Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Service de renseignement de la Confédération SRC

Rapport explicatif

au sujet de l'ordonnance sur le Service de renseignement (Ordonnance sur le Service de renseignement, ORens) et de l'ordonnance sur les systèmes d'information et les systèmes de stockage de données du Service de renseignement de la Confédération (OSIS-SRC)

1 Remarque préliminaire

Deux ordonnances sont prévues pour la loi du 25 septembre 2015 sur le renseignement[1] (LRens): une or-donnance de portée générale sur le Service de renseignement (ORens), et une ordon-nance de portée technique sur les systèmes d'information et les systèmes de stockage de données du Service de renseignement de la Confédération (OSIS-SRC). La structure de l'ORens ne correspond pas exactement à celle de la LRens. Elle traite en premier les sujets en lien avec les utilisateurs externes et aborde les affaires internes au Service de renseignement de la Confédération à la fin.

2 Commentaires des dispositions ORens

Chapitre 1: Collaboration

Section 1 : Collaboration du SRC avec des services nationaux

Les principes généraux régissant la collaboration avec les principaux partenaires du SRC en Suisse sont inscrits dans la section 1. Ils ne changent rien à la situation actuelle et s'appuient sur le principe de soutien mutuel. Les formes concrètes de la collaboration, notamment avec les organes d'exécution cantonaux, ne sont pas décrites dans la section 1. Les décisions et compétences y relatives pour la recherche autonome d'informations sont déjà réglées de façon exhaustive à l'art. 85 LRens (Exécution par les cantons). Evidemment, le SRC a la possibilité de confier l'exécution d'autres mesures aux autorités d'exécution cantonales. Le cas échéant, ces dernières n'agissent pas de façon autonome mais sur mandat exprès du SRC, qui en assume aussi la responsabilité.

Art. 1 Collaboration du SRC avec d'autres services et personnes

L'ordonnance ne mentionne pas explicitement la collaboration et les mandats en matière de recherche d'informations au sens de l'art. 34 LRens, ni la communication de données personnelles à des tiers selon l'art. 62 LRens, car elles sont prévues expressément dans la loi et donc pleinement applicables. Il s'agit surtout d'éviter des doublons inutiles entre la loi et l'ordonnance.

Art. 5 Collaboration du SRC avec fedpol

Il est explicitement prévu que le SRC et l'Office fédéral de la police (fedpol) s'épaulent mutuellement dans l'engagement et l'exploitation des ressources et des moyens opérationnels. Cette collaboration permet d'éviter des doublons au niveau des achats et de l'entretien d'appareils onéreux ou dans le cadre de la formation lorsque les tâches sont compatibles. La communication des informations mentionnée à l'al. 2 n'est pas exhaustive; fedpol et le SRC collaborent étroitement aussi dans des commissions et comités directeurs communs ainsi que pour la coordination opérationnelle de la lutte contre le terrorisme ou encore dans l'état-major Prise d'otage. La pratique actuelle, fondée sur des conventions entre le SRC et fedpol, est ainsi maintenue.

Section 2 : Collaboration du SRC avec des services étrangers

La collaboration avec des services étrangers s'appuie sur la situation juridique actuelle et complète cette dernière sur la base d'une pratique qui a fait ses preuves.

Art. 7 Fixation annuelle des principes de la collaboration

La fixation annuelle des principes de collaboration correspond à la pratique actuelle. Elle est désormais inscrite dans la loi par voie d'ordonnance. Une appréciation sommaire au sujet de la pertinence de ces contacts au niveau du Conseil fédéral apparaît conforme à l'échelon et se justifie notamment par le fait que la Délégation du Conseil fédéral pour la sécurité (Délséc) examine la proposition au préalable et peut aussi procéder à des appréciations approfondies.

Art. 8 Compétences

Comme c'est actuellement le cas, le SRC est le seul point de contact (single point of contact) dans le cadre de la LRens pour établir des contacts avec des services de renseignement étrangers accomplissant des tâches au sens des dispositions de la LRens. Ce concept qui a fait ses preuves devrait être maintenu. Le SRC représente aussi la Suisse dans les instances de renseignement internationales. Dans les deux cas, des exceptions sont possibles avec l'autorisation du SRC. Dans le domaine militaire, le Renseignement militaire (RM) est l'interlocuteur du SRC pour déterminer une politique commune à l'égard des services partenaires et planifier les contacts. Le RM collabore de son côté avec le commandement des forces spéciales (CFS) et Swiss Armed Forces International Command (SWISSINT).

Art. 9 Types de collaboration

Cet article concrétise l'art. 12, al. 1, let. c, LRens, selon lequel le SRC peut mener des activités communes visant à rechercher des informations, à les évaluer et à apprécier la menace avec des services de renseignement étrangers et des autorités étrangères compétentes en matière de sécurité. Dans cette perspective, le SRC peut collaborer avec des services étrangers de différentes manières comme c'est déjà le cas. Outre la recherche d'informations et la conduite conjointe d'opérations sont également prévues la réalisation commune de produits (les produits au sens de l'art. 9, al. 2, let. c, de l'ordonnance sont par exemple des analyses, des appréciations de la situation et des évaluations), la collaboration en matière de formation (dans le domaine de l'activité d'analyse ou de la sécurité p. ex.) et la réalisation de projets communs (développement de moyens de communication sécurisés entre services ou répartition du travail d'analyse de sources OSINT p. ex.).

---

1 **RS…; FF** 2015 **6597**

Art. 10 Conventions internationales de portée limitée

Le SRC a désormais la possibilité de conclure de manière indépendante des conventions internationales avec des services de renseignement étrangers ou d'autres services étrangers qui accomplissent des tâches au sens des dispositions de la LRens. En vertu de l'art. 48a de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration[2], le Conseil fédéral peut déléguer à un département la compétence de conclure un traité international. Concernant les traités internationaux de portée mineure, il peut également déléguer cette compétence à un groupement ou à un office. Par voie de conséquence, le SRC n'est autorisé à conclure de manière indé-pendante des conventions internationales de portée limitée que pour régler des questions techniques en matière de service de renseignement Il peut notamment s'agir de conclure avec un service étranger une convention régissant les normes techniques d'un système d'échange d'informations conforme au droit suisse. De telles conventions devraient évidemment aussi être soumises au Conseil fédéral si les conditions énumérées à l'art. 80, al. 3, LRens, étaient (exceptionnellement) remplies.

Chapitre 2: Recherche d'informations

Section 1 : principes

Art. 12 Opérations

L'introduction du terme «opérations» est nécessaire, car dans le cadre des mesures de recherche soumises à autorisation, l'obligation légale d'informer les personnes surveillées (ou le report voire la dérogation à cette obligation) au sens de l'art. 33 LRens débute à la fin d'une opération. Le terme d'opérations permet également de distinguer le traitement simple de problématiques relevant du renseignement de la conduite d'une affaire complexe en la matière, aux nombreuses ramifications et faisant l'objet d'une attention particulière de la part des organes de surveillance. Par ailleurs, le SRC doit débuter et terminer formellement les opérations et les documenter séparément Il reste à souligner que les organes de surveillance bénéficient, indépendamment de la qualification d'une opération en termes de processus connexes, d'un accès complet à l'ensemble des informations et documents pertinents ainsi qu'à tous les locaux du SRC.

Art. 13 – 16 Collaboration avec des services nationaux en matière de recherche d'informations et mandats ad hoc, Collaboration avec des services étrangers en matière de recherche d'informations et de mandats ad hoc, Collaboration avec des particuliers en matière de recherche d'informations et mandats ad hoc, Collaboration avec des services étrangers ou des particuliers basés à l'étranger en matière de recherche d'informations et de mandats ad hoc

Selon l'art. 34 LRens, le SRC peut mettre en œuvre lui-même les mesures de recherche d'informations, collaborer à cet effet avec des services nationaux ou étrangers ou mandater ces services, pour autant qu'ils présentent la garantie que la recherche d'informations respectera les dispositions de la présente loi. Lorsque des raisons techniques ou d'accès au renseignement l'imposent, il peut aussi collaborer exceptionnellement avec des particuliers ou leur confier des mandats, pour autant qu'ils présentent la garantie que la recherche d'informations respectera les dispositions de la présente loi.

Il est surtout nécessaire de régler la collaboration en Suisse avec

- des services nationaux,
- des services étrangers,
- des particuliers.

Une recherche d'informations en Suisse conforme à la loi est garantie au sens de l'ordonnance si

- la recherche est exécutée dans le cadre de l'activité ordinaire du service national ou si le service national semble approprié pour la recherche d'informations et dispose en outre des aptitudes et connaissances requises des dispositions légales en vigueur, ou que le SRC l'a instruit en détail à ce propos;
- le service étranger ou le particulier a été informé des dispositions pertinentes en matière de recherche d'informations en Suisse et que ces dispositions lui ont été expliquées dans toute la mesure nécessaire, et que le service étranger ou le particulier s'engage à respecter les dispositions suisses.

Des conditions simplifiées s'appliquent à la collaboration avec des services étrangers ou des particuliers basés à l'étranger en matière de recherche d'informations et de mandats ad hoc. Cette procédure se justifie par le fait que le SRC est en contact avec plus d'une centaine d'autorités étrangères de sécurité partout dans le monde et qu'il doit tenir compte des spécificités propres à chaque pays ainsi que de la souveraineté des services de sécurité étrangers.

Art. 18 Protections des sources

Les principes élémentaires en matière de protection des sources sont déjà inscrits à l'art. 35 LRens. L'ordonnance précise la nature des sources d'informations en matière de renseignement, à savoir les informateurs, les services de renseignement nationaux et étrangers ainsi que les autorités de sécurité avec lesquels le SRC collabore, ainsi que les sources techniques. Pour les cas qui ne sont pas réglés par la loi, l'ordonnance ancre le principe de la pesée des intérêts de la source à protéger et des services qui demandent des informations. Un informateur doit être protégé intégralement lorsqu'il est exposé à un grave danger menaçant son intégrité physique ou psychique. Comme jusqu'à présent, les proches des informateurs sont aussi protégés lorsque les circonstances l'exigent (membres de la famille, conjoint/e, etc.). Les sources techniques doivent être protégées de sorte à ce qu'une transmission des données ne risque pas de menacer la mission du SRC. A noter que la protection des sources est d'une importance capitale pour le SRC, car s'il n'est pas en mesure de la garantir suffisamment, il serait sans nul doute très rapidement exclu de l'échange international d'informations avec les conséquences que cela implique pour la sécurité de la Suisse. La collaboration prévue avec fedpol au cas par cas à l'al. 4 au sujet des informateurs repose sur

2 RS **172.010**

l'art. 14 de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration[3], et concerne des mesures de protection. Le SRC assume la totalité des coûts. Une solution est convenue au cas par cas d'entente avec l'AFF et fedpol.

Section 2 : obligation de fournir et de communiquer des renseignements

L'obligation de fournir et de communiquer des renseignements est régie pour l'essen-tielle par la réglementation existante selon des procédures bien rodées. Le SRC collabore étroitement avec les cantons tout en leur laissant une grande marge d'auto-nomie dans l'accomplissement de leurs tâches.

Comme l'appréhension de personnes à des fins d'identification et d'interrogatoire est effectuée exclusivement par des membres d'un corps de police cantonal conformément aux nouvelles dispositions de l'art. 24 LRens, elle n'a pas besoin d'être réglementée par voie d'ordonnance.

Art. 19 Abs. 2 Obligation de fournir des renseignements en cas de menace concrète

La liste des organisations auxquelles la Confédération ou les cantons ont confié des tâches publiques à l'annexe 1 a été complétée par l'Autorité fédérale de surveillance des marchés financiers, la Commission fédérale de l'électricité et la Commission fédérale de la communication.

Conformément à l'art. 20, al. 4, LRens, le Conseil fédéral détermine dans une liste non publique les événements et les constatations qui doivent être communiqués spontanément au SRC. Il définit l'étendue de l'obligation et règle la procédure de communication. Contrairement aux explications (parfois contradictoires) figurant dans le message relatif à la loi sur le renseignement suite à une erreur rédactionnelle, cette liste non publique peut contenir des communications obligatoires en lien avec des opérations ou des constatations qui ne doivent pas être publiées pour des raisons de maintien du secret, ainsi que des informations non soumises au secret. Comme l'obligation de communiquer concerne la recherche d'informations, il convient de tenir également compte de l'art. 67 LRens, selon lequel les documents officiels portant sur la recherche d'informations ne sont expressément pas soumis au principe de la transparence et ne doivent donc pas être publiés.

Section 3 : mesures de recherche soumises à autorisation

La réglementation des mesures de recherche soumises à autorisation est très détaillée et complète dans la loi. Il n'est donc quasiment pas nécessaire de l'approfondir au niveau de l'ordonnance.

Art 20 Fouilles de locaux, de véhicules ou de conteneurs

Il convient de documenter les fouilles de locaux, de véhicules ou de conteneurs. Comme la fouille intervient de façon discrète, autrement dit en l'absence de la personne concernée, la documentation sert en premier lieu à réfuter d'éventuels reproches ultérieurs à l'encontre du SRC et/ou des demandes de dommages-intérêts. Si les conditions sur place le permettent, la documentation peut recourir à des enregistrements visuels et sonores. Pour les autres mesures de recherche soumises à autorisation, il est possible de renoncer explicitement à l'obligation de documentation s'il est possible d'exclure toute accusation d'utilisation abusive à l'encontre du SRC ou si la probabilité en est très réduite.

Art. 21 Procédure d'autorisation et aval

Le SRC et le DDPS documentent la procédure d'autorisation et la procédure d'aval afin de pouvoir les retracer à tout moment.

