possibilité de recours devrait suivre. Par ailleurs, le principe de la transparence demandait une réponse au requérant dans les meilleurs délais possibles. Le volume de travail excessif qu'invoque le législateur à l'al. 8 ne devrait pas être une excuse, car cela ne devrait pas entrer en ligne de compte pour le requérant.

Pour le *CCCZH*, ce genre de droit d'être informé équivaldrait à une « déclaration de nullité » et c'est pour cela même qu'il convient de modifier cette disposition – en soi inacceptable.

Alnt fait remarquer que le droit à l'information se réfère justement aussi à des personnes non enregistrées, mais cette disposition restreindrait alors la portée de l'alinéa 2. Quant à l'al. 9, il convient de mettre en évidence qu'il a été formulé d'une manière très restrictive; dans d'autres cas encore, le droit à l'information pourrait être plus important que les intérêts à maintenir le secret à ce sujet. *Alnt* est aussi d'avis que le renversement du fardeau de la preuve à charge du requérant de l'information renforce encore davantage l'ingérence dans les droits fondamentaux d'une personne et recommande dès lors de s'inspirer ici du libellé tel qu'il ressort de l'art. 18, al. 9 LMSI en vigueur ou alors de trouver une autre formulation qui tiendra pleinement compte du droit à l'information des personnes.

La *DigGes* suggère de simplifier absolument la procédure d'information à la personne et de l'aménager de manière à ce qu'elle soit aisée pour le citoyen. Il convient toujours de répondre immédiatement et de manière détaillée à de telles demandes lorsqu'il ne plane aucune menace sur la sûreté intérieure et extérieure. Sinon ce devrait être le PFPDT que l'on devrait pouvoir invoquer en tant qu'instance indépendante.

Selon *droitsfondamentaux.ch*, *Les Verts*, les *JDS* et la *SPF*, le droit indirect à l'information de la personne s'est avéré inapte et être une pure tracasserie administrative, à telle enseigne que peu ou prou personne n'empruntera cette voie. Autant dire alors que dans les faits, le droit à l'information de la personne est inexistant. Le droit à l'information devrait enfin être aménagé selon les règles prescrites par la LPD. Sinon, il convient de supprimer purement et simplement la restriction énoncée à l'al. 8 selon laquelle une réponse est donnée autant qu'elle n'entraîne pas un volume de travail excessif

Article 59

Pour le *PS*, il est crucial que les données dont le service compétent n'a plus besoin ou qui sont destinées à être détruites ne soient pas supprimées, mais au contraire proposées aux Archives fédérales aux fins d'archivage. Savoir que des actes du service de renseignement sont certes secrets à l'heure qu'il est, mais qu'à l'expiration de quelques bonnes décennies, ces éléments jadis secrets pourraient être publiés par des milieux indépendants et, partant, être discutés, contribue à un agissement responsable de la part du service de renseignement.

Le *PS* suggère d'introduire une réglementation semblable à celle que l'on trouve dans le projet LFRC, art. 6I, al.1:

¹ *Le SRC propose les données et les dossiers devenus inutiles ou destinés à être détruits aux Archives fédérales aux fins d'archivage. Afin d'empêcher la destruction de données et de dossiers méritant d'être archivés, les Archives fédérales ont le droit de consulter périodiquement l'Index pour une telle vérification.*

Il est tout à fait évident qu'une fois ces données et ces dossiers archivés, le SRC ne pourra plus y avoir accès. Il convient dès lors de s'assurer par un nouvel alinéa que le SRC ne disposera pas d'un blanc-seing lui donnant accès à des données qui avaient certes été destinées à être détruites, puis avaient en fin de compte quand même été archivées.

^{1bis} *Si les Archives fédérales ont archivé des données et dossiers destinés à être détruits, elles veilleront à ce que ni le SRC ni toute autre autorité en relation avec lui n'y aient accès pendant le délai de protection.*

Si d'aventure, il était quand même indispensable d'y accéder dans un cas isolé pour sauvegarder un intérêt public prépondérant, il faudra alors qu'une responsabilité politique claire soit endossée. Voilà pourquoi une telle décision ne devrait être prise exclusivement que par le Conseil fédéral (ou alors tout au moins par le chef du DDPS) :

^{1ter} *Le Conseil fédéral peut, en vue de sauvegarder un intérêt public prépondérant ou pour protéger la vie ou l'intégrité corporelle de tiers, autoriser le SRC de consulter au cas par cas pendant le délai de protection les données personnelles qu'il a remises aux Archives fédérales aux fins d'archivage.*

L'obligation prévue à l'al.1 que toutes les données et dossiers du SRC provenant directement de services de sûreté étrangers soient détruits est, elle aussi, inacceptable. Le PS suggère dès lors de prévoir une règle analogue au projet de la LFRC, à l'al. 6I, al. 3 et 4:

^{1quater} *Les Archives fédérales (AFS) archivent les données et les dossiers du SRC qui proviennent directement de services de sûreté étrangers et qui résultent de l'activité de renseignement opérationnelle dans des locaux hautement sécurisés du SRC. Ces données et dossiers sont soumis à un délai de protection de 50 ans.*

^{1quinquies} *Il détruit les données et les dossiers que les Archives fédérales jugent sans valeur archivistique.*

Le CCCZH trouve absurde de disposer que des données sensibles devront être protégées pendant 50 ans. Ce faisant, on surveillerait ainsi des personnes quasiment pendant toute leur vie.

Alinéa 3:

Le PPS demande la suppression de cette disposition en faisant allusion au cas Tinner.

Article 60

Pour le PS, la nécessité d'instaurer une base légale pour que le SRC puisse fournir des prestations de services en faveur de tiers est une évidence. Les exemples donnés au sujet de cet alinéa 1 dans les commentaires coulent de source et méritent son soutien. Toutefois le rapport sur l'avant-projet reste muet sur le libellé de l'al. 2. De quels individus et de quelles corporations s'agit-il ici? Et dans quel cas et dans quel scénario les dispositions de l'al. 2 entreraient-elles en vigueur?

Le PS demande donc à ce propos soit de supprimer complètement l'al. 2 de l'art. 60, soit tout au moins de le compléter avec des critères restrictifs et de rendre plausible cette disposition dans le message du Conseil fédéral.

Le CCCZH soutient l'augmentation de la sécurité TI des systèmes d'ordinateurs du pays, mais ces services devaient être hébergés chez MELANI ou SCOCI et pas au SRC.

économiesuisse cite l'exemple de la crise que notre pays a connue avec la Libye pour illustrer un exemple s'appliquant au 2^e al. Dans ces cas de figure, il faudrait aussi pouvoir disposer des prestations de services proposées par le SRC lorsqu'aucun intérêt direct du renseignement n'est en jeu mais qu'il y a un intérêt public (y compris au niveau économique général). Il convient donc de supprimer la restriction émise à l'al. 2, respectivement d'étendre le champ d'application de cet alinéa.

