Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Mai 2022

Rapport explicatif concernant la révision de la loi fédérale du 25 septembre 2015 sur le renseignement

en vue de l'ouverture de la procédure de consultation

Rapport explicatif

1 Contexte

1.1 Mesures requises et objectifs

La loi du 25 septembre 2015 sur le renseignement (LRens)[1] est entrée en vigueur le 1er septembre 2017. Lors des débats parlementaires, il avait déjà été question de compléter et d'examiner ultérieurement certaines dispositions.

Par conséquent, le Conseil fédéral a chargé le Département fédéral de la défense, de la protection de la population et des sports (DDPS), par décision du 16 août 2017 concernant l'entrée en vigueur de la LRens et de ses ordonnances d'exécution, de créer une base légale dans la LRens et dans la loi du 13 septembre 2002 sur le Parlement (LParl)[2] pour que l'autorité de surveillance indépendante puisse établir son budget de manière autonome et ainsi gagner encore en indépendance. Le 20 février 2019, le Conseil fédéral a ainsi chargé le DDPS de lui soumettre jusqu'à fin juin 2020 un avant-projet de révision de la LRens à même d'être mis en consultation. Cet avant-projet devait en particulier se pencher sur la transmission des tâches de l'ACI à l'AS-Rens, sur les modifications dans le domaine des mesures de recherche soumises à autorisation, ainsi que sur des modifications formelles.

Principes généraux:

Par décision du 26 août 2020, le Conseil fédéral a chargé le DDPS de réviser les dispositions relatives aux systèmes d'information ainsi que les demandes d'accès relatives à la protection des données du Service de renseignement de la Confédération (SRC). Ce mandat découlait des propositions formulées dans le rapport annuel 2019 de la Délégation des Commissions de gestion des Chambres fédérales (DélCdG)[3] pour le traitement des données du renseignement. Les conditions-cadres du traitement des données changeront avec l'entrée en vigueur de la loi sur la protection des données révisée (nLPD)[4], adoptée le 25 septembre 2020, ainsi qu'avec l'évolution des technologies liées aux données. Par conséquent, le Conseil fédéral souhaite revoir les modalités de traitement des données relevant du renseignement (voir la préface aux explications des art. 44 ss). La majeure partie du présent rapport y est consacrée. Le Conseil fédéral a prolongé en conséquence le délai pour présenter le projet législatif jusqu'à fin 2021.

La présente révision aborde également les thèmes suivants:

- Mesures supplémentaires de détection précoce et de prévention de l'extrémisme violent, en réponse à plusieurs initiatives parlementaires s'inquiétant de la dégradation de la situation sécuritaire (voir les explications de l'art. 27).
- Nouvelle réglementation de la recherche sur le financement des menaces graves pour la sûreté de la Suisse en réaction à la détérioration de la situation sécuritaire dans divers domaines de la sûreté intérieure et extérieure, à savoir le terrorisme, l'espionnage et l'extrémisme violent. En raison de la gravité des atteintes aux droits fondamentaux, cette réglementation est proposée sous la forme d'une mesure de recherche soumise à autorisation (voir les explications de l'art. 26).
- Propositions d'amélioration de la mise en œuvre pratique de la LRens, essentiellement sur la base des premières expériences d'exécution récoltées par les services externes.
- Adaptations d'ordre linguistique afin d'uniformiser la terminologie dans les trois langues officielles.

1.2 Genèse du présent projet

Les travaux préparatoires ont rassemblé des représentants de l'AS-Rens, de l'ACI, du DDPS (Secrétariat général, Office fédéral de la protection de la population OFPP, Service de renseignement militaire, Centre des opérations électroniques COE), du Département fédéral des affaires étrangères (DFAE: Secrétariat général), du Département fédéral de justice et police (DFJP: Secrétariat général, Office fédéral de la justice OFJ, Office fédéral de la police fedpol et Service Surveillance de la correspondance par poste et télécommunication SCPT), du Ministère public de la Confédération (MPC), de la Chancellerie fédérale (ChF et Préposé fédéral à la protection des données et à la transparence PFPDT), ainsi que de la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) et la Conférence des commandants des polices cantonales de Suisse (CCPCS).

Des groupes de travail interdépartementaux se sont consacrés aux différents thèmes du projet. Les modifications de la surveillance (art. 77 à 78*d*) ont été rédigées de manière autonome par l'AS-Rens et l'ACI. Leurs propositions ont ensuite été intégrées au projet. En raison de la situation sanitaire, la plupart des travaux et des consultations ont eu lieu par correspondance.

Le Tribunal administratif fédéral (TAF) a choisi de ne pas participer aux groupes de travail. Le SRC l'a toutefois tenu informé de l'avancée des travaux, aussi il a eu l'opportunité de se prononcer par écrit dans le cadre d'une consultation préalable. Il a également été consulté par écrit durant la consultation des offices.

2 Commentaire des dispositions

Par souci de lisibilité, toutes les modifications d'ordre linguistique qui concernent une seule langue et n'ont aucune conséquence matérielle sont énumérées en premier.

Ne concerne que le texte français:

1 RS **121**
2 RS **171.10**
3 FF **2020** 2865 ss, 2950
4 FF **2020** 7397

Art. 15, 18 et 35

Dans le cadre des activités de renseignement, on parle aujourd'hui de « source humaine ». Par conséquent, le terme « informateur » est remplacé par « source humaine » dans toute la loi.

Art. 23, al. 2

Le terme « audition » est remplacé par « interrogatoire », également employé à l'art. 24.

Art. 39, 41 et 42

L'expression « du réseau câblé » est supprimée. Cette précision n'est pas utile, puisque la section 7 est expressément consacrée à l'exploration du réseau câblé.

« Réseau filaire » est remplacé par « réseau câblé » afin d'unifier la terminologie dans tout le texte de loi (art. 39, al. 1 et 41, al. 1, let. d).

Ne concerne que le texte allemand:

Dans tout le texte de la loi, le verbe « orientiert » est remplacé par « informiert ».

Art. 19, al. 3, et art. 20, al. 2

Cette adaptation vise à étendre l'usage uniforme de la tournure « geheim halten » à l'ensemble de la loi.

Art. 32

Titre

Le titre est précisé afin d'indiquer de manière évidente qu'il concerne la fin de la mesure de recherche.

Al. 1, let. c

La formulation est adaptée afin de correspondre à la terminologie «Vorsteherin oder Vorsteher des VBS», établie par l'art. 37 de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[5].

Ne concerne que le texte italien:

Art. 39, al. 4, let. c

L'expression «dei segnali via cavo» est supprimée. Cette précision n'est pas utile, puisque la section 7 est expressément consacrée à l'exploration du réseau câblé.

Les modifications concernant le contenu sont expliquées ci-après.

Art. 1

Let. a

La formulation actuelle de la LRens donne l'impression que le SRC n'accomplit que les tâches qui lui sont prescrites par la LRens. Or, comme tous les autres services de l'administration fédérale, le SRC effectue des tâches purement administratives en vertu de la LOGA. Il participe ainsi à des consultations des offices dans le cadre de procédures législatives, au traitement d'interventions parlementaires et contribue à répondre aux demandes des médias. En outre, le SRC recrute, conduit et accompagne son personnel, exploite ses services informatiques, acquiert ses fournitures conformément au droit des marchés publics et gère ses finances. Mentionner expressément l'activité de renseignement à l'art. 1 rappelle clairement que les diverses activités administratives du SRC ne sont pas réglées par la LRens, mais découlent des dispositions générales applicables à l'administration fédérale.

Let. d

Etant donné que la LRens distingue les données administratives de celles relevant du renseignement et établit certains principes de traitement des données administratives, le traitement des données du SRC est désormais mentionné explicitement à l'art. 1.

Art. 5

Même si seul le SRC est mentionné dans cet article, ce dernier s'applique également aux autorités d'exécution cantonales. Ce principe vaut en outre pour toutes les normes générales du présent projet. Les autorités d'exécution cantonales ne sont mentionnées expressément que lorsqu'une disposition les concerne exclusivement ou lorsqu'il est nécessaire de souligner leurs droits et devoirs, c'est-à-dire lorsqu'elles sont sinon dans l'impossibilité d'identifier clairement l'action à effectuer.

Al. 5

Les restrictions actuelles en matière de traitement des données relatives aux activités politiques ou à l'exercice de la liberté d'opinion, d'association ou de réunion demeurent inchangées. Les exceptions nécessaires sont toutefois décrites à l'al. 6 plus précisément qu'auparavant. La nouvelle disposition précise que les données traitées par le SRC pour accomplir ses tâches administratives ne tombent pas sous le coup des restrictions en matière de traitement des données. Par exemple, si le SRC traite des affaires parlementaires qui lui sont

5 RS **172.010**

confiées dans le cadre de ses tâches administratives, elles sont de nature politique. Ces activités peuvent concerner des données personnelles, sans qu'elles soient toutefois significatives pour l'exécution des tâches de renseignement. Les noms des auteurs et des cosignataires d'interventions parlementaires consacrées à la sûreté intérieure ou extérieure sont connus du SRC, car ils figurent notamment dans le titre formel de chaque intervention. De même, le traitement des demandes d'accès relatives à la protection des données implique la connaissance de données personnelles dans le cadre de la procédure d'information. Ces données sont conservées par le SRC afin de garantir la traçabilité de l'utilisation des informations et d'assurer le suivi en cas de saisine du PFPDT. Le SRC est tenu de les conserver un certain temps, même si elles ne sont pas requises pour son activité de renseignement.

Al. 6

Let. a

Il peut arriver qu'au moment de la réception des données, un lien avec les tâches paraisse probable sans pour autant être certain, en raison de la source, du contenu ou du contexte. Des contrôles supplémentaires sont alors nécessaires. Par exemple, il se peut qu'un service de renseignement étranger demande des renseignements sur une personne qui diffuse dans son pays une idéologie radicale d'extrême-droite, ce qui fonde la compétence de l'autorité étrangère. Imaginons que cette personne se rende à une rencontre en Suisse. Le service partenaire souhaite alors savoir si le SRC dispose d'informations à ce sujet. Le SRC transmet alors un mandat de recherche à l'autorité d'exécution cantonale où la personne concernée se trouve. Seul le résultat de ces recherches permet de déterminer s'il s'agit d'une rencontre d'extrémistes, donc si le lien avec les tâches du SRC est établi et si un traitement ultérieur des données est admis. Cette situation peut bien entendu également se produire avec des données reçues des autorités d'exécution cantonales. La nécessité de traiter des données personnelles lors du contrôle de la relation supposée avec les tâches du SRC est désormais mentionnée expressément par souci de transparence (voir également les explications de l'art. 46, al. 2).

Let. b

Dans la précédente version, les exceptions mentionnées à l'al. 6 se limitaient au terrorisme, à l'espionnage et à l'extrémisme violent. Ce champ d'application est un reliquat de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)[6], qui ne traitait pas encore le domaine cyber et partait du principe que les activités de prolifération ne constituaient pas des atteintes aux droits fondamentaux. Il n'existe cependant aucune raison de protéger le recours abusif aux droits fondamentaux cités à l'art. 5, al. 5, dans les domaines de la non-prolifération et des activités importantes en matière de politique de sécurité dans le cyberespace. Par conséquent, le champ d'application de cette disposition a été élargi à toutes les activités visées à l'art. 6, al. 1, let. a. Il en ressort donc clairement que le SRC peut, par exemple, se consacrer à des déclarations d'intention sur les cyberattaques ou à des informations sur des rencontres en préparation. En revanche, les groupes d'amitié parlementaires avec les pays concernés par la prolifération ne sont plus susceptibles d'être observés par le service de renseignement. Les membres de ces groupes sont suffisamment sensibilisés pour ne pas se laisser utiliser à de telles fins.

Let. c

Du point de vue du renseignement, il est capital de savoir contre qui une menace est dirigée. Ce n'est qu'à cette condition que le SRC peut établir un rapport correct et que les autorités compétentes peuvent prendre les mesures appropriées pour avertir et protéger les personnes et organisations menacées. Si ces dernières ne font pas usage des droits fondamentaux mentionnés à l'art. 5, al. 5, aucun problème ne se pose. Par exemple, si le SRC apprend qu'une attaque est prévue sur le siège d'une multinationale, il peut en informer l'entreprise et la police cantonale concernée, mais aussi traiter des données en lien avec cette menace. En revanche, dans de rares cas, des personnes ou organisations doivent être protégées dans des situations en lien avec leurs droits fondamentaux protégés. Par exemple, si le SRC apprend qu'une personnalité politique va être agressée physiquement lors d'une apparition publique, il doit être autorisé à titre exceptionnel à traiter les données relatives à son travail afin de la protéger. D'autres exemples seraient des attaques relevant du cyberespionnage visant directement des membres du parlement ou encore des dommages à la propriété à l'encontre d'un membre du gouvernement responsable du système de santé. Cette exception ne saurait avant tout être invoquée qu'afin de protéger des intérêts prépondérants (p. ex. vie et intégrité corporelle, mais également la protection de la sphère privée). L'admissibilité exceptionnelle du traitement de ces données est expressément étendue aux personnes et aux organisations potentiellement menacées par les activités citées à l'art. 6, al. 1, let. a. Ainsi, des associations étrangères sont souvent la cible d'autorités étrangères et victimes de cyberattaques, d'espionnage politique ou encore d'agressions.

Let. d

Il est tout aussi important de connaître l'origine des informations pour les évaluer (p. ex. pour vérifier leur exactitude). Le SRC ne peut correctement juger la fiabilité d'une information que s'il sait d'où elle vient. Il traite ainsi différemment l'opinion sur la lutte contre le terrorisme exprimée par un passant de celle d'une experte reconnue du domaine. Le SRC ne s'intéresse en l'occurrence ni au passant, ni à l'experte, mais à l'information sur l'événement. Afin de pouvoir l'évaluer, il est primordial qu'il sache de qui elle provient. De telles sources accessibles au public fournissent nombre d'informations de base utiles à l'activité de renseignement.

Il en va de même pour la conduite des sources humaines: la source proprement dite est le moyen de l'activité de renseignement du SRC, et non sa fin. Malgré cela, le SRC doit connaître des données personnelles sur la source et les traiter, y compris dans les rares cas où l'activité de renseignement de la source est liée à sa propre activité politique ou à l'exercice de sa liberté d'opinion, de réunion ou d'association.

Let. e

Le SRC a pour tâche d'informer au fur et à mesure les autorités fédérales et cantonales des menaces potentielles et de les alerter au besoin (voir art. 6, al. 2, LRens). Il a également pour tâche de les informer des événements et renseignements susceptibles d'avoir une incidence sur leurs tâches de maintien de la sûreté intérieure ou extérieure (voir art. 6, al. 3, LRens). Le SRC effectue cela dans le cadre du renseignement intégré, en vertu duquel les autorités fédérales et cantonales chargées des questions de sécurité s'autorisent mutuellement à accéder à des informations en rapport avec la situation en vue de maintenir la sûreté intérieure ou extérieure. Avec la participation de tous les partenaires, le SRC établit la présentation intégrale de la situation qu'il actualise en permanence. (cf. rapport du Conseil fédéral sur la politique de sécurité de la Suisse, FF 2016 7665, note de bas de page 79, ainsi que le message concernant la LRens, commentaires *ad* art. 6 LRens, FF 2014 2067 s.).

6 RS **120**

Dans son rapport annuel 2019, la DélCdG est parvenue à la conclusion que l'appréciation de ces risques par les services de renseignement pour la planification de mesures de police de sûreté peut notamment reposer sur des données qui tombent sous le coup de l'art. 5, al 5. La Délégation estime que le traitement de telles données à cette fin est admissible s'il dure moins d'un an. La nouvelle lettre e concrétise cette directive précise. Elle s'applique aux données que le SRC traite pour la conduite des renseignements intégrés conformément à l'art. 54, al. 1, et pour l'établissement de la présentation électronique de la situation. Ainsi, il serait nécessaire de nommer un parti politique dont l'assemblée générale fait l'objet de menaces afin que les autorités compétentes puissent en assurer la protection. Notons ici que les mesures de police de sûreté ne sont pas prises par le SRC proprement dit, mais par les autorités compétentes de la Confédération et des cantons. Cette disposition vise également des données concernant les personnes au cœur des enjeux sécuritaires d'un événement donné, même si elles ne sont pas directement menacées (p. ex. en cas d'appel à une manifestation violente contre un discours public d'un politicien ou la visite d'une cheffe d'Etat étrangère).

Al. 7

Les termes « données relatives à des personnes » et « saisie des informations » sont remplacés par « données personnelles ». La formulation de cet alinéa est modifiée, car l'al. 6 règle désormais le lien avec les tâches et les menaces. Son contenu demeure inchangé.

Al. 8

Le terme « représentants » a suscité diverses discussions, car il n'est défini nulle part. La nouvelle disposition précise qu'il s'agit des personnes qui font partie d'organisations ou de groupements de ce type, qui les soutiennent personnellement ou matériellement, qui organisent des actions de propagande pour accomplir leurs objectifs, qui font leur promotion ou qui encouragent leurs activités d'une autre manière au sens de l'art. 6, al. 1, let. a. Le contenu de la règle demeure inchangé.

Art. 6

Al. 1, let. b

Le terme employé jusqu'ici dans la LRens, « infrastructures critiques », s'est avéré trop restrictif pour inclure adéquatement tous les événements importants en matière de politique de sécurité dans le cyberespace. De plus, les cyberattaques sont souvent significatives à cet égard depuis quelques années. Elles ne sont pas seulement le fait de pirates informatiques individuels ou de groupes criminels, mais de plus en plus d'acteurs soutenus par des Etats, des forces armées et des services de renseignement. La détection précoce et la prévention par les services de renseignement doivent pouvoir tenir compte de cette nouvelle facette des menaces pour la sûreté intérieure et extérieure de la Suisse. La recherche de renseignements permet au SRC d'évaluer correctement la gravité des cyberattaques de ce type et pose les bases de l'étude d'éventuelles contre-mesures politiques (extérieures). Le SRC est déjà chargé de fournir au Groupe Cyber une vue d'ensemble de la situation en matière de cybermenaces (art. 8, al. 6, de l'ordonnance du 27 mai 2020 sur les cyberrisques[7]). Il ne peut donc pas se limiter aux aspects cybernétiques de son domaine de compétences classique. Ainsi, les cyberattaques contre des organisations internationales ou des ONG établies en Suisse ainsi que l'usage abusif d'infrastructures de télécommunication en Suisse pour des cyberattaques peuvent par exemple revêtir une importance considérable en termes de politique de sécurité, surtout si elles proviennent directement ou indirectement d'organismes étatiques étrangers. Par conséquent, le SRC doit également être en mesure d'identifier, de prévenir et d'analyser ces cyberincidents du point de vue du renseignement.

Pour ces raisons, il est pertinent d'étendre le mandat du SRC à l'ensemble du cyberespace. Afin d'éviter que le SRC devienne l'autorité de cybersécurité universelle, l'importance en matière de politique de sécurité doit cependant demeurer le critère principal. L'expression «activités importantes en matière de politique de sécurité» désigne dès lors les événements et les développements dans le cyberespace qui sont susceptibles de mettre en danger l'autodétermination de la Suisse en matière d'information, la Suisse en sa qualité de place économique et de recherche comme de siège d'organisations internationales, de causer un préjudice grave à la Suisse du point de vue de la politique de sécurité ou d'entraver la capacité d'action de ses autorités et de ses infrastructures critiques. Dans ce domaine, le SRC fournit principalement des prestations visant à protéger la Suisse contre les cyberrisques, comme le prévoient les stratégies de la Confédération en la matière.

Al. 2bis

Le réseau de renseignement est une forme particulière d'organisation permettant de regrouper les informations pertinentes pour la situation qui sont fournies au SRC par différents partenaires faisant partie du système de suivi coordonné de situation en Suisse ou par des services partenaires étrangers. Il peut notamment s'agir d'informations sur les déplacements de personnes enclines à la violence, sur les appels à la violence ou d'informations sur les menaces. La présentation électronique de la situation (voir art. 54, al. 1 et les explications qui s'y rapportent) doit contenir toutes les informations nécessaires aux autorités suisses compétentes pour prendre des mesures de sécurité. Cela inclut également les données que le SRC ne traiterait pas dans l'accomplissement de ses tâches en vertu de l'al. 1. Toutefois, le traitement dans le cadre de la présentation électronique de la situation se limite à cet instrument et au motif indiqué ici (voir art. 5, al. 6, let. e, et les explications qui s'y rapportent).