Art. 22 Protection de secrets professionnels

La protection des personnes au sens de l'art. 28 LRens qui appartiennent à l'un des groupes professionnels visés aux art. 171 à 173 Code de procédure pénale (CPP)[4] est précisée au niveau de l'ordonnance: Si une personne cible appartenant à l'un des groupes professionnels visés aux art. 171 à 173 CPP est surveillée en application de l'art. 27 LRens, il y a lieu de veiller, par une sélection préalable des données collectées (triage), qu'aucun secret professionnel ne soit révélé au SRC, excepté si la menace concrète intervient de manière ciblée sous prétexte de secret professionnel. Le cas échéant, le SRC doit l'indiquer dans la procédure d'autorisation et demander ladite sélection. Le tri et la destruction des données protégées sont soumis à la surveillance du Tribunal administratif fédéral. Il n'est pas autorisé d'ordonner une mesure de recherche soumise à autorisation à l'encontre d'un tiers appartenant à l'un des groupes professionnels visés aux art. 171 à 173 CPP.

Section 4: infiltration dans des systèmes et réseaux informatiques à l'étranger

Art. 23

En vertu de l'art. 37, al. 1, LRens, le SRC peut infiltrer des systèmes et réseaux informatiques qui se trouvent à l'étranger et qui sont utilisés pour attaquer des infrastructures critiques en Suisse. Le Conseil fédéral décide de la mise en œuvre d'une telle mesure. Il convient de distinguer l'infiltration dans des systèmes et réseaux informatiques étrangers au sens de l'art. 37, al. 2, LRens, en vue de rechercher les informations qu'ils contiennent ou qui ont été transmises à partir de ces systèmes et réseaux. Le cas échéant, c'est le chef du DDPS qui décide de mettre en œuvre une telle mesure après avoir consulté le chef du DFAE et le chef du DFJP.

Pour alléger la charge des décideurs et assurer une prise de décision rapide, l'ordon-nance prévoit que la consultation du chef du DFAE et du chef du DFJP ainsi que la décision subséquente du chef du DDPS puissent intervenir une seule fois pour le traitement d'un cas ou d'un groupe de cas (p. ex. enlèvement de XY). Une telle autorisation pour un cas ou un groupe de cas comprend si nécessaire plusieurs infil-trations dans des systèmes et réseaux informatiques d'une seule ou de plusieurs

[3] RS **172.010.1**
[4] RS **312.0**

personnes (si elle est ou elles sont en lien avec le cas ou le groupe de cas autorisé). En d'autres termes, il s'agit d'une autorisation globale bien que limitée à un cas ou un groupe de cas (autorisation globale pour un cas ou un groupe de cas comme l'infil-tration dans les systèmes informatiques des ravisseurs pendant toute la durée d'un enlèvement, ou après une cyberattaque déjouée, autorisation à durée limitée d'infil-tration dans les systèmes informatiques du pirate pour découvrir son identité et/ou d'autres attaques et/ou victimes).

Section 5: exploration du réseau câblé

Le SRC confie des mandats d'exploration du réseau câblé. Ce n'est pas lui qui procède à l'exploration du réseau câblé, mais le Centre des opérations électroniques (COE) de la Base d'aide au commandement de l'armée, qui est le service exécutant. Le COE s'assure d'une part, par le biais de mesures internes, que la mission est effectuée exclusivement dans le cadre de l'autorisation délivrée par le Tribunal administratif fédéral. D'autre part, il acquiert les installations techniques nécessaires et fonctionne comme interlocuteur des exploitants de réseaux filaires et des opérateurs de télécommunications. Ces derniers accordent en tout temps au COE l'accès à leurs locaux afin qu'il puisse installer les composants techniques nécessaires à la collecte des données techniques et à l'exécution des mandats d'exploration du réseau câblé.

Aucun contenu de communication ni aucune donnée relative aux communications établies n'est enregistré dans le cadre de la collecte des données techniques par les exploitants de réseaux filaires et les opérateurs de télécommunications ou par le COE. Des données statistiques sur les flux de données provenant des réseaux câblés sont par contre relevées en permanence. Ces données statistiques permettent d'identifier les pays émetteurs et récepteurs ainsi que les protocoles et procédés techniques utilisés. Elles sont suffisantes pour déterminer le type et la quantité d'équipements nécessaires en cas d'exploitation ultérieure des données. Ces données statistiques sont requises pour adresser au Tribunal administratif fédéral une demande fondée et conforme au droit. Elles permettent de lui prouver, en cas d'utilisation avérée, auprès de quels exploitants de réseaux filaires et opérateurs de télécommunications se trouvent des données potentiellement intéressantes.

Par ailleurs, des données enregistrées dans le cadre d'une exploration radio peuvent aussi être utilisées au profit de mandats d'exploration du réseau câblé.

Les contacts du COE avec des services étrangers relevant du renseignement inter-viennent par l'intermédiaire du SRC.

Art. 29 Abs. 2 et 3 Traitement des données

La notion de données désigne l'ensemble des saisies issues de l'exploration radio et de l'exploration du réseau câblé (terme générique). Elle regroupe d'une part le terme de communication, qui se réfère à proprement parler au contenu de communication des données saisies (voies, textes, images, etc.), et d'autre part le terme de données relatives aux communications établies. Les données relatives aux communications établies constituent la partie des données saisies qui n'est pas contenue dans la communication à proprement parler et qui est complétée par des informations tirées des systèmes de saisie ("Session Related Informations", par ex. le moment de la saisie). Il convient également de distinguer le terme de résultat, qui n'est pas constitutif de la notion de données. Il désigne les produits (autrement dit, les informations conformes au mandat) établis sur la base des données et qui sont transmis au SRC.

Les délais de 18 mois (destruction des communications enregistrées) et de 5 ans (destruction des données relatives aux communications établies) sont identiques à ceux qui s'appliquent à la destruction des communications et des données de liaison dans le cadre de l'exploration radio (cf. art. 4 de l'ordonnance sur la guerre électronique et l'exploration radio, entièrement révisée à fin 2012, OGE; RS 510.292). Comme pour l'exploration radio, le délai de 18 mois pour l'exploration du réseau câblé correspond à la durée dans laquelle une recherche rétroactive, c'est-à-dire la recherche dans des contenus de communications enregistrées dans le cadre d'un nouveau mandat d'exploration du réseau câblé ou d'un mandat placé sous un nouvel angle, peut se révéler pertinente du point de vue du renseignement ou offrir une rétrospective intéressante en matière de renseignement (délai de 5 ans).

Art. 30 Indemnisation des exploitants des réseaux filaires et des opérateurs de télécommunications

Les exploitants de réseaux câblés et les opérateurs de télécommunications ont droit à une rémunération pour les prestations qu'ils fournissent dans le cadre de l'exploration du réseau câblé. La révision actuelle de la Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication[5] a conservé la pratique en vigueur selon laquelle l'utilisation de l'infrastructure de surveillance ne peut pas faire l'objet d'une indemnisation totale des coûts qu'elle a induits et que seule une indemnisation adéquate peut être réclamée; ce principe doit aussi s'appliquer aussi à l'exploration du réseau câblé, faute de quoi il n'existe aucune incitation pour les exploitants de réseaux câblés et les opérateurs de télécommunications à rechercher des solutions avantageuses.

Chapitre 3: Protection des données et archivage

Section 1 : dispositions particulières relatives à la protection des données et exceptions au principe de la transparence

La réglementation de la communication de données personnelles en vertu du droit actuel ayant fait ses preuves, elle est largement reprise par l'ordonnance.

Art. 32 Communication de données personnelles par les autorités d'exécution cantonales

L'art. 31 repose en premier lieu sur l'art. 46, al. 3, LRens, qui règle le traitement des données par les cantons.

La communication de données au sens de l'al. 3 de l'ordonnance revêt un caractère exceptionnel afin de permettre une action rapide des autorités dans les situations d'urgence ou de légitime défense. Les autorités d'exécution cantonales décident de

5 RS **780.1**

leur propre chef du niveau d'urgence de la situation. Conformément à l'al. 4, le SRC doit être informé immédiatement comme dans les autres cas d'urgence.

Art. 33 Communication d'informations aux autorités de poursuite pénale Renvoi à l'art. 112CPP pour les autorités de poursuite pénale dans le domaine civil

L'Office de l'auditeur en chef, la justice militaire et la police militaire appartenant aux autorités de poursuite pénale dans le domaine militaire, une base légale est nécessaire pour l'échange d'informations.

Art. 35 Exception au principe de la transparence

La nouveauté par rapport à la situation actuelle est que selon l'art. 67 LRens, la loi sur la transparence du 17 décembre 2004[6] ne s'applique pas (plus) à l'accès aux documents officiels portant sur la recherche d'informations. L'ordonnance précise que les documents officiels qui permettraient de tirer des conclusions directes ou indirectes sur la recherche d'informations sont concernés par la disposition d'exception. Elle énumère à titre d'exemple trois cas d'application particuliers et non exhaustifs (informations sur les moyens opérationnels, méthodes et contacts du SRC p. ex.). Concernant les produits du renseignement mentionnés à la let. a (rapport au Conseil fédéral par ex.), il convient de préciser qu'il ne s'agit que des produits dont le contenu porté à la connaissance de personnes non autorisées pourrait nuire aux intérêts nationaux. Comme la liste n'est pas exhaustive, cette disposition d'exception peut s'appliquer à d'autres documents officiels, notamment ceux qui permettent de tirer des conclusions sur les techniques d'enquête dans le cadre de la recherche d'informations ou de déduire d'autres mesures de recherche d'informations.

2. Abschnitt. Archivage

Art. 36 Archivage

Se référer aux commentaires suivants sur l'art. 57*a*.

Chapitre 4: Pilotage politique et interdictions

Art. 37 Sauvegarde d'autres intérêts nationaux importants

La loi sur le renseignement confie le domaine touchant de près à la police de sécurité au DDPS. Les demandes concernant la sauvegarde d'autres intérêts nationaux importants devraient donc provenir en premier lieu de l'extérieur du DDPS. Il est ainsi possible que le Département fédéral des finances demande l'intervention du SRC pour obtenir des informations sur les intentions d'Etats susceptibles de vouloir nuire à la place financière suisse pour des motifs économiques.

Chaque département et chaque canton peuvent déposer une demande. A titre de prescription d'ordre, l'ordonnance prévoit une consultation préalable du SRC pour s'assurer que l'intervention demandée soit réalisable . La demande doit comporter entre autres des indications sur la menace concrète ainsi que la durée de la mission du SRC, ou la décision du Conseil fédéral quant à la durée d'engagement. S'il n'est pas possible de limiter la durée de la mission en jours, mois ou années, il convient de définir à quel intervalle l'intervention du SRC doit être réexaminée et/ou quels critères sont déterminants pour la poursuite ou la fin de ladite intervention. Les moyens de renseignement à déployer doivent aussi être définis. Avant tout, il y a lieu de décider s'il convient de renoncer à certains moyens de renseignement, par exemple l'infiltration dans des systèmes et réseaux informatiques étrangers (art. 37, al. 2, LRens) ou le recrutement d'informateurs à l'étranger.

Pour augmenter les chances de réussite, les missions nécessitant l'attribution de ressources humaines et de compétences particulières doivent s'étendre sur une durée suffisante. Le SRC ne dispose pas d'une réserve de ressources humaines ou finan-cières à cet effet.

Art. 38 und 39 Procédure d'examen et Suspesion de procédure d'examen

La LRens ne prévoit expressément aucune procédure d'examen. Une procédure d'examen sert à déterminer si une personne ou une organisation doit figurer sur la liste d'observation. Le SRC recherche et traite toutes les informations pertinentes en vertu de l'art. 5, al. 8, LRens. La procédure d'examen doit être suspendue dès que la suite des opérations est connue. Cette suspension intervient notamment en cas d'intégration dans la liste d'observation (le soupçon est confirmé), lorsque les indices ayant entraîné la procédure d'examen sont infirmés et que l'intégration dans la liste d'observation n'est pas nécessaire (le soupçon n'est pas confirmé) ou lorsqu'aucune information nouvelle importante en matière de sûreté n'a pu être obtenue en l'espace de deux ans à compter de l'ouverture de la procédure d'examen (le soupçon initial n'a pas résisté à l'épreuve du temps). Une procédure d'examen suspende peut toujours être rouverte si les conditions sont remplies.

Art. 41 Interdiction d'exercer une activité

En vertu de l'art. 73, al. 3 , LRens, le département qui présente la demande d'interdiction doit vérifier régulièrement si les conditions justifiant l'interdiction continuent d'être remplies. L'ordonnance fixe une fréquence de contrôle annuelle. Cette fréquence s'avère adéquate parce qu'une fois prononcée, une interdiction d'exercer une activité repose sur un arrêté du Conseil fédéral et, de fait, sur un examen minutieux de la situation des faits et la situation juridique, est limitée à cinq ans au plus et soumise à un contrôle approfondi par le Tribunal administratif fédéral, dont la décision peut faire l'objet d'un recours auprès du Tribunal fédéral. Seules les activités représentant une menace concrète pour la sûreté intérieure ou extérieure et servant à promouvoir des activités terroristes ou l'extrémisme violent peuvent être interdites. L'interdiction se limite donc dès le début pour la personne concernée aux activités indésirables du point de vue de la politique de sécurité. Les autres activités demeurent toujours possibles. Par ailleurs, même si l'autorité n'a plus connaissance d'activités susceptibles d'être interdites, il n'en découle pas forcément la levée de l'interdiction (parce que la personne en question a adapté en conséquence son comportement en matière de communication, qu'elle parvient à le cacher aux autorités ou encore qu'elle transmet ses

6 RS **152.3**

directives à des tiers par oral, etc.) La décision de maintien de l'interdiction d'exercer une activité doit donc se limiter en priorité à l'examen des effets de l'interdiction sur les activités terroristes ou l'extrémisme violent du groupement (ou du particulier) concerné, et dont la promotion doit être empêchée par l'interdiction. Un contrôle annuel semble offrir un intervalle adéquat.