L'*USAM* demande une liste exhaustive des prestations de services envisagées.

Article 61

Pour le *PLR*, la liste d'observation est un outil pertinent qui sert à la transparence.

droitsfondamentaux.ch, *Les Verts*, les *JDS* et la *SPF* demandent que les priorités thématiques et régionales spécifiées dans le mandat de base soient obligatoirement soumises à l'organe de contrôle parlementaire. Il en va de même de la liste de certains groupements qui doivent faire l'objet d'une telle observation, tout comme la liste d'observation tout court. De l'avis de ces partis précités, ces listes devraient également être soumises à la réserve d'un juge.

Alinéa 2:

Le *PPS* pense que le mandat politique de base du Conseil fédéral ainsi que la liste d'observation devaient être publiques. Le *PPS* demande de supprimer l'al. 2. La *DigGes*, elle aussi, est d'avis que la liste d'observation devrait être publique.

Le *CCCZH* considère que cette disposition constitue un risque pour le contrôle public du SRC. Ce dernier devrait s'accommoder de devoir traiter des demandes d'accès et des demandes de conciliation ainsi que de faire face à des procès.

Alinéa 3:

L'*UDC* et la *DigGes* ne veulent pas octroyer de compétences au Conseil fédéral pour qu'il puisse conclure seul de tels traités internationaux.

Article 62

Dans l'esprit d'une liberté d'action et d'une flexibilité, la *CAPS* est d'avis que l'on peut saluer le fait que le Conseil fédéral puisse charger le SRC de sauvegarder d'autres intérêts essentiels de la Suisse grâce à son appréciation et au-delà de son mandat ordinaire. Il peut d'ailleurs le faire parce que les exceptions en vertu de l'al. 2 devaient être restreintes.

L'*USAM* estime que ces dispositions sont formulées d'une manière trop vague. Selon elle, il convient tout au moins de réglementer explicitement les cas d'exclusion (par exemple les domaines relevant du droit fiscal, du droit des contrats ou des domaines sociétaux). Le rapport sur l'avant-projet ne donne aucun élément pour rendre crédible les missions que le SRC pourrait accomplir à ce titre. Le rapport se tait aussi sur les missions que le SRC ne devrait pas du tout accomplir; bref, il y aurait là des zones grises.

Article 63

GE est d'avis que vu le statut particulier de la Suisse, le Conseil fédéral devrait avoir les compétences de déterminer lui-même une liste de critères. *BE*, lui aussi, estime que la formulation est trop étroite et il craint que les groupements nationaux qui menacent exclusivement la sûreté intérieure puissent ainsi ne jamais figurer dans la liste d'observation.

Alinéa 1:

De l'avis du PS, il est faux de prévoir un automatisme dans la deuxième phrase de l'al. 2. L'élaboration de ses listes de sanctions ne répondait pas dans tous les cas aux exigences posées par l'Etat de droit. D'ailleurs, même le Conseil de l'Europe était arrivé à cette conclusion. Voilà pourquoi il convient de renoncer à cet automatisme.

¹ *La liste d'observation comporte [...] intérieure ou extérieure. (Supprimer la deuxième phrase).*

Article 64

ZH et la CAPS demandent que dans les cas où une telle interdiction d'exercer une activité est liée à une procédure pénale, la marche à suivre devrait être harmonisée avec le Parquet compétent.

droitsfondamentaux.ch, Les Verts, les JDS et la SPF craignent que suivant la composition politique du Conseil fédéral, il puisse y avoir des abus en la matière et c'est la raison pour laquelle il convient de supprimer purement et simplement cette ingérence préventive aussi inutile que disproportionnée dans les libertés démocratiques.

Alinéa 1:

Le PBD suggère de remplacer le « et » par un « ou », étant donné que pour une interdiction d'exercer une activité, les facteurs individuels devraient déjà amplement suffire en tant que conditions.

Alinéa 2:

Le PBD pense que l'interdiction devrait pouvoir être valide et éventuellement levée par une demande (et non pas par un délai imparti).

PP1 part de l'idée qu'une interdiction d'exercer une activité décrétée par le Conseil fédéral en vertu des dispositions de l'art. 72, al.1 est soumis à la supervision du Tribunal administratif fédéral et PP1 se demande alors comment il y aurait lieu d'agir devant un tribunal avec des moyens de preuves qui devraient rester secrètes. Il se pose la question de savoir si les art. 27, al.1, let. a et 28 PA s'appliquent à de tels cas.

Section 2: Contrôle et surveillance du Service de renseignement (Art. 65 à 70)

BS pense que le réseau dense d'instances de contrôle et de surveillance prévu dans ce projet de loi et institué ainsi sous cette forme dans l'Etat est tout à fait unique en son genre. Evidemment, cela ne suffit pas en soi à rendre meilleure la surveillance exercée sur les activités du renseignement. On répète fréquemment le trio « adéquation (ou conformité à la loi) », « efficience » et « efficacité » en tant qu'étalon de mesure pour le contrôle du service de renseignement.

Il est impossible de renoncer à des contrôles efficaces et à la haute surveillance des activités du service de renseignement si l'on veut éviter des dépassements de compétences, des manquements aux tâches dévolues, du zèle et des exagérations. Une surveillance efficace procure en effet la légitimité étatique nécessaire au service de renseignement de la Confédération. Il en a d'ailleurs absolument besoin, puisqu'il se trouve dans une activité préventive importante qu'il déploie dans un champ d'action entre les libertés personnelles et la sûreté collective.

Pour la CAPS, les contrôles et la surveillance en vertu des dispositions des articles 65 et suivants sont adéquats et légitiment les compétences du SRC.

L'UDC estime que les mécanismes proposés garantissent la légitimité et la proportionnalité des activités déployées par le SRC.

PP1 se permet de poser une question, à savoir: le Département, le Conseil fédéral et la DélCdG, outre leurs nombreuses tâches à accomplir, peuvent-ils réellement appréhender une activité de contrôle efficace ? Il conviendrait d'examiner si le Conseil fédéral, dans le cadre des dispositions de l'article 68 (en lieu et place du département, art. 16, al. 3), ne devrait pas désigner une instance de surveillance indépendante et compétente sur le plan technique qui ne soit liée qu'au SRC et non pas aux directives d'autorités et qui puisse dès lors exercer son contrôle politique extrêmement important pour l'activité du SRC.

La *privatim* déplore qu'il n'ait pas été tenu compte que le traitement de données personnelles soit assujéti à la surveillance cantonale indépendante de la protection des données. L'art. 68, al.3, let. b, ne peut pas englober la surveillance de la protection des données des cantons, étant donné qu'une ordonnance du Conseil fédéral ne présente pas l'échelon idoine pour pouvoir modifier la Constitution et les lois. Une réglementation claire et nette de la surveillance en matière de protection des données par les préposés cantonaux à la protection des données permettraient pourtant d'éviter des incertitudes et des litiges en matière de compétences.