Al. 5

Afin d'assurer un service d'alerte précoce en vue de protéger les infrastructures critiques, le SRC doit établir et entretenir des contacts avec les exploitants de telles infrastructures. La tenue et la mise à jour de l'inventaire des éléments des infrastructures critiques relève pour sa part de la compétence de l'Office fédéral de la protection de la population (OFPP). Il est donc nécessaire que le SRC et l'OFPP échangent étroitement et régulièrement pour établir et entretenir des contacts avec les exploitants d'infrastructures critiques. Cet échange sera réglé plus avant dans ordonnance du 16 août 2017 sur le Service de renseignement (ORens)[8]. La précision ajoutée à cet alinéa répond à un besoin des exploitants concernés. Elle reflète en outre la Stratégie nationale du Conseil fédéral pour la protection des infrastructures critiques 2018–2022[9].

Art. 7

Al. 1, let. e et f et 1bis

7 RS **120.73**
8 RS **121.1**
9 FF **2018** 491

Un soupçon initial de menace grave pour la sécurité du SRC ou de violation des prescriptions de service peut naître de plusieurs manières et remonter par différents canaux. Par exemple, un collaborateur du SRC ou même d'un service partenaire peut envoyer une annonce de sécurité qui appelle un éclaircissement des faits. Il est également possible qu'un conflit entre employés engendre des risques de sécurité qui font alors l'objet d'un signalement. Certains indices peuvent conduire à des soupçons initiaux, comme l'introduction de téléphones portables privés ou d'autres appareils d'enregistrement dans des zones sensibles du lieu de travail ou des contacts problématiques dans l'environnement privé ou professionnel.

Ainsi, lorsque des indices concrets laissent par exemple présumer que des collaborateurs du SRC travaillent pour un service de renseignement d'un autre Etat ou sont recrutés par un tel service, le SRC doit être en mesure de donner suite à ce soupçon initial sans informer directement les individus concernés des recherches effectuées. Il y aurait sinon un risque que des indices soient détruits ou que le comportement change. L'analyse de données personnelles demeure en tous les cas soumis à l'approbation du maître des données concernées au niveau de la direction du SRC.

Quant à l'analyse des accès d'une personne en particulier aux données du SRC, elle requiert l'approbation écrite d'un membre de la direction ainsi que celle du maître des données concernées et ne peut dans certains cas être exécutée qu'avec l'aide de domaines techniques du SRC. Le principe du double contrôle au minimum est donc garanti dans tous les cas. En fonction de la sévérité du soupçon, il peut être nécessaire que le directeur du SRC mandate la Sécurité du SRC, p. ex. pour l'ouverture et l'exécution d'une procédure disciplinaire. Si le SRC constate un comportement punissable présumé, il dépose une plainte auprès des autorités de poursuite pénale compétentes.

Dans l'éventualité où un événement soulève des questions de sécurité, le SRC peut également procéder à des vérifications au sujet des collaborateurs déjà engagés et au bénéfice d'un contrôle de sécurité relatif aux personnes (CSP) en vertu de la loi du 18 décembre 2020 sur la sécurité de l'information[10] (LSI). En fonction du résultat, il entreprend ensuite un renouvellement du CSP. Contrairement aux mesures visées à la let. e, les investigations visées à la let. f nécessitent le consentement de la personne concernée. Cette mesure permet d'éviter que des collaborateurs du SRC doivent s'attendre à tout moment à de tels contrôles sur leur personne.

Al. 1, let. g et h

Le SRC doit s'assurer que les derniers candidats en lice pour un emploi au SRC, ainsi que les personnes ou entreprises répondant à des appels d'offres pour son compte ou exécutant de tels mandats, ne présentent aucun risque pour la sécurité de ses collaborateurs, de ses installations et des données qu'il traite. Les collaborateurs du SRC chargés des mesures de protection et de sécurité doivent donc récolter des informations sur ces personnes et ces entreprises. À l'instar du CSP, ces vérifications sont effectuées avec l'accord de la personne ou de l'entreprise concernée. Selon la date d'entrée en vigueur de la LSI (a priori en 2023), une coordination avec la révision de la LRens sera nécessaire.

Les vérifications consistent à consulter des données internes et externes à la disposition du SRC, à prendre des renseignements oraux et écrits, notamment auprès des personnes ou des entreprises concernées, et à consulter des sources d'information publiques. Ce travail vise des informations existantes: les vérifications prévues par la présente disposition ne fondent aucune compétence pour obtenir de nouvelles données. Les vérifications préalables en question ne remplacent par les contrôles de sécurité relatif aux personnes ni les procédures de sécurité relative aux entreprises au sens de la LSI. Celles-ci ne peuvent toutefois pas toujours être réalisées à temps avant l'engagement. Le SRC les initie avant l'entrée en fonction du collaborateur, conformément à l'art. 33 LSI. Pour des raisons d'organisation, il est cependant rarissime que le service spécialisé CSP rende une décision avant le début des rapports de travail. Ainsi, les personnes engagées ont déjà accès aux locaux du SRC et aux documents classifiés avant le résultat du CSP. Un travail efficace n'est possible que si la personne dispose d'un accès suffisant aux données générales relevant du renseignement du SRC. Le SRC demande l'accord écrit de la recrue pour effectuer le contrôle et l'informe de ses obligations relatives au secret de fonction et à la protection des données.

Lorsque le SRC souhaite recruter une personne en qualité de source humaine, il réalise certains examens préalables à son insu afin de s'assurer de sa fiabilité.

Al. 2

Etant donné que la LRens ne contient plus aucune disposition visant les systèmes d'information individuels, le terme « systèmes d'information » est remplacé par « données ». Le contenu ne s'en trouve pas modifié.

Al. 3

Afin de protéger ses collaborateurs face aux services de renseignement étrangers, le SRC tient une liste de pays présentant des risques particuliers. Certains pays tentent de surveiller les collaborateurs des services de renseignement étrangers lorsqu'ils se rendent sur leur territoire. Il peut s'agir déjà de contrôles renforcés à la frontière. Certains pays essaient de découvrir avec qui les agents de renseignement entretiennent des contacts. Il n'est pas rare non plus que les téléphones portables soient surveillés afin d'espionner les échanges de données ainsi que les mouvements dans le pays en question, ou encore qu'ils soient piratés de manière à observer également les activités du propriétaire à son retour en Suisse. Pour ces types de surveillance, aucune distinction n'est faite entre les voyages privés et professionnels.

Si un collaborateur du SRC veut visiter un des pays concernés sur son temps libre, il doit donc demander l'autorisation du service du SRC compétent pour les mesures de protection et de sécurité. Le réseau international informel des services de renseignement occidentaux étudie actuellement une éventuelle standardisation de ces mesures afin d'assurer la collaboration internationale future. Soumettre à autorisation les voyages privés constitue une certaine atteinte des droits fondamentaux du collaborateur, aussi cette mesure requiert une base légale.

Art. 8, al. 1

Par souci d'harmonisation de la terminologie, le terme « risques » a été remplacé par « menaces ».

[10] RS… (FF **2020** 9665)

Art. 9, al. 3

Les autorités d'exécution cantonales ont l'obligation d'enquêter sur tous les indices de menaces au sens de l'art. 6, al. 1, let. a. À cet égard, il est possible que l'enquête sur l'activité ne révèle aucun lien avec les tâches du SRC (p. ex. si un enseignant craint une radicalisation d'un élève affichant sa croyance islamique et s'adresse à une autorité d'exécution cantonale, mais que cette dernière infirme les soupçons). Dans de tels cas, les autorités d'exécution cantonales peuvent conserver les données traitées à des fins de traçabilité pendant cinq ans (voir art. 46, al. 4), mais n'en informent pas le SRC. À l'inverse, si une menace pour la sûreté intérieure ou extérieure au sens de la LRens se concrétise, elles soumettent immédiatement un rapport au SRC. Étant donné que l'actuel art. 85, al. 2, contient une disposition identique, il peut être supprimé (voir les explications concernant cet article).

Al. 4

Ce nouvel alinéa précise que le SRC est responsable du traitement des données des autorités d'exécution cantonales, au sens de l'art. 5, let. j, nLPD, dès lors que leur traitement se fonde sur la LRens, et ce indépendamment du fait que ces autorités aient agi spontanément ou sur mandat concret du SRC: Le SRC ne court ici toutefois aucun nouveau risque, car il assume déjà cette responsabilité et minimise les risques qui en découlent par l'auto-contrôle (voir art. 75 LRens). Les demandes d'accès reçues par les autorités cantonales sont traitées par le SRC en vertu des art. 63 ss.

Art. 14, al. 3

Le droit en vigueur autorise le SRC à observer des événements et des installations dans des lieux publics et librement accessibles et à y effectuer des enregistrements visuels et sonores. Cela inclut également l'observation en accompagnement, c'est-à-dire le suivi et l'observation d'une personne (en règle générale) ou d'un véhicule pendant une certaine durée par une équipe.

Les collaborateurs affectés à de telles observations sont tenus de respecter la législation en vigueur. En l'état, il est donc d'autant plus facile pour la personne suivie de se soustraire à l'observation et d'autant plus difficile pour l'équipe de maintenir le contact visuel. Il suffit ainsi d'un feu rouge grillé, d'un excès de vitesse ou d'un changement de direction dans un trafic dense pour que l'équipe d'observation perde le contact. Les lois cantonales sur la police (par ex. FR, GE, GR, NE, SZ, TG, TI, ZH) sont donc de plus en plus souvent modifiées pour permettre l'utilisation d'appareils de localisation (émetteurs GPS) durant ces observations afin de retrouver rapidement la personne ou l'objet cible si le contact visuel est perdu.

Le Tribunal fédéral a connu en avril 2020 d'un recours soumis par différentes organisations visant une nouvelle disposition sur l'utilisation d'appareils de localisation dans la loi sur la police du canton de Berne[11]. À cet égard, il a jugé que la surveillance (en temps réel) par un émetteur GPS posé sur un véhicule constituait une atteinte significative à la sphère privée de la personne visée et a donc abrogé l'art. 118, al. 2, de la loi bernoise sur la police. Le Tribunal fédéral a notamment souligné que la disposition en question ne se restreignait pas aux soupçons concrets ou urgents d'infractions et ne prévoyait aucune limitation de temps. La disposition bernoise était certes intitulée « Observation », mais formulée de manière trop ouverte (« Elle peut utiliser à cette fin des dispositifs techniques de surveillance pour localiser une personne ou une chose ») pour déterminer s'il s'agissait d'une forme d'observation dans l'espace public à part entière ou d'une mesure d'accompagnement du travail de l'équipe d'observation. Par conséquent, le Tribunal fédéral a jugé qu'il s'agissait d'une mesure autonome et l'a comparée aux dispositions analogues du Code de procédure pénale[12] (CPP, art. 280 ss) et de la LRens (art. 26, al. 1, let. b). Il a donc conclu que sans conditions restrictives, sans autorisation du tribunal et, dans certains cas, sans notification ultérieure, une telle mesure n'est pas admissible.

Le Conseil fédéral considère que cet arrêt ne ferme pas la porte à l'utilisation de dispositifs de localisation comme mesure d'accompagnement d'observations légalement autorisées et soumises à des conditions restrictives, lorsque la localisation ne constituerait pas une atteinte à la sphère privée nettement plus grave que l'observation proprement dite.

L'utilisation d'un appareil de localisation proposée ici se limite donc à la transmission des coordonnées actuelles de l'objet durant l'observation et dans le seul but d'en assurer la continuité. Si le contact visuel avec l'objet observé est durablement perdu, la transmission des données doit être interrompue. Cette durée doit rester courte: elle doit être adaptée aux circonstances sans dépasser une heure. L'utilisation d'un appareil de localisation durant une observation est dès lors uniquement un appui. Les données ne peuvent être stockées pour une analyse ultérieure ni à d'autres fins. Si, pour des raisons techniques, l'enregistrement des données est nécessaire au fonctionnement de l'appareil de localisation, elles doivent être détruites immédiatement à la fin de l'observation. Si l'objet de l'observation ne se trouve pas dans un lieu public et librement accessible, la transmission des données de l'appareil de localisation doit être interrompue. Il en va de même lorsque l'équipe met fin à l'observation. Si elle souhaite reprendre l'observation ultérieurement, elle doit retrouver l'objet par les moyens usuels. La transmission des données de localisation ne peut être relancée qu'une fois que l'objet de l'observation est en vue de l'équipe. Ces dispositions détaillées relèvent toutefois du droit de l'ordonnance, qui sera révisée par la suite.

Dès lors, l'utilisation d'un appareil de localisation prévue par cet article est à distinguer clairement de celle prévue par les art. 280, let. c, CPP et 26, al. 1, let. b, LRens. Ces deux dispositions visent avant tout à localiser durablement un objet ou une personne et à suivre ses déplacements durant une période prédéfinie. Elles sont soumises à des conditions strictes, prévues pour un usage durable et constituent ce que le Tribunal fédéral définit comme une atteinte significative à la sphère privée.

A l'inverse, la présente disposition règle simplement l'utilisation d'un appareil de localisation afin de faciliter et d'assurer la réussite d'une observation. De cette manière, les manœuvres de dépassement dangereuses dans un trafic dense peuvent être évitées, car l'équipe d'observation est capable de retrouver l'objet suivi grâce au dispositif de localisation s'il est sorti un court instant de son champ de vision. De même, il est plus facile pour l'équipe de ne pas être détectée si elle n'a pas besoin de garder la même distance à la cible. À cet égard, l'atteinte à la vie privée n'est pas plus grave que celle déjà constituée par l'observation proprement dite. Cette dernière consiste non seulement à déterminer où se trouve la cible, mais aussi son comportement, ses contacts éventuels, etc. Soutenir une observation en accompagnement par l'utilisation d'appareils de localisation sans autorisation du tribunal apparaît donc proportionné au regard de la jurisprudence fédérale. Le SRC demeure quoi qu'il en soit tenu aux règles de la recherche de données, qui prescrit la proportionnalité dans la sélection de la mesure de recherche (art. 5, al. 3).

[11] Arrêt 1C_181/2019; ATF 147 I 103
[12] RS **312.0**

L'utilisation d'un appareil de localisation en vertu du présent article ne remplacera pas la surveillance permanente prévue par l'art. 26, al. 1, let. b, LRens en cas de menace grave pour la sûreté de la Suisse. L'utilisation d'un appareil de localisation prévue par l'art. 26, al. 1, let. b, LRens a quant à elle lieu sans observation et les données recherchées sont saisies et évaluées en continu ou a posteriori au siège de l'autorité.

Art. 18

Lorsque le SRC collabore avec des services nationaux pour rechercher des informations, il peut être nécessaire qu'il protège leurs collaborateurs au même titre que les siens ou ceux des autorités d'exécution cantonales Sont concernés en première ligne les services du DDPS mandatés par le SRC pour des acquisitions dans le cyberspace (Computer Network Operations du Centre des opérations électroniques de la Base d'aide au commandement de l'armée, à l'avenir a priori le commandement Cyber). L'art. 18, al. 1, est complété en conséquence par une let. b^{bis}.

La LRens emploie le terme « autorités d'exécution cantonales », aussi la formulation de l'al. 2, let. a, est harmonisée en ce sens.

Art. 19

Al. 2, let. f

À l'instar de la nouvelle formulation de l'art. 6, al. 1, let. b, le catalogue des menaces possibles en lien avec le droit d'accès en cas de menace concrète est complété pour inclure les activités importantes en matière de politique de sécurité dans le cyberespace.

Art. 20

Al. 1, let. b

Cette modification est requise pour refléter le nouveau nom de l'autorité citée depuis la réorganisation des gardes-frontières et des douanes, mais n'est pas de nature matérielle. Étant donné que la nouvelle loi définissant les tâches d'exécution de l'Office fédéral de la douane et de la sécurité des frontières (OFDF)[13] est encore à l'état de projet, sa date d'entrée en vigueur déterminera si la présente disposition est caduque.

Al. 1, let. i

Les autorités exploitant des systèmes informatiques ou qui en soutiennent d'autres à cette fin sont tenues de fournir au SRC les renseignements dont il a besoin sur les cyberattaques importantes en matière de politique de sécurité, et ce afin que le SRC puisse établir une présentation exhaustive de la situation et prendre les mesures nécessaires afin de déceler et de prévenir les cyberattaques. Cette disposition ne remplace en aucun cas les prescriptions visant à protéger le secret des télécommunications, qui doivent être respectées en cas de mesures de surveillance spécifiques.

Une proposition de réglementation analogue figure également dans le projet de modification de la loi sur la sécurité de l'information, qui était en consultation du 12 janvier au 14 avril 2022[14]. Si l'art. 73c, al. 1, qui y est prévu, devait entrer en vigueur avant, l'ajout concernant le centre national pour la cybersécurité "ou contribuant à protéger des systèmes informatiques" deviendrait superflu.

Al. 1, let. j

Seul le sigle de la loi du 10 octobre 1997 sur le blanchiment d'argent (LBA)[15] a été ajouté afin de correspondre aux directives sur la technique législative.

Art. 25

Al. 1, let. a

L'obligation faite aux particuliers de fournir des renseignements est étendue aux exploitants d'établissements d'hébergement. À l'instar des entreprises de transport déjà soumises à la même obligation, ils disposent souvent d'informations et de données requises pour déceler à temps et prévenir les menaces pour la sûreté intérieure ou extérieure. Le SRC peut ainsi identifier les lieux de séjour temporaires de personnes cibles ainsi que, selon la situation, les contacts d'une personne cible, p. ex. si elle paie plusieurs chambres d'hôtel ou si sa chambre est payée par un tiers. Il peut également déterminer quelles organisations louent des locaux afin d'organiser des rencontres. Les principes applicables à la conservation des données ou aux obligations faites aux établissements d'hébergement de communiquer des renseignements demeurent régis par le droit cantonal. La LRens ne crée pas de nouvelles obligations en matière de collecte et de conservation des données; elle se contente de prévoir l'accès aux données existantes à la demande du SRC ou de l'autorité cantonale d'exécution. Comme auparavant, des renseignements ne seront exigés que dans des cas particuliers.

Le terme « établissement d'hébergement » inclut tous les exploitants qui proposent (le plus souvent à titre payant) des nuitées à des tiers. Les données sur l'échange de logements organisé de manière commerciale sont également concernées par cette disposition.

Al. 3

À l'instar des autorités visées aux art. 19 et 20, les particuliers ont désormais l'interdiction de divulguer à des tiers les éventuelles demandes de renseignements du SRC. Cette disposition respecte le principe de dissimulation de la recherche d'informations prévue par l'art. 5, al. 4.

Section 4: Mesures de recherche soumises à autorisation

Les dispositions en vigueur concernant les mesures de recherche soumises à autorisation (MRSA) doivent être modifiées en raison des premières expériences avec leur application et des adaptations requises par plusieurs interventions parlementaires[16]. D'une part, une

13 FF **2020** 7196
14 Disponible sous : www.fedlex.admin.ch >Procédures de consultations >Terminées >2022 >DFF >Obligation de signaler les cyberattaques contre les infrastructures critiques
15 RS **955.0**
16 P. ex: Po 17.3831 et Mo 20.4568.

nouvelle mesure de recherche soumise à autorisation comblera une lacune dans la recherche de données. En effet, le SRC ne dispose actuellement d'aucun outil pour obtenir des informations sur les intermédiaires financiers dans le cadre du financement de personnes ou de groupes importants pour la sécurité. Il sera désormais possible de surveiller certaines personnes par le biais de leurs relations financières par l'intermédiaire des banques et d'autres institutions financières (voir les explications de l'art. 26, al. 1, let. f et g).

D'autre part, le domaine d'application des mesures de recherche soumises à autorisation sera étendu à l'extrémisme violent (voir les explications de l'art. 27, al. 1, let. a). L'obtention de renseignements financiers et les recherches sur l'extrémisme violent seront soumises aux conditions strictes imposées par l'art. 27 au même titre que les autres mesures de cet ordre.

Par ailleurs, l'actuel art. 29 est scindé en plusieurs articles afin de proposer une structure qui distingue mieux le contenu des dispositions relatives à la procédure d'autorisation.

Art. 26

Al. 1

Let. b

Une précision est ajoutée ici pour rappeler que des appareils de localisation peuvent être utilisés sans requérir d'autorisation dans le cadre de mesures d'observation. On se référera à cet égard aux explications de l'art. 14, al. 3.