Par ailleurs, la nature juridique concrète d'une interdiction d'exercer une activité fait actuellement l'objet d'un examen approfondi par l'Office fédéral de la justice.

Art. 42 Interdiction d'association

En vertu de l'art. 74, al. 2, LRens, une interdiction d'organisations se fonde sur une décision des Nations unies ou de l'Organisation pour la sécurité et la coopération en Europe. Cette condition est remplie au sens de l'ordonnance lorsque l'organisation ou le groupement est mentionné expressément dans la décision (let. a) ou le but et les moyens d'une organisation ou d'un groupement figurant nommément dans la décision coïncident (let. b). La let. b permet au Conseil fédéral de réagir dans les meilleurs délais et avec toute la souplesse requise aux changements rapides de situation, comme en cas de transformation purement formelle d'une menace pour la sécurité de la Suisse (création d'une organisation de camouflage ou de remplacement par ex.) mais conservant le même fond. Le même principe s'applique à l'examen de la prolongation d'une interdiction après l'expiration du délai. Le maintien de l'organisation ou du groupement interdit sur la liste d'observation et la persistance d'une menace concrète pour la sûreté intérieure ou extérieure de la Suisse si l'organisation ou le groupement interdit peut (ou pourrait) poursuivre ses activités sont déterminants pour la décision de prolongation.

L'engagement d'experts dans le cadre de la politique gouvernementale de la Suisse en matière de promotion de la paix, de défense des droits de l'homme et d'aide humanitaire (observateurs électoraux p. ex.) ne sert pas à promouvoir ni à soutenir une organisation ou un groupement interdit et ne représente pas donc pas un comportement répréhensible. Concernant la présence éventuellement nécessaire sur le territoire suisse de personnes punissables (participation à des négociations de paix p. ex.), il convient de trouver une solution tenant compte des particularités de chaque cas en collaboration avec les autorités compétentes en matière de poursuite pénale, les instances politiques et d'autres autorités impliquées.

Chapitre 5: Prestations

Art. 44 Emoluments

Les prestations fournies par le SRC doivent en principe être rémunérées. Comme cela ne semble pas toujours approprié, l'ordonnance prévoit que le SRC puisse renoncer totalement ou au moins réduire ses émoluments dans certaines conditions, notamment lorsque la perception de l'émolument engendre un coût supérieur à la prestation proprement dite ou lorsque d'autres raisons, dans le contexte de la prestation ou concernant le payeur de l'émolument, portent à en déduire que la perception d'un émolument est disproportionnée.

Chapitre 6: Contrôle

Art. 45 Auto-contrôle au sein du SRC

L'al. 4 exerce une fonction transversale par rapport à l'OSIS-SRC: l'application SCC (Sensor Control Center) utilisée pour l'exploitation du système d'information SICO (voir art. 55ss OSIS-SRC) peut aussi être utilisée pour le pilotage d'autres capteurs (IMINT, TECHINT). Les données concernées ne faisant toutefois pas partie du système SICO (exploration radio et exploration du réseau câblé), elles ne peuvent pas être réglées par les dispositions particulières y relatives. Comme ni la partie générale de l'OSIS-SRC ni celle relative au système GEVER ne sont adéquates pour accueillir la réglementation de cette application, elle est intégrée dans le devoir d'auto-contrôle inscrit à l'art. 45 ORens. Par ailleurs, les dispositions de l'ordonnance sur les systèmes d'information et les systèmes de stockage de données du Service de renseignement de la Confédération (OSIS-SRC) règlent le traitement des données personnelles issues de la recherche d'informations.

Chapitre 7: Mesures internes de protection et de sécurité

Concernant les mesures de protection et de sécurité, l'ordonnance reprend en grande partie la réglementation des directives existantes, qui ont fait leurs preuves, et de la pratique.

Art. 47 Service chargé de l'exécution

Le projet d'ordonnance prévoit que le SRC peut faire appel à des tiers pour le contrôle des sacs ou mallettes, des personnes et des locaux. Il ne s'agit pas de déléguer la responsabilité de l'exécution de la mesure (qui incombe totalement au SRC), mais uniquement de recourir à des «auxiliaires» agissant sous la responsabilité du SRC.

Art. 48 Fouilles de personnes et de leurs effets

La compétence du SRC ancrée dans la loi au sens formel en matière de contrôle des effets personnels et des personnes inclut, dans le respect du principe de proportion-nalité, le recours aux moyens de contrainte nécessaires pour procéder aux contrôles en question. Le SRC est habilité à procéder à ces contrôles. S'il s'avère lors du contrôle que les éléments constitutifs d'un crime ou d'un délit (vol de données par ex.) sont réunis, le SRC est autorisé, en vertu de l'art. 218 CPP (Arrestation par des particuliers), à retenir une personne surprise en flagrant délit jusqu'à l'arrivée de la police (arrestation provisoire). Ici aussi, le principe de proportionnalité doit être respecté. Cette mesure ne peut être appliquée que si la situation l'exige, et la force ne peut être utilisée qu'en dernier recours (art. 200 CPP). Une arrestation n'est pas autorisée s'il existe des moyens moins contraignants de poursuivre pénalement une personne. Le contenu du courrier sortant peut aussi faire l'objet de contrôles aléatoires à titre de mesure de protection. Il n'y a pas de violation de la correspondance par poste et par télécommunication, car le contrôle ne concerne pas du courrier privé mais le courrier officiel du SRC (l'expéditeur SRC ouvre le courrier destiné à être envoyé en son nom).

Art. 51 Déploiement d'appareils de transmission et d'enregistrement d'images, utilisation d'appareils électroniques

Les principaux compléments concernent au surplus le déploiement d'appareils de transmission et d'enregistrement d'images dans les locaux d'archivage, chambres fortes et entrepôts ainsi que les zones d'accès aux locaux du SRC. L'ordonnance précise à cet égard d'une part que les personnes concernées doivent être informées, par un panneau indicateur bien visible, de la présence d'appareils de transmission et d'enregistrement d'images, et d'autre part que les enregistrements qui ne sont pas utilisés doivent être effacés le plus rapidement possible, autrement dit après 30 jours en principe, sauf s'ils sont requis pour prouver un cas d'utilisation abusive. Ce n'est qu'à cette condition que les enregistrements peuvent être conservés jusqu'à la clôture définitive de la procédure. Le délai de 30 jours est adapté car il ne s'agit pas, comme dans l'utilisation ordinaire de systèmes de vidéosurveillance, de prévenir des actes de vandalisme, mais bien d'empêcher ou de reconstituer ultérieurement des vols ou manipulations de données, dont la détection prend souvent un certain temps.

Chapitre 8: Armement

Concernant l'armement, l'ordonnance reprend en grande partie la réglementation des prescriptions actuelles.

Art. 53 Autorisation de port d'une arme de service

Le Conseil fédéral détermine les catégories de collaborateurs autorisés à porter une arme en vertu de l'art. 3 LRens. Il s'agit des collaborateurs du SRC encourant un danger particulier dans l'exercice de leurs fonctions. Le directeur du SRC confirme l'appartenance à la catégorie correspondante en autorisant le port d'une arme de service. Sont réputées armes de service les substances irritantes et les armes à feu dont l'utilisation n'est autorisée qu'à des fins d'autoprotection ou dans des cas de légitime défense et d'état d'urgence, dans le respect du principe de proportionnalité.

Chapitre 9: Dispositions finales

Art. 57a Disposition transitoire relative à l'archivage

Une réglementation transitoire (art. 57*a*) est introduite pour les dossiers constitués jusqu'à l'entrée en vigueur de la LRens. Conformément à cette réglementation transitoire, le délai de protection est prolongé de 30 ans (avec notification correspondante aux Archives fédérales suisses) pour tous les dossiers (autrement dit, pas uniquement les dossiers contenant des communiqués de services de sûreté étrangers). Les dispositions de l'art. 68 LRens s'appliquent par contre sans restriction aux données destinées à être livrées aux Archives fédérales suisses après l'entrée en vigueur de la LRens.

Annexe 3 : Communication de données personnelles à des autorités et services suisses

Chiffre 8.3.13

fedpol reçoit du SRC aussi des données personnelles utiles pour assurer la sécurité des passagers voyageant à bord d'aéronefs suisses. La nouvelle loi du 21 décembre 1948 sur l'aviation[7] réglementera les données que fedpol peut traiter pour établir des analyses des risques et de la menace ainsi que des plans d'engagement en lien avec le recours à des préposés à la sécurité dans le trafic aérien, les droits d'accès et la communication de données (art. 21b ss. du projet LA; en consultation à l'automne 2015). La communication de données par le SRC à fedpol doit toutefois être régie dans l'ORens.

Annexe 4 : Abrogation et modification d'autres actes

Abrogation:

1. Ordonnance du 1er décembre 1999 concernant les prestations financières allouées aux cantons pour le maintien de la sûreté intérieure[8]

Avec la loi sur le renseignement, la plupart des réglementations contenues dans l'ordonnance sur les prestations financières allouées aux cantons pour le maintien de la sûreté intérieure (Ordonnance LMSI sur les prestations financières) n'ont plus lieu d'être. Les art. 3, 4 et 4a restants devraient être régis par l'ordonnance sur la sécurité relevant de la compétence fédérale (RS 120.72) et l'art. 5 par l'ordonnance concernant l'exécution de tâches de police judiciaire au sein de l'Office fédéral de la police (RS 360.1). L'ordonnance LMSI sur les prestations financières peut donc être abro-gée.

Modification:

2. Ordonnance du 27 juin 2001 sur la sécurité relevant de la compétence fédérale[9] (OSF)

La modification de l'OSF est induite par la modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure[10] (LMSI) dans le cadre de la loi sur le renseignement. Les modifications matérielles entraînent en outre des adaptations formelles.

Art. 2, al. 4, reprend la réglementation actuelle de l'art. 3, al. 2, let. a.

L'art. 3 a un nouveau titre et se limite à des commentaires sur le droit de domicile. L'al. 1 reprend la disposition concrète sur l'exercice du droit de domicile comme elle est formulée dans le texte de loi actuel (art. 23, al. 2, LMSI), mais d'une manière plus générale («Confédération»). L'al. 2 reprend le contenu de l'al. 1 actuel. L'actuel al. 2, let. b, doit être abrogé en raison de l'abrogation de la base légale correspondante (actuel art. 23, al. 1, let. c, LMSI).

7 SR **748.0**
8 RS **120.6**
9 RS **120.72**
10 RS **120**

L'art. 6, al. 1bis et 1ter ainsi que l'art. 7, al. 1bis, sont adaptés à la nouvelle base légale (art. 23, al. 1bis, LMSI). Les personnes protégées par le droit international sont énumérées séparément à l'art. 6, al. 1bis, let. c, car d'autres bases légales s'appliquent, notamment plusieurs conventions internationales[11] et le droit coutumier international, en corrélation avec l'art. 4 de la loi du 22 juin 2007 sur l'Etat hôte[12], ainsi que l'art. 24 LMSI.

L'abrogation de l'ordonnance LMSI sur les prestations financières entraîne l'intégration dans l'OSF des dispositions relatives aux indemnités versées aux cantons qui accomplissent dans une large mesure des tâches de protection des personnes et des bâtiments (art. 28, al. 2, LMSI). Les nouveaux art. 12*a* à 12*c* OSF correspondent aux actuels art. 3 à 4a de l'ordonnance LMSI sur les prestations financières.

L'art. 13 concrétise la nouvelle base légale formelle avec les art. 23*a*–23*c* LMSI. Il porte sur le système d'information et de documentation du Service fédéral de sécurité (SFS) de fedpol. Le SFS se procure des données sur des événements pertinents du point de vue de la sécurité et de personnes en lien avec ces événements et procède à leur traitement conformément à la section 5 de la LMSI.

Les renvois explicites actuels dans *l'art. 15, al. 2 et 3* (vers l'art. 23, al. 2, LMSI, et l'art. 20 de l'ordonnance sur la protection des données, et art. 23 de l'ordonnance sur l'informatique et la télécommunication dans l'administration fédérale) ne sont pas repris car ces actes ont été modifiés ou abrogés. Le renvoi dans *l'al. 3* à la sécurité des données comprend toutes les dispositions en matière de protection des données. Pour tenir compte de la situation actuelle, *l'al. 2* précise que des personnes exerçant un droit de domicile dans les bâtiments de la Confédération, peuvent demander au SFS d'utiliser des appareils de prise de vues et d'enregistrement d'images dans et à l'extérieur de ces bâtiments afin d'en surveiller les environs immédiats. La nouvelle réglementation dans l'art. 23*a*, al. 3, LMSI, selon laquelle les données sont détruites au plus tard cinq ans après que les personnes ou bâtiments concernés n'ont plus besoin d'être protégés doit être explicitée pour les enregistrements visuels. Le délai actuel fixé à *l'al. 5* pour la destruction des signaux d'image enregistrés contenant des données concernant des personnes (au plus tard deux semaines après leur enregistrement) s'est avéré nettement trop court dans les cas où les données étaient saisies dans le cadre de procédures pénales, civiles ou administratives. Conformément à l'art. 15, al. 4, les données du SFS ne peuvent être mises à disposition qu'en vertu d'une décision judiciaire. Dans la pratique, il n'est quasiment pas possible qu'un événement (effraction p. ex.) soit découvert et instruit et qu'une décision judiciaire soit notifiée et entrée en force dans un délai de 14 jours. Avec la prolongation du délai à 30 jours, les données ne doivent donc plus être détruites après 14 jours déjà.