Article 70

² *S'agissant de la surveillance de la protection des données sur les autorités d'exécution cantonales, seule et exclusivement est compétente la surveillance cantonale sur la protection des données.*

Article 65

BS est d'avis qu'au titre d'autocontrôle du SRC, il y conviendra de régler expressément les éléments suivants: l'obligation de collaborer avec les organes de contrôle cantonaux; la coordination des activités de contrôle; l'élaboration de rapports.

Outre l'adéquation, l'efficacité, l'efficacé et le principe dit économique devront être les objets de l'autocontrôle.

Pour la SPD-TG, un tel autocontrôle du SRC est d'une part inadéquat vu le manque d'indépendance du SRC. D'autre part, il faut bien admettre que cet autocontrôle constitue une ingérence dans les droits des cantons. Le législateur refuserait dès lors aux cantons d'instituer leurs propres autorités de sûreté dans le domaine de la loi prévue pour pouvoir exercer leur propre contrôle de manière vaste et surtout indépendante.

Le PPS demande de désigner une instance de contrôle qui soit indépendante et non subordonnée au chef du DDPS.

Pour le CCCZH cette disposition ne serait que de la poudre aux yeux et ne servirait qu'à calmer le jeu.

Article 66 ss

Pour le PS, il est tout à fait déterminant que la haute surveillance politique et le contrôle exercés par le DDPS, le Conseil fédéral et la DélCdG soient assurés de très près.

Article 66

Alinéa 1:

Au sujet de l'autocontrôle administratif interne, BS demande que l'activité du SRC ne soit pas seulement supervisée du point de vue de son adéquation, efficacité et de son efficacité, mais aussi de sa rentabilité (principe économique).

Alinéa 4:

Le CCCZH ne veut pas que l'accès aux documents officiels soit restreint par la LTrans.

Article 67

Alinéa 1:

BS demande une supervision de l'exploration radio non seulement sur la base de légitimité mais encore sur celle de l'opportunité.

Alinéa 2:

BS aimerait que l'on complète cet alinéa par une phrase supplémentaire:

« *Il accomplit les tâches qui lui sont dévolues de manière autonome et indépendante.* »

Alinéa 6:

Le CCCZH ne veut pas que l'accès aux documents officiels soit restreint par la LTrans.

Article 68

Alinéa 1:

BS demande que le contrôle de l'activité du SRC ne s'exerce pas seulement sur l'adéquation, l'efficience et l'efficacité, mais aussi sur la rentabilité (principe économique).

Alinéa 2:

BS aimerait rajouter à cet alinéa une disposition selon laquelle le Conseil fédéral, une fois renseigné par le DDPS, informe régulièrement l'Assemblée fédérale, les cantons et le grand public. Ce sera à la loi de disposer ce que doit contenir au juste cette information.

Alinéa 3:

Le CCCZH veut supprimer toute réglementation selon laquelle la surveillance financière à propos du SRC doit rester secrète, car le SRC est financé par l'argent du contribuable et que le grand public devrait dès lors connaître ses dépenses. Par ailleurs, le Peuple suisse a le droit de savoir comment la Confédération engloutit des sommes pour violer la sphère privée des personnes.

Article 69 et 70

AR, BE, BL et la CLI se demandent si la DéICdG est à même d'assurer la surveillance sur les 26 services d'exécution cantonaux dans l'intensité commandée.

BL rejette le modèle de surveillance que propose le législateur. Il y a lieu de reformuler les articles 69 et 70. Les cantons devaient pouvoir bénéficier pleinement des droits de surveillance quant à leurs propres collaborateurs et collaboratrices. Font donc partie de ces droits le droit de regard des autorités de surveillance cantonales des services ainsi que de celui des commissions de gestion parlementaires cantonales dans les activités du personnel cantonal.

La CLI présente les demandes suivantes (tout comme AR, BE, BS, JU et TI):

- La restriction prévue aux articles 69 et 70, al. 2 de la haute surveillance parlementaire à la seule DéICdG doit être supprimée.
- La surveillance cantonale des services et la haute surveillance cantonale doivent être maintenues de manière illimitée et ce tant en droit qu'en fait.
- Il y aura lieu de créer une réglementation qui n'admette aucune faille dans la surveillance et dans la haute surveillance et qui ne soit pas en contradiction avec le

principe que la haute surveillance cantonale aille aussi loin que la surveillance des services (principe du droit accessoire)

Article 69

Selon l'ASIN, la Délégation des Commissions de gestion des Chambres fédérales devrait pouvoir exercer ses fonctions de surveillance de manière illimitée, donc sans être tributaire de délais et avec un accès à toutes les mesures et applications de l'activité du service de renseignement.

Article 70

En prévoyant les dispositions de l'art. 70, le Conseil fédéral tient à son concept de la surveillance partagée entre la Confédération et les cantons sur les services d'exécution cantonaux. La CCPCS, AR, BE, GR, SO et UR saluent cette intention et déclarent que finalement, les dispositions de l'art. 35 OSRC avait fait ses preuves. En revanche, une solution intégrale « confédérée » prévoyant la reprise du personnel des services d'exécution cantonaux au sein de l'Administration fédérale serait entachée de graves inconvénients.

BS est en principe d'accord que le législateur tienne à une organisation existante décentralisée avec des autorités d'exécution cantonales tout en ayant recours à des organes de surveillance aptes à soutenir la surveillance des services cantonaux (art. 2, 7 et 70).

AG se demande si la supervision par les préposés cantonaux à la protection des données s'étend également à la conformité à la loi et à la proportionnalité de la recherche des données et si la consultation des données de la Confédération que le canton traite exigera l'assentiment du SRC comme le demandent les dispositions de l'art. 35a OSRC pour la surveillance de service. AG constate en effet que le projet de loi n'a pas réglé ces questions, pas plus du reste que le rapport sur l'avant-projet n'a approfondi le sujet. Il s'agit maintenant de saisir l'occasion et de clarifier ces questions.

Aux termes de l'al 1, les membres des autorités d'exécution cantonales auxquels le canton a confié des tâches relevant de la présente loi sont soumis au droit de service cantonal et à la surveillance de service de leurs supérieurs hiérarchiques. Pourtant, la surveillance en matière de protection des données exercée sur les autorités d'exécution cantonales ne relève pas exclusivement des services subordonnés aux autorités d'exécution cantonales comme expliqué en page 72 du rapport sur l'avant-projet. En effet, la surveillance en matière de protection de données fait en particulier partie des tâches des autorités cantonales chargées de la protection des données, qui contrôlent le traitement des données des organes publics au sein du canton respectif. Le contrôle du traitement des données des organes publics de la Confédération (SRC) est ici l'affaire du PFPDT. C'est donc sur cette toile de fond et pour clarifier cette affirmation qu'il semble opportun à BL, BS, GR, TI et à la SPD-TG de rajouter un autre alinéa encore pour compléter l'art. 70. Ce nouvel alinéa aurait la teneur suivante:

« La surveillance cantonale de la protection des données est compétente s'agissant de la surveillance en matière de protection des données exercée sur les organes d'exécution cantonales ».