Let. f et g

Ces nouvelles mesures de recherche soumises à autorisation se fondent sur les art. 284 et 285 CPP, qui règlent la surveillance des relations entre une personne cible du SRC et les institutions soumises à la loi sur le blanchiment d'argent. Le renvoi à l'art. 2 LBA permet de faire correspondre la liste des personnes et institutions assujetties à l'obligation de renseigner par la nouvelle mesure de recherche soumise à autorisation à celle du champ d'application de la LBA.

Le financement du terrorisme, en particulier, ne passe pas uniquement par de grandes banques, mais également par de plus petites entreprises qui proposent des services de transfert internationaux d'argent ou encore par des personnes qui échangent de l'argent liquide. Par conséquent, la LRens reprend la définition fixée dans la LBA des personnes potentiellement concernées et auprès desquelles l'obtention de renseignements sur les transactions et les relations commerciales est possible. La transparence de ces flux monétaires, rendue possible par la surveillance des relations, sert au SRC à accomplir ses tâches en vertu de l'art. 6 LRens.

Le SRC s'intéresse au contexte du financement des organisations et des groupes qui ont déjà retenu son attention sur la base d'autres informations. Une surveillance ciblée permet de mieux évaluer la menace que représente une organisation ou un groupe pour la sûreté intérieure ou extérieure de la Suisse. On pensera notamment aux entreprises, aux organisations idéologiques ou aux institutions religieuses pour lesquelles il existe des indices fondés qu'elles sont impliquées dans des activités de terrorisme, de renseignement ou d'extrémisme violent (voir les explications de l'art. 27, al. 1, let. a), et en particulier dans leur financement. Les informations sur l'origine du financement peuvent fournir au SRC des éléments probants supplémentaires pour déceler à temps et prévenir une menace pour la sûreté intérieure et extérieure de la Suisse.

A l'heure actuelle, le SRC n'a que très peu de solutions pour obtenir des informations sur le financement d'une telle structure. Dans des cas particuliers et à certaines conditions, il peut ainsi obtenir des informations du Bureau de communication en matière de blanchiment d'argent (MROS; art 29, al. 2bis et 2ter, en relation avec les art. 30 s. LBA ainsi que l'art. 20, al. 1, let. j, LRens).

En sa qualité de cellule de renseignements financiers (CRF) et conformément à la LBA, le MROS est l'office central et national qui réceptionne et analyse les annonces faites par les institutions soumises à la LBA de cas suspects de blanchiment d'argent, de financement du terrorisme, d'infractions préalables au blanchiment ou à la criminalité organisée (art. 23, al. 2, LBA), qui échange des informations à l'échelle nationale et internationale (art. 29 et 30 LBA) et qui dénonce les cas fondés à l'autorité de poursuite pénale compétente (art. 23, al. 4, LBA).

A première vue, l'énumération des tâches du Bureau de communication pourrait laisser penser que l'échange d'informations entre lui et le SRC remplit déjà l'objectif de la nouvelle loi. Il n'en est pourtant rien: les annonces des intermédiaires financiers au MROS présupposent un soupçon fondé, p. ex. de financement du terrorisme (art. 9 LBA). Le simple fait qu'une organisation idéologique appelle ses membres à la violence ne justifie pas une annonce de l'intermédiaire financier au MROS. Il en découle qu'il ne communique une annonce qu'une fois qu'il a également identifié les fins de financement du terrorisme. Enfin, le MROS est également tenu strictement à la règle de la spécialité en vigueur à l'échelle internationale pour les CRF lors de la communication d'informations. D'après ce principe fondamental de la collaboration internationale, les informations échangées entre les CRF devraient exclusivement être utilisées aux fins pour lesquelles elles ont été sollicitées ou fournies (ch. 3 de la note interprétative de la recommandation 40 du Groupe d'action financière). Lorsqu'il reçoit des informations, le Bureau de communication doit respecter les conditions de l'autorité qui les a transmises. Ce principe s'applique également lorsqu'il transmet des informations reçues d'un homologue étranger à une autorité nationale avec l'autorisation de ce dernier (art. 29, al. 2ter, LBA).

Les tâches du SRC sont différentes de celles du MROS: le SRC recherche des informations à titre préventif et demeure seul responsable de l'acquisition d'informations visant à maintenir la sûreté intérieure et extérieure. S'il dispose d'indices concrets selon lesquels, par exemple, une institution religieuse recrute des personnes dans le but de menacer gravement la sûreté intérieure ou extérieure de la Suisse, il doit être en mesure d'exiger des informations sur le financement de cette institution, mais aussi sur son réseau, afin de compléter son évaluation de la menace. Dans certains cas, ces informations peuvent constituer une base importante pour prendre des mesures supplémentaires, telles qu'une interdiction d'exercer une activité au sens de l'art. 73 LRens. La nouvelle disposition vise donc à combler une lacune importante dans les moyens de recherche de données du SRC.

Cette mesure de recherche devra être soumise à autorisation au sens de la LRens, car elle constitue en particulier une atteinte à la liberté économique et à la liberté personnelle. Les mesures de recherche soumises à autorisation sont soumises à des conditions très strictes et requièrent à la fois une autorisation du Tribunal administratif fédéral et l'aval du chef du DDPS.

Cette nouvelle mesure de recherche de données vient donc compléter l'échange d'informations entre le SRC et le MROS (voir art. 29, al. 2bis et 2ter, en relation avec les art. 30 s. LSA et 20, al. 1, let. j, LRens). Il est toutefois capital qu'elle ne viole pas l'interdiction d'informer au sens de l'art. 10*a* LBA, qui met en œuvre l'interdiction d'informer la personne concernée, conformément aux standards du Groupe d'action financière. Le client de l'institut financier ne doit pas apprendre qu'il a fait l'objet d'une annonce de cas suspect, au risque de mettre en péril la poursuite pénale et en particulier l'administration des preuves.

Cette mesure de recherche soumise à autorisation supplémentaire ne sera pas utile au SRC uniquement pour l'exécution de ses tâches dans le domaine du terrorisme. Les informations tirées de données financières serviront également à déceler à temps et à prévenir les menaces pour la sûreté intérieure ou extérieure constituées par l'espionnage. Par exemple, les informations sur le financement des infrastructures utilisées comme couverture, telles que les logements ou les abonnements aux raccordements de télécommunications utilisés pour contacter les sources, peuvent être d'un grand intérêt. Il est également possible de découvrir ou de confirmer l'existence d'une société écran si seules des personnes identifiées par le SRC comme des agents sous couverture utilisent les comptes de cette société. Selon la situation, il est donc possible d'identifier les personnes qui travaillent en Suisse pour un autre Etat.

Dans le contexte de l'extrémisme violent (voir les explications de l'art. 27, al. 1, let. a), les informations sur les transactions financières peuvent permettre de savoir quels immeubles ont été acquis ou sont entretenus par des personnes identifiées comme extrémistes violents, quels biens ces personnes acquièrent et quelles personnes et organisations les soutiennent financièrement ou sont soutenues par elles. De même, les informations sur le financement des événements de grande envergure des groupements extrémistes violents peuvent fournir les éléments nécessaires à l'exploration du réseau.

Art. 27

Al. 1, let. a

Par souci de lisibilité, cette lettre est scindée en plusieurs chiffres.

Ch. 1

Depuis l'entrée en vigueur de la LRens, les réactions violentes des extrémistes de droite et de gauche se sont amplifiées. L'agressivité envers les forces de sécurité et le potentiel de violence global de ces groupes augmentent. Les extrémistes de droite ont encore relativement rarement recours à la violence, mais ils s'entraînent aux arts martiaux et s'arment de plus en plus. Les extrémistes de gauche sont fortement interconnectés à l'international et ils ont plus fréquemment recours à la violence contre les autorités et les groupes idéologiquement opposés.

La notion d'extrémisme violent désigne les organisations et les personnes qui rejettent les fondements de la démocratie et de l'Etat de droit et qui commettent, encouragent ou approuvent des actes de violence pour atteindre leurs buts (voir art. 19, al. 2, let. e). Lors de la promulgation de la loi sur le renseignement, l'extrémisme violent a certes été exclu des mesures de recherche soumises à autorisation, mais les événements survenus à l'étranger ont montré que ces activités peuvent également prendre des proportions telles qu'elles menacent gravement la sûreté intérieure ou extérieure. Dans certains cas, il s'agissait d'extrémistes violents connus des autorités, mais qui ont commis des actes d'une ampleur relevant du terrorisme (p. ex. les attentats de Christchurch en Nouvelle-Zélande ou de Halle en Allemagne). La radicalisation et la propension à la violence d'une partie de ces groupes de personnes sont également en nette augmentation en Suisse. L'acquisition d'armes, de munitions, d'explosifs et la formation à leur utilisation ne permettent pas en soi de supposer qu'un extrémiste violent franchira le seuil du terrorisme. Le fait qu'un cas isolé relève d'une activité extrémiste violente ou terroriste dépend de l'objectif, de l'intensité et de la gravité de l'acte ainsi que de son contexte. La distinction ne peut souvent être effectuée qu'après l'acte.

Sans employer de mesures de recherche soumises à autorisation, ces développements sont particulièrement durs à identifier. Les milieux concernés recourent de plus en plus à des méthodes secrètes, sur lesquelles le SRC ne peut enquêter que de manière insuffisante avec les mesures de recherche actuellement autorisées et non soumises à autorisation. C'est pourquoi, dans le cas des formes graves d'activités extrémistes violentes pouvant porter atteinte à la vie et à l'intégrité corporelle, le recours à des mesures de recherche soumises à autorisation doit également être permis. On pensera au cas dans lequel des renseignements indiquent que les extrémistes violents s'arment et s'entraînent tout en s'isolant plus fortement du monde extérieur d'une part, et d'autre part en commentant de plus en plus (notamment sur les réseaux sociaux) les attaques extrémistes violentes ou terroristes qui ont déjà eu lieu. Le seuil des actes préparatoires délictueux n'est en l'occurrence pas encore franchi et les personnes concernées n'ont pas de liens avec des groupements terroristes connus. Cependant, l'ensemble des informations obtenues peut indiquer une menace grave pour la sûreté qui doit être examinée plus avant (voir le rapport du Conseil fédéral du 13 janvier 2021 en réponse au postulat 17.3831 Glanzmann-Hunkeler[17]: Instruments efficaces pour lutter contre l'extrémisme violent).

Si les instruments de prévention s'avèrent lacunaires, la Suisse court le risque considérable de devenir un lieu de repli ou de rencontre pour les extrémistes violents étrangers (voir l'avis du Conseil fédéral du 13 mai 2020 sur le postulat 20.3100 Jositsch : Evaluation de l'efficacité de la nouvelle loi sur le renseignement[18]). Par conséquent, des mesures de recherche soumises à autorisation sont requises aujourd'hui à la fois à l'échelle cantonale et fédérale (voir p. ex. le postulat 17.3831 mentionné précédemment) pour la détection précoce et la prévention de l'extrémisme violent qui menace gravement la sûreté. L'expérience acquise à ce jour avec les mesures de recherche soumises à autorisation montre que leur utilisation est adaptée à des clarifications ciblées et précises dans des cas graves. Le SRC emploie ces instruments avec parcimonie et uniquement en cas de menace grave. Ces mesures sont également soumises à l'autorisation du Tribunal administratif fédéral, qui examine leur nécessité et leur proportionnalité. Ainsi, elles ont seulement été employées quatre fois en 2017, huit fois en 2018, cinq fois en 2019 et quatre fois en 2020. Ces chiffres montrent que le SRC utilise cet outil avec retenue et uniquement dans les cas de menaces graves, tel que la loi le prévoit.

Le domaine d'application des mesures de recherche soumises à autorisation est étendu à l'extrémisme violent grâce à la suppression de la restriction aux let. a à d de l'art. 19, al. 2, LRens. Les conditions strictes auxquelles l'utilisation de ces mesures est soumise en vertu de l'art. 27, al. 1, demeurent toutefois inchangées et s'appliquent également aux mesures de recherche visant l'extrémisme violent. En particulier, la mesure doit être justifiée par la gravité de la menace.

Ch. 2

La pratique a montré que le Tribunal administratif fédéral ne peut autoriser des mesures de recherche soumises à autorisation dans le domaine des télécommunications (au demeurant uniquement exécutables en Suisse pour des raisons techniques) pour enquêter sur des activités terroristes que lorsque la sûreté de la Suisse proprement dite est menacée concrètement et immédiatement au sens de l'art. 19, al. 2, LRens. Il en va de même pour les affaires liées à des organisations terroristes interdites au niveau national et international, telles

[17] Disponible sous: www.parlament.ch >17.3831> Rapport en réponse à l'intervention parlementaire.
[18] Disponible sous: www.parlament.ch > 20.3100.

qu'Al-Qaïda ou l'« Etat islamique ». Leurs dirigeants à l'étranger utilisent parfois des services de télécommunications suisses, qui ne peuvent être explorés que par des mesures de recherche soumises à autorisation. Par le passé, le Tribunal administratif fédéral a dû rejeter une demande du SRC parce que la gravité de la menace (immédiate) pour la sûreté de la Suisse n'était pas suffisamment concrète. Il a rappelé qu'il appartenait au législateur de créer une base juridique pour l'application des mesures de recherche soumises à autorisation à de tels cas.

Le Conseil fédéral propose donc, en référence à l'art. 2, let. d, LRens, d'introduire la menace grave pour des intérêts internationaux importants en matière de sécurité comme critère supplémentaire pour ordonner en Suisse des mesures de recherche soumises à autorisation. Pour des raisons techniques, certaines enquêtes sur les communications entre des personnes qui représentent une menace grave pour la sûreté internationale ne sont possibles qu'en Suisse. Si une telle personne, par exemple un dirigeant de haut rang d'une organisation terroriste internationale, utilise un service de communication transitant par la Suisse ou si des acteurs étrangers mènent des cyberattaques graves contre d'autres pays via des infrastructures suisses, le SRC doit également pouvoir mener des enquêtes dans l'intérêt de la sûreté internationale et non seulement en cas de menace immédiate pour la Suisse. À l'instar de la protection des intérêts de la Suisse en matière de sécurité, les intérêts internationaux en la matière devraient être limités aux domaines cités par l'art. 6, al. 1 let. a et b, à savoir la lutte contre le terrorisme, l'espionnage, la prolifération, les cyberattaques et l'extrémisme violent ainsi que les événements importants en matière de politique de sécurité se produisant à l'étranger et dans le cyberespace. Une telle aptitude à la coopération pourrait en outre faciliter la coopération internationale au profit de la sûreté de la Suisse.

Le Conseil fédéral se prononce en faveur d'un usage aussi restrictif qu'auparavant de ces nouvelles possibilités de détection précoce des menaces graves liées à l'extrémisme violent ou des intérêts internationaux importants en matière de sécurité et ne s'attend pas à une augmentation significative du nombre de cas dans lesquels ces mesures seront employées. Les conditions juridiques à leur utilisation demeurent strictes et soumises à l'examen indépendant du Tribunal administratif fédéral. Ces mesures requérant l'aval du chef du DDPS, elles peuvent en outre être contrôlées activement à l'échelle des institutions politiques. Au total, si la situation de la menace reste inchangée, il faudra probablement compter sur environ cinq à dix cas supplémentaires par an dans lesquels des mesures de recherche soumises à autorisation seront utilisées pour enquêter sur des menaces graves d'extrémisme violent ou des menaces pour des intérêts internationaux importants en matière de sécurité. Les tâches qui en découlent peuvent, dans la situation actuelle, être traitées avec les ressources existantes.

Art. 28

Cet article est reformulé pour préciser qu'il inclut également les cas dans lesquels la personne visée n'a pas accès à l'infrastructure de la tierce personne à surveiller (téléphone, véhicule, adresse postale, etc.), mais l'utilise pour transmettre des informations, y compris à cette tierce personne. Prenons pour exemple un djihadiste suisse à l'étranger dont on sait qu'il communique régulièrement avec un tiers en Suisse, par exemple un ami ou un membre de sa famille. Il est techniquement impossible de surveiller ses télécommunications à l'étranger, à l'inverse du raccordement du tiers en Suisse. Dès lors, des informations importantes pour la sûreté de la Suisse peuvent être obtenues afin d'écarter les menaces terroristes. L'ajout de « à partir de cet emplacement ou vers cet emplacement » précise qu'il est également possible d'ordonner une mesure de recherche soumise à autorisation à l'encontre d'un tiers s'il ne fait que recevoir des informations à destination de la personne à surveiller. Par ailleurs, les exigences strictes concernant la gravité de la menace et la proportionnalité de la mesure s'appliquent également ici.

Le second alinéa de l'actuel art. 28 est supprimé. On se réfèrera à la place à l'art. 50, al. 2, lui aussi applicable lorsque qu'une mesure de recherche soumise à autorisation (MRSA) est ordonnée à l'encontre d'un tiers. La pratique a montré qu'une personne soumise au secret professionnel (p. ex. y c. un assistant médical) peut souscrire de nombreux abonnements de téléphonie mobile à titre privé et transférer entièrement leur utilisation à d'autres personnes. La personne soumise au secret professionnel n'utilise jamais ces raccordements, ce qui signifie que le secret professionnel n'est en réalité pas affecté. Si l'utilisateur réel du raccordement représente une menace suffisamment grave pour la sûreté de la Suisse, il n'est pas pertinent d'en exclure la surveillance. Ici aussi, la solution appropriée consiste à effectuer un triage sous la surveillance du Tribunal administratif fédéral.

Art. 29

Dans l'al. 1, la let. c est complétée et une nouvelle let. d ajoutée. Le reste de l'alinéa demeure inchangé.

Al. 1, let. c

Dans la pratique, les mesures de recherche soumises à autorisation ne peuvent parfois pas être mises en œuvre sans mesures d'accompagnement. Par exemple, un véhicule sur lequel doit être fixé un appareil de localisation, après obtention de l'autorisation du tribunal et de l'aval politique, peut être garé sur une propriété publique ou privée librement accessible, dans un parking souterrain privé à accès limité, dans un garage individuel verrouillable ou sur une place de stationnement privée appartenant à un tiers, etc. Pour installer (et plus tard retirer) l'appareil de localisation, il est donc nécessaire de pénétrer dans les locaux et les lieux concernés, les rapports de propriété n'étant pas toujours clairement identifiables au premier coup d'œil. Sur la base de l'art. 269ter, al. 2, CPP, la LRens devrait également prévoir la possibilité d'autoriser les mesures d'accompagnement nécessaires en même temps que la mesure principale (p. ex. la pose d'un appareil de localisation).

Celles-ci varient selon les cas et ne peuvent donc pas toutes être énumérées dans la loi. Le SRC doit donc les décrire précisément dans les documents requis pour obtenir l'autorisation et l'aval. En cas d'autorisation, le Tribunal administratif fédéral évalue l'admissibilité des exigences comparables en termes d'aptitude, de nécessité et de subsidiarité au même titre que pour la mesure principale.

Al. 1, let. d

A la suite de la modification de l'art. 29*a*, al. 3 (voir plus bas), de l'information sur les mesures ordonnées par les autorités de poursuite pénale et le service SCPT, les données sur la procédure pénale font désormais partie de la demande.

Art. 29a

Al. 1

Cet alinéa correspond à l'actuel art. 29, al. 2. En raison de la modification de l'art. 29, al. 1, let. c, il est précisé ici expressément en référence à l'art. 274, al. 4, CPP, que le Tribunal administratif fédéral doit se prononcer sur les éventuelles mesures d'accompagnement.

Al. 2

Cet alinéa reflète essentiellement la première phrase de l'actuel art. 29, al. 3. La disposition en vigueur interdit au Tribunal administratif fédéral d'autoriser une MRSA lorsque *celle-ci* a déjà été autorisée sur la base d'une procédure pénale engagée à l'encontre des personnes visées. Une ambiguïté subsiste: entend-on par « celle-ci » une mesure identique (donc une autre surveillance des télécommunications) ou toute autre mesure de contrainte (p. ex. une surveillance technique en vertu du droit de procédure pénale, tandis que le SRC demande une surveillance des télécommunications)? Il est donc nécessaire de préciser de quelle mesure il s'agit.

En outre, l'alinéa en vigueur ne concerne que le moment de l'autorisation et ne contient pas de disposition explicite pour le cas où une mesure de contrainte identique relevant de la procédure pénale ne serait ordonnée que pendant la MRSA en cours. Une subsomption en vertu de l'art. 32, al. 1, let. b (fin de la mesure de recherche lorsque les conditions ne sont plus remplies) n'est pas indispensable, en particulier parce que les conditions pour ordonner une MRSA sont citées à l'art. 27, al. 1, tandis que la disposition relative aux mesures identiques relevant de la procédure pénale figure sous le titre « Procédure d'autorisation ».