5. Ordonnance du 30 novembre 2001 concernant l'exécution de tâches de police judiciaire au sein de l'Office fédéral de la police[13]

Comme déjà mentionné au ch. 1, l'art. 5 de l'ordonnance LMSI sur les prestations financières est entièrement remanié dans *l'art. 10a de l'ordonnance concernant l'exécution de tâches de police judiciaire au sein de l'Office fédéral de la police.*

7. Ordonnance du 15 octobre 2008 sur le système informatisé de la Police judiciaire fédérale[14]

Le Service de renseignement de la Confédération (SRC) accède au système RIPOL pour éviter les dangers pour la sécurité publique au sens de la loi sur le renseignement et en vertu de *l'art. 5. let. j, de l'ordonnance du 15 octobre 2008 sur le système de recherches informatisées de police*[15] (Ordonnance RIPOL), pour la recherche du lieu de séjour de personnes et la recherche de véhicules ainsi qu'à des fins de surveillance discrète ou de contrôle ciblé de personnes et de véhicules, ce qui est nouveau. Cette modification découle de l'adaptation de l'art. 15, al. 4, let. i, de la loi fédérale sur les systèmes d'information de police de la Confédération (LSIP ; RS 361).

8. Ordonnance du 8 mars 2013 sur la partie nationale du Système d'information Schengen (N-SIS) et sur le bureau SIRENE16

Conformément à l'art. 7, let. h, de l'ordonnance sur la partie nationale du Système d'information Schengen (N-SIS) et sur le bureau SIRENE, les unités du Service de renseignement de la Confédération compétentes pour l'exécution de la loi sur le renseignement ont accès aux données du SIS pour la recherche du lieu de séjour de personnes et la recherche de véhicules ainsi qu'à des fins de surveillance discrète ou de contrôle ciblé de personnes et de véhicules, ce qui est nouveau.

3 Commentaires des dispositions OSIS-SRC

Au sujet de la structure

La structure du projet repose en grande partie sur l'ordonnance du 8 octobre 2014 sur les systèmes d'information du Service de renseignement de la Confédération[17] (OSI-SRC). Pour des raisons de transparence et de cohérence, les dispositions générales ont par ailleurs été divisées en dispositions générales relatives au traitement des données et à l'archivage ainsi qu'en dispositions générales relatives à la protection et à la sécurité des données.

Les dispositions particulières applicables aux systèmes d'information du SRC sont développées dans les sections 4 à 12. La section 13 est dédiée aux systèmes de stockage, tandis que la section 14 contient les dispositions finales. Le catalogue des

11 Art. 39 de la Convention de Vienne du 18 avril 1961 sur les relations diplomatiques (RS **0.191.01**);
Art. 53 de la Convention de Vienne du 24 avril 1963 sur les relations consulaires (RS **0.191.02**);
Art. 43 de la Convention du 8 décembre 1969 sur les missions spéciales (RS 0.191.2)
12 RS **192.12**
13 RS **360.1**
14 RS **361.0**
15 RS **361.0**
16 RS **362.0**
17 SR **121.2**

données personnelles ainsi que les droits d'accès individuels aux systèmes d'information et de stockage de données sont réglés aux annexes 1 à 18.

Section 1 : Objet et définitions

Art. 1 Objet

L'art. 1 énumère les systèmes d'information et de stockage de données régis par le projet d'ordonnance. La base légale formelle des systèmes d'information est énoncée aux art. 47 ss LRens. Les systèmes de stockage de données sont régis aux art. 36, al. 5, et 58 LRens.

Art. 2 Définitions

La terminologie a été reprise en grande partie de l'OSI-SRC en vigueur.

La définition de «tiers» a été reformulée pour davantage de clarté, mais reste identique sur le fond. L'utilisation de ce terme lors de la saisie, comme cela a été le cas jusqu'à présent, dans le système d'information « Sécurité intérieure » (ISIS) est prévue à l'avenir dans le système d'analyse intégrale pour l'extrémisme violent (IASA-EXTR).

L'application SIDRED et le réseau SiLAN sont actuellement décrits aux art. 4 et 10 OSI-SRC.

Section 2 : Dispositions générales relatives au traitement des données et à l'archivage

Art. 3 Classement de données

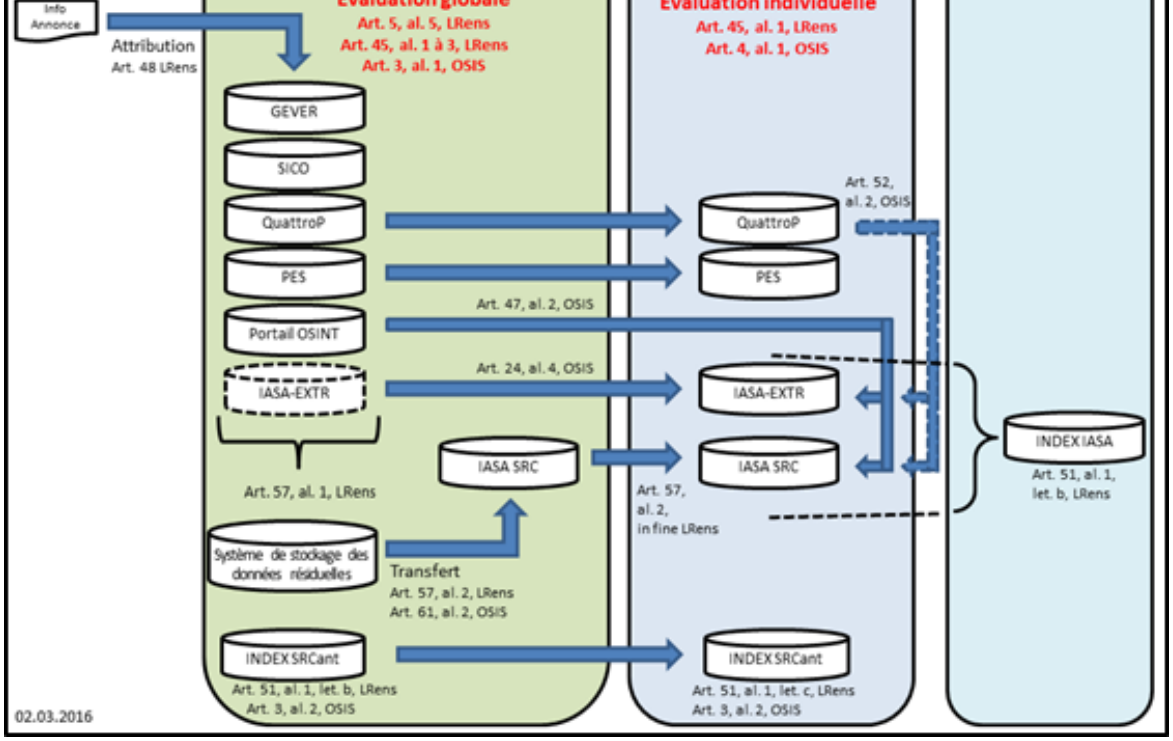
L'al. 1 prévoit que les collaborateurs chargés du tri lors de l'attribution des données au portail ROSO et au système de stockage des données résiduelles examinent s'il y a suffisamment d'éléments indiquant qu'elles ont une relation avec les tâches visées à l'art. 6 LRens. Les communications portant sur diverses données personnelles sont alors évaluées dans leur globalité. Comme toutes les données communiquées de façon non automatisée au SRC passent par les collaborateurs chargés du tri à l'entrée, ces derniers ne peuvent pas examiner en détail chaque communication. Ils sont toutefois parfaitement en mesure d'évaluer les sources fournissant des données et de procéder à l'examen susmentionné en fonction de l'objet de la communication. Pour les communications entrantes, il s'agit en partie de réponses ou de résultats en lien avec des mandats, ce qui en facilite l'évaluation. De plus, cela répond à la systématique du projet d'ordonnance que seules les données classées ne puissent être utilisées ou transmises avant d'avoir été versées dans le système d'analyse intégrale (IASA SRC) ou IASA-EXTR SRC au terme d'un examen approfondi et d'une saisie structurée. Si les collaborateurs chargés du tri des données entrantes ont des doutes, ils sont tenus d'en vérifier le contenu. Ils peuvent aussi faire appel à des collaborateurs en charge de la saisie des données ou à des spécialistes d'autres domaines. Comme c'est déjà le cas aujourd'hui, les données dont les résultats sont négatifs doivent être détruites si elles proviennent d'une autorité d'exécution cantonale.

Les autorités d'exécution cantonales procèdent au même contrôle lors du stockage de données dans le système INDEX SRC (voir al. 2).

La technique ROC est conforme au droit en vigueur. La Délégation des Commissions de gestion (DélCdG) approuve aussi cette procédure moyennant l'observation de certaines obligations. La DélCdG demande que le droit des personnes concernées d'être informées s'applique à toutes les personnes apparaissant dans le système ISIS suite à une recherche plein texte. En cas de suppression de données personnelles dans les systèmes IASA/IASA-EXTR, elle demande aussi que tous les passages en lien avec la personne concernée contenus dans des communications soient effacés. En outre, les communications concernant les activités politiques de personnes ne devraient pas être accessibles par une recherche plein texte si rien n'indique que lesdites personnes pratiquent ces activités dans le but de nuire à l'Etat. La possibilité de détruire des documents originaux traités par la reconnaissance optique de caractères (ROC) à des fins de recherche ainsi que des documents au format papier numérisés et classés en tant que documents originaux est conforme au droit actuellement en vigueur (voir al. 3 et 4 du projet d'ordonnance, et art. 5 OSI-SRC).

Art. 4 Examen individuel et saisie de données personnelles

Selon l'art. 45, al. 1 et 2, LRens, le SRC évalue la pertinence, l'exactitude des données personnelles et leur relation avec les tâches visées à l'art. 6 LRens avant de les saisir dans l'un de ses systèmes d'information. Cette obligation ne concerne pas que les collaborateurs du SRC chargés de la saisie des données (voir al. 1), mais désormais aussi les collaborateurs des autorités d'exécution cantonales en charge de la saisie de données provenant d'enquêtes préalables dans le système INDEX SRC (voir al. 2). Cette appréciation requiert une formation adéquate des collaborateurs des autorités d'exécution cantonales. Comme c'est déjà le cas aujourd'hui, les données dont les résultats sont négatifs doivent être détruites si elles proviennent d'une autorité d'exécution cantonale.



Art. 5 Octroi et retrait des droits d'accès

Comme le prévoit le droit actuel (voir art. 3 OSI-SRC), les droits d'accès à un système d'information ne sont accordés qu'à la suite d'une demande individuelle et à titre personnel (voir al. 1). Cette disposition s'applique désormais également aux systèmes de stockage visés à l'art. 1, al. 2, du projet d'ordonnance. L'accès au système PES peut aussi être octroyé selon les fonctions exercées par la personne. En effet, un accès à ce système doit pouvoir être accordé rapidement à un cercle de personnes dont l'identité n'est pas connue au préalable en cas d'événement particulier. En outre, il est courant que des services de piquet externes dont les membres changent constamment doivent y accéder. En l'occurrence, l'octroi individualisé des droits d'accès n'est ici pas réalisable avec des moyens raisonnables. L'individualisation des droits d'accès intervient plutôt au niveau de la fonction. Etabli en premier lieu uniquement pour une fonction donnée, le profil d'accès est attribué à une personne précise. L'organisation des utilisateurs est tenue de documenter l'identité des personnes qui accèdent au système PES. Cette mesure garantit la traçabilité des accès en tout temps.

Il est désormais explicitement que la demande doit aussi préciser, outre les coordonnées personnelles et la fonction de la personne, la relation avec un but inscrit dans la LRens (voir al. 2). Cette disposition est conforme à la pratique en vigueur. Elle constitue une condition impérative pour l'examen formel.

Ce n'est d'ailleurs plus le responsable de l'unité de direction (voir al. 3) qui est compétent pour l'examen formel des demandes d'accès. Conséquence: les autorisations d'accès pour l'ensemble du SRC ainsi que pour tous les systèmes d'information et de stockage de données sont octroyées de façon centralisée et selon des critères identiques. Le retrait de droits d'accès inutilisés pendant 6 mois est aussi prévu explicitement (voir al. 4). Le service de gestion des applications du SRC est déjà familier des mandats de ce type.

L'al. 5 précise que le SRC n'est compétent que pour l'exécution des droits d'accès aux systèmes d'information qu'il exploite lui-même.

Art. 6 Accès à plusieurs système et classements temporaires

Les autorisations régies par les al. 1 et 2 en lien avec l'accès à plusieurs systèmes (concerne tous les systèmes d'information), la saisie dans plusieurs systèmes (ne concerne que IASA SRC et IASA-EXTR SRC) ainsi que la fonction de recherche et de distribution d'informations sont conformes au droit actuel (voir art. 4 OSI-SRC). Les systèmes de stockage de données visés à l'art. 1, al. 2, du projet d'ordonnance sont intentionnellement exclus car ils ne sont accessibles qu'à des spécialistes et ne doivent pas être mis en réseau avec les systèmes d'information du SRC.

L'al. 3 précise qu'en vue du pilotage de la recherche d'informations ou de l'analyse opérationnelle dans le cadre de projets thématiques limités dans le temps (groupes de travail, cellules de crise), des copies des données issues des systèmes d'information et de stockage de données du SRC peuvent être versées séparément et à titre temporaire dans le réseau SiLAN, afin de n'être accessibles qu'aux membres du projet en question. Cette mesure peut être ordonnée pour remplir le devoir de protection des sources inscrit à l'art. 35 LRens. Elle est conforme à la pratique actuelle et au concept de conservation des données du SRC. Ces évaluations temporaires doivent être autorisées par le SRC. Le concept de protection des données du SRC désigne le service interne chargé de l'octroi de ces autorisations. Au terme des travaux, tous les résultats sont versés dans les systèmes d'information ordinaires du SRC. Les copies de données présentes sur la plate-forme d'analyse sont détruites.

Le service du SRC chargé d'assurer la qualité intègre ces évaluations et leur nécessité dans ses activités de contrôle par sondage.