BE déplore que la nouvelle LRens ne se prononce pas sur la surveillance de la protection des données. Pour éviter des questions de compétences entre la Confédération et les cantons, il y aurait lieu de confier la surveillance globale de la protection des données au Préposé fédéral à la protection des données et à la transparence, étant donné que le SRC exploite les systèmes d'information prévus (cf. art. 42, en corrélation avec l'art. 41, al. 1).

Quant à l'art. 69, il conviendrait de le compléter avec la réglementation régissant la surveillance de la protection des données (il y aurait encore une autre option, à savoir un complément à la 4^e section intitulé « Dispositions particulières sur la protection des données »).

Pour OW, il y a un flou. Il se demande en effet si les autorités d'exécution cantonales qui accomplissent des tâches strictement à la demande du SRC devraient alors être considérées comme étant des organes de la Confédération et seraient alors par conséquent assujetties à la surveillance de la Confédération en matière de protection des données. Cela correspondrait à la pratique actuelle à laquelle il s'agit de rester fidèle. OW demande par conséquent de régler concrètement à l'article 70 la compétence fédérale pour la surveillance en matière de protection des données exercée sur les organes d'exécution cantonales. Ne tomberaient cependant pas sous le coup de la surveillance de la Confédération en matière de protection des données le traitement des données au sens des dispositions de l'art. 41, al. 2 des services de renseignement cantonaux ou des services de la police judiciaire.

SZ est d'avis que les autorités cantonales compétentes selon les dispositions de l'art. 7 – et pour autant qu'elles exercent une activité dans le champ d'application de la LRens –, doivent être considérées comme étant des organes de la Confédération et, par conséquent, qu'elles sont assujetties à la surveillance en matière de protection des données de la Confédération. Cela correspondrait à la pratique actuelle. SZ n'en recommande pas moins d'ancrer les compétences de la Confédération pour la surveillance en matière de protection des données par le biais des organes cantonaux compétents soit à l'article 70 (surveillance cantonale) ou alors de consigner cette problématique dans le message relatif à la LRens.

TI pense qu'il s'agit de préciser (éventuellement à l'art. 41 et également dans les commentaires) que les données relevant de la présente loi sont soumises à la législation fédérale en matière de protection des données et à celle des cantons en la matière.

ZH a également invité le préposé cantonal à la protection des données à se prononcer sur le projet. Ce dernier soulève la question de la protection cantonale des données. A ce propos, tout en se référant aux dispositions de l'art. 41 et aux explications données dans les commentaires (en page 58), il fait valoir notamment que jusqu'à ce que les données traitées par les organes d'exécution cantonales dans les systèmes d'information de la Confédération, c'est bel et bien le droit cantonal sur la protection des données qui s'applique. Le préposé cantonal demande aussi que soit élaborée une réglementation aux art. 65 ss (chapitre 6, section 2) à propos de la surveillance cantonale en matière de protection des données. A son avis, il convient d'éclaircir globalement tout ce complexe de questions et de l'exposer dans le message du Conseil fédéral.

La CAPS ne pense pas que les règles actuelles qui devraient continuer en vertu des articles 2, 7 et 70 aient fait leurs preuves dans l'optique de l'Etat de droit. Qu'on en juge: pendant des années, il n'y a pratiquement eu aucune surveillance des organes d'exécution cantonaux. Mais une telle absence de surveillance dans un domaine aussi sensible que ça est tout à fait intolérable.

La délimitation complexe entre la surveillance cantonale des services et la surveillance fédérale ne fonctionne en pratique que si le SRC vient généreusement à la rencontre des cantons.

Dans le cadre de la LRens, il s'agit maintenant de saisir les opportunités d'éliminer la situation hybride du point de vue du droit que connaissent les organes d'exécution cantonaux. Il conviendra alors de régler de manière claire et facilement applicable dans une disposition ad hoc tant la délimitation des compétences du SRC et des cantons que la coopération entre le service de renseignement, la police et le Parquet.

Alinéa 3:

BS estime que grâce à la réglementation prévue à l'art. 70, al. 3, l'institution ou la continuation d'un organe de contrôle demeure possible. A son avis, elle reste conséquente si l'on maintient l'organisation décentralisée des autorités d'exécution cantonales. Si l'on tient au modèle existant à l'échelon cantonal, il conviendra alors également de maintenir sur ce plan une surveillance globale et efficace. Dans cet ordre d'idées, pour qu'une surveillance soit efficace dans le canton, *BS* est alors d'avis qu'il est indispensable de conférer au canton un droit de regard étendu et surtout inconditionnel.

BS estime que la thématique de la surveillance cantonale doit être réglée en détail sur le plan de la loi. Fait partie de cette thématique en particulier la réglementation selon laquelle la surveillance cantonale des services et tous les organes de contrôle qui l'épaulent doivent bénéficier d'un droit de regard illimité, mais au minimum du droit de consulter les données et les dossiers ainsi que les informations auxquelles les autorités cantonales ont accès (INDEX SRC, PES). La description du contenu de la surveillance cantonale des services dans les commentaires, en page 72, devra aussi expressément être réglée au niveau de la loi.

Article 71

Le *PLR* est favorable à l'indication des voies de recours proposées en tant que garantie qu'offre l'Etat de droit.

Le *TAF* laisse entendre qu'il pourrait être problématique, dans certains cas, d'interjeter recours à la chambre compétente contre des décisions rendues justement par le président de la chambre concernée. Il est vrai que l'on ne résoudrait pas davantage ce problème en instituant une autre chambre du Tribunal administratif fédéral pour recevoir ledit recours.

Le *TAF* saluerait alors une séparation stricte entre les autorités judiciaires qui sont compétentes pour l'autorisation des mesures de recherche d'informations et celles qui le sont pour recevoir des recours. Cette séparation aurait d'ailleurs également l'avantage d'éviter des cumuls de fonctions dans la même autorité judiciaire. Le *TAF* propose dès lors de faire apprécier le recours dans une toute autre autorité judiciaire fédérale et l'attribuer dans ce cas au Tribunal fédéral pénal. Cette solution présente également l'avantage que le recours prévu à l'al. 1 puisse être déféré au Tribunal fédéral.

Le *TF* déclare que le droit de recours proposé est contraire aux voies de recours générales du Tribunal fédéral. Le *TF* est d'avis que les graves ingérences éventuelles dans les droits fondamentaux pourraient aussi être corrigées dans le domaine du service de renseignement par la Cour suprême dans le cadre des dispositions générales du droit de recours de la LTF. Toujours est-il que la dernière phrase de l'al. 2 devrait par conséquent être supprimée et remplacée par un alinéa ou un article en propre :

« Le recours contre des décisions de recours du Tribunal administratif fédéral interjeté devant le Tribunal fédéral est recevable. La procédure se fonde sur les dispositions de la LTF. »

Article 73

GE salue la volonté ancrée dans la LRens de vouloir coopérer avec les cantons, en particulier concernant la mise à disposition de moyens techniques.