Comme prévu auparavant, différentes mesures doivent pouvoir être prises en parallèle par les autorités de poursuite pénales comme par le Service de renseignement, tout en excluant mutuellement les mesures produisant le même effet. L'ajout du terme *identique* dans le texte met donc l'accent sur cette subtilité. Si, par exemple, une écoute téléphonique est effectuée sur le réseau fixe sur ordre du Ministère public de la Confédération, le SRC devrait être autorisé à s'infiltrer en même temps sur un téléphone mobile attribuable à la personne visée et à enquêter sur cette communication, car bien que les mesures soient similaires, elles ne sont pas identiques (et elles sont effectuées à des fins différentes). En revanche, l'écoute simultanée d'un même numéro de téléphone fixe par le Ministère public de la Confédération et le SRC ne serait pas autorisée, car les mesures sont identiques.

Le Conseil fédéral estime que les doutes exprimés par le Tribunal administratif fédéral peuvent être levés de manière adéquate par la procédure d'autorisation. Ce dernier craint en effet que cette disposition ne vienne à mélanger la surveillance relevant de la procédure pénale et de celle relevant des services de renseignement si une MRSA ne peut être exclue que dans le cas de mesures de contrainte identiques relevant du droit de procédure pénale, servant des buts différents et liées à d'autres conditions (prévention/répression). Dans ses demandes, le SRC doit faire référence aux mesures de contrainte relevant du droit de procédure pénale et expliquer pourquoi les MRSA demandées ne sont pas redondantes. Dans le cas où des informations obtenues grâce à des MRSA sont transmises aux autorités de poursuite pénale, le SRC doit indiquer leur origine afin que ces autorités puissent s'assurer que les garanties de procédure pénale dont bénéficie la personne inculpée ne sont pas compromises ni contournées.

Al. 3

Cet alinéa correspond pour l'essentiel à la seconde phrase de l'actuel art. 29, al. 3. Il reflète la pratique actuelle, selon laquelle le SRC s'informe directement des éventuelles mesures entreprises par les autorités de poursuite pénale ou le service SCPT et transmet ces données dans sa demande au Tribunal administratif fédéral.

Al. 4

Le contenu de cet alinéa reflète essentiellement celui de l'actuel art. 29, al. 4 et 5.

Il est complété par une mention des mesures d'accompagnement. Celles-ci sont donc placées au même niveau que les mesures de recherche dans le cadre de la demande d'autorisation.

Il indique en outre que le Tribunal administratif fédéral peut assortir de certaines conditions ou obligations l'autorisation, comme c'est déjà le cas dans la pratique. La nouvelle formulation efface ainsi une différence entre les trois langues.

Al. 5

Par souci de clarté, il est précisé ici que le Tribunal administratif fédéral ne peut statuer que sur les mesures relevant de l'ordre juridique suisse. Si la personne visée par une mesure en cours d'exécution se rend à l'étranger, les dispositions des art. 36 ss s'appliquent, notamment l'art. 37 pour l'infiltration dans des systèmes et réseaux informatiques. Le Tribunal administratif fédéral ne peut autoriser de mesures réalisées à l'étranger. Le chef du DDPS décide de mettre en œuvre une telle mesure après avoir consulté le chef du DFAE et le chef du DFJP (art. 37, al. 2).

Art. 29b

Al. 1

D'après la législation en vigueur, le délai de trois mois pour l'autorisation court dès le moment où elle est rendue, et ce qu'importe le temps requis pour l'aval politique ou que le SRC soit réellement en mesure de mettre en œuvre la mesure de recherche autorisée. La durée effective de la mesure peut s'en trouver raccourcie, tout comme le délai pour déposer une demande de prolongation. À l'avenir, le délai de trois mois d'une mesure de recherche d'informations ne courra plus automatiquement à partir du jour de la décision du tribunal, mais à partir d'une date ultérieure fixée par ce dernier. Il faut tenir compte non seulement du moment de l'obtention de l'aval politique, mais aussi d'une date future pour des raisons logistiques, comme l'entrée en Suisse d'une personne donnée ou la survenue d'un événement, tel que le début d'une manifestation constituant une menace pour la sécurité. Les mesures de recherche soumises à autorisation devraient pouvoir être traitées avec un calendrier plus précis sans qu'il soit nécessaire de modifier le délai légal (trois mois) ni la procédure établie.

Al. 2

En cas de retard dans la procédure d'autorisation et d'aval d'une demande de prolongation des mesures de recherche déposée à temps, le risque subsiste que le SRC doive suspendre lesdites mesures jusqu'à l'entrée en force de l'autorisation. Dès lors, il convient de prévoir dorénavant que le délai s'arrête durant la procédure de prolongation, donc que le SRC est libre de poursuivre les mesures. Cela évite qu'une mesure de recherche soit interrompue en raison d'un retard dans la procédure. Bien entendu, le SRC doit immédiatement mettre fin à la mesure si le Tribunal administratif fédéral n'autorise pas la prolongation. Aucune procédure d'aval n'a lieu ensuite. Le dépôt en temps utile de la demande de prolongation tient compte des cinq jours ouvrables prévus par l'art. 29*a*, al. 1, pour la décision du Tribunal administratif fédéral et le nombre moyen de jours requis par la procédure d'aval, qui n'est soumise à aucun délai.

Al. 3

À l'instar de la procédure en cas d'urgence, le SRC détruit immédiatement les données obtenues si le tribunal n'autorise pas la demande ou si le chef du DDPS ne donne pas son aval.

Art. 29c

Cet article correspond à l'actuel art. 29, al. 8.

Art. 30

Al. 3 et 4

La prolongation d'une mesure de recherche en cours a uniquement un impact temporel. La mesure proprement dite ne s'en trouve pas modifiée. Une décision politique de principe sur sa mise en œuvre n'est donc pas nécessaire, ce qui signifie que les chefs du DFAE et du DFJP peuvent être libérés de la consultation, qui, avec les dispositions en vigueur, représente une charge en partie non négligeable. À l'avenir, le chef du DDPS n'assumera seul plus que la responsabilité de la prolongation. Le chef du DDPS demeure libre de consulter les chefs du DFAE et du DFJP dans les cas d'importance particulière. Ils peuvent également en convenir entre eux.

Lors d'extensions mineures de mesures déjà autorisées et avalisées, il n'y a généralement pas de nouveaux enjeux de taille. C'est ainsi le cas si une personne cible acquiert un téléphone portable supplémentaire avec un nouveau numéro, qui devra être inclus dans la surveillance existante de ses raccordements. Dans ce type de situation, il est également justifié que le chef du DDPS puisse décider d'avaliser la prolongation directement après l'autorisation rendue par le Tribunal administratif fédéral. Ici aussi, le chef du DDPS est libre de consulter les chefs du DFAE et du DFJP s'il l'estime nécessaire en raison des risques politiques que la mesure présente. S'ils y ont des intérêts particuliers, les chefs du DFAE et du DFJP peuvent également demander, lors de la consultation initiale, à être consultés à nouveau en cas d'extension ou de prolongation de la mesure. En tous les cas, le chef du DDPS est tenu d'informer ses homologues du DFAE et du DFJP de sa décision.

Art. 33

Al. 1, 2bis, 3 et 4

Afin de lever l'ambiguïté créée par la formulation « un mois », le délai pour informer les personnes surveillées est désormais fixé à 30 jours.

La pratique de l'obligation d'informer les personnes surveillées a montré que la réglementation actuelle occasionne parfois une charge disproportionnée par rapport à la protection des droits de ces personnes. Le droit en vigueur dispose que le report de l'information doit faire l'objet d'une nouvelle demande tous les trois mois devant le tribunal et être ensuite avalisé par le chef du DDPS après consultation des chefs du DFAE et du DFJP, selon la procédure prévue pour les mesures de recherche soumises à autorisation. L'autorisation reste valable trois mois au maximum. À ce jour, les cas de report de l'information ont concerné principalement des personnes visées par une procédure pénale en cours en lien avec la surveillance effectuée auparavant. Si la personne concernée n'a pas encore été informée de la surveillance par les autorités de poursuite pénale pour des raisons relevant des techniques d'enquête, le SRC risquerait de mettre en péril la procédure pénale en informant cette personne. Par conséquent, cette situation aboutit toujours à un report ou à une prolongation du délai. L'information a uniquement lieu lorsque l'autorité de poursuite pénale a informé la personne concernée ou a suspendu la procédure.

Ainsi, il devrait être possible à l'avenir de reporter l'information jusqu'à six mois au lieu de trois seulement, ou encore de l'associer à un événement spécifique (p. ex. la poursuite d'une procédure pénale). Comme auparavant, le SRC doit indiquer dans sa demande les motifs du report et désormais, le cas échéant, l'événement précis signifiant la fin du report. Le Tribunal administratif fédéral statue sur le report et expose, le cas échéant, ses motifs. Le simple report de l'information ne constituant pas une mesure définitive, celui-ci devrait être uniquement soumis à la procédure d'approbation. Il n'y a pas de raison qu'un report légalement requis soit refusé pour des motifs politiques. En revanche, un report de l'information justifié par les relations de la Suisse avec d'autres pays implique des enjeux politiques et doit donc être avalisé.

Quant au fait de renoncer définitivement à l'information, cette mesure doit demeurer soumise à l'aval politique. Si le report de l'information est approuvé par le Tribunal administratif fédéral, il peut être judicieux d'en faire part aux départements appelés à donner leur aval. Au besoin, cela sera réglé dans le cadre de la modification de l'ordonnance, une fois la loi révisée.

Comme auparavant, l'obligation de notification ne s'applique qu'aux mesures qui ont été effectivement mises en œuvre. Les mesures approuvées et avalisées, mais qui n'ont pas pu être mises en œuvre. p. ex. pour des raisons techniques, n'ont porté atteinte à aucun droit fondamental et ne sont donc pas soumises à l'obligation d'information.

Art. 37

Al. 3 à 6

L'art. 37 ne mentionne actuellement aucune mesure d'urgence analogue à celles prévues par l'art. 31 pour les mesures de recherche soumises à autorisation. L'infiltration dans des systèmes et réseaux informatiques qui se trouvent à l'étranger afin de les perturber, de les bloquer ou de les ralentir et ainsi de se défendre contre des attaques sur des infrastructures critiques est généralement une mesure délicate, aux effets immédiatement détectables et qui devra toujours être décidée par le Conseil fédéral.

A l'inverse, l'infiltration en vue de rechercher des informations est effectuée en toute discrétion et doit pouvoir être réalisée immédiatement en cas d'urgence afin d'obtenir à temps les données requises. Il est donc justifié d'ajouter des dispositions d'urgence similaires à celles en vigueur pour les mesures de recherche soumises à autorisation. Celles-ci ont fait leurs preuves et prévoient que le directeur du SRC peut ordonner la mise en œuvre immédiate des mesures et les soumettre a posteriori à la procédure d'autorisation et d'aval.

Si le chef du DDPS refuse de poursuivre la mesure immédiatement ou après consultation du DFAE et du DFJP, il doit au surplus décider de l'utilisation des données éventuellement acquises jusqu'alors. Il est envisageable qu'une mesure ne puisse être poursuivie en raison des risques politiques qu'elle crée, mais que le SRC soit néanmoins autorisé à utiliser les données déjà obtenues et utiles pour l'appréciation de la situation en matière de sécurité.

Art. 39

Al. 3

La modification de l'al. 3 vise à clarifier que toutes les personnes se trouvant en Suisse sont protégées contre l'exploration ciblée du réseau câblé (voir art. 42, al. 2, qui mentionne les « personnes qui se trouvent en Suisse »). Le SRC ne peut ainsi pas enquêter sur ces personnes au moyen d'une exploration du réseau câblé, ce qui reflète la pratique actuelle. En revanche, il peut être pertinent et nécessaire d'enquêter de la sorte sur des citoyens suisses lorsqu'il est établi qu'ils se trouvent à l'étranger. Là encore, cette disposition correspond à la pratique de l'exploration radio, p. ex. dans le cas de Suisses aux motivations terroristes se rendant dans des régions de djihad ou de filiales étrangères d'entreprises inscrites au registre du commerce en Suisse (en particulier lorsqu'elles sont gouvernées de l'étranger) et ayant des liens présumés avec des activités de prolifération. D'une part, il est justifié que ces personnes ne bénéficient pas de davantage de protections lorsqu'elles sont à l'étranger que les étrangers eux-mêmes, et d'autre part, il n'est pas possible d'exécuter des mesures de recherche soumises à autorisation dans ces cas-là, faute d'accès techniques et physiques.

Comme auparavant, les mots-clés sont des combinaisons de caractères, de chiffres et de lettres (ou un assemblage de ceux-là) qui servent à filtrer les données afin de générer un résultat (p. ex. des noms de personnes morales ou physiques, des numéros de téléphone, des adresses IP, des algorithmes, des coordonnées, etc.).

Art. 41

Al. 1, let. b

Le terme de « nécessité », actuellement inscrit dans la loi, devrait être complété par la notion de caractère approprié et exigible afin de refléter la pratique actuelle du Tribunal administratif fédéral, eu égard aux demandes d'autorisation.

Al. 1bis

Les demandes d'exploration du réseau câblé sont le plus souvent complexes sans être urgentes, aussi il est pertinent d'étendre à dix jours le délai pour rendre la décision.

Al. 2

Dans cet alinéa, l'expression «la procédure est régie au surplus » est remplacée par « le reste de la procédure est régi ». Cette modification précise en particulier que la décision est également prise par un juge unique.

Al. 3

À l'instar d'une mesure de recherche soumise à autorisation, l'exploration du réseau câblé nécessite une autorisation du Tribunal administratif fédéral, puis l'aval politique du chef du DDPS après consultation des chefs du DFAE et du DFJP. La législation actuelle prévoit que l'autorisation est d'abord accordée pour six mois au maximum et peut être prolongée à plusieurs reprises, selon la même procédure, de trois mois au plus.

L'exploration du réseau câblé est une mesure particulièrement complexe qui nécessite beaucoup de travail. À l'heure actuelle, pour le moins, elle ne convient que pour la recherche prolongée d'informations sur des événements importants en matière de politique de sécurité à l'étranger. Or, puisqu'elle implique une longue durée, les délais actuellement prévus par la LRens se sont avérés nettement trop brefs. Afin d'assurer la continuité de la mesure d'exploration du réseau câblé, le SRC doit à l'heure actuelle systématiquement demander sa prolongation après seulement deux mois. Il convient également de noter que les ajustements du système ou d'autres mesures (p. ex., les extensions de ligne) se traduisent rarement tout de suite par des résultats: au contraire, ils nécessitent davantage de temps. En outre, l'exploration du réseau câblé en est encore à ses débuts en Suisse, ce qui signifie que le développement continu des connaissances requises prend lui aussi du temps.

La prolongation de l'autorisation tient compte de l'orientation stratégique de l'exploration du réseau câblé. Dans le cas de l'exploration à l'étranger, les menaces, et donc les besoins en termes de renseignement, ne changent pas tous les trois mois, aussi les capacités du SRC et du Tribunal administratif fédéral peuvent être utilisées de manière plus judicieuse que pour des procédures d'autorisation à répétition.

Afin de pouvoir continuer à réagir rapidement et en souplesse aux évolutions de la situation et aux besoins d'exploration, il demeure possible d'adapter le mandat malgré la prolongation de l'autorisation. Par exemple, de nouveaux fournisseurs de services de télécommunication, de nouveaux sites d'un fournisseur existant ou de nouvelles catégories de mots-clés peuvent être ajoutés à un mandat d'exploration du réseau câblé. Le SRC suivra la procédure habituelle pour procéder à ces modifications.

Art. 42

Al. 3bis

Lors de la promulgation de la LRens, il était admis que les exploitants de réseaux filaires et opérateurs de télécommunications étaient en mesure, comme prévu par l'art. 43, de fournir les renseignements requis, en particulier sur les flux de données internationaux routés par leurs infrastructures. Les premiers cas concrets d'exploration du réseau câblé ont cependant montré que ce n'est guère le cas. Les exploitants suisses ne connaissent généralement que les points de départ et d'arrivée des flux de données des pays voisins, et non pas leur origine absolue ni leur destination finale. Les trajets empruntés par ces flux ainsi que le type de données communiquées changent en permanence à une fréquence très élevée.

Les flux de données internationaux sont acheminés via des réseaux très dynamiques dont le routage change rapidement et ne peut être prédit à long terme. Les fournisseurs de services de télécommunications optimisent constamment leurs flux de données, que ce soit afin d'améliorer la qualité de transmission ou pour des raisons économiques. Le service chargé de l'exploration devrait donc désormais être autorisé à analyser techniquement les signaux et les données enregistrés dans le cadre des mandats existants afin d'obtenir une image aussi actuelle et réaliste que possible des flux de données traités, des signaux que ces derniers transmettent ainsi que de l'origine et de la destination des données communiquées. Il est tout aussi important de déterminer la nature technique des signaux captés, car elle influe directement sur les moyens techniques à employer par le service chargé de l'exploration afin de les capter et de les traiter.

Ce type d'évaluation est de nature technique et n'est pas lié aux informations contenues dans les données collectées. Ces informations techniques sont stockées par le service COE chargé de l'exploration afin de servir de point de départ aux mandats ultérieurs. Il s'agit

d'identifier la destination des différents types de flux de données et de cerner ceux qui peuvent contenir des informations pertinentes pour le renseignement. Le service chargé de l'exploration peut partager les connaissances acquises avec le SRC afin que celui-ci formule les mandats d'exploration du réseau câblé de manière plus ciblée (c'est-à-dire désigner des flux de données à surveiller dans le mandat).

Chapitre 4: Traitement des données et contrôle de qualité

Remarques générales

Dans son rapport annuel 2019, la DélCdG a suggéré d'envisager une nouvelle stratégie de traitement des données dans laquelle la finalité des systèmes d'information (art. 47 à 57 LRens), les règles de transfert des données d'un système à l'autre (art. 44 LRens) et l'applicabilité des restrictions prévues à l'art. 5 LRens aux systèmes spécifiques seraient redéfinies en combinaison avec de nouveaux délais de suppression des données. L'objectif est de proposer des dispositions nettement moins complexes et plus claires. Le but fondamental des restrictions prévues par l'art. 5 LRens ne devrait cependant pas être remis en question.

Le présent projet tient compte de ces recommandations. La nouvelle stratégie de traitement des données se distingue par l'accent mis sur les données et leur traitement. Le contrôle initial, le contrôle de qualité des données et leur communication sont réglementés de manière uniforme. La renonciation à une différenciation entre les différents systèmes d'information et de stockage (la nouvelle loi sur la protection des données renonce également au terme de système d'information) représente l'élément central. Le règlement est donc neutre sur le plan technologique, couvre toutes les données du SRC sans exception et améliore de manière significative les possibilités de contrôle de qualité.