Des classements temporaires peuvent être réalisés en cas d'enlèvement par exemple. Les collaborateurs chargés de l'affaire ont besoin que toutes les informations en lien avec l'enlèvement puissent être regroupées à partir de d'ensemble des systèmes d'information du SRC pour être analysées ensemble sur une seule plateforme. Au terme des travaux, tous les résultats sont

versés dans les systèmes d'information ordinaires du SRC. Les copies de données présentes sur la plate-forme d'analyse sont effacées.

Art. 7 Données relatives à des opérations

Pour des raisons de protection des sources en vertu de l'art. 35 LRens ou de protection de l'exécution d'une opération, il est souvent nécessaire de traiter les données se rapportant à des opérations (par ex. des informations nécessaires pour l'opération au sujet d'informateurs du SRC, de leur identité, de la sélection, de l'évaluation des risques, de la conduite des sources, etc.) en dehors des systèmes d'information du SRC (voir al. 1). Cette mesure permet de s'assurer que seul un cercle très restreint de personnes a accès à ces données sensibles, autrement dit la personne chargée de la conduite d'une opération ou son suppléant (voir al. 3). Il n'est pas possible de consulter ces données en ligne.

Pour des raisons de sécurité, elles sont conservées dans des conteneurs (coffre-fort par ex.) ou des locaux faisant l'objet d'une protection particulière (avec accès restreint) (voir al. 2).

Les informations fournies par les sources sont anonymisées et intégrées sous la forme de rapports HUMINT dans des données pertinentes en matière de renseignement (IASA SRC ou IASA-EXTR SRC) (voir al. 4). Le droit des personnes concernées d'être informées peut être exercé par le biais de ces systèmes, et il est garanti par les plate-formes des données relatives aux opérations.

Le responsable de la recherche d'informations est tenu de vérifier périodiquement si, compte tenu de la situation actuelle, les données sont encore nécessaires à l'accomplissement des tâches dévolues au SRC en vertu de l'art. 6 LRens (voir al. 5).

Comme c'est le cas aujourd'hui, ces données peuvent être conservées 45 ans au plus (voir al. 6).

Art. 8 Effacement des données

Les dispositions contenues dans cet article respectent le droit en vigueur (voir art. 7 OSI-SRC).

La durée de conservation maximale est régie pour chaque système d'information et de stockage de données. Elle dépend de l'origine, du but du traitement des données et des tâches (voir al. 1).

Les objets doivent être effacés dans les systèmes IASA SRC et IASA-EXTR SRC quand ils ne sont plus en lien avec des informations supplémentaires (documents sources). Cette mesure sert à éviter de répertorier une personne au sujet de laquelle il n'existe pas d'informations supplémentaires et dont la raison de la saisie dans les systèmes en question n'est plus connue (voir al. 2).

Comme c'est aujourd'hui le cas pour le système ISIS, il n'est pas autorisé de classer des documents originaux dans IASA-EXTR SRC s'ils n'ont pas été saisis de façon structurée par documents sources et objets (voir la nouvelle réglementation explicite à l'art. 24, al. 4, du projet d'ordonnance). Inversement, cela signifie qu'un document original doit être effacé lorsque le dernier document source référencé a été effacé (voir al. 3) en raison du contrôle de la saisie prévu pour le système IASA-EXTR SRC, lequel n'est possible que si les documents originaux ont été saisis de façon structurée.

Cette prescription ne s'applique pas à IASA SRC, où des documents originaux non référencés peuvent aussi être conservés au besoin et au plus tard jusqu'à l'expiration de la durée de conservation (voir al. 4).

L'al. 5 ne contient pas de nouveauté sur le fond. Il précise toutefois que seules les données effacées et destinées à l'archivage sont transférées dans un module d'archivage. Les données effacées qui ne doivent pas être livrées aux Archives fédérales suisses (saisies erronées, informations déjà livrées par d'autres services, informations versées dans un autre système d'information qui alimente aussi les Archives fédérales suisses, etc.) ne sont pas enregistrées dans le module d'archivage et doivent être détruites.

Art. 9 Archivage

La remise de données provenant des systèmes d'information du SRC est décrite en détail à l'art. 68 LRens.

Les données provenant d'enquêtes préliminaires et relatives à la gestion des mandats des autorités d'exécution cantonales sont versées dans IASA SRC, IASA-EXTR SRC, INDEX SRC ou dans le système de gestion des affaires (GEVER) si ces données sont nécessaires à l'accomplissement des tâches dévolues au SRC en vertu de l'art. 6, al. 1, LRens. Elles sont livrées par le biais de ces systèmes d'information (voir al. 2). Une double livraison ne se justifie pas.

3. Abschnitt: Dispositions générales relatives à la protection et à la sécurité des données

Art. 10 Droit des personnes concernées d'être informées

Le droit des personnes concernées d'être informées est décrit en détail à l'art. 63 LRens. Aucune disposition d'exécution supplémentaire n'est donc nécessaire au niveau de l'ordonnance.

Art. 11 Contrôle de qualité

L'art. 11 du projet d'ordonnance est fondamental pour le contrôle de qualité des données du SRC. Conformément à l'art. 45, al. 4, LRens, le SRC vérifie périodiquement dans tous les systèmes d'information que les blocs de données personnelles qu'ils contiennent sont encore nécessaires à l'accomplissement de ses tâches. Cette tâche incombe en priorité aux services chargés de la saisie, donc aux spécialistes, ce qui permet une plus grande implication de l'expertise interne, par exemple sur le plan de l'évaluation, dans le processus de contrôle de la qualité. Cette sollicitation des compétences analytiques dans le contrôle qualité des données satisfait une exigence explicite que la DélCdG a formulée dans le rapport de 2010. Cette exigence avait déjà été mise en œuvre par le Conseil fédéral au niveau du contrôle de la qualité des données du SRC provenant de l'étranger dans le cadre de la révision de la LFRC. Les compétences et les délais ainsi que l'ampleur de la vérification périodique sont réglés dans les dispositions particulières applicables à chaque système d'information (voir al. 1).

L'al. 2 correspond à l'actuel art. 13, al. 4, OSI-SRC. L'obligation du contrôle par sondage est toutefois étendue à tous les systèmes d'information (actuellement, ISIS et le système d'information pour la sécurité extérieure ISAS en sont exclus). A la différence de la vérification périodique incombant en priorité aux services chargés de la saisie, seul le service du SRC chargé d'assurer la qualité procède au contrôle par sondage. Il ne vérifie pas toutes les données des systèmes d'information, mais uniquement une sélection établie à des fins de contrôle par sondage. Les résultats des contrôles par sondage sont intégrés dans les recommandations et les formations, en particulier celles destinées aux services chargés de la saisie.

Aujourd'hui déjà, le service de contrôle de la qualité du SRC vérifie après chaque approbation de la liste d'observation par le Conseil fédéral les données dans ISIS en lien avec des organisations et des groupements ayant été radiés de ladite liste et efface les données soumises aux restrictions de traitement des données énoncées à l'art. 3 de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI). Ces vérifications doivent être poursuivies sous le régime de la LRens et concernent aussi les systèmes IASA-EXTRA SRC et IASA SRC, comme mentionné explicitement à l'al. 3. Les restrictions de traitement des données énoncées actuellement à l'art. 3 LMSI sont désormais réglées à l'art. 5, al. 5, LRens.

Si des données sont exceptionnellement recherchées et reliées à des personnes au sens de l'art. 5, al. 5 LRens, en dehors de la liste d'observation ou d'une procédure pénale, il convient de s'assurer qu'elles seront effacées si les activités énumérées à l'art. 5, al. 6, LRens, peuvent être exclues, ou si aucune preuve ne vient confirmer ces activités un an après la saisie des données. Le service de contrôle de la qualité du SRC sera donc chargé de vérifier au moins une fois par année les blocs de données contenant de telles données et de les effacer (voir al. 4). Aujourd'hui, cette vérification ne se fait que dans le cadre d'évaluations globales.

Le service du SRC chargé d'assurer la qualité voit son rôle renforcé par un mandat de formations internes et de contrôles réguliers du respect des dispositions de la nouvelle ordonnance (voir al. 5).

Comme c'est déjà le cas aujourd'hui, le directeur du SRC peut lui confier d'autres contrôles inhérents aux systèmes d'information (voir al. 6).

Art. 12 Responsabilités et compétences

Les responsabilités et compétences n'ont pas changé. Cette disposition correspond à l'actuel art. 13, al. 1 à 3, OSI-SRC, sans trop entrer dans les détails en ce qui concerne l'établissement des règlements de traitement.

Art. 13 Sécurité des données

Les dispositions relatives à la sécurité des données n'ont pas été modifiées par rapport à la situation actuelle et correspondent à l'art. 8 OSI-SRC.

Art. 14 Réseau SiLAN

L'utilisation et l'exploitation du réseau SiLAN ne connaissent pas de modification. Conformément à l'al. 2, toutes les données classifiées peuvent être traitées dans le réseau SiLAN, quel que soit leur échelon de classification.

Désormais, les collaborateurs des autorités d'exécution cantonales auront aussi accès au réseau SiLAN pour y gérer leurs enquêtes préliminaires (INDEX SRCant), leurs rapports et les mandats qui leur sont confiés dans un environnement TIC spécialement prévu à cet effet et sécurisé (voir al. 3). Cette mesure s'est révélée nécessaire puisque les SRCant ne peuvent plus constituer de fichier en vertu de l'art. 46 LRens. Il n'en découle toutefois pas de charges financières.

Art. 15 Transmission de données hors du réseau SiLAN

Cette disposition reprend aussi en grand partie le droit actuel (voir art. 11 OSI-SRC).

Toutefois, ce n'est plus la transmission de données aux cantons qui est financée, mais leur accès au réseau SiLAN et les données qu'ils y traitent (voir al. 2).

Section 4 : Dispositions particulières applicables au système IASA SRC

Art. 16 Structure

La structure du système IASA SRC correspond à celle du système actuel ISAS ou ISIS. L'index pour déterminer si le SRC traite des données sur une personne physique ou morale, un événement ou un objet dans IASA SRC figure désormais séparément à la section 6 des dispositions particulières applicables au système INDEX SRC.

Art. 17 Données

IASA SRC remplace dans une très large mesure les systèmes d'information actuels ISIS et ISAS. Il sert à la saisie, la recherche, l'évaluation et le contrôle de la qualité du point de vue du renseignement des données relatives à des personnes physiques et morales, des objets et des événements en lien avec tous les domaines d'activités du SRC, à l'exception des données sur l'extrémisme violent (voir al. 1).

Les al. 2, 4 et 5 correspondent au droit actuel et ont été repris de l'art. 16, al. 2, 3 et 4, OSI-SRC. Les objets et documents sources ainsi que les relations qu'ils ont entre eux peuvent toujours être visualisés, et cette présentation visuelle peut être enregistrée. L'annexe 1 énumère le catalogue des données personnelles. Le Département fédéral de la défense, de la protection de la population et des sports (DDPS) continue de définir les champs de données (voir l'ordonnance actuelle du DDPS du 27 juillet 2015 sur les champs de données et les droits d'accès aux systèmes d'information ISAS et ISIS[18]).

[18] SR **121.22**

L'al. 3 a été repris de l'art. 6c, al. 2, LFRC. Aujourd'hui aussi, des données personnelles sensibles et des profils de la personnalité peuvent être traités dans ISAS (et ISIS) et cette possibilité devrait être maintenue à l'avenir (voir art. 44, al. 1, LRens).

Art. 18 Saisie des données

Conformément à l'art. 45, al. 1 et 2, LRens, et l'art. 4, al. 1, du projet d'ordonnance, les collaborateurs du SRC (et des autorités d'exécution cantonales) chargés de saisir des données doivent évaluer la pertinence, l'exactitude des données personnelles et leur relation avec les tâches visées à l'art. 6 LRens avant chaque saisie dans les systèmes d'information du SRC. Ils doivent également tenir compte des restrictions de traitement des données énoncées à l'art. 5, al. 5, LRens. Cette disposition s'applique en particulier à la saisie de données personnelles dans IASA SRC (voir al. 1).

Pour simplifier l'évaluation des données et le contrôle subséquent de la qualité, il convient en outre de marquer les données qui sont évaluées comme désinformations ou informations erronées, mais dont la saisie est nécessaire à l'appréciation de la situation ou d'une source (voir al. 2, let. a, et art. 44, al. 2, LRens). Pour la même raison, il convient de marquer les informations qui ont été collectées exceptionnellement en se fondant sur l'art 5, al. 6, LRens, (voir let. b) et les informations qui ont été collectées sur la base de la liste d'observation en vertu de l'art. 72 LRens ou d'une procédure d'examen (voir let. c).

Art. 19 Droits d'accès

Les droits d'accès au système IASA SRC étant réglés à l'art. 49, al. 3, LRens, l'al. 1 renvoie uniquement à cette disposition. Ils correspondent aux droits d'accès actuels pour ISIS et ISAS. Les droits d'accès à INDEX SRC figurent désormais séparément à la section 6 des dispositions particulières applicables au système INDEX SRC.

Comme c'est actuellement le cas, l'al. 2 renvoie à l'annexe 2 pour une vue d'ensemble des droits d'accès individuels.

Art. 20 Vérification périodique des données personnelles

L'al. 1 reprend l'obligation actuelle de vérification périodique des données personnelles dans ISAS (voir art. 18, al. 1, OSI-SRC). La seule différence réside (comme dans tout le projet d'ordonnance) dans la mention de personnes physiques ou morales au lieu de personnes et d'organisations. Les domaines spécialisés responsables de la saisie des données continuent de vérifier périodiquement dans leur domaine de compétence les données enregistrées dans IASA SRC, ce qui permet une plus grande implication de l'expertise interne dans le processus de contrôle de la qualité, comme souligné précédemment.