Aux dires de *NE*, les tâches dévolues aux autorités d'exécution cantonales découleraient de cet article, mais pas les moyens qu'elles pourraient utiliser à cet effet. Il se pourrait qu'il s'agisse ici des mesures de recherche d'informations non soumises à autorisation, mais le texte du projet ne le précise pas.

Le CCCZH voit dans cette réglementation la confirmation que le SRC doit pouvoir assumer une fonction de coordination entre la Confédération et les cantons avec une prétention de souveraineté sur les informations. Mais un tel contrôle sur l'information n'est pas tolérable dans un Etat démocratique.

Modification du droit en vigueur

Chiffre 2 Lar:

Selon *BE* et la *privatim*, les données dont on n'a plus utilité selon le principe de la proportionnalité doivent en principe être détruites. Mais il est possible de déroger à ce principe pour des raisons historiques: au lieu de détruire des données et des dossiers, on peut aussi les archiver. Pour les personnes concernées, ce fait a pratiquement le même effet qu'une destruction des informations puisque le service ayant remis données et fichiers aux Archives fédérales ne pourra plus les utiliser pour accomplir les tâches qui lui furent dévolues à l'origine. Cela étant, on tient donc compte de la protection de la personne. Mais la modification prévue dans la LRens transformerait en son contraire la solution choisie par le législateur pour la Lar vu qu'avec l'exception prévue, les données que les services remettent aux Archives fédérales demeureraient maintenant à disposition de ces services pour une période illimitée. Non seulement le SRC en serait le bénéficiaire, mais également tous les autres services remettant de tels documents. L'archivage deviendrait dès lors un instrument en vue de la conservation de données durable pour lesdits services.

La *privatim* propose dès lors de renoncer complètement à cette modification.

Selon *BE*, il conviendrait, dans le texte de la loi, de fixer des conditions restrictives pour consulter les documents déposés aux Archives fédérales. La nécessité de les consulter pour pouvoir apprécier des menaces de la sûreté intérieure et extérieure est une condition très ouverte permettant des ingérences prépondérante dans les droits de la personne. Par ailleurs, *BE* aimerait que le rapport expose pourquoi, à propos du domaine de la protection des données si sensible en ce qui concerne la protection de l'Etat, le législateur veut soudain déroger à ce principe légal.

Le CCCZH considère que cette modification est inacceptable.

Chiffre 3 LTrans:

Le *PDC* partage l'appréciation que les informations découlant du renseignement doivent être particulièrement protégées, mais il salue encore la décision de vouloir renoncer à une exclusion totale du SRC du champ d'application de la LTrans.

Pour le CCCZH, il ne faut pas toucher aux prérogatives de la LTrans. Il s'agira plutôt que le SRC – qui a besoin d'une attention particulière – apprenne tant à manier les demandes d'accès que de motiver les refus.

L'*Université de Genève* doute fort que pour des documents relevant de la recherche d'informations, une exception par rapport à la LTrans se justifie, à plus forte raison que dans ce domaine, il n'y a eu que très peu de demandes d'accès. Par conséquent, le mécanisme d'exception que le législateur a mis en place pour la protection de données sensibles devrait suffire. Par ailleurs, le SRC, par une telle exception, se soustrairait au contrôle final du juge.

Chiffre 5 CC:

Le CCCZH n'aimerait pas conférer au SRC de droit « forfaitaire » pour pouvoir fouiner dans les registres.

Chiffre 6 CP:

D'après le *CCCZH*, il est scandaleux d'inscrire de tels passages dans le CP, étant donné que l'on s'aperçoit ainsi l'Etat de droit (voir également les critiques à l'égard des art. 15 et 16).

PP1 suggère d'examiner s'il ne convient pas d'adapter la note marginale de l'art. 267 CP, lorsque la divulgation d'informations internes (au sens des art. 267 et 320 CP) provenant du SRC à des tiers doit être saisie.

Chiffre 8 LAAM:

La *SSO* et l'*ASOR* expriment leur satisfaction à l'égard de l'autorisation légale formelle pour l'observation aérienne et de l'espace donnée au service de renseignement de l'armée.

Chiffre 9 LSIA:

D'après le *CCCZH*, il est inutile de donner au SRC un accès aux données personnelles de l'armée.

Chiffre 11 LCR:

Selon le *CCCZH*, constater qui a le droit de conduire est strictement une affaire de police.

Chiffre 12 LSCPT:

SG fait observer que les dispositions prévues dans la *LRens* devraient se référer au projet de la révision totale de la *LSCPT*.

Chiffre 13 LTC:

Le *CCCZH* n'aimerait pas que l'Etat soit considéré comme « perturbateur » dans la loi.

Chiffre 14 LAVS :

Le *CCCZH* critique que l'Etat ne joue pas son rôle de modèle s'il figure comme pourvoyeur d'argent sale.

Chiffre 15 LAI:

Le *CCCZH* souhaite faire cesser l'acharnement du SRC à vouloir collecter des données.

Chiffre 16 LPP:

Le *CCCZH* souhaite faire cesser l'acharnement du SRC à vouloir collecter des données.

Chiffre 17 LAMal:

Le *CCCZH* souhaite faire cesser l'acharnement du SRC à vouloir collecter des données.

Chiffre 18 LAA:

Le *CCCZH* souhaite faire cesser l'acharnement du SRC à vouloir collecter des données.

Chiffre 20 LACI:

Le CCCZH souhaite faire cesser l'acharnement du SRC à vouloir collecter des données.

6. Autres remarques

BS souligne que la nécessité de densité normative, telle qu'elle est mentionnée dans le projet, est également requise pour les prescriptions d'exécution qui doivent être fixées par le Conseil fédéral.

Dans le rapport sur l'avant-projet, il est indiqué que la haute surveillance parlementaire sur l'exécution de la présente loi est exclusivement confiée à la DélCdG des Chambres fédérales. Il est indéniable que la DélCdG, compte tenu de son mandat fixé à l'art. 53 de la loi sur le Parlement, assume la charge principale de la haute surveillance sur les activités relevant de la sécurité de l'Etat et du renseignement. Dans son art. 51, la loi sur le Parlement confie toutefois la tâche de la haute surveillance sur les finances à la DélFin. Sur la base d'une convention, ces deux délégations travaillent en étroite collaboration dans les domaines où leurs compétences se recoupent. Les explications concernant l'avant-projet sont donc incomplètes.

La *DélFin* demande que cet élément soit pris en compte dans le message relatif à la LRens. Cela permettra d'éviter toute imprécision dans l'interprétation ultérieure de la loi.