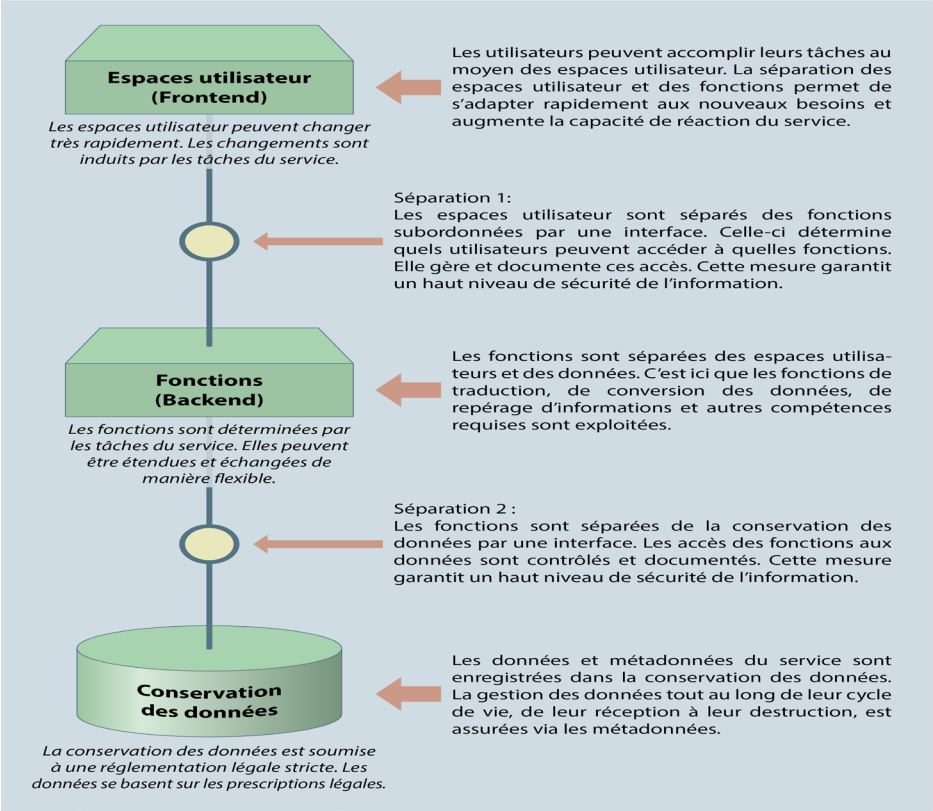
Les nouvelles dispositions ne s'éloignent pas résolument des fondements de la loi actuelle. En particulier dans le cas de l'accès sélectif aux données, les catégories existantes sont conservées. De nouvelles sous-catégories sont toutefois aoutées par souci de transparence. Il s'agit à cet égard de mentions, donc de métadonnées, et non de catégories au sens de la nLPD, comme les données personnelles sensibles citées à l'art. 5, let. c, nLPD. De même, les droits d'accès attribués à d'autres autorités sont conservés à quelques exceptions près qui sont indiquées dans les explications de la section 5.

Les systèmes d'information ne sont plus nommés afin de correspondre à la conception contemporaine des architectures informatiques, qui prévoit une séparation claire des systèmes d'information, de la logistique et des données. Il est aujourd'hui dépassé de travailler avec des systèmes d'information monolithiques, c'est-à-dire d'unir physiquement les données et les logiciels. Les données sont désormais sauvegardées de manières sûre et redondante sur des supports de stockage techniquement appropriés. L'enregistrement sur une couche de stockage des données, associé en toute logique à une connexion aux solutions logicielles d'accès, permet d'éviter les enregistrements multiples et la gestion uniforme des données (vérification périodique, correction, suppression, archivage) sur tout le cycle de vie de ces dernières.

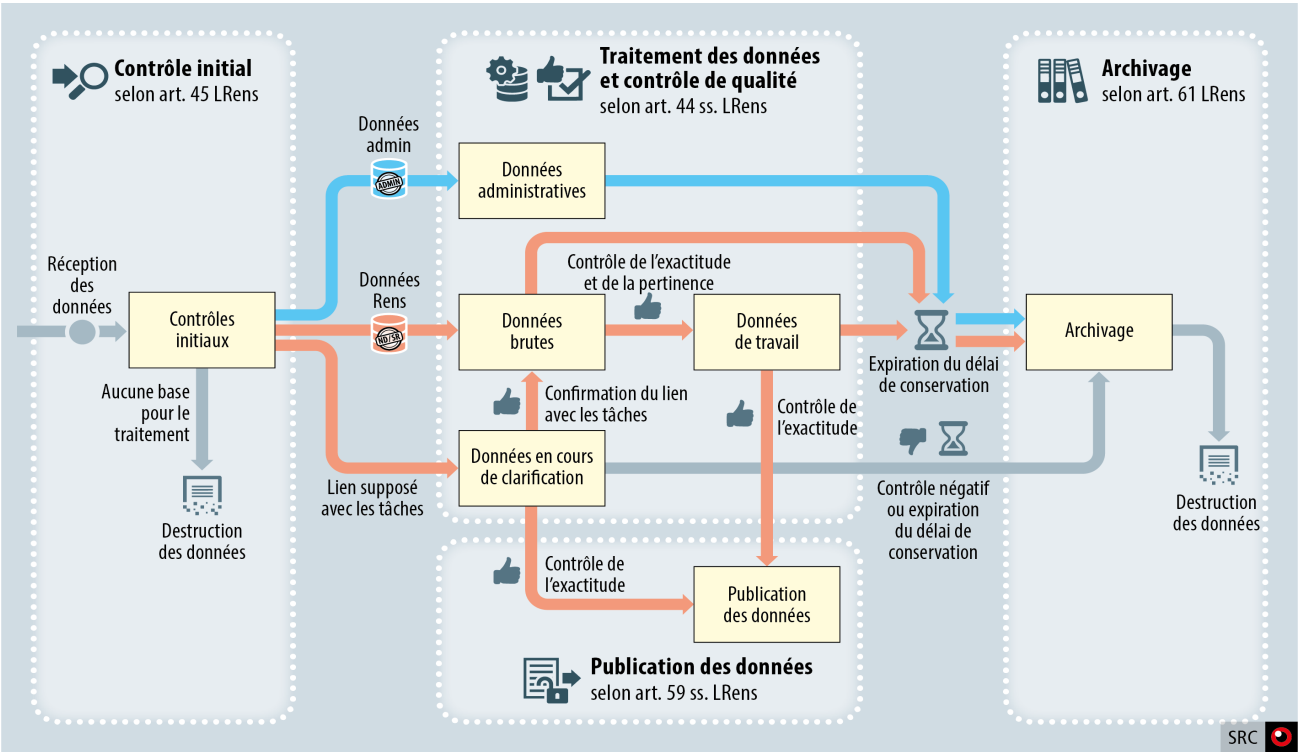
Même sans recourir à des systèmes d'information individuels, les accès peuvent être contrôlés de manière différenciée, comme auparavant. Toutefois, étant donné que les accès sont désormais régis à des échelons plus élevés de l'architecture (couche de service de données et couche de service d'application), ils peuvent être définis non seulement de manière approximative au niveau des systèmes d'information, comme c'est le cas aujourd'hui, mais aussi plus précisément jusqu'à l'échelon du traitement des données et de l'information individuelle. Les autorisations fonctionnelles (quels outils sont disponibles pour quels rôles) et spécialisées (quelles données sont disponibles pour quels rôles et peuvent être traitées par ceux-ci) peuvent être contrôlées précisément. De la sorte, les exigences légales en matière d'accès pourront être mises en œuvre facilement à l'avenir. La loi suit désormais les quatre étapes du cycle de vie des données: réception, utilisation, communication à d'autres services puis suppression et archivage.

Les explications suivantes font toutes référence à la LPD révisée.

Vue d’ensemble de l’architecture informatique



Vue d’ensemble du traitement des données par le SRC



Lors de la réception des données, le SRC détermine si elles relèvent du renseignement ou sont de nature administrative (contrôle initial). Les données administratives désignent toutes les données que le SRC traite en vertu de la LOGA et que les autorités d’exécution cantonales traitent en vertu de leur législation cantonale à des fins administratives, c’est-à-dire qui ne servent pas à l’accomplissement de tâches citées à l’art. 6 LRens. Cette notion inclut notamment des données sur les collaborateurs du SRC et des autorités d’exécution cantonales, sur les personnes qui prennent contact avec le SRC, par exemple pour demander des renseignements ou des informations,

sur des projets, des affaires politiques, etc. Les données administratives sont marquées en tant que telles et traitées conformément aux bases légales applicables. Les données relevant du renseignement concernent toutes les tâches énumérées à l'art. 6 LRens. Il s'agit de toutes les données traitées par le SRC et les services d'exécution cantonaux pour l'accomplissement de ces tâches, ainsi que des informations nécessaires à l'obtention de ces données. Les données relevant du renseignement sont contrôlées de manière séquentielle avec les questions suivantes: le lien avec les tâches citées à l'art. 6 est-il établi? Les données proviennent-elles de sources accessibles au public? Si tel n'est pas le cas, font-elles l'objet des restrictions citées à l'art. 5 en matière de traitement des données? Le contrôle du lien avec les tâches est en principe effectué avant le contrôle des restrictions. Les données provenant de sources accessibles au public, telles que les médias imprimés ou électroniques, font uniquement l'objet d'un contrôle du lien avec les tâches lors de leur réception, car le SRC n'a pas d'influence sur leur contenu et ces données sont générées en grand nombre. Un contrôle des restrictions a cependant lieu si le SRC souhaite utiliser ces données pour l'établissement de produits du renseignement.

L'utilisation des données implique notamment l'évaluation, la synthétisation et la mise en réseau des données ainsi que la création de produits. Les données administratives n'ont pas de sous-catégories et ne sont pas examinées plus avant durant leur utilisation. Leur traitement ultérieur est avant tout régi par la LOGA.

Après réception, les données relevant du renseignement sont classées différemment en fonction des résultats du contrôle initial. Il s'agit de données brutes si le lien avec les tâches est établi et si (sauf pour les données provenant de sources accessibles au public) le contrôle des restrictions en matière de traitement des données a été effectué. Les données brutes ont généralement une durée de conservation moyenne et sont régulièrement contrôlées par sondage par le service de contrôle de qualité du SRC. Elles ne peuvent être communiquées à des tiers sans contrôle supplémentaire ni utilisées dans des produits du SRC. La seconde catégorie est celle des données de travail. Il s'agit de données brutes relevant du renseignement qui sont destinées à un traitement ultérieur approfondi par le SRC et été marquées en tant que telles, mais aussi des produits de ce traitement des données (p. ex. rapports d'analyse, rapports de situation, alertes). Les données de travail sont généralement conservées plus longtemps que les données brutes. Le contrôle auquel ces données sont soumises en vue de leur traitement ultérieur approfondi a valeur de première vérification périodique. Les données de travail sont ensuite contrôlées et gérées périodiquement par des spécialistes puis contrôlées par sondage par le service de contrôle de qualité. En outre, elles sont contrôlées avant leur communication, ce qui constitue également une vérification périodique.

Lorsqu'elles sont communiquées à des tiers, les données de travail sont soumises à un contrôle selon trois critères: la communication est-elle nécessaire, est-elle adéquate, et les conditions juridiques à la communication à des tiers sont-elles respectées? Le contrôle préalable à la communication implique également de vérifier si le SRC a encore besoin des données en question pour accomplir ses tâches. Les données qui ne sont plus nécessaires sont supprimées et celles qui le sont encore sont confirmées (vérification périodique).

Le SRC propose les données administratives et relevant du renseignement aux Archives fédérales suisses (AFS) dès qu'elles ne lui sont plus nécessaires en permanence. Les AFS décident de la nécessité de l'archivage. Le SRC remet aux AFS les données qui ont une valeur archivistique et les détruit de son côté. La nomenclature correspondante (supprimer, verser, détruire) est employée uniformément dans la LRens.

Chapitre/titre

Afin d'en assurer une meilleure vue d'ensemble, le chap. 4 a été restructuré (1. Catégories de données, 2. Contrôle initial, 3. Traitement des données de travail, 4. Présentation électronique de la situation, 5. Droits d'accès et 6. Contrôle de la qualité). Les dispositions particulières relatives à la protection des données et l'archivage sont désormais traités dans un nouveau chap. 4*a*. Pour cette raison, le titre du chap. 4 a également été modifié. Comme évoqué plus haut, l'ordre des sections suit essentiellement les étapes de la procédure, de la réception des données par le SRC jusqu'à leur archivage ou leur destruction. En référence à la nLPD, les termes « données » et « données personnelles » sont employés uniformément.

Section 1: Catégories de données

Art. 44

Al. 1

Cet alinéa définit les deux catégories principales auxquelles sont affectées les données reçues et déjà stockées: d'une part les données relevant du renseignement, que le SRC et les autorités d'exécution cantonales traitent pour accomplir leurs tâches prévues par l'art. 6, et d'autre part les données administratives, qu'ils traitent pour accomplir leurs tâches administratives ou pour la maintenance et le développement de solutions informatiques (voir les exemples cités dans les remarques générales ci-dessus au sujet des tâches administratives). Cette seconde catégorie comprend notamment le code source ou les données de base des applications (p. ex. des cartes ou l'attribution d'adresses à des coordonnées dans un système d'information géographique).

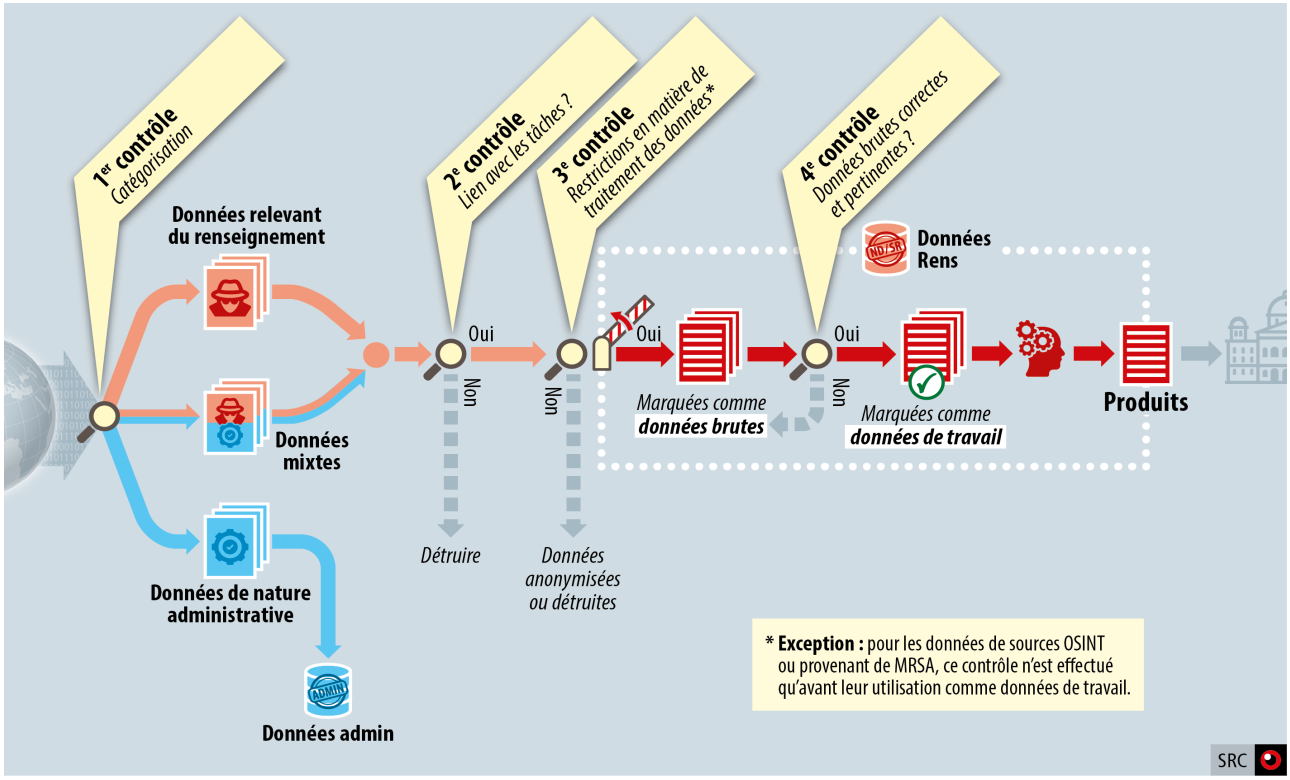
Al. 2

Les données relevant du renseignement sont scindées en données brutes et en données de travail. Elles ne sont enregistrées qu'à l'issue du contrôle initial par le SRC et les autorités d'exécution cantonales. Les données brutes ne peuvent être utilisées sans contrôle de leur exactitude et de leur pertinence. Les données de travail sont des données brutes dont l'exactitude a été contrôlée et dont la pertinence actuelle fonde le traitement ultérieur, ainsi que les produits résultant de ce traitement.

Section 2: Contrôle initial

Art. 45

Vue d'ensemble du contrôle initial



Al. 1

Comme indiqué plus haut, le SRC et les autorités d'exécution cantonales déterminent d'abord si les données reçues sont de nature administrative ou relèvent du renseignement, puis les marquent en conséquence. Ce contrôle est effectué lors de l'enregistrement des données (normalement dans la journée, sous réserve des exceptions citées aux art. 45, al. 4, et 46, al. 2).

Al. 2

Si les données peuvent être attribuées aux deux catégories, le SRC les marque en conséquence. Afin de satisfaire les exigences plus strictes en matière de protection des données en cas de doute, elles sont traitées comme des données relevant du renseignement – exception faite des demandes d'accès relatives à la protection des données, qui sont traitées selon les critères moins restrictifs des données administratives.

Al. 3

Si les données ne peuvent être attribuées à aucune des deux catégories, le SRC les détruit, les anonymise ou les renvoie à l'expéditeur.

Al. 4

Il peut arriver qu'au moment de la réception des données, un lien avec les tâches soit incertain. Par exemple, il se peut qu'un service partenaire du SRC demande des renseignements sur une personne qui diffuse dans son pays une idéologie radicale d'extrême droite et raciste, ce qui fonde la compétence de l'autorité étrangère. Imaginons que cette personne se trouve en Suisse pour une longue période. Le service partenaire souhaite alors savoir si le SRC dispose d'informations supplémentaires à son sujet. Le SRC transmet alors un mandat de recherches à l'autorité d'exécution cantonale où la personne concernée se trouve. Seul le résultat de ce contrôle permet de déterminer s'il s'agit d'un d'extrémiste *violent*, donc si le lien supposé avec les tâches du SRC est établi et si un traitement ultérieur des données est admis. Il est également concevable que des tiers (des particuliers) soient approchés. Il peut p. ex. s'agir, dans le cadre d'un signalement, d'une personne auprès de laquelle des questions doivent être clarifiées, des parents d'un élève suspecté de radicalisation violente ou de l'épouse d'un voyageur du djihad suspecté. Dans de tels cas, la communication permet de réaliser le contrôle initial. Elle demeure soumise aux restrictions imposées par les art. 59 à 61 et n'est autorisée que si elle est nécessaire pour déterminer le lien avec les tâches. Cette situation peut bien entendu également se produire avec des données reçues des autorités d'exécution cantonales. Par souci de transparence, la marche à suivre pour déterminer le lien avec les tâches est désormais inscrite expressément dans la LRens.

Art. 46

Al. 1

Si le lien avec les tâches est établi, le SRC et les autorités d'exécution cantonales s'assurent que les données ne contiennent aucune information soumise aux restrictions de l'art. 5, al. 5, en matière de traitement des données, à moins que l'une des exceptions prévues

par l'art. 5, al. 6 ou 8, ne s'applique. La disposition de l'actuel art. 45, al. 1, qui indique que les communications portant sur diverses données personnelles sont évaluées dans leur globalité, est supprimée, car elle est critiquée par l'autorité de surveillance parlementaire. Désormais, le SRC et les autorités d'exécution cantonales s'assurent que les communications pertinentes en matière de renseignement ne contiennent aucune donnée personnelle tombant sous le coup des restrictions prévues par l'art. 5, al. 5, même lorsque ces communications comportent des données sur plusieurs personnes ou affaires.

Al. 2

Etant donné que les informations publiques (telles que les médias imprimés ou électroniques) peuvent en règle générale être consultées à tout moment par n'importe qui, il n'est pas pertinent de les soumettre à restrictions de l'art. 5, al. 5, en matière de traitement des données lorsqu'il s'agit simplement de les stocker ou d'évaluer leur exactitude. L'exactitude des contenus médiatiques ne peut souvent être vérifiée qu'après un certain temps, et ces contenus ne respectent pas les exigences de la LRens pour les rapports des autorités d'exécution cantonales. En effet, les articles de journaux sur des événements pertinents pour la LRens (p.ex. attaques terroristes et affaires d'espionnage) contiennent souvent des déclarations politiques. Le SRC et les autorités d'exécution cantonales devraient pouvoir les enregistrer sans les soumettre au préalable à un long travail de censure inutile. Dans le cas des données provenant de sources accessibles au public, ils contrôlent d'abord les restrictions en matière de protection des données avant de les utiliser en tant que données de travail. Dans un avis de droit rédigé en février 2020 sur mandat du DDPS, l'Office fédéral de la justice a estimé que cette pratique est défendable.

Une exception similaire existe pour les données provenant de mesures de recherche soumises à autorisation, qui font seulement l'objet d'un contrôle des restrictions en matière de protection des données lorsqu'elles sont marquées pour un traitement ultérieur. Cela correspond à la procédure actuelle, qui prévoit le contrôle dans le cadre de l'enregistrement dans IASA SRC.