Les tâches assumées par les personnes chargées de la vérification n'ont pas changé par rapport à la situation actuelle (voir al. 2 et art. 18, al. 2, OSI-SRC). Il est toutefois précisé que le résultat du contrôle n'est consigné que si le bloc de données est modifié ou effacé partiellement. En l'absence de modifications, l'enregistrement du contrôle est automatique.

La réglementation actuelle de l'art. 18, al. 3, OSI-SRC, selon laquelle le contrôle périodique doit avoir lieu chaque fois qu'un bloc de données est complété entraîne dans la pratique une affectation inutile de ressources et des doublons, notamment lorsque le même bloc de données est complété et vérifié plusieurs fois par jour par des collaborateurs différents du SRC. Les règles actuelles relatives à la vérification périodique du système ISIS (voir art. 25 OSI-SRC) ont été reprises pour éviter ces désagréments et en vue du futur traitement d'une grande partie des données ISIS dans le système IASA SRC. Autrement dit, les blocs de données sont vérifiés au plus tard lorsque les délais maximaux depuis la saisie de l'objet dans un système d'information ou depuis la dernière vérification périodique sont échus (voir al. 3). Par contre, les délais maximaux ont été repris des dispositions actuelles (art. 18, al. 3, OSI-SRC) relatives à ISAS: 10 ans dans le domaine du terrorisme international, 15 ans dans le domaine du service de renseignement prohibé et de la prolifération des armes de destruction massive, et 20 ans pour les autres informations importantes relevant de la politique de sécurité. L'al. 4 précise que le délai le plus court s'applique lorsqu'un bloc de données contient des documents sources provenant de plusieurs domaines présentant plusieurs délais maximaux.

Art. 21 Durée de conservation

Les durées de conservation des données dans IASA SRC correspondent exactement à celles qui s'appliquent aujourd'hui au système ISAS (voir art. 19 OSI-SRC).

Section 5 : Dispositions particulières applicables au système IASA-EXTR SRC

Art. 22 Structure

La structure du système IASA-EXTR SRC correspond à celle du système actuel ISAS ou ISIS. L'index pour déterminer si le SRC traite des données sur une personne physique ou morale dans IASA-EXTR SRC figure désormais séparément à la section 6 des dispositions particulières applicables au système INDEX SRC.

Art. 23 Données

Les données figurant dans IASA-EXTR SRC proviennent en majeure partie du système ISIS actuel. IASA-EXTR SRC sert à la saisie, la recherche, l'évaluation et le contrôle de la qualité du point de vue du renseignement des données relatives à des personnes physiques et morales, des objets et des événements en lien avec le domaine de l'extrémisme violent. Les données personnelles traitées dans IASA-EXTR SRC entretiennent une relation avec les groupements déterminés par le Conseil fédéral en vertu de l'art. 70, al. 1, let. c, LRens, (voir al. 1, let. a), ou il s'agit de données relatives à des personnes physiques et morales qui rejettent la démocratie, les droits de l'homme ou l'Etat de droit et qui, pour atteindre leurs buts, commettent des actes de violence, les préconisent ou les soutiennent (voir al. 1, let. b). Si une personne physique ou morale ne présente qu'un lien indirect avec l'extrémisme violent tel qu'il a été défini, elle peut être désignée comme tiers dans IASA-EXTR SRC (voir art. 2, let. g, du projet d'ordonnance). Ses données seront effacées lors du premier contrôle périodique (voir art. 27, al. 4, du projet).

Les al. 2 à 5 sont repris de l'art. 22, al. 3 et 4, ainsi que de l'art. 23, al. 4, OSI-SRC, et correspondent au droit actuel. Le DDPS continue de définir les champs de données.

Art. 24 Saisie des données

L'al. 1 a été repris sans changement de l'actuel art. 23, al. 1, OSI-SRC, et prévoit toujours qu'avant la saisie d'une nouvelle information, il soit vérifié si cette information confirme ou infirme la pertinence de la personne physique ou morale concernée pour l'accomplissement des tâches de renseignement que la LRens assigne au SRC. Si ce n'est pas le cas, le bloc de données est effacé dans IASA-EXTR SRC.

Comme aujourd'hui, les collaborateurs du SRC chargés de saisir les données sont tenus d'évaluer les données saisies et de les marquer pour simplifier leur évaluation ainsi que le contrôle subséquent de la saisie et de la qualité (voir al. 2). Ces opérations interviennent (comme dans IASA SRC) au niveau du document source et concernent les informations incertaines, les informations collectées sur la base de la liste d'observation en vertu de l'art. 72 LRens ou d'une procédure d'examen selon l'art. 38 ORens, et, ce qui est nouveau, les désinformations ou informations erronées ainsi que les informations ayant été exceptionnellement collectées en se fondant sur l'art. 5, al. 6, LRens.

Comme déjà mentionné, les objets relatifs à des personnes physiques et morales qui n'entretiennent qu'un lien indirect avec l'extrémisme violent sont marqués comme tiers. Les objets relatifs à des personnes physiques et morales qui n'appartiennent à aucun groupement déterminé par le Conseil fédéral en vertu de l'art. 70, al. 1, let. c, LRens, doivent aussi être marqués pour que leur nombre puisse être communiqué chaque année au Conseil fédéral (voir al. 3). Des objets ne peuvent être reliés qu'à des personnes physiques et morales présentant un danger pour la sécurité de la Suisse.

L'al. 4 précise désormais explicitement que des documents originaux ne peuvent être classés dans IASA-EXTR SRC que s'ils sont saisis de façon structurée en lien avec des documents sources et des objets. Cette réglementation s'applique aujourd'hui déjà au système ISIS, mais elle ne pouvait être déduite que des dispositions relatives à l'effacement des données ISIS (voir art. 7, al. 4, OSI-SRC). Le contrôle des données saisies prévu dans IASA-EXTR SRC en est la raison, et il ne peut être réalisé que si les données personnelles pertinentes des documents originaux sont saisies de façon structurée (avec document source, objet et relations).

Comme actuellement dans ISIS, les données sont d'abord saisies provisoirement dans IASA-EXTR SRC. Leur statut ne change qu'après le contrôle de la saisie (voir al. 5).

Si un document original contient des données sur des personnes physiques ou morales qui ne figurent pas encore dans IASA-EXTR SRC en lien avec des objets, ces données ne peuvent être utilisées ou transmises qu'après la saisie d'objets correspondants dans le système et le contrôle de la saisie (voir al. 6). Cette réglementation s'applique aujourd'hui à ISIS (voir art. 23, al. 5, OSI-SRC).

Art. 25 Contrôle de la saisie

Cette disposition a été reprise telle quelle de l'art. 24 OSI-SRC. Seul le renvoi aux restrictions de traitement a été actualisé, car elles sont désormais régies par l'art. 5, al. 5, LRens. Le contrôle de la saisie est maintenu, comme pour ISIS aujourd'hui. Les données que le service du SRC chargé d'assurer la qualité n'a pas confirmées doivent être effacées, et le service qui a saisi ces données doit en être informé afin d'améliorer constamment la qualité de la saisie (voir al. 3).

Art. 26 Droit d'accès

Les droits d'accès au système IASA-EXTR SRC étant réglés à l'art. 50, al. 3, LRens, l'al. 1 renvoie uniquement à cette disposition. Ils correspondent aux droits d'accès actuels pour ISIS. Les droits d'accès à INDEX SRC figurent désormais séparément à la section 6 des dispositions particulières applicables au système INDEX SRC.

Comme c'est actuellement le cas, l'al. 2 renvoie à l'annexe 2 pour une vue d'ensemble des droits d'accès individuels.

Art. 27 Vérification périodique des données personnelles

L'instrument de la vérification périodique est repris tel quel des dispositions relatives au système ISIS (voir art. 25 OSI-SRC). Le service du contrôle qualité du SRC vérifie les blocs de données au plus tard cinq ans après leur saisie dans un système d'information du SRC. Il procède ensuite au moins tous les trois ans à une vérification périodique des blocs de données.

Pour des raisons de transparence, l'al. 2 énumère désormais en détail les tâches du service du SRC chargé d'assurer la qualité et précise que le résultat de la vérification doit être consigné. Le contenu et l'ampleur de cette vérification correspondent à ceux de l'évaluation globale du système actuel ISIS.

Comme c'est aujourd'hui le cas pour ISIS (voir art. 25, al. 3, OSI-SRC), les données qui sont marquées comme incertaines ne peuvent continuer à être utilisées jusqu'au prochain contrôle périodique qu'aux conditions inscrites à l'al. 3. Sur demande de l'organe de surveillance du service de renseignement, la durée de conservation des données incertaines a été alignée sur la fréquence de la vérification périodique et s'élève donc à cinq ans désormais.

Les objets marqués comme tiers doivent aussi être effacés après le premier contrôle périodique (voir al. 4). Leur durée de conservation maximale s'élève donc à cinq ans. Cette adaptation à la fréquence de la vérification périodique répond également à une suggestion de l'organe de surveillance du service de renseignement.

Art. 28 Durée de conservation

Les durées de conservation des données dans IASA-EXTR SRC correspondent exactement à celles qui s'appliquent aujourd'hui au système ISIS (voir art. 26 OSI-SRC).

Section 6 : Dispositions particulières applicables au système INDEX SRC

Art. 29 Structure

Le système INDEX SRC est désormais réglementé comme un système d'information à part entière, dont la base légale formelle repose sur l'art. 51 LRens. Il est divisé en trois domaines.

Il comprend un répertoire pour déterminer si le SRC traite des données relatives à une personne physique ou morale, à un objet ou à un événement dans les systèmes IASA SRC ou IASA EXTR SRC (INDEX IASA; voir let. a). Ce répertoire regroupe les mêmes objets en lien avec des personnes physiques ou morales, des objets et des événements dans l'index actuel ISIS et ISAS.

A ce répertoire s'ajoute un système pour classer, saisir, traiter, consulter et évaluer des données provenant d'enquêtes préalables des autorités d'exécution cantonales (INDEX SRCant; voir let. b). C'est ici que les autorités d'exécution cantonales traitent des données et les condensent avant leur transmission au SRC sous la forme de rapport. Même si ces données sont gérées aujourd'hui par les autorités d'exécution cantonales, elles sont soumises aux dispositions de la LMSI et doivent être strictement séparées des autres données des autorités d'exécution cantonales. Elles seront désormais gérées dans un système d'information du SRC, ce qui facilitera leur consultation et leur vérification par le service de contrôle qualité du SRC. Le traitement des demandes de renseignement au sens de l'art. 63 LRens sera aussi simplifié. Cette solution contribue en outre à la sécurité des données (lors de leur transmission au SRC par les autorités d'exécution cantonales).

INDEX SRC comporte également un système pour établir et gérer les mandats, classer les rapports des autorités d'exécution cantonales ainsi que pour classer les produits que le SRC a reçus (voir al. c). Le SRC n'acceptera un rapport des autorités d'exécution cantonales que s'il est conforme au mandat qu'il a attribué ou si ledit rapport a été établi de façon autonome sur la base du mandat général d'information, s'il est en lien avec les tâches visées à l'art. 6 LRens et si les informations du rapport sont pertinentes et exactes. La gestion des mandats, à laquelle s'appliquent les dispositions de la LMSI, incombe aussi à ce jour aux autorités d'exécution cantonales. Les informations que le SRC fait parvenir aux autorités d'exécution cantonales pour l'exécution de leurs tâches légales peuvent aussi être classées dans ce système.

Art. 30 Données

Le contenu de l'index étant réglé en détail à l'art. 51, al. 3, LRens, le projet d'ordonnance renonce à des dispositions d'exécution supplémentaires (voir al. 1).

Comme c'est le cas aujourd'hui (voir art. 16, al. 5, et 22, al. 5, OSI-NDB), l'al. 2 énonce une réserve quant à la protection des sources en vertu de l'art. 35 LRens. Si des raisons commandent de protéger des sources, les données traitées dans IASA SRC ou IASA-EXTR SRC concernant des personnes physiques ou morales ne sont exceptionnellement pas versées dans le système INDEX IASA SRC. Cette pratique a fait ses preuves par le passé.

L'art. 44, al. 1, LRens, autorise aussi les autorités d'exécution cantonales à traiter des données personnelles sensibles et des profils de la personnalité. Par voie de conséquence, INDEX SRC peut aussi contenir de telles données (voir al. 3).

Conformément à la pratique actuelle, les données relatives à des tiers (ISIS) ne sont pas versées dans l'index et ne le seront pas non plus à l'avenir, car des tiers ne peuvent être pertinents en lien avec les tâches du SRC visées à l'art. 6 LRens qu'en relation avec une autre personne physique ou morale. Cette restriction est désormais ancrée expressément à l'al. 4.

Comme dans l'ordonnance actuelle, les al. 5 et 6 spécifient que le catalogue des données personnelles figure en annexe et que c'est le DDPS qui définit les champs de données.

Art. 31 Traitement des données par les autorités d'exécution cantonales

Les autorités d'exécution cantonales sont tenues de respecter les restrictions de traitement des données de la LRens pour le traitement des mandats concrets du SRC et l'établissement autonome de rapports (voir al. 1). Autrement dit, il doit toujours y avoir une relation avec les tâches du SRC visées à l'art. 6 LRens (aussi pour la saisie de données personnelles dans des enquêtes préliminaires au sens de l'art. 29, let. b, du projet d'ordonnance), et les restrictions de traitement des données énoncées à l'art. 5, al. 5, LRens, doivent être respectées.