Le *PBD* et l'*Université de Genève* attirent l'attention sur le fait que le présent projet doit être coordonné avec des projets législatifs en cours, en particulier avec la révision totale de la LSCPT. A ce sujet, la *Swico* demande un ajournement du projet LRens jusqu'à la conclusion de la révision de la LSCPT, de sorte à pouvoir examiner la LRens en fonction des nouvelles dispositions de la LSCPT.

Le *PBD* demande par intervention parlementaire que soit créé un centre de compétence national pour la sécurité TIC et il attend que le SRC mette aussi en place un tel service.

BS et *ZH* font remarquer que le projet ne contient pas de dispositions sur la délimitation impérative entre l'activité de la police, l'activité du service de renseignement et l'activité des autorités de poursuite pénale. Ce point devrait être explicité dans le message.

La *SSO* souligne qu'à sa connaissance, c'est la première fois que la Délégation du Conseil fédéral pour la sécurité (Délséc) est mentionnée dans une loi fédérale et qu'il faut y renoncer car il ne s'agit pas d'un organe de notre Etat fédéral.

PP1 recommande que l'ordonnance d'exécution de la LRens approuvée par le Parlement, qui sera certainement volumineuse, fasse l'objet d'une consultation ou d'une audition auprès des principales associations professionnelles et économiques ainsi que des organisations TIC.

PP2 aimerait que la loi prescrive la publication de statistiques détaillées sur le nombre de mesures autorisées, le nombre de mesures refusées, le type de mesures et le nombre de communications qui ont été ajournées ou auxquelles il a été renoncé. .

Manque de base constitutionnelle formelle:

Nombre de points relatifs à la portée et à l'étendue de la compétence (inhérente) de la Confédération restent à éclaircir. *BS* est d'avis qu'une base constitutionnelle formelle est nécessaire pour créer clarté et transparence dans ce domaine important. Par ailleurs, le projet prévoit une extension significative des attributions du SRC en matière de recherche d'informations. Cette extension est liée à de fortes atteintes - inévitables - aux droits

fondamentaux, ce qui exige par définition une légitimation constitutionnelle du service de renseignement.

BS considère que dans une première étape, un article constitutionnel qui confère sa légitimité au SRC doit être présenté au Peuple et aux cantons, qui doivent pouvoir décider s'ils veulent un service de renseignement qui, comparé à aujourd'hui, poursuivra des buts nettement plus ambitieux.

BS saluerait le fait qu'une codification uniforme pour l'activité du SRC ne soit créée dans une loi formelle qu'une fois cette première étape franchie.

SO estime que dans le rapport sur l'avant-projet, les explications sur la thématique de l'absence de base constitutionnelle formelle sont lacunaires et que le fait de ne pas indiquer explicitement qu'il est renoncé à créer une telle base manque de transparence.

Au vu de l'impact sur les droits fondamentaux relevé dans le rapport sur l'avant-projet, *SO* est d'avis qu'il est politiquement inopportun d'élargir les tâches de la protection de l'Etat sans disposition constitutionnelle correspondante, un point faible du projet qui peut mettre en danger l'approbation politique des nouvelles mesures de recherche d'informations (que *SO* salue d'ailleurs).

Alnt relève que le projet part du principe que la compétence législative de la Confédération pour édicter la *LRens* découle pour l'essentiel des art. 54 (Affaires étrangères) et 57 (Sécurité) Cst. Cette déduction est controversée. La compétence législative est néanmoins reconnue par l'indication de « compétence inhérente ».

Le projet *LRens* est au centre de fortes tensions entre la protection constitutionnelle des droits fondamentaux et des droits de l'homme, raison pour laquelle un projet législatif de ce type doit reposer sur des garanties constitutionnelles particulières. Les ingérences à des fins de renseignement dépassent de loin la seule protection de l'Etat. De l'avis d'*Alnt*, la base constitutionnelle pour l'établissement d'une loi sur le service de renseignement est donc insuffisante.

Le *CP* et la *CVAM* estiment que les explications concernant la base constitutionnelle démontrent clairement que cette question doit être étudiée plus avant. Pour une thématique aussi délicate, une base constitutionnelle formelle (par exemple par un ajout à l'art. 57 Cst.) est indispensable.

La *SSO* et l'*ASOR* sont convaincus que la base constitutionnelle indirecte pour le service de renseignement est donnée et qu'elle suffit amplement. En plus des art. 54 et 57 Cst. indiqués dans le rapport sur l'avant-projet, elle découle déjà de l'art. 2 Cst., en particulier de ses al. 1 et 4, deuxième partie, en lien avec tous les autres articles sur les tâches concrètes de la Confédération, dont font aussi partie la sauvegarde des intérêts essentiels de la Suisse. La base constitutionnelle indirecte découle aussi de l'histoire récente de la Cst.: lors de sa mise à jour dans les années 90 — où tout le droit constitutionnel implicite jusqu'à ce moment-là a été codifié — les services de renseignement existaient déjà et il n'a pas été jugé nécessaire de créer une base constitutionnelle formelle pour ces services.

Collaboration avec les cantons

La *CCPCS*, *AR*, *BE*, *FR*, *SG*, *SO*, *SZ*, *TG*, *TI*, *UR*, *VD* et *ZG* sont d'avis que la réglementation concernant les activités et compétences des services d'exécution cantonaux n'est pas satisfaisante. Selon les dispositions du projet, et comme cela a été le cas jusqu'à présent, ces services seront mandatés (art. 7, al. 2) et indemnisés (art. 73, al. 5) par les autorités de la Confédération, mais, dans le domaine des activités dont ils sont chargés, ils travailleront à l'avenir exclusivement avec les banques de données de la Confédération (art. 41, al. 1) et seront contrôlés par divers organes de la Confédération, y compris la Délégation des Commissions de gestion des Chambres fédérales (art. 65 ss). L'organisation de la formation continue en matière de renseignement relève également du SRC (art. 73, al. 3).

Cette réglementation correspond pour l'essentiel à la situation actuelle: les moyens des services cantonaux qui recherchent des informations sont dans leur majorité engagés en faveur des tâches stipulées dans la LMSI (c'est ainsi que l'attribution de mandats, la direction technique, le contrôle, la responsabilité et la coordination des services relèvent principalement du SRC). Mais en plus de ces activités, les services cantonaux, avant des interventions de service d'ordre, sont également chargés d'activités dans le cadre d'investigations de police de sécurité, activités dont la coordination relève de la police cantonale concernée. Bien que les services d'exécution cantonaux soient des instruments importants du SRC, ils ne sont pratiquement pas mentionnés dans la nouvelle loi; cette dernière ne parle pour ainsi dire que du SRC. Cette contradiction n'est corrigée ni à l'art. 2 (autorités et personnes concernées) ni à l'art. 73 (exécution par les cantons). Comme le projet de loi prévoit d'importantes ingérences dans les droits fondamentaux, il doit répondre à des exigences élevées quant au principe de la précision. La terminologie choisie crée une confusion sur la question de savoir si le terme « SRC » englobe ou non les collaborateurs des services d'exécution cantonaux. Ce doute doit absolument être levé. Les cantons sont tributaires d'une base légale très claire. En effet, récemment encore, lorsque les collaborateurs et collaboratrices de la protection cantonale de l'Etat investiguaient auprès d'autres autorités dans l'accomplissement des tâches qui leur sont dévolues, ces autorités leur demandaient sur quelle base légale concrète ils justifiaient leur recherche d'informations. Puisque la compétence de la Confédération de légiférer dans le domaine des activités de renseignement des cantons dans le cadre de la sûreté intérieure de la Suisse n'est pas controversée, la question des compétences peut être clarifiée. Le projet devrait en ce sens être complété comme suit:

Nouvel al. 3 à l'art. 7: « *Dans le cadre des activités dont elles sont chargées par la présente loi, les autorités d'exécution cantonales disposent de compétences analogues au SRC pour la recherche d'informations selon les art. 11 à 21.* »

ou

en ajoutant « *Le SRC et les autorités d'exécution cantonales...* » aux art. 11 à 21.

AG se réjouit de la grande importance donnée aussi à l'avenir à la collaboration avec les autorités cantonales.

GR salue le concept du projet qui prévoit que le SRC réalise les tâches de renseignement en collaboration avec les autorités d'exécution cantonales et que ces autorités soient de ce fait un instrument important du SRC. Le projet de loi s'en tient à la forme d'organisation décentralisée et à l'étroite collaboration avec les cantons, ce qui est particulièrement réconfortant. Le fait que dans le champ d'application de la loi, les autorités d'exécution cantonales ne gèrent plus de banques de données qui leurs soient propres, doit également être salué.

JU et NW approuvent les règles concernant l'indemnisation des cantons et la poursuite de la collaboration au niveau de la formation, une pratique qui a fait ses preuves.

Le PDC estime que le projet ne règle pas clairement jusqu'à quel point les autorités d'exécution cantonales sont habilitées à rechercher elles-mêmes des informations et à appliquer des mesures dans le cadre de leurs activités régies par cette loi.

Le pvl juge opportun que la collaboration avec les cantons se poursuive comme jusqu'à présent mais il se pose la question s'il est utile et même praticable de confier la haute surveillance des activités cantonales en rapport avec la nouvelle loi à la Délégation des commissions de gestion. Dans la perspective de l'élaboration du message, ce point doit à nouveau être analysé avec les cantons et, le cas échéant, adapté.

Conséquences financières du projet de loi sur les cantons:

La *CCPCS*, *AR*, *BE*, *GR*, *SO*, *TG*, *VD*, *ZG* et *ZH* exigent que les cantons soient indemnisés pour les efforts supplémentaires qu'impliquent pour les autorités d'exécution cantonales les instruments et procédures de la nouvelle LRens (voir art. 73, al. 5). Il s'agit notamment de tenir compte du fait que l'application des nouveaux instruments de recherche d'informations va entraîner un important travail supplémentaire. Pour le SRC, dans le rapport sur l'avant-projet, le besoin additionnel en personnel pour les nouvelles mesures de recherche d'informations est estimé à 16 postes de travail.

NE et *SZ* partent du principe qu'il n'y aura pas de modifications au niveau financier, que les cantons ne doivent donc rien entreprendre à ce sujet.

Pour *BS*, il découle de l'obligation faite aux cantons de participer à l'exécution de la LRens que la Confédération doit assumer financièrement les charges pour tous les efforts supplémentaires au niveau technique et du personnel. Faute de quoi la plupart des cantons ne pourraient sans doute remplir ni totalement ni même partiellement les mandats du SRC avec leurs propres effectifs et moyens techniques.

Remarques concernant le rapport sur l'avant-projet:

Pour l'*USAM*, les explications fournies au chap. 1.5 du rapport sur l'avant-projet sont claires, complètes et compréhensibles et elles exposent les intentions du projet de loi, ce qui ne veut pas dire qu'elles soient correctes. Y manquent, par exemple, des éclaircissements sur la différenciation entre terrorisme et extrémisme violent, des précisions sur la notion des « intérêts essentiels de la Suisse » ou pour le moins de son intégration dans une stratégie et des explications sur les mesures de prévention contre un activisme débordant des autorités.

7. Résumé des réponses aux questionnaire

Participants:

PBD, *pvl*, *CAPS*, *CDSVS*, *SSO*, *PS*, *UDC*, *ASOR*, *AG*, *AI*, *BE*, *BS*, *FR*, *GL*, *LU*, *OW*, *SG*, *SO*, *SZ*, *TG*, *TI*, *VS*, *ZG* (23)

1. Questions d'ordre général

a) A l'exception du *pvl*, tous les participants estiment que les principaux points du projet au chap. 1.5 du rapport sur l'avant-projet sont complets et compréhensibles et qu'il ne manque aucun élément déterminant.

Le *PBD* fait remarquer que des descriptions trop détaillées auraient un effet limitatif sur ce projet complexe, en particulier en ce qui concerne de nouvelles menaces encore inconnues ou de futurs systèmes informatiques.

SO trouve qu'il faudrait mentionner l'absence de base constitutionnelle.

Il manque au *pvl* la mention de l'exploration du réseau câblé (même remarque de la part de la *SSO* et de l'*ASOR*) et des modifications dans le domaine de la haute surveillance sur les activités des cantons.

SZ souhaite des explications sur la manière dont la Confédération entend procéder pour la recherche d'informations sur l'extrémisme violent. Y renoncer signifierait en effet que l'on ignorerait des risques majeurs.

b) Pour ainsi dire tous les participants trouvent que le projet de loi est formulé et structuré de manière compréhensible (à l'exception du *PBD*, *SG* et *TG*).

La *CAPS* suggère de renoncer à mentionner des évidences.

Pour SG, le nombre d'articles très longs avec de multiples paragraphes rendent la compréhension quelque peu difficile et la systématique peu claire, deux éléments problématiques pour un acte législatif avec de fortes ingérences dans les droits fondamentaux.

La SSO et l'ASOR trouvent que les diverses dispositions qui vont de pair sont trop dispersées dans l'avant-projet de loi (par exemple les dispositions pour la protection des personnes tels que la protection des sources, l'armement, les identités d'emprunt, etc.).

2. Objet et but (art. 1)

a) La CAPS, la SSO, l'ASOR, LU, SZ et le TI estiment que les conditions requises pour charger le SRC de sauvegarder d'autres intérêts essentiels de la Suisse selon l'al. 3 et l'art. 62 ne sont pas formulées avec suffisamment de précision.

Le PBD suggère que le législateur puisse autoriser immédiatement une telle mission et que l'autorisation puisse être requise après coup. . .

La CAPS considère que cette disposition ressemble à une situation où le serpent se mord la queue, autrement dit, il la trouve absurde.

Pour LU, la formulation des dispositions est trop vague et il manque des exemples.