Art. 47

Lorsque le SRC doit mandater et former l'expéditeur de données entrantes, il peut lui confier le contrôle du lien avec les tâches et des restrictions en matière de traitement des données, puis enregistrer automatiquement les données. Aujourd'hui, c'est notamment le cas des données provenant de sources accessibles au public, dans la mesure où la Base d'aide au commandement (COE BAC) transmet au SRC les dépêches d'agence et de presse qui présentent un lien établi avec les tâches de ce dernier. Les collaborateurs du COE BAC sont formés chaque année par le service de contrôle de qualité du SRC. Ce service contrôle chaque année par sondage que les données reçues de la sorte ont un lien avec les tâches au sens de l'art. 6.

Art. 48

Le SRC a déjà le droit d'enregistrer dans des systèmes d'information distincts les données provenant de l'étranger et similaires à des mesures de recherche soumises à autorisation, les données provenant de mesures de recherche soumises à autorisation et les données particulièrement sensibles (voir art. 36, al. 5, art. 58, al. 1, LRens et art. 7, al. 2 de l'ordonnance du 16 août 2107 sur les systèmes d'information et les systèmes de stockage de données du Service de renseignement de la Confédération; OSIS-SRC[19]). Sont déterminants à cet égard l'ampleur des données, le secret (notamment la protection des sources) ou la sécurité (notamment en cas de risque de contamination des données et des systèmes informatiques). L'enregistrement distinct ne peut toutefois durer que pour un temps limité fixé par le Conseil fédéral et devra être adapté dans le cadre du droit d'exécution au type de données et au motif de l'enregistrement distinct.

Art. 49

Al. 2

Cet article énumère les sous-catégories de données relevant du renseignement. Ces sous-catégories remplacent les désignations actuelles des systèmes d'information et permettent ainsi au SRC de maintenir les différentes directives de traitement des données applicables aujourd'hui aux systèmes d'information, et en particulier l'accès sélectif. Certaines données peuvent rentrer simultanément dans plusieurs catégories. Les sous-catégories de données suivantes correspondent aux données dans les systèmes d'information existants:

Let. a:	IASA SRC, Quattro P, SICO;
Let. b:	IASA-EXTR SRC;
Let. c:	Portail ROSO:
Let. d:	Systèmes de stockage MRSA;
Let. e:	Systèmes de stockage MRSA;
Let. f:	Système pour les données particulièrement sensibles (cf. art. 7 OSIS-SRC);
Let. g:	PES;
Let. h:	IASA SRC, IASA-EXTR SRC et INDEX SRCant en vertu de l'art. 29, let. b, OSIS-SRC;
Let. i:	IASA SRC, IASA-EXTR SRC et INDEX SRCant en vertu de l'art. 29, let. b, OSIS-SRC;
Let. j:	Il s'agit de données du laboratoire technique Cyber SRC stockées et évaluées sur un réseau distinct. Elles sont employées pour des travaux d'analyse dynamique et dans le cas de réseaux ou d'ordinateurs compromis techniquement. Aucune donnée personnelle n'est traitée ici. La synthétisation et l'évaluation des données sont effectuées aujourd'hui dans IASA SRC;
Let. k:	INDEX SRCant en vertu de l'art. 29, let. b, OSIS-SRC;
Let. l:	Classement temporaire «contrôle du classement»;
Let. m:	IASA INDEX en vertu de l'art. 29, let. a, OSIS-SRC.

[19] RS **121.2**

Art. 50

Al. 1

Cet alinéa correspond en grande partie à l'actuel art. 58, al. 2. Il prévoit désormais que le contrôle initial des données en question doit être effectué au plus tard jusqu'à la fin de l'opération correspondante au sens de l'art. 45. Cette mesure est nécessaire, car les données ne peuvent souvent pas être contrôlées immédiatement lors de leur enregistrement et doivent également être placées dans le contexte d'autres données collectées dans le cadre de l'opération. Ces données ne peuvent toutefois être utilisées qu'à l'issue du contrôle initial. Si les données ont un lien avec des opérations en cours, elles sont marquées comme données brutes ou comme données de travail dans le cadre du contrôle initial. Si tel n'est pas le cas, elles sont détruites. À cet égard, le critère du délai de suppression est modifié. En effet, une opération peut durer plusieurs mois, voire plusieurs années, même si certaines mesures de recherche individuelles prennent fin après quelques jours seulement. Selon l'expérience du SRC, une opération dure en moyenne entre six mois et deux ans. Cela signifie que des données doivent être détruites aujourd'hui, alors que leur évaluation n'est pas encore terminée ou que leur pertinence ne se serait peut-être révélée que durant la suite de l'opération.

Prenons les exemples suivants. Le SRC mène une opération visant un agent de renseignement étranger en Suisse connu de lui (personne A) en relation avec l'empoisonnement d'un politicien de l'opposition à l'étranger afin de déterminer s'il est impliqué dans l'empoisonnement. Dans le cadre de cette opération, des MRSA sont engagées à l'encontre de la personne A et les données secondaires de ses moyens de communication sont interrogées. Dans ces données secondaires, le SRC découvre des contacts entre la personne A et divers organismes publics, d'autres agents de renseignement et la personne B. La personne B n'est pas connue du SRC, aussi celui-ci doit détruire les données la concernant un mois après la fin de la MRSA, c'est-à-dire après avoir obtenu les données secondaires. L'opération se poursuit et deux mois plus tard, le SRC apprend qu'une personne B est soupçonnée de faire partie du programme d'armes chimiques du pays concerné. Les résultats de la MRSA ayant déjà été détruits, le SRC ne peut établir aucun lien entre les personnes A et B, alors que l'opération dans son ensemble n'est pas encore achevée.

En particulier lors de l'évaluation ultérieure des données secondaires des raccordements de télécommunications, le délai actuel d'un mois est très problématique, car la transmission des données secondaires dans le cadre de la MRSA se termine au plus tard après six mois, tandis que l'évaluation des données peut prendre bien plus d'un mois. Le SRC doit identifier les abonnés et les utilisateurs présumés des partenaires de communication de la personne surveillée. Il est alors essentiel de pouvoir comparer les résultats des différentes MRSA afin de découvrir d'éventuelles personnes clés. Les identifications et les clarifications avec les services partenaires étrangers du SRC durent souvent jusqu'à la fin d'une opération. La destruction prématurée de l'information peut donc mettre en péril à la fois le succès de l'opération et la crédibilité du SRC vis-à-vis de ses partenaires.

Par conséquent, il est nécessaire de fixer le moment de la destruction à un mois après la fin de l'opération.

Al. 2

Cet alinéa correspond à l'actuel art. 58, al. 3, et n'apporte que des éclaircissements formels.

Al. 3

Cet alinéa correspond à l'actuel art. 58, al. 4, et n'apporte que des éclaircissements formels.

Section 3: Traitement des données de travail

Art. 51

Al. 1

Contrôler l'exactitude des données implique de les replacer dans le contexte d'autres informations. Il n'est pas possible de confronter le contenu de ces données dès l'enregistrement. Cette étape doit attendre le marquage des données brutes en données de travail, et le résultat du contrôle est maintenu. En principe, les données non contrôlées (donc brutes) ne peuvent être utilisées pour l'évaluation et la production à des fins de renseignement. Une exception très limitée subsiste à l'art. 57, al. 2 pour l'accès des autorités d'exécution cantonales aux données provenant de sources accessibles au public. Toute autre utilisation nécessite également un contrôle des données.

Al. 2

Les termes « désinformation » et « fausses informations » sont remplacés par « données personnelles fausses ». Le SRC ne doit pas seulement pouvoir traiter des données personnelles pour évaluer une situation ou une source, mais aussi pour accomplir d'autres tâches énumérées à l'art. 6. Ces dernières années, de hautes instances de gouvernements étrangers ainsi que des particuliers ont de plus en plus utilisé de fausses informations, p. ex. pour influencer de façon dissimulée des processus de décision politique ou l'opinion publique, pour détourner l'attention d'un événement ou pour orienter un débat public et ainsi déstabiliser des sociétés entières dans d'autres pays. Il s'agit d'attaquer directement des personnes et de diffuser de fausses informations à leur sujet. Le SRC doit être en mesure de traiter ces informations pour accomplir les tâches qui lui sont confiées. Afin d'identifier clairement ces données, il les marque comme incorrectes.

Art. 52

Al. 1

Dans cet alinéa sont énumérés les buts dans lesquels le SRC et les autorités d'exécution cantonales peuvent traiter des données personnelles. Les buts du traitement sont réglés aujourd'hui dans le cadre des systèmes d'information et de stockage des données et ne sont pas modifiés (voir à ce propos les explications de l'art. 49).

Al. 2

La nLPD n'emploie plus le terme de profil de la personnalité. Il est remplacé par « des données personnelles qui permettent d'évaluer la menace qu'une personne représente », formule reprise ici.

À l'avenir, le SRC s'appuiera davantage sur l'évaluation automatisée de ses données afin de pouvoir reconnaître et évaluer les caractéristiques d'une personne en partie de manière automatisée ou encore pour comparer automatiquement des données reçues ou obtenues

de lui-même avec les données existantes relevant du renseignement. Ce système est concevable pour l'évaluation d'un profil de déplacement d'une personne cible, pour l'analyse temporelle d'événements ou pour révéler des changements dans le comportement d'une personne (p. ex. radicalisation). L'utilisation de programmes intelligents pour la recherche et la catégorisation des informations est aujourd'hui indispensable à l'accomplissement efficace des tâches du SRC. Les organes de contrôle l'exigent également. L'utilisation de l'intelligence artificielle au sens de décisions individuelles automatisées (art. 21 nLPD) ou au sens d'une utilisation d'appoint de l'intelligence artificielle avec le risque de porter gravement atteinte aux droits fondamentaux (art. 34, al. 2, let. c, DSG) n'est toutefois pas prévue. Si une telle utilisation était envisagée, des bases légales devraient être créées à cet effet. Enfin, il est à noter que la formulation retenue dans le présent projet correspond notamment à celle de la loi du 20 mars 1981 sur l'assurance-accidents [20].

Etant que le traitement et l'évaluation automatisés des données (donc via un système informatique et non sur papier) est aujourd'hui la norme, la clause de justification correspondante est supprimée dans la loi (actuel art. 44, al. 4; voir aussi art. 7 nLPD, qui présuppose un traitement automatisé des données).

Al. 3

Pour des raisons de transparence, il est désormais disposé clairement que le SRC et les autorités d'exécution cantonales peuvent également traiter des données personnelles à décharge, à condition toutefois que des données à charge sur la même personne aient déjà été traitées et écartées en partie ou entièrement. Selon la signification de ces données, cela peut aboutir à ce qu'elles seront supprimées et archivées ou détruites de manière anticipée.

Al. 4

Cet alinéa correspond en grande partie à l'actuel art. 47, al. 2. Les compétences en matière de traitement des données ont toutefois été supprimées, puisqu'elles découlent toutes de la matrice des droits d'accès. Par souci de transparence, la destruction des données est ajoutée à la let. e. Les remarques suivantes sont à noter pour les différentes compétences:

- Let. a: Le catalogue des données personnelles est actuellement réglé dans les annexes à l'OSIS-SRC. Il ne fait pas l'objet de modifications ni de compléments.
- Let. b: Les droits d'accès sont actuellement définis dans les annexes à l'OSIS-SRC. Ils ne font pas l'objet de modifications conséquentes ni de compléments, (excepté Groupement de la Défense et OFDF).
- Let. c: La fréquence du contrôle de la qualité est actuellement définie séparément dans l'OSIS-SRC pour chaque système d'information. Elle ne fait pas l'objet de modifications ni de compléments.
- Let. d: La durée de conservation est elle aussi définie séparément dans l'OSIS-SRC pour chaque système d'information. Elle ne fait pas l'objet de modifications ni d'extensions.
- Let. e: La suppression et la destruction des données sont actuellement réglées aux art. 8, 9 et 69 OSIS-SRC. Ces dispositions ne font pas l'objet de modifications.
- Let. f: La sécurité des données est actuellement régie par l'art. 13 OSIS-SRC. Il n'est pas prévu de modifier cette disposition.

Al. 5

Le contenu de cet alinéa correspond à celui de l'actuel art. 55, al. 1 et 4.

Art. 53

Al. 1

Le contenu de l'al. 1 correspond à l'actuel art. 46, al. 1. La nLPD supprime le terme « fichier », ici remplacé par « environnement de travail ». Les autorités d'exécution cantonales traitent les données pertinentes au sens de la LRens dans l'environnement de travail fourni par le SRC. Elles ne sont pas autorisées à employer leurs propres outils informatiques. En outre, pour des raisons de transparence, il est précisé que les autorités d'exécution cantonales sont autorisées à stocker temporairement et pour une courte durée des données dans leur environnement de travail cantonal en vue de leur transfert vers le réseau hautement sécurisé dans lequel se trouve l'environnement de travail fourni par la Confédération. Il est dans l'ordre des choses que les autorités d'exécution cantonales doivent d'abord numériser et stocker temporairement les données qu'elles obtiennent (p. ex. photos, extraits de registres ou de sites Internet) avant de pouvoir les traiter dans l'environnement de travail fourni par la Confédération. Seuls ont accès aux données se trouvant dans l'environnement de travail cantonal le chef de l'autorité d'exécution cantonale et son suppléant ainsi que la personne qui a enregistré les données. Les autorités d'exécution cantonales sont actuellement tenues de détruire les données de leur environnement de travail au plus tard 60 jours après leur enregistrement, ce que le service de contrôle de qualité du SRC vérifie dans le cadre de ses activités de contrôle par sondage. Les données sont prises en compte lors du traitement des demandes d'accès en vertu de l'art. 63.

Al. 2

Cet alinéa correspond à l'actuel art. 46, al. 2, et n'apporte que des éclaircissements formels. Il précise en particulier que lorsque les autorités d'exécution cantonales traitent des données en vertu du droit cantonal (p. ex. relatif à la police), il s'agit de données cantonales. Celles-ci doivent être séparées clairement des données qu'elles traitent en vertu de la LRens.

Al. 3

Les nouveaux art. 33 et 33bis ORens ne règlent pas uniquement la communication des données que les cantons reçoivent du SRC, mais aussi la communication des données que les cantons ont recherchées de leur propre compétence. Le présent alinéa est complété afin d'offrir une base légale suffisante à cet égard. Le terme « appréciation de la situation » est supprimé, car il ne constitue plus des données au sens de la nLPD. Cette disposition a par ailleurs été adaptée à celle de l'art. 6, al. 1, puisque la formulation « préserver la sécurité ou écarter une menace importante » a été remplacée par « déceler à temps et prévenir les menaces pour la sûreté intérieure ou extérieure».

Al. 4

[20] RS **832.20**

Les autorités d'exécution cantonales pourront toujours conserver les résultats des enquêtes préliminaires que pendant cinq ans au maximum. Durant cette période, elles ont la possibilité de faire un rapport au SRC. Dès lors, le délai de conservation des informations est prolongé et la liste des personnes ayant le droit d'y accéder est étendue aux collaborateurs autorisés du SRC et des autorités d'exécution cantonales. Eu égard à leur courte durée de conservation, il est toujours renoncé au contrôle périodique des enquêtes préliminaires par les autorités d'exécution cantonales.

Section 4: Présentation électronique de la situation

Art. 54

Al. 1

Le contenu de cet alinéa correspond à celui de l'actuel art. 53, al. 1 et 3, et autorise le SRC à poursuivre son utilisation du système d'information présentation électronique de la situation (PES) de l'Office fédéral de la protection de la population (voir art. 55, al. 1, de l'ordonnance du 11 novembre 2020 sur la protection de la population[21]).

Al. 2

Outre les informations traitées par le SRC lui-même, la PES contient des informations provenant d'autres autorités soumises à des dispositions moins strictes en matière de protection des données. Il se peut donc que la PES contienne des informations que le SRC ne serait pas habilité à traiter lui-même en vertu de la LRens. La PES ne doit toutefois pas couvrir les seuls besoins du SRC, mais ceux de toutes les autorités suisses de sûreté. Cette situation a également des répercussions sur le contrôle de la qualité: étant donné que chaque autorité est soumise à des directives différentes, l'art. 58*b*, al. a, prévoit que chacune sera à l'avenir responsable des données qu'elle a enregistrées. Les directives spécifiques à fedpol sont réglées par l'art. 44, al. 4, OSIS-SRC. Eu égard aux éventuelles violations des restrictions de la nLPD en matière de traitement des données, le délai de conservation des données enregistrées par fedpol est aujourd'hui plus court (voir art. 45, al. 2, OSIS-SRC). À l'avenir, cela ne devrait pas être le cas de toutes les données enregistrées par le SRC ou les autorités d'exécution cantonales (voir également les considérations sur le renseignement intégré dans les explications de l'art. 5, al. 5, let. e).

Section 5: Droits d'accès

Les droits d'accès de l'autorité de surveillance indépendante sont réglés à l'art. 78, al. 3.

Art. 55

Al. 1

À l'instar de la règle actuellement prévue par l'art. 51, les autorités d'exécution cantonales et les autorités fédérales n'ont pas accès à toutes les données du SRC, mais en principe uniquement à celles des index nécessaires pour pouvoir déterminer si le SRC a associé des données à une personne, à une organisation, à un groupement, à un objet ou à un événement dans l'accomplissement de ses tâches en vertu de l'art. 6, al. 1. Il s'agit aujourd'hui des objets saisis dans IASA-EXTR et IASA-SRC, qui sont également répertoriés dans IASA INDEX. Comme aujourd'hui, ces autorités ne pourront pas accéder aux données rattachées à une personne, à une organisation ou autre: elles ne verront que les résultats correspondant à un nom, un prénom et une date de naissance ou à une entreprise. Pour que d'autres données leur soient communiquées, elles doivent soumettre au SRC une demande d'assistance administrative dûment motivée (voir al. 2).

Les droits d'accès au sein du SRC comme au sein des autorités d'exécution cantonales et d'autres externes qui ont déjà des accès demeurent inchangés Le principe de proportionnalité, qui exige que l'accès soit accordé sur la base « need-to-know » (principe du besoin d'en connaître), s'applique toujours. L'art. 52, al. 4, let. b, charge comme auparavant le Conseil fédéral de définir les droits d'accès exacts.

Let. a

Les droits d'accès des autorités d'exécution cantonales ne font l'objet d'aucune modification.

Let. b

Les droits d'accès de l'Office fédéral de la police ne font l'objet d'aucune modification (voir l'actuel art. 51, al. 4, let. c). Ses accès sont maintenus afin qu'il puisse déterminer si le SRC traite des données relevant du renseignement relatives à une personne, à une organisation, à un groupement, à un objet ou à un événement spécifique. Il ne peut toutefois pas accéder aux données rattachées à une personne, à une organisation ou autre. La communication de ces données doit faire l'objet d'une demande au SRC dûment motivée.

Let. c

Aujourd'hui, deux services sont chargés des contrôles de sécurité relatifs aux personnes: un au sein de la Chancellerie fédérale et un au DDPS. À cette fin, ces deux services ont accès aux données du SRC relevant du renseignement. La nouvelle formulation plus générique vise à éviter qu'une modification de la loi devienne nécessaire en cas d'adaptation de la structure organisationnelle d'un service. En outre, les accès pour les deux services sont définis au même endroit. Les modifications sont donc purement formelles. Les droits d'accès ne font l'objet d'aucune modification (voir l'actuel art. 51, al. 4, let. c). Les accès des services responsables des contrôles de sécurité relatifs aux personnes sont maintenus afin qu'ils puissent déterminer si le SRC traite des données relevant du renseignement relatives à une personne, à une organisation, à un groupement, à un objet ou à un événement spécifique. Ils ne peuvent toutefois pas accéder aux données rattachées à une personne, à une organisation ou autre. Pour que celles-ci leur soient communiquées, ils doivent soumettre au SRC une demande d'assistance administrative dûment motivée (voir al. 2).

Let. d

[21] RS **520.12**

Désormais, les collaborateurs de l'OFDF chargés de la poursuite pénale et de l'analyse des risques (voir let. e), doivent obtenir des accès en raison de leurs tâches légales. Eux aussi peuvent uniquement constater que le SRC traite des données relevant du renseignement relatives à personne, à une organisation ou autre. Pour que d'autres données leur soient communiquées, ils doivent soumettre au SRC une demande d'assistance administrative dûment motivée.