Lors de la consultation sur la LRens, les autorités d'exécution cantonales avaient exprimé le souhait d'avoir accès à leurs enquêtes préliminaires respectives comme le prévoit l'art. 29, let. b, du projet d'ordonnance, afin de vérifier si une autre autorité d'exécution cantonale a déjà enquêté sur une personne physique ou morale, un objet ou un événement. Le nombre de personnes vivant, travaillant ou actives dans les cantons a considérablement augmenté. La procédure des autorités d'exécution cantonales gagnerait en efficacité et en souplesse si les travaux induits par les enquêtes préliminaires pouvaient être coordonnés. Cette requête a été prise en compte à l'al. 2. Si des objets sont saisis dans le cadre d'enquêtes préliminaires, il sera possible d'octroyer un accès à d'autres autorités d'exécution cantonales.

Variante à l'al. 2

La CCPCS a suggéré que les autorités d'exécution cantonales soient toujours en mesure de vérifier si une autre autorité d'exécution a déjà traité, dans le cadre de ses attributions, des informations relatives à une personne ou une organisation donnée. Elle est d'avis qu'une formulation potestative n'est pas suffisante et que les cantons devraient pouvoir procéder de leur propre initiative à une comparaison exhaustive des domaines cantonaux dans le système INDEX SRC.

Deux variantes de l'art. 31, al. 2, sont donc proposées. La procédure de consultation déterminera quelle variante sera retenue.

Art. 32 Droit d'accès

Les droits d'accès aux données contenues dans INDEX SRC reposent sur l'art. 51, al. 4, LRens, et correspondent à la situation actuelle.

Comme déjà mentionné, l'art. 31 du projet d'ordonnance prévoit que les autorités d'exécution cantonales puissent accéder à leurs enquêtes préliminaires respectives conformément à l'art. 29, let. b, ceci afin d'éviter des doublons. Les collaborateurs

du SRC ne disposent que d'un droit de lecture dans le système de gestion des mandats de l'index SRCant et n'ont pas accès aux enquêtes préliminaires. Seul le service du SRC chargé d'assurer la qualité peut accéder aux données des enquêtes préliminaires pour la vérification périodique des données personnelles dans l'index SRCant en vertu de l'art. 33, let. b. Comme c'est actuellement le cas, l'al. 2 renvoie à l'annexe 4 pour une vue d'ensemble des droits d'accès individuels.

Art. 33 Vérification périodique des données personnelles

Seules les données saisies dans IASA SRC et IASA-EXTR SRC et vérifiées (périodiquement) dans le respect des prescriptions régissant ces systèmes d'information sont copiées dans INDEX IASA au sens de l'art. 29, let. a. Une vérification périodique de ce dernier s'avère donc superflue. Il est toutefois nécessaire que le service de contrôle qualité du SRC vérifie périodiquement le respect des prescriptions régissant l'introduction de données dans les systèmes IASA SRC et IASA-EXTR SRC. Ce contrôle sera réalisé une fois par an (voir al. 1, let. a).

Les données visées à l'art. 29, let. b et c, du projet d'ordonnance seront versées dans IASA SRC et IASA-EXTR SRC si elles sont pertinentes, suffisamment condensées et vérifiées périodiquement conformément aux prescriptions régissant ces systèmes d'information. Le service du SRC chargé d'assurer la qualité est aussi tenu de vérifier une fois par an si les autorités d'exécution cantonales traitent les données conformément à la LRens, respectent les restrictions de traitement des données énoncées à l'art. 5, al. 5, LRens, et si les données ne sont pas conservées plus longtemps que cinq ans (voir al. 1, let. b). Le cas échéant, il corrige ou efface des données et organise des formations. En fonction de son plan de contrôle, il se concentre sur le traitement des données par une ou plusieurs autorités d'exécution cantonales.

Pour garantir une meilleure traçabilité, le service de contrôle qualité consigne le résultat de la vérification dans un rapport à l'attention du directeur du SRC (voir al. 2).

Art. 34 Durée de conservation

La durée de conservation maximale des données dans INDEX IASA au sens de l'art. 29, let. a, du projet d'ordonnance repose sur les dispositions qui régissent les systèmes d'information dont ces données proviennent (art. 21 du projet d'ordonnance pour les données issues de IASA SRC, et art. 28 du projet d'ordonnance pour les données issues de IASA-EXTR SRC). L'effacement de données dans ces systèmes d'information entraîne automatiquement la suppression des données correspondantes dans INDEX IASA, puisqu'il ne s'agit que de copies (voir al. 1).

Les données des autorités d'exécution cantonales au sens de l'art. 29, let. b et c, du projet d'ordonnance continuent d'être conservées pendant cinq ans comme c'est actuellement le cas (voir al. 2).

Conformément à l'al. 3 en relation avec l'art. 45, al. 5, let. d, LRens, le service de contrôle qualité du SRC efface les données au sens de l'art. 29, let. b et c, du projet d'ordonnance sur demande des autorités d'exécution cantonales ou à l'échéance de la durée visée à l'al. 2. Les autorités cantonales d'exécution peuvent détruire de leur propre chef les saisies erronées dans un délai de 10 jours.

Section 7 : Dispositions particulières applicables au système GEVER SRC

Art. 35 Structure

La structure du système GEVER est reprise telle qu'elle existe aujourd'hui. Elle comprend un système de traitement et de classement des données servant à la gestion et au contrôle du traitement des affaires ainsi qu'à l'efficacité des processus de travail du SRC (voir let. a), un système dans lequel les mandats en cours et terminés des collaborateurs du SRC peuvent être consultés et traités (voir let. b) ainsi qu'un moteur de recherche permettant la recherche en plein texte à l'intérieur du système GEVER (voir let. c).

Art. 36 Données

Le contenu du système GEVER SRC se fonde sur l'art. 52, al. 2, LRens, et reste identique même si le contrôle des affaires du service de documentation sur le racisme n'est plus mentionné explicitement (voir al. 1 et art. 38, al. 1, OSI-SRC). Le contrôle des affaires en matière d'exploration radio est réglé dans le projet d'ordonnance à la section 11, sous les dispositions particulières applicables au système d'information SICO.

Comme la réglementation actuelle de l'art. 38, al. 2, OSI-SRC, s'est révélée inapplicable dans la pratique (les données utilisées pour établir les contenus visés à l'art. 38, al. 1, let. a à c, ne peuvent pas être traitées dans GEVER avec des moyens raisonnables en raison de l'absence de marquage), elle n'a pas été reprise dans le projet d'ordonnance. Au lieu de cela, les données sont soumises à une vérification périodique et systématique (voir art. 38 du projet).

L'al. 2 prévoit comme aujourd'hui qu'en dérogation à l'art. 12, al. 2 et 3, de l'ordonnance du 30 novembre 2012 sur la gestion électronique des affaires dans l'administration fédérale[19], les données classifiées CONFIDENTIEL et SECRET peuvent être versées dans le système GEVER SRC sans être chiffrées (voir art. 37, al. 2, OSI-SRC, et les mesures de sécurité particulières en lien avec GEVER).

Le catalogue des données personnelles figure en annexe au projet d'ordonnance.

Art. 37 Droits d'accès

Les droits d'accès sont régis par l'art. 52, al. 3, LRens, et ne changent pas (voir al. 1). Comme c'est actuellement le cas, l'al. 2 renvoie à l'annexe correspondante pour une vue d'ensemble des droits d'accès individuels.

[19] RS **172.010.441**

Art. 38 Periodische Überprüfung der Personendaten

Conformément à l'al. 1, la vérification périodique des données GEVER incombe désormais au service du SRC chargé d'assurer la qualité. Il s'assure entre autres que les données utilisées pour établir les contenus au sens de l'art. 52, al. 2, let. a et b, LRens, ne sont pas conservées trop longtemps. A cette fin, il vérifie les répertoires et sous-répertoires du plan de registre au moins tous les 10 ans et, en tenant compte de la situation actuelle, apprécie si les données qu'ils contiennent sont encore nécessaires au traitement et au contrôle des affaires ainsi qu'à l'efficacité des processus de travail du SRC.

Dans le cas contraire, ces données sont effacées et transmises aux Archives fédérales suisses (voir al. 2). Pour garantir une meilleure traçabilité, le service de contrôle qualité consigne le résultat de la vérification dans un rapport à l'attention du directeur du SRC.

Art. 39 Embargo sur l'utilisation

La directive du directeur du SRC du 9 septembre 2013 concernant le traitement des données dans le système de gestion électronique des mandats et des affaires (GEVER SRC) prévoit au ch. 3 que les rapports des services et les rapports sur la situation ou les sorties d'annonces ne doivent pas être établis exclusivement sur la base de données contenues dans le système GEVER. Autrement dit, avant d'utiliser des données jointes à un mandat dans GEVER et provenant de IASA SRC ou IASA-EXTR SRC, il convient de vérifier leur présence dans ces systèmes d'information. En effet, il est possible que dans l'intervalle, les données en question aient été effacées des systèmes IASA SRC ou IASA-EXTR SRC par le service de contrôle qualité. Cet embargo sur l'utilisation est désormais énoncé à l'al. 1. Le terme d'utilisation désigne l'intégration d'informations dans un produit.

L'embargo ne s'applique pas au système PES. Seules des données provenant directement du système PES sont utilisées pour le suivi de la situation. Il est aussi nécessaire de pouvoir utiliser directement ces données pour l'établissement de produits du renseignement, même si elles n'ont pas été saisies dans un autre système d'information. La courte durée de conservation des données dans le système PES évite les conflits avec les autres systèmes.

Conformément à l'al. 2, le service du SRC chargé d'assurer la qualité contrôle par sondage une fois par an si l'embargo sur l'utilisation est respecté.

Art. 40 Durée de conservation

La durée de conservation maximale des données dans le système GEVER reste fixée à 45 ans (voir art. 40, al. b, OSI-SRC).

Section 8 : Dispositions particulières applicables au système PES

Art. 41 Structure

Malgré la nouvelle formulation de la disposition, la structure du système PES ne change pas par rapport à la situation actuelle (voir art. 29, al. 2, OSI-SRC).

Art. 42 Données

Le contenu du système PES se fonde sur l'art. 53, al. 2, LRens, et reste identique (voir art. 30, al. 1, OSI-SRC). Le système PES ne contient des données personnelles que si elles sont indispensables à la présentation et l'appréciation de la situation.

Art. 43 Droit d'accès

Les droits d'accès se fondent sur l'art. 53, al. 3 et 4, LRens, et correspondent à la situation actuelle (voir al. 1 et art. 32 OSI-SRC).

Comme c'est déjà le cas, le SRC peut accorder, sous certaines conditions et en cas d'événement impliquant un risque accru pour la sécurité, un accès au système PES limité dans le temps et restreint quant au contenu à des services privés ainsi qu'à des services de sécurité et des autorités de police étrangers (voir al 3). L'al. 4 prévoit la possibilité de contrôler l'utilisation des données par ces services et autorités. Les droits d'accès individuels figurent à l'annexe 8 (voir al. 5). Les al. 2 à 5 du projet d'ordonnance ont été repris tels quels de l'art. 32, al. 2 à 4, OSI-SRC.

Art. 44 Vérification périodique

La vérification périodique des données contenues dans le système PES incombe désormais aux collaborateurs du SRC chargés du stockage des données dans le système PES (voir al. 1). Toutes les informations qui ne sont plus nécessaires au pilotage et à la mise en œuvre des mesures des mesures de police de sécurité et dont la saisie remonte à plus de trois ans sont effacées et transmises aux Archives fédérales suisses (voir al. 2). Le service du SRC chargé d'assurer la qualité procède en outre à des contrôles par sondage au sens de l'art. 11, al. 2 (voir al. 4).

Pour garantir une meilleure traçabilité, les collaborateurs chargés de la vérification périodique en consignent le résultat dans un rapport à l'attention du service du SRC chargé d'assurer la qualité (voir al. 3).

Art. 45 Durée de conservation

La durée de conservation maximale de trois ans a été reprise telle quelle de l'art. 31 OSI-SRC.

Section 9 : Dispositions particulières applicables au portail ROSO

Art. 46 Structure

La structure du portail ROSO ne figure pas dans l'actuelle OSI-SRC. C'est désormais chose faite dans le projet d'ordonnance pour des raisons de transparence. Le portail ROSO comprend un système de stockage de données classées par sources. Il est utilisé pour la saisie et l'évaluation de données provenant de sources d'informations publiques.

Art. 47 Données

Comme c'est actuellement le cas avec le stockage intermédiaire OSINT (voir art. 42, al. 1, OSI-SRC), les données classées dans le portail ROSO proviennent de sources d'informations publiques. Il ne s'agit toutefois pas de simples copies de données d'Internet, mais d'informations de qualité élevée toujours en lien avec un domaine d'activité du SRC. Ces données proviennent en partie de sources payantes (abonnements à des médias en ligne) ou sont le résultat de recherches ciblées (surveillance du djihadisme). Toutes les données contenues dans le portail ROSO sont saisies de façon structurée par sources et thématiques. Elles peuvent être évaluées et utilisées au moyen d'outils d'analyse (voir al. 1).

Avant d'être utilisées ou communiquées, les données du portail ROSO doivent être versées dans les systèmes IASA SRC, IASA-EXTR SRC ou GEVER selon les règles qui s'appliquent au classement et à la saisie d'informations (voir al. 2).

Si des données sont stockées automatiquement sans tri manuel, la qualité des sources doit être vérifiée au préalable sur la base de processus et directives prédéfinis (voir al. 3). Comme seules des données de source publique sont classées dans le portail ROSO, la saisie automatique concerne par exemple des dépêches d'agence.

La liste des données personnelles et les droits d'accès individuels figurent à l'annexe 9 (voir al. 4).

Art. 48 Droits d'accès

Tous les collaborateurs du SRC ont déjà accès aux données du portail ROSO. Cet accès est désormais aussi octroyé aux collaborateurs des autorités d'exécution cantonales (voir al. 1 en relation avec l'art. 54, al. 3 et 4, LRens). Les droits d'accès individuels figurent à l'annexe 10 (voir al. 2).