SZ souhaite une description plus précise de cette notion afin qu'elle ne permette pas toutes sortes d'engagements.

Pour la SSO et l'ASOR, il est nécessaire de préciser que les autres intérêts essentiels de la Suisse relèvent de la compétence constitutionnelle de la Confédération ou qu'une demande en ce sens doit avoir été déposée par plusieurs cantons.

b) A l'exception du pvl, du PS, de TG et du TI, les participants trouvent que les explications dans le rapport concernant cette future possibilité de sauvegarde attribuée au SRC sont suffisamment explicites et compréhensibles.

AI aimerait que les infrastructures sensibles et les réseaux d'informations soient mentionnés. BS pense qu'il sera sans doute difficile et inutile de qualifier ou de quantifier davantage la protection du régime constitutionnel de notre pays, etc.

Le pvl, la SSO, l'ASOR et VS aimeraient disposer d'exemples relatifs aux autres intérêts de la Suisse. VS attire l'attention sur le fait que dans d'autres lois, cette notion est utilisée de manière totalement différente.

Pour la CAPS, il faut renoncer à des explications plus détaillées afin de garantir les marges de manœuvre nécessaires.

3. Mesures de recherche d'informations soumises à autorisation (art. 22 ss)

a) A l'exception de BE et SG, tous les participants trouvent que les conditions pour la mise en œuvre des nouvelles mesures de recherche d'informations soumises à autorisation sont formulées avec suffisamment de précision, aussi en ce qui concerne leurs restrictions.

SG critique que les mesures de recherche indiquées soient aussi prévues dans la procédure pénale, mais que les termes utilisés ne coïncident pas entre eux. Il s'agirait, en partie du moins, de reprendre ici la terminologie adoptée dans la révision de la LSCPT (qui heureusement procède déjà à l'adaptation des intitulés du CPP portant à confusion).

LU estime que la formulation « non soumises à autorisation » et « soumises à autorisation » n'est pas judicieuse. Par ailleurs, dans la perspective du choix dans le catalogue des mesures, le critère de proportionnalité de la mesure concrète de recherche devrait être décrit avec plus de précision et ancré dans la loi.

BE considère que le rôle des cantons pour l'exécution des mesures n'est pas clair.

Etant donné que la formulation doit ultérieurement permettre des méthodes d'enquêtes encore inconnues à ce jour, le PBD craint que la procédure complexe d'autorisation soit trop

lente pour certaines missions (scénarios d'urgence) et qu'elle ne soit pas conforme aux exigences modernes.

b) A l'exception de *SO* et *ZG*, les mesures proposées sont considérées par les participants comme complètes et utiles.

La *CAPS* trouve que l'ouverture pour de futurs développements est assurée.

SZ se demande si la liste détaillée de l'art. 22, al. 1, let. b à d est nécessaire ou si ces mesures ne sont pas déjà contenues dans la let. a.

TI trouve que la coordination entre le SRC et la police est problématique puisque des besoins de prévention existent également à l'échelon cantonal et qu'un échange réciproque n'est pas régulièrement pratiqué aujourd'hui.

c) Pour tous les participants, la présentation de la double procédure d'autorisation dans le projet est suffisamment transparente. Seuls le *TI* et le *VS* trouvent que cette procédure n'est pas suffisamment équilibrée par rapport à la protection des droits fondamentaux.

Pour *AI*, la procédure est plus que mesurée et pour *SZ*, le contrôle politique est inutile: le contrôle par le Tribunal administratif fédéral suffisant largement.

La *SSO* et l'*ASOR* demandent que le Conseil fédéral, dans le message et devant les Chambres, explique une nouvelle fois qu'en situation normale, les cas d'ingérences ne dépasseront pas le nombre cité. Par ailleurs, après consultation de la Délégation du Conseil fédéral pour la sécurité, c'est d'abord le département et ensuite seulement le Tribunal administratif fédéral qui doit juger.

4. Recherche d'informations sur des événements se produisant à l'étranger (art. 32 ss)

a) Tous les participants estiment que la réglementation concernant la recherche d'informations à l'étranger est appropriée et suffisante. Seul *FR* trouve que les mesures de recherche prévues devraient être mentionnées dans la loi.

SO considère que l'obligation de documenter les recherches d'informations sur les événements se produisant à l'étranger est une règle appropriée, compte tenu du traitement différent des mesures de recherche en Suisse et à l'étranger.

Au niveau de la systématique, la *SSO* et l'*ASOR* se demandent si les al. 5 et 6 sont à la bonne place.

b) Seul le *pvl* trouve que l'argument sur le fait de renoncer à une procédure d'autorisation pour des mesures de recherche d'informations à l'étranger n'est pas compréhensible, car les explications à ce sujet sont imprécises et équivoques. Dans le domaine de l'exploration du réseau câblé, l'information indiquant qu'une procédure d'autorisation n'est pas requise à l'étranger n'est pas tout à fait juste et, de plus, il ne ressort pas clairement des explications pourquoi une procédure d'autorisation n'est pas nécessaire pour l'exploration radio.

5. Traitement des données et archivage (art. 39 ss)

a) La délégation au Conseil fédéral pour fixer la durée de conservation des données dans les divers systèmes d'information du SRC (art. 42, al. 2, let. d) est approuvée par tous les participants.

SZ salue le fait que cette délégation augmente la flexibilité par rapport à de futurs développements.

La *SSO* et l'*ASOR* aimeraient que les affectations concrètes des divers systèmes, catégories pour l'instant prévues de façon générale et abstraite dans la loi, soit réglée dans l'ordonnance.

b) La SSO, l'ASOR, le PS, SO, TG et TI considèrent que les critères pour fixer la durée de conservation des données ne sont pas appropriés et qu'ils sont insuffisants.

SO estime que « l'utilité », comme seul critère, ne suffit pas. Des critères suffisamment concrets pour les divers systèmes d'information devraient pour le moins être définis dans l'ordonnance. Il faudrait aussi parler d'une durée de conservation « maximale ».

La SSO et l'ASOR rappellent qu'il faudrait aussi tenir compte du « droit d'oublier » des personnes concernées.

6. Prestations (art. 60)

a) Seul SO a répondu que la réglementation pour la fourniture de prestations du SRC en faveur de tiers n'est ni appropriée ni nécessaire. La SSO et l'ASOR n'en sont pas sûrs.

b) Le pvl, le PS, FR et LU estiment que les prestations que le SRC peut fournir ne sont pas définies avec suffisamment de précision. Aucun participant ne relève des prestations essentielles en faveur de tiers qui feraient défaut.

FR aimerait que ces prestations soient précisées dans la loi.

Le pvl trouve qu'il faut aussi prévoir des dispositions pour l'indemnisation et la compensation de ces prestations.

SZ apprécie le fait que la formulation ouverte concernant ces prestations ne les fixe pas de manière définitive et qu'elles puissent ainsi être adaptées aux besoins.