Ces accès sont également spécifiés dans la révision de la loi du 18 mars 2005 sur les douanes (LD)[22] et, dès lors, dans la nouvelle loi définissant les tâches d'exécution de l'OFDF[23]. Les collaborateurs de l'OFDF chargés de la poursuite pénale ont besoin de droits d'accès afin d'accomplir leurs tâches en la matière, si et dans la mesure où le droit fédéral le prévoit. Cette mesure devrait permettre de gagner en efficience et de répondre au besoin d'accélération de la procédure pénale. De plus, elle permet de mieux évaluer les accusés et fournit de nouveaux outils d'enquête, en particulier en ce qui concerne l'environnement des accusés. Elle facilite en outre l'évaluation des signalements de personnes potentiellement dangereuses dans le domaine de compétences du SRC qui apparaissent dans une procédure pénale de l'OFDF. Les collaborateurs de l'OFDF ne peuvent toutefois pas accéder aux données rattachées à une personne, à une organisation ou autre. Pour que celles-ci leur soient communiquées, ils doivent soumettre au SRC une demande d'assistance administrative dûment motivée (voir al. 2).

Let. e

Les collaborateurs de l'OFDF chargés de l'analyse des risques ont besoin de droits d'accès afin de surveiller et de contrôler le trafic de personnes et de marchandises à travers la frontière. Ce but de l'accès correspond également à la formulation des tâches de l'OFDF. L'utilisation de ces données aide l'OFDF à coordonner de manière ciblée les résultats des analyses de risque avec le SRC et à identifier les liens possibles entre les différents événements. Elle permet également de formuler des instructions à l'intention des collaborateurs de l'OFDF chargés de contrôler les personnes, les marchandises et les moyens de transport. Ils ne peuvent toutefois pas accéder aux données rattachées à une personne, à une organisation ou autre. Pour que celles-ci leur soient communiquées, ils doivent soumettre au SRC une demande d'assistance administrative dûment motivée.

Let. f

Le Groupement de la Défense obtient également un accès en vue de protéger l'armée à titre préventif contre l'espionnage, le sabotage et d'autres activités illicites dans le cadre du service de promotion de la paix ou le service actif. Ce droit d'accès tient compte du fait que le Service pour la protection préventive de l'armée (SPPA) doit continuellement enquêter sur des personnes dans le cadre de la promotion de la paix (engagement dans les Balkans). Il a ainsi adressé plus de cent demandes écrites au SRC en 2020. En raison des tâches du service de promotion de la paix, le SPPA a accès à des informations en lien avec le terrorisme, l'extrémisme violent et l'espionnage. Eu égard à la diaspora des Balkans en Suisse, de telles informations sont souvent pertinentes pour la sûreté intérieure de la Suisse, ou à l'inverse pour la sûreté de l'Armée suisse dans le service de promotion de la paix. Un échange rapide et efficient d'informations peut donc jouer un rôle déterminant pour la sécurité. L'octroi d'un droit d'accès permet donc de réduire considérablement la charge de travail (en particulier pour les personnes qui ne figurent pas dans le système, soit environ 50%). Les seuls collaborateurs du SPPA qui obtiennent ce droit sont ceux qui se chargent des affaires opérationnelles (fonction « commissaire SPPA »). Eux aussi peuvent uniquement constater que le SRC traite des données relevant du renseignement relatives à personne, à une organisation ou autre. Pour que celles-ci leur soient communiquées, ils doivent soumettre au SRC une demande d'assistance administrative dûment motivée.

Al. 2

Pour des raisons de transparence, la loi dispose désormais que si le contrôle révèle que des données existent, les autorités fédérales et d'exécution cantonales peuvent demander au SRC de leur communiquer ces dernières. La demande doit être motivée et la communication est soumise aux restrictions formulées aux art. 59 à 61.

Al. 3

À l'avenir, le SRC devrait être en mesure de fournir ses produits (présentations de la situation, analyses et rapports composés à partir de données citées à l'art. 49, let. a, b, c, g, h et i) en ligne à ses clients en vue d'évaluer les conséquences des menaces relevant de la politique de sécurité et pour les besoins en matière de conduite de la politique de sécurité. Cette méthode a fait ses preuves dans le cas des autorités d'exécution cantonales, dans la mesure où le SRC enregistre à leur intention les rapports de situation classifiés ou les produits de monitoring OSINT sur la plateforme d'information de l'environnement de travail fourni par la Confédération. De la sorte, le SRC n'a plus besoin de recopier ces produits et de les distribuer à de nombreux destinataires par courriel ou sur papier. Il s'agit en outre de la garantie pour le SRC qu'il peut gérer ces données et les supprimer après un certain temps, ce qui n'est pas le cas avec les autres formes de communication. Ces produits sont communiqués dans le respect des restrictions formulées aux art. 59 à 61.

Al. 4

Le SRC est tenu de s'assurer que les clients n'abusent pas de leur droit d'accès. Il réalise donc des contrôles par sondage et se réserve le droit de leur demander d'indiquer quand ils ont accédé à quel produit et pour quelle raison.

Art. 56

Les droits d'accès des collaborateurs du SRC sont réglés aujourd'hui dans le cadre des systèmes d'information et de stockage des données. À une exception près, ils ne sont pas modifiés. À l'avenir, la Sécurité SRC aura accès aux données relevant du renseignement, afin de pouvoir p. ex. contrôler si des données sont traitées sur les nouveaux collaborateurs du SRC lors de leur recrutement (sur les tâches de la Sécurité SRC, voir aussi l'art. 7, al. 1). Le principe de proportionnalité, qui exige que l'accès soit accordé sur la base « need-to-know » (principe du besoin d'en connaître), s'applique toujours aux droits d'accès des collaborateurs du SRC. Comme auparavant, seuls les collaborateurs chargés de la mise en œuvre de la mesure de recherche et de l'évaluation de ses résultats auront donc accès en ligne aux données concernées.

Art. 57

Al. 1

[22] RS **631.0**
[23] FF **2020** 7196

Le droit d'accès des collaborateurs des autorités d'exécution cantonales à leurs propres données demeure lui aussi inchangé.

Al. 2

Les collaborateurs des autorités d'exécution cantonales auront toujours accès aux rapports établis par ces autorités de manière autonome ou à la demande du SRC puis transmis à celui-ci, ainsi qu'aux données relevant du renseignement issues de sources accessibles au public. La loi en vigueur en dispose de même aux art. 51, al. 3, let. b, et 54, al. 4.

Al. 3

Certaines autorités d'exécution cantonales et la CCDJP ont demandé à obtenir de leurs homologues un accès réciproque à leurs données relevant du renseignement. Cela leur permettrait de savoir plus facilement si l'autorité d'exécution d'un canton voisin traite déjà des données relatives à une personne ou à une organisation. Cette solution est particulièrement utile dans le cas d'enquêtes préliminaires en cours, c'est-à-dire alors que la personne ou l'organisation concernée n'a pas encore été signalée au SRC et demeure donc inconnue de celui-ci. Les autorités d'exécution cantonales ne sont aujourd'hui pas en mesure de déterminer de la sorte si une homologue traite des données sur la personne ou l'organisation concernée. Étant donné que toutes les autorités d'exécution cantonales ne sont pas d'accord avec ce droit d'accès, celui-ci n'est proposé ici qu'à titre de disposition potestative. Les détails des droits d'accès peuvent ainsi être réglés dans les ordonnances.

Al. 4

Le service de contrôle de qualité du SRC est chargé de contrôler par sondage la manière dont les autorités d'exécution cantonales traitent les données (voir art. 58*c*, al. 1). À cet égard, il a déjà accès aux données des autorités d'exécution cantonales, ce qui est précisé par souci d'exhaustivité.

Art. 58

Al. 1

Cet alinéa correspond en grande partie à l'actuel art. 53, al. 3. En raison de l'étroite collaboration dans le domaine de la sécurité, la police nationale du Liechtenstein obtient désormais un accès permanent à la PES. Auparavant, elle n'y avait accès que lors d'événements particuliers.

Al. 2

Cet alinéa correspond à l'actuel art. 53, al. 4.

Art. 58a

Al. 1 et 2

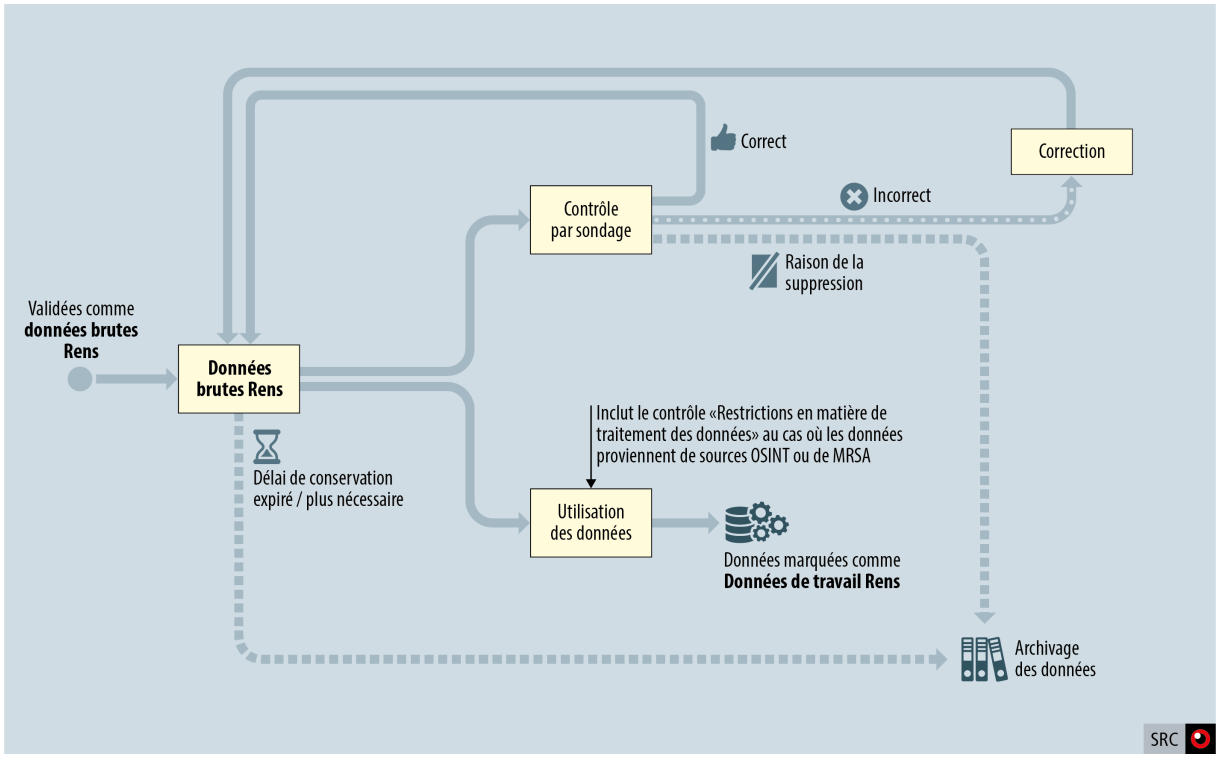
L'accès aux données administratives n'est pas modifié (voir art. 52, al. 3). L'accès des autorités d'exécution cantonales au système de gestion des mandats qui leur est attribué par l'art. 29, let. c, OSIS-SRC, n'est toutefois aujourd'hui pas réglé de manière explicite .

Al. 3

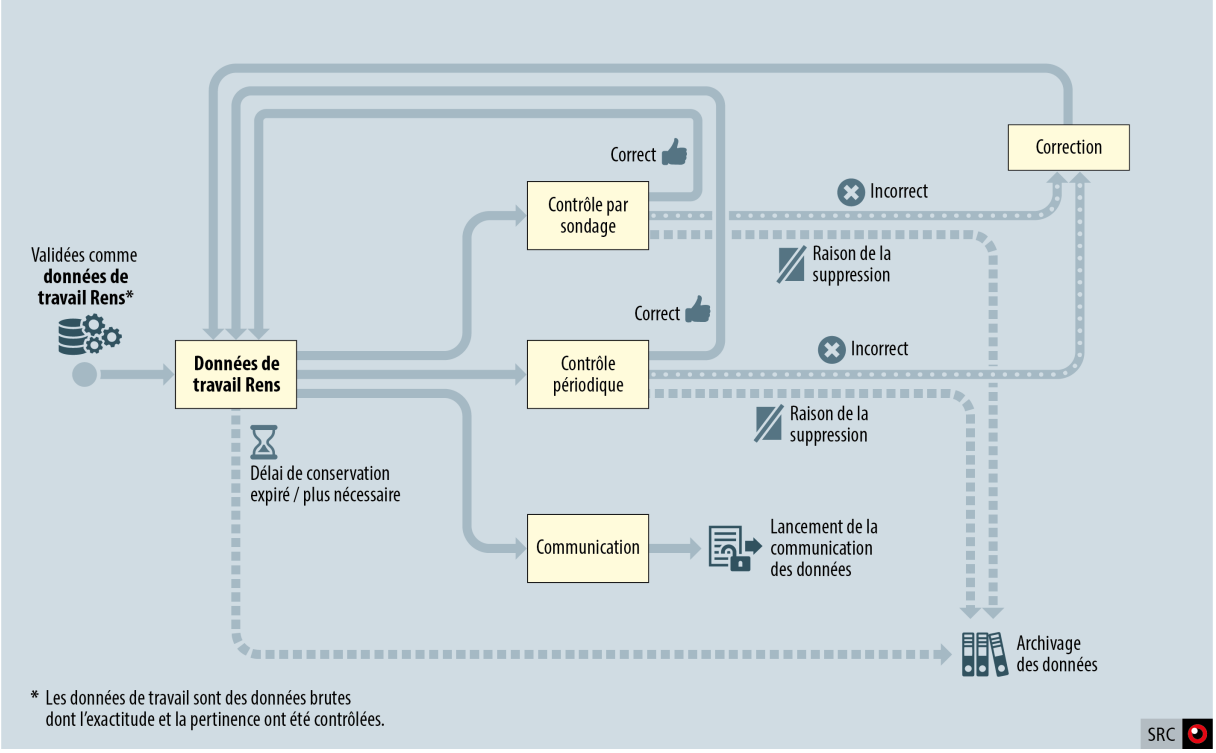
L'accomplissement des missions du SRC repose sur sa collaboration avec des prestataires externes. C'est le cas, d'une part, pour l'entretien et le développement de son infrastructure informatique. En raison de la complexité des logiciels, le SRC a souvent besoin de savoir-faire externes, ne serait-ce que pour trouver les causes des problèmes. Il en va a fortiori pour leur résolution. Par exemple, si un collaborateur supprime un compte utilisateur par erreur, seul le prestataire externe est en mesure de le restaurer avec toutes les données, tâches et processus associés. Les prestataires externes n'ont cependant accès qu'aux métadonnées, et non aux données proprement dites. Toutefois, ils sont également requis pour des travaux de développement ultérieurs dans le cadre desquels une expertise externe est indispensable, bien que des données des dossiers de projet correspondants doivent être traitées. D'autre part, le SRC fait régulièrement traduire des textes par des traducteurs externes sur la base de mandats. Le fait que ces traducteurs n'aient actuellement pas accès aux données administratives complique l'attribution et l'exécution des mandats tout en compromettant la sécurité des informations, car ils doivent travailler en dehors du réseau sécurisé du SRC.

Section 6: Contrôle de qualité

Vue d'ensemble du traitement et du contrôle de la qualité des données brutes


Validées comme
données brutes Rens
Données brutes Rens
Délai de conservation expiré / plus nécessaire
Contrôle par sondage
Correct
Incorrect
Correction
Raison de la suppression
Inclut le contrôle «Restrictions en matière de traitement des données» au cas où les données proviennent de sources OSINT ou de MRSA
Utilisation des données
Données marquées comme **Données de travail Rens**
Archivage des données
SRC

Vue d'ensemble du traitement et du contrôle de la qualité des données de travail



Art. 58b

Al. 1

Le contenu de cet alinéa correspond à celui de l'actuel art. 45, al. 4. Étant donné que la LRens ne règle plus les différents systèmes d'information, il est question de données de travail. L'ancienne formulation de cette disposition a occasionné divers malentendus et discussions. Cet alinéa est désormais rédigé de manière à indiquer clairement qu'il s'agit des données associées à une personne ou à une organisation.

Al. 2

Le contenu de cet alinéa correspond à celui de la dernière phrase de l'actuel art. 45, al. 4. Bien entendu, les données expressément marquées comme inexactes (voir art. 51, al. 2) ne sont pas corrigées dans le cadre du contrôle périodique. Le renvoi à la réserve a en outre été adapté.

Al. 3

Cet alinéa correspond en grande partie à l'actuel art. 45, al. 5. L'actuelle let. b, qui prévoit une vérification périodique des rapports des autorités d'exécution cantonales par le service de contrôle de qualité du SRC, a été supprimée sans remplacement, car il n'y a aucune raison de traiter ces données de manière particulière. Elles peuvent également être contrôlées par les spécialistes responsables, comme le prescrit le nouvel art. 58*b*, al. 1, pour toutes les données de travail que le SRC a associées à une personne ou à une organisation dans l'accomplissement de ses tâches en vertu de l'art. 6, al. 1.

Aujourd'hui, il est interdit aux autorités d'exécution cantonales d'effacer elles-mêmes des données (voir l'actuel art. 45 al. 5, let. d). Cette disposition n'a désormais plus de justification plausible. Au contraire, elle a conduit à un mécanisme de suppression complexe qui mobilise inutilement les ressources des autorités d'exécution cantonales et du service de contrôle de qualité du SRC. Cette lettre est donc elle aussi supprimée sans remplacement. À l'avenir, les autorités d'exécution cantonales pourront de nouveau (comme avant l'entrée en vigueur de la LRens) supprimer elles-mêmes leurs données lorsqu'elles n'en ont plus besoin ou que leur délai de conservation est expiré.

L'ajout de l'adverbe « en particulier » rappelle que la liste n'est pas exhaustive et que le service de contrôle de qualité du SRC assume d'autres tâches encore.

Let. a

Le contenu de cette lettre correspond à celui de l'actuel art. 45, al. 5, let. a. Comme aujourd'hui, les données dans le domaine de l'extrémisme violent (reconnaissables à leur sous-catégorie; voir les explications de l'art. 49) devront à l'avenir faire l'objet de contrôles plus poussés et plus précoces. Ils ont actuellement lieu immédiatement après la saisie/l'enregistrement structuré des données. À l'avenir, il sera question d'associer des données à des personnes et à des organisations. Le contrôle a cependant toujours lieu au même moment. Le terme « pertinence » est remplacé systématiquement par « lien avec les tâches » dans le présent projet. Il est désormais précisé que le respect des restrictions en matière de traitement des données est également contrôlé.

Let. b

Le contenu de cette lettre correspond à celui de l'actuel art. 45, al. 5, let. c. Étant donné que la LRens ne règle plus les différents systèmes d'information, le contrôle par sondage effectué par le service de contrôle de qualité ne porte plus sur les différents systèmes d'information, mais sur toutes les données du SRC relevant du renseignement (données brutes et données de travail). Les termes

«efficacité» et «adéquation» ne sont plus employés, car ils sont obsolètes au regard du droit de la protection des données. Un traitement de données est efficace s'il produit un résultat et adéquat si le but visé peut être atteint avec ce résultat. Dès lors, l'adéquation présuppose l'efficacité. De même, si le but peut être atteint avec une mesure donnée, c'est qu'elle est adéquate. L'adéquation est l'une des trois conditions préalables à la notion de proportionnalité. Si le contrôle porte non plus sur l'efficacité et l'adéquation, mais sur la proportionnalité, il gagne en exhaustivité, car outre le caractère approprié des données, la nécessité et le caractère exigible sont examinés. Les contrôles par sondage des données relevant du renseignement des autorités d'exécution cantonales sont réglés à l'art. 58*c*, al. 1.

Let. c

À l'avenir, le responsable de la protection des données du SRC sera chargé d'organiser des formations en matière de respect des dispositions de la présente loi concernant le traitement des données. Cette lettre précise en outre que ces formations s'adressent aussi aux collaborateurs des autorités d'exécution cantonales.

Al. 4

Par souci de transparence, il est précisé au sujet de la PES que le SRC assume uniquement la responsabilité et le contrôle de la qualité des données traitées par lui ou par les autorités d'exécution cantonales. Les données traitées par d'autres autorités (p. ex. fedpol) sont de la responsabilité de ces dernières.

Art. 58c

Al. 1

Le contrôle par sondage du traitement des données relevant du renseignement par les autorités d'exécution cantonales n'est certes pas nouveau, mais il n'a jusqu'à présent pas fait l'objet de dispositions expresses (voir l'actuel art. 45, al. 5, let. c, qui ne mentionne que «tous les systèmes d'information»). Eu égard au terme de proportionnalité, on se référera aux explications de l'art. 58*b*, al. 3, let. b.