Art. 49 Vérification périodique

La vérification périodique des données contenues dans le portail ROSO incombe désormais aux collaborateurs du SRC chargés du stockage des données dans le système PES (voir al. 1). Ces derniers doivent vérifier au moins tous les cinq ans, en tenant compte de la situation actuelle, si les données en question sont encore nécessaires à l'accomplissement des tâches du SRC visées à l'art. 6 LRens. Ils effacent toutes les données classées depuis plus de 15 ans et les transmettent aux Archives fédérales suisses (voir al. 2). Le service du SRC chargé d'assurer la qualité procède en outre à un contrôle par sondage au sens de l'art. 11, al. 2 (voir al. 4).

Pour garantir une meilleure traçabilité, les collaborateurs chargés de la vérification périodique en consignent le résultat dans un rapport à l'attention du service du SRC chargé d'assurer la qualité (voir al. 3).

Art. 50 Durée de conservation

La durée de conservation a été fixée à 20 ans pour assurer l'utilisation des données de qualité élevée du portail ROSO sur une longue période et une évaluation pertinente au moyen d'outils d'analyse (suivi de l'apparition et de la propagation du groupe Etat islamique ainsi que de ses activités dans les domaines publics d'Internet par ex.).

Section 10 : Dispositions particulières applicables au système Quattro P

Art. 51 Structure

Cette disposition a été reprise telle quelle de l'art. 33, al. 2, OSI-SRC.

Art. 52 Données

Le contenu de Quattro P ne change pas et correspond à l'actuel art. 34, al. 1, OSI-SRC (voir al. 1).

Avant d'être utilisées ou communiquées, les données du système Quattro P doivent d'abord être versées dans les systèmes IASA SRC, IASA-EXTR SRC ou GEVER selon les règles qui s'appliquent au classement et à la saisie d'informations (voir al. 2).

Si des données sont stockées automatiquement sans tri manuel, la qualité des sources doit être vérifiée au préalable sur la base de processus et directives prédéfinis (voir al. 3). Les données classées automatiquement dans le système Quattro P peuvent provenir par exemple d'une liste de pays confidentielle approuvée par le Conseil fédéral. En cas de résultat positif, il est procédé à un contrôle manuel et le service du SRC chargé d'assurer la qualité vérifie dans le cadre de contrôles par sondage si des données ont été saisies au sujet de pays ne figurant pas dans ladite liste.

La liste des données personnelles et les droits d'accès individuels figurent à l'annexe 11 (voir al. 4).

Art. 53 Droits d'accès

Les droits d'accès restent identiques et correspondent à l'actuel art. 35 OSI-SRC.

Art. 54 Vérification périodique

L'al. 1 spécifie que les collaborateurs du SRC chargés de la saisie des données dans le système Quattro P doivent désormais procéder à une vérification périodique. Dans cette optique, ils vérifient au moins tous les cinq ans si les données transmises au SRC par les organes de contrôle à la frontière et classées dans le système Quattro P coïncident avec la liste établie par le Conseil fédéral en vertu de l'art. 55, al. 4, LRens, et si ces données sont encore nécessaires à l'accomplissement des tâches du SRC visées à l'art. 6 LRens. Si le Conseil fédéral modifie la liste, les bases de données doivent aussi l'être. Le service du SRC chargé d'assurer la qualité procède en outre à des contrôles par sondage au sens de l'art. 11, al. 2 (voir al. 3).

Les données qui ne sont plus nécessaires doivent être effacées et transmises Archives fédérales suisses (voir al. 2).

Art. 55 Durée de conservation

Comme c'est actuellement le cas, la durée de conservation maximale des données dans le système Quattro P est de cinq ans (voir art. 36 OSI-SRC).

Section 11 : Dispositions particulières applicables au système SICO

Art. 56 Structure

Pour des raisons de transparence, le système SICO figure désormais comme un système d'information à part entière servant au stockage de données pour gérer et diriger les moyens de l'exploration, le contrôle de gestion et les rapports. Le classement des données concernées est réglé dans les dispositions actuelles relatives au système GEVER (voir en particulier l'art. 38, al. 1, let. e, OSI-SRC).

Art. 57 Données

Le contenu du système SICO se fonde sur l'art. 56, al. 2, LRens, (voir al. 1) et provient notamment de mandats d'exploration menés en collaboration avec le Centre des opérations électroniques (COE) de la Base d'aide au commandement de l'armée (COE BAC). Les résultats de l'exploration radio et de l'exploration du réseau câblé ne sont toutefois pas classés dans le système SICO, mais dans IASA SRC ou le système de stockage des données résiduelles. Ils peuvent être référencés dans le système SICO. Exemple de procédure: un objet saisi dans IASA SRC (numéro de téléphone) doit être exploré par le COE BAC. Le numéro de téléphone et le mandat confié au COE BAC sont saisis dans le système SICO afin d'en assurer un suivi conforme et intégral. Le numéro de téléphone est ensuite transmis comme cible au COE BAC. Le résultat de l'exploration est communiqué au SRC sous la forme d'un rapport COMINT et classé comme document original dans IASA SRC avec référence au système SICO.

Si des données sont stockées automatiquement sans tri manuel, la qualité des sources doit être vérifiée au préalable sur la base de processus et directives prédéfinis (voir al. 3). Les collaborateurs du SRC vérifient le mandat de prestations (numéro de téléphone par ex.) et le classent manuellement. Un capteur (collaborateur du COE BAC par ex) vérifie les résultats (données relatives aux communications établies par ex.) quant à leur relation avec les tâches visées à l'art. 6 LRens. Ces résultats sont transmis au SRC et classés automatiquement dans le système SICO.

Art. 58 Droits d'accès

Seuls les collaborateurs du SRC directement chargés de diriger l'exploration radio et l'exploration du réseau câblé ont accès au système SICO (à l'heure actuelle, moins de dix personnes).

Art. 59 Vérification périodique

Aujourd'hui déjà, l'utilité et la proportionnalité des mandats d'exploration et des bases de données sont vérifiées périodiquement, en tenant compte de la situation actuelle (voir al. 1). Cette pratique désormais ancrée expressément à l'al. 1 incombe aux collaborateurs du SRC chargés du stockage des données dans le système SICO.

Pour garantir une meilleure traçabilité, les collaborateurs chargés de la vérification périodique en consignent le résultat dans un rapport à l'attention du service du SRC chargé d'assurer la qualité (voir al. 3).

Art. 60 Durée de conservation

La durée de conservation maximale des données figurant dans le système SICO est de cinq ans au plus après l'achèvement du mandat d'exploration concerné.

Section 12 : Dispositions particulières relatives au système de stockage des données résiduelles

Art. 61 Structure

Le système de stockage des données résiduelles contient toutes les informations qui n'ont pas pu être attribuées à un autre système lors du tri suivant le contrôle des données entrantes (voir al. 1 en relation avec l'art. 57 LRens). Les données sont contrôlées à l'entrée pour vérifier si leur relation avec les tâches visées à l'art. 6 LRens peut être suffisamment établie (voir art. 3, al. 1, du projet d'ordonnance).

Les données nécessaires à l'accomplissement des tâches du SRC doivent être versées dans les systèmes IASA SRC, IASA-EXTR SRC ou GEVER et détruites dans le système de stockage des données résiduelles, car elles sont transmises aux Archives fédérales suisses par lesdits systèmes d'information (voir al. 2). Les dispositions de l'art. 3, al. 1, s'appliquent au classement des données. Si des données personnelles doivent être utilisées ou communiquées, les dispositions de l'art. 4, al. 1, s'appliquent au transfert. Autrement dit, les données personnelles doivent être vérifiées au préalable quant à leur relation avec les tâches du SRC, leur pertinence, leur exactitude et les restrictions de traitement visées à l'art. 5, al. 5, LRens, et saisies de façon structurée dans le système IASA SRC (il existe déjà une obligation générale de saisie structurée pour le système IASA-EXR SRC).

Art. 62 Données

Le contenu du système de stockage des données résiduelles se fonde sur l'art. 57, al. 2, LRens. Il s'agit surtout de communiqués d'autorités de sécurité étrangères, de données provenant de l'exploration radio et de l'exploration du réseau câblé, d'informations de sources humaines et d'informations n'ayant pas fait l'objet de recherches actives par le SRC.

Art. 63 Droits d'accès

Les collaborateurs du SRC chargés de la saisie, de la recherche, de l'évaluation et du contrôle de la qualité des données ont accès en ligne au système de stockage des données résiduelles (voir art. 57, al. 3, LRens).

Art. 64 Vérification périodique

Conformément à l'al. 1, le service du SRC chargé d'assurer la qualité vérifie au moins tous les dix ans, en tenant compte de la situation actuelle, si les bases de données figurant dans le système de stockage des données résiduelles sont encore nécessaires à l'accomplissement des tâches visées à l'art. 6 LRens et si elles n'ont pas été classées depuis plus de 10 ans. Les données qui ne sont plus nécessaires et celles classées depuis plus de 10 ans sont effacées et transmises aux Archives fédérales suisses (voir al. 2).

Le service du SRC chargé d'assurer la qualité vérifie en outre que les obligations en matière de transfert ont été respectées et que les données transférées ont été détruites (voir al. 3). Pour garantir une meilleure traçabilité, il consigne le résultat de la vérification dans un rapport à l'attention du directeur du SRC. Si le service de contrôle qualité constate un manquement lors la vérification, il formule des recommandations dans son rapport et leur mise en œuvre est ajoutée à la liste des points en suspens de la direction du SRC (aussi valable pour le système GEVER).

Le service du SRC chargé d'assurer la qualité procède en outre à un contrôle par sondage au sens de l'art. 11, al. 2 (voir al. 4).

Art. 65 Durée de conservation

La durée de conservation maximale des données dans le système de stockage des données résiduelles est de 10 ans au plus..

Section 13 : Données provenant de mesures de recherche soumises à autorisation et de recherches à l'étranger

Art. 66 Structure

Les systèmes de stockage comprennent une base de données servant à saisir, traiter et consulter par cas des données issues de mesures de recherche soumises à autorisation et de recherches à l'étranger (voir al. 1).

L'art. 58, al. 1, LRens, prévoit que les données provenant de telles mesures de recherche soient enregistrées et consultées dans des systèmes distincts des autres systèmes d'information (voir al. 2).

Art. 67 Données

Comme dans IASA NDB et IASA-GEX NDB, des données relatives à des personnes physiques et morales, des objets et des événements, des données personnelles sensibles et des profils de la personnalité peuvent être traitées dans les systèmes de stockage.

Art. 68 Droits d'accès

Les droits d'accès sont réglés à l'art. 58, al. 5, LRens (voir al. 1).

Des droits d'accès particuliers doivent être créés pour chaque opération (voir al. 2) afin d'assurer que seules les personnes qui dirigent l'opération ou qui sont chargées de l'exécution des mesures de recherche et de l'évaluation des résultats ont accès aux données (voir art. 58, al. 5, LRens).

Les droits d'accès individuels sont soumis à autorisation du SRC pour chaque mesure de recherche (voir al. 3).

Art. 69 Embargo sur l'utilisation

Avant d'être utilisées ou communiquées, les données doivent être versées au préalable dans le système IASA SRC moyennant le respect des dispositions en la matière (voir al. 1). Contrairement au système de stockage des données résiduelles et compte tenu de la courte durée de conservation, les données ne doivent pas être détruites dans les systèmes de stockage.

Il existe un embargo total sur l'utilisation des données de personnes non impliquées et des données relatives à des personnes ayant un droit confirmé de refuser de témoigner en vertu des art. 171 à 173 CPP. Ces données doivent être détruites au plus tard 30 jours après la levée de la mesure (voir al. 2). Cette disposition permet d'éviter que lesdites données ne figurent dans des produits du SRC ou soient communiquées.

Le service du SRC chargé d'assurer la qualité contrôle par sondage si cet embargo sur l'utilisation est respecté (voir al. 3).

Art. 70 Durée de conservation

Les systèmes de stockage peuvent contenir de très gros volumes de données et un grand nombre d'informations sans lien avec le but de l'exploration, en raison de leur nature strictement privée notamment. Il convient de tenir compte de la protection des données personnelles de tiers qui utilisent par exemple le raccordement de télécommunication de la personne surveillée. Souvent, il n'est pas possible de savoir dès le début si certaines communications sont importantes, parce que le réseau de contacts de la personne surveillée doit encore être identifié ou parce que cette dernière utilise des éléments conspiratifs dans sa communication afin de protéger ses contacts. Les données qui ne sont pas nécessaires à une procédure judiciaire en cours seront donc effacées dans les meilleurs délais (voir al. 1).

Lorsque la réponse est reportée, les données doivent être effacées au plus tard six mois après l'envoi de la communication (voir al. 2).

La surveillance de la destruction des données par le Tribunal administratif fédéral prévue à l'art. 58, al. 3, LRens, est garantie par le dépôt d'une demande préalable comportant des indications relatives aux données sélectionnées et destinées à être détruites (voir al. 3).

La durée de conservation des données issues de recherches au sens de l'art. 36, al. 5, LRens, est de trois ans (voir al. 5).

Annexes 1, 3, 5, 7, 9, 11, 13, 15 et 17: Catalogues des données personnelles

Les annexes susmentionnées répertorient en vertu de l'art. 47, al. 2, let. a, LRens, les données concernant une personne ou une organisation ou en corrélation avec l'une ou l'autre. Les catalogues des données personnelles seront complétés avec le numéro AVS à 13 chiffres dès que la base légale correspondante sera entrée en vigueur.

Annexes 2, 4, 6, 8, 10, 12, 14, 16 et 18: Droits d'accès

Les annexes susmentionnées répertorient en vertu de l'art. 47, al. 2, let. c, LRens, les droits d'accès aux systèmes d'information du SRC.