Al. 2

Le renvoi des rapports des autorités d'exécution cantonales qui ne sont pas entièrement en lien avec les tâches du SRC ou qui enfreignent les restrictions en matière de traitement des données n'est pas expressément prévu par la LRens en vigueur (contrairement aux art. 3, al. 3, et 4, al. 2, OSIS-SRC, qui prescrivent déjà une telle obligation). Par souci de transparence et parce que le traitement des données des autorités d'exécution cantonales doit être corrigé le cas échéant, cette manière de procéder est expressément inscrite dans la loi, et reflète au demeurant la pratique actuelle.

Chapitre 4a: Dispositions particulières relatives à la protection des données

Conformément à la nouvelle structure de la loi, la section 4 du chap. 4 devient le chap. 4a.

Section 1: Communication de données personnelles par le SRC

Comme évoqué précédemment au début du chap. 4, à quelques exceptions près, les données brutes ne peuvent être utilisées, resp. communiquées. Dès lors, le présent chapitre est consacré avant tout aux données de travail, qui ont déjà fait l'objet de contrôles poussés (voir cependant les exceptions citées aux art. 5, al. 6, et 46, al. 3).

Art. 59

Cet article correspond en grande partie à l'actuel art. 59. Le contenu de cette disposition demeure inchangé. Par souci de clarté, il est toutefois précisé dans le titre qu'il s'agit de la vérification de données personnelles. Étant donné que les produits du renseignement contiennent également des données personnelles, ils ne sont plus mentionnés. Par ailleurs, il est précisé que les données personnelles incluent les données personnelles sensibles et les données personnelles sensibles reposant sur un profilage. La restriction de cette disposition à la LRens est supprimée, car la communication doit respecter toutes les dispositions légales applicables.

Art. 60

Cet article correspond en grande partie à l'actuel art. 60.

Al. 1

Il est également précisé dans cet alinéa que les données personnelles incluent les données personnelles sensibles et les données personnelles sensibles reposant sur un profilage.

Al. 3

Par souci d'harmonisation avec la nLPD, seul le terme « données » est remplacé par « données personnelles ».

Art. 61, al. 1

Il est également précisé dans cet alinéa que les données personnelles incluent les données personnelles sensibles et les données personnelles sensibles reposant sur un profilage. Étant donné que, du point de vue de la protection des données, le fait que des données personnelles figurent sur une liste ne fait aucune différence, la référence correspondante a été supprimée. Il importe uniquement de s'assurer que les conditions légales à la communication sont respectées pour chaque donnée personnelle communiquée.

Art. 62

Il est également précisé dans cet article que les données personnelles incluent les données personnelles sensibles et les données personnelles sensibles reposant sur un profilage.

Let. a

Le terme « transmission » est remplacé par « communication », employé dans la LPD. Le contenu de cette disposition ne s'en trouve pas modifié.

Let. b

Ne concerne que les textes allemand et italien.

Let. c

Le terme « demande de renseignement » est remplacé par « requête d'accès ». Cette modification précise qu'il ne s'agit pas d'une demande d'accès au sens des art. 63 et 63*a*., mais d'une requête du SRC ou d'une autorité d'exécution cantonale. Le contenu de cette disposition ne s'en trouve pas modifié.

Let. d

Le renvoi à la communication à des tiers dans le cadre de l'art. 45, al. 4, est ajouté ici.

Section 2: Droit d'accès

La réglementation du droit d'accès actuellement en vigueur est complexe. Elle se base d'une part sur la nLPD et d'autre part sur les dispositions légales particulières de la LRens (voire sur les deux lois en ce qui concerne le système d'information GEVER SRC). Cette législation se doit d'être simplifiée, notamment dans l'intérêt des requérants.

Alors que la nLPD continuera de s'appliquer aux données administratives, les données relevant du renseignement seront soumises en principe à la réglementation actuellement prévue pour fedpol concernant le système de traitement des données relatives aux infractions fédérales (cf. art. 8 de la loi du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP)[24]) et les signalements en vue d'une arrestation aux fins d'extradition (cf. art. 8*a* LSIP), la sensibilité des données relevant du renseignement étant comparable à celle des données de fedpol. Le SRC ne pourra désormais différer la communication de renseignements que dans des cas exceptionnels et au cas par cas. Si le requérant ne figure pas dans le système, le SRC peut immédiatement lui faire part de cette absence.

Art. 63

Par analogie avec la LSIP, les demandes d'accès aux données administratives (cf. art. 7 LSIP) et aux données relevant du renseignement (cf. art. 8 et 8*a*. LSIP) sont régies par deux articles distincts. Cette disposition permet de distinguer plus clairement les données administratives, soumises à une procédure administrative et à une décision du SRC pouvant être contestée devant le Tribunal administratif fédéral ou le Tribunal fédéral, des données relevant du renseignement, pour lesquelles il n'existe qu'un droit d'accès indirect.

Par conséquent, le droit d'accès aux données exclusivement administratives est régi par les art. 25 et 26 nLPD (cf. art. 7, al. 1, LSIP).

Art. 63a

La question de la conformité avec le droit constitutionnel et international du renoncement à une voie de droit ordinaire pour la personne concernée en cas de restriction ou de refus du droit d'accès est encore controversée et sera éclaircie lors de la procédure de consultation.

Al. 1

La restriction de la communication des renseignements se base désormais sur les motifs énumérés à l'art. 26 nLPD. Contrairement à l'art. 8, al. 1, LSIP, la LRens ne prévoit aucune dérogation aux dispositions de la nLPD. Cet alinéa remplace les al. 1 et 2 de l'actuel art. 63. En ce qui concerne la communication de renseignements sur des données personnelles, l'art. 25, al. 2, let. b, nLPD précise que seules les données personnelles «en tant que telles» sont fournies (et non les copies de documents).

Al. 2

Cet alinéa correspond à l'actuel art. 63, al. 4. Outre les intérêts étatiques relevant de la sauvegarde du secret, il existe d'autres raisons de refuser, restreindre ou différer la communication des renseignements, notamment la protection de tiers (par ex. d'une source). Celle-ci peut continuer à s'appliquer après l'expiration du délai. Par souci de transparence, il est donc signalé que les motifs visés à l'art. 26, al. 2, nLPD peuvent s'appliquer même si ceux visés à l'art. 26, al. 1, nLPD ne sont plus pertinents. Contrairement à la disposition similaire de l'art. 8, al. 6, LSIP, la LRens prévoit que les personnes ne faisant l'objet d'aucun traitement de données peuvent en être informées immédiatement. L'expérience acquise en matière de droit d'accès indirect indique que l'intérêt d'une personne à être informée rapidement qu'aucune donnée la concernant n'est traitée devrait primer nettement sur le risque théorique que les connaissances du SRC fassent l'objet d'activités d'espionnage.

Al. 3

Cet alinéa correspond en grande partie à l'actuel art. 63, al. 3. Outre le report, il réglemente désormais le refus et la restriction éventuels de la communication des renseignements. Il prévoit en outre que le PFPDT contrôle également si les renseignements ont été communiqués correctement en vertu de l'al. 1, ce qui n'est pas prévu dans la disposition similaire de l'art. 8, al. 2, LSIP. Tout recours étant exclu, la conformité de la communication ne peut toutefois pas être vérifiée plus avant.

Al. 4

Cet alinéa correspond à l'actuel art. 64, al. 1 (avec référence adaptée). Il renvoie au principe de la nLPD selon lequel le PFPDT est autorisé à ouvrir une enquête en cas d'erreurs. Ici aussi, il est désormais également question de refus et de restriction (voir la disposition similaire à l'art. 8, al. 3, LSIP).

Al. 5

La nLPD confère désormais au PFPDT le droit de rendre des décisions. Les recommandations actuelles (voir l'actuel art. 64, al. 2) seront supprimées (voir la disposition similaire de l'art. 8, al. 4, LSIP). Le contenu de l'actuel al. 4 est donc également obsolète.

[24] RS **361**

Al. 6

Par analogie avec les dispositions de la LSIP (art. 8, al. 5), il est indiqué que la communication visée à l'al. 4 est toujours communiqué de manière identique et n'est pas motivée. Contrairement à la LSIP, la LRens prévoit cependant la saisie du Tribunal administratif fédéral pour vérification de la communication, ce qui constitue une voie de recours indirecte contre les décisions du SRC.

Al. 7

L'actuel art. 64, al. 5, doit être adapté de sorte que le préposé puisse ordonner au SRC de fournir immédiatement au requérant le renseignement demandé si les conditions prévues par cette disposition sont remplies. Ici aussi, le refus et la restriction de la communication des renseignements sont désormais mentionnés. Cette disposition correspond à l'art. 8, al. 7, LSIP.

Al. 8

Afin d'éviter toutes procédures parallèles, les renseignements visés aux al. 1 et 2, ainsi que les communications visées aux al. 3 et 4 ne sont pas sujets à recours.

Art. 64

Il va de soi que le SRC ne peut fournir des renseignements que sur les domaines de la PES dans lesquels lui-même ou les autorités d'exécution cantonales traitent des données. Si la PES contient des données personnelles provenant d'autres autorités, le SRC transmet à ces dernières les demandes d'accès correspondantes.

Art. 65

Al. 1

Cette disposition correspond à l'actuel art. 66, al. 1. Seule la référence à la vérification a été adaptée.

Al. 2

Cet alinéa correspond à l'actuel art. 66, al. 2. Étant donné que le PFPDT n'émet plus de recommandations, les explications à ce sujet ont été supprimées.

Section 3: Archivage

Conformément à la nouvelle structure, l'actuelle section 5 du chap. 4 devient la section 3.

Art. 68

Cet alinéa correspond en grande partie à l'actuel art. 68.

Al. 1

Dans la LRens et les ordonnances d'exécution subséquentes, une distinction est faite entre les termes « supprimer » et « détruire ». Le SRC propose les données destinées à être supprimées aux Archives fédérales suisses à des fins d'archivage. Il détruit les données jugées sans valeur archivistique ou qui ont déjà été remises aux Archives fédérales suisses. L'al. 1 porte sur l'archivage de données dont le SRC n'a plus besoin en permanence. Cette phase concerne donc la « suppression » et non la « destruction » de données. Il est désormais précisé que l'autorité indépendante de surveillance propose elle aussi aux AFS les données dont elle n'a plus besoin en permanence qui sont destinées à être supprimées, que les AFS stockent ces données dans des locaux hautement sécurisés, et que celles-ci sont soumises à un délai de protection prolongé. Les données de l'autorité indépendante de surveillance proviennent en grande partie du SRC et des autorités d'exécution cantonales, raison pour laquelle ses intérêts relatifs au maintien du secret sont tout aussi élevés.

Al. 4

Cet alinéa précise que le SRC détruit les données que les Archives fédérales suisses jugent sans valeur archivistique, ceci immédiatement après leur suppression même si leur délai de conservation n'a pas encore expiré. Il en va de même pour l'autorité indépendante de surveillance. Les destructions sont enregistrées selon l'ordonnance.

Art. 70

Al. 1, let. d

La let. d de l'actuel art. 70, al. 1, doit être supprimée pour éviter les doublons. Une appréciation annuelle supplémentaire de la situation en matière de politique de sécurité n'est plus nécessaire aujourd'hui, d'autant plus que le Conseil fédéral fournit des informations beaucoup plus complètes à ce sujet via ses rapports sur la politique de sécurité, qui sont désormais publiés tous les quatre ans. Le pilotage politique du Service de renseignement est suffisamment couvert par les autres dispositions de l'article. Cette suppression ne concerne pas les rapports du DDPS sur le renseignement et la politique de sécurité à l'intention des commissions parlementaires compétentes (art. 80). Ces derniers sont maintenus conformément aux besoins du Parlement.

La suppression permet en outre d'éviter une certaine contradiction avec l'al. 2, qui dispose que les documents liés aux tâches visées à l'al. 1 ne sont pas accessibles au public. Le rapport de situation annuel du SRC, qui présente les principaux aspects de l'évolution de la situation du point de vue du renseignement, informe dans tous les cas le public sur l'appréciation de la situation.

Al. 3

La disposition existante selon laquelle le Conseil fédéral est autorisé à conclure seul des traités internationaux dans le domaine du renseignement doit être étendue et préciser, conformément à la pratique internationale, que lesdits traités peuvent être tenus secrets s'ils doivent être classifiés « secret » en vertu de l'art. 13, al. 3, LSI. À l'heure actuelle, la collaboration internationale en matière de renseignement a tendance à se formaliser. Il est toutefois peu probable qu'un pays soit prêt à conclure des traités publiés dans ce domaine dans un avenir proche.

La nouvelle LSI prévoit l'autorisation générale du Conseil fédéral de conclure des traités internationaux en matière de sécurité de l'information. Afin d'éviter toute ambiguïté, la mention de cette compétence est maintenue dans la LRens, au même titre que les domaines dans lesquels le Conseil fédéral peut conclure seul des traités portant sur la collaboration en matière de renseignement.

Le Conseil fédéral rend compte chaque année à l'Assemblée fédérale des traités internationaux qu'il a conclus de manière indépendante. En revanche, seule la DélCdG est informée des traités confidentiels ou secrets conclus dans le domaine du renseignement (art. 48*a*, al. 2, LOGA). De plus, les organes de surveillance des services de renseignement AS-Rens et DélCdG conservent, en vertu de leurs droits de surveillance, un droit de regard global sur ces documents. Le contrôle et la surveillance sont ainsi garantis.

Art. 74 (voir les explications de l'art. 83*a* pour la numérotation des alinéas)

Les alinéas abrogés sont désormais intégrés au nouvel alinéa sur les dispositions pénales, intégré avant les dispositions finales. Les dispositions pénales figurent ainsi à la fin du texte de loi, comme à l'accoutumée.

Section 2: Contrôle et surveillance du SRC

Lors des débats parlementaires, les commissions compétentes et le Conseil fédéral ont convenu de développer, dans un premier temps, la nouvelle AS-Rens créée avec la LRens, tout en laissant l'ACI poursuivre ses contrôles et étendre ces derniers à l'exploration du réseau câblé. À l'heure actuelle, l'AS-Rens et l'ACI collaborent et coordonnent leurs activités afin d'éviter toute lacune en termes de surveillance. L'objectif initial de cet accord était d'assurer et de renforcer la surveillance. Une fusion des deux instances avec transfert des connaissances devait être examinée dans un second temps. Une telle mesure permettrait notamment de se passer de la coordination des activités. Par ailleurs, la haute surveillance parlementaire ainsi que le SRC n'auraient plus qu'un seul interlocuteur, tandis que le contrôle exercé resterait le même. L'indépendance de l'autorité de surveillance resterait garantie.

Les tâches de l'ACI doivent désormais être transmises à l'AS-Rens après une évaluation des avantages et des inconvénients. L'AS-Rens dispose aujourd'hui déjà de compétences de surveillance étendues. Elle surveille les activités de renseignement du SRC, des autorités d'exécution cantonales ainsi que des autres entités et des tiers mandatés par le SRC, ceci en termes de légalité, d'adéquation et d'efficacité.

L'ACI vérifie spécifiquement la légalité de l'exploration radio et surveille l'exécution des missions d'exploration du réseau câblé autorisées et avalisées. Afin de mener à bien leurs activités de surveillance, l'AS-Rens et l'ACI ont accès à toutes les informations et à tous les documents utiles ainsi qu'à tous les locaux utilisés par les entités soumises à la surveillance. Les deux instances collaborent régulièrement.

Etant donné que les compétences de surveillance de l'AS-Rens couvrent en principe celles de l'ACI, il semble judicieux de fusionner les activités de surveillance de ces deux services pour former un organisme unique bénéficiant d'emblée d'une vue d'ensemble des activités de renseignement. Cette mesure garantit que la surveillance de l'exploration radio comme de l'exploration du réseau câblé demeure efficace et complète. Par conséquent, l'actuel art. 79 LRens devient obsolète et est supprimé.

De plus, le mandat de surveillance de l'AS-Rens garantit également une surveillance plus complète, qui s'étend non seulement à la légalité des activités de renseignement, mais aussi à leur adéquation et à leur efficacité. Enfin, le transfert de tâches crée également des synergies: l'AS-Rens se consacre exclusivement à l'examen des activités de renseignement. L'ACI, en revanche, travaille avec un système de milice. Compte tenu de la rapidité des évolutions techniques et de la complexité des problématiques qui en résultent dans les processus quotidiens, il devient de plus en plus difficile pour cette instance de maintenir le niveau de connaissances requis pour l'activité de contrôle sans y consacrer excessivement de temps. Au vu des autres tâches qui lui incombent, l'AS-Rens est quant à elle tenue d'acquérir ces connaissances. Elle compte aujourd'hui déjà des experts en la matière. Grâce aux synergies existantes, la qualité de la surveillance peut être maintenue et adaptée aux changements sans efforts disproportionnés. La suppression d'une autorité de surveillance réduit le travail de coordination sans que les résultats des examens ne perdent en qualité. Le fait de regrouper les compétences (de surveillance) permet d'effectuer un contrôle complet d'un seul tenant. Grâce au transfert des tâches et des connaissances de l'ACI à l'AS-Rens, il sera possible de mettre en œuvre la solution envisagée par le Parlement lors du débat sur la LRens en 2015.

La révision de la LRens est aussi l'occasion de rendre la loi plus lisible, notamment par une simplification de sa structure. Il est donc proposé que l'art. 78 soit divisé en quatre dispositions distinctes, dans le respect des différentes tâches incombant à l'AS-Rens en vertu de la loi, à savoir la surveillance, la coordination et l'information du public. Dans la mesure où le DDPS est chargé de mettre en œuvre les recommandations de l'AS-Rens, ce point fera désormais l'objet d'une disposition à part entière, toujours par souci de clarté.

Art. 75

La LRens emploie le terme « autorités d'exécution cantonales », aussi la formulation de l'article est harmonisée en ce sens.

Art. 77, al. 2

La procédure concernant la soumission du projet de budget annuel au Conseil fédéral par l'AS-Rens via le DDPS et sa transmission sous forme inchangée à l'Assemblée fédérale, jusqu'alors uniquement réglée à l'art. 4 de l'ordonnance du 16 août 2017 sur la surveillance des activités de renseignement (OSRens)[25], est désormais intégrée à l'art. 77, al. 2, LRens, étant donné qu'une base légale formelle est en principe nécessaire à cet égard.

Art. 78

Cette disposition reprend la formulation exacte des al. 1 et 4 de l'ancien art. 78 (il s'agit désormais des al. 1 et 2) et détaille au sens strict l'activité de surveillance de l'autorité de surveillance indépendante. Pour garantir l'accomplissement des tâches de cette dernière, notamment la surveillance de l'exploration du réseau câblé, le nouvel al. 4 précise que l'AS-Rens peut exiger la participation des fournisseurs de services postaux et de télécommunication ainsi que l'accès à leurs locaux.

25 RS **121.3**

Les termes relatifs à la conservation des données figurant à l'al. 3, qui reprend l'ancien al. 5, sont adaptés au nouveau concept de conservation des données de la nLPD. Le contenu ne s'en trouve pas modifié.

Art. 78a

Cette disposition comprend les al. 6 et 7 de l'ancien art. 78. Elle porte sur la forme du résultat des contrôles effectués par l'autorité de surveillance indépendante ainsi que sur le destinataire des rapports qu'elle établit, et précise la responsabilité de la mise en œuvre des recommandations formulées.

La DélCdG a exigé des éclaircissements sur les activités de l'AS-Rens dans le cadre de la surveillance des autorités d'exécution cantonales et sur ses éventuelles recommandations. Des précisions sont donc apportées au texte de loi. Si l'art. 78, al. 1, LRens dispose clairement que les activités de surveillance de l'AS-Rens s'étendent également aux activités des autorités cantonales d'exécution, la question des recommandations que l'AS-Rens adresse à ces dernières n'a jusqu'à présent été que partiellement réglée dans l'OSRens (art. 13, al. 1). Le nouvel art. 78*a* résout ce manque de clarté en précisant à l'al. 1 que l'AS-Rens peut adresser des recommandations à toutes les entités dont elle assure la surveillance en vertu de l'art. 78, al. 1. Grâce à cette précision, il est désormais clair que les recommandations de l'AS-Rens peuvent être adressées à une ou plusieurs entités s'il est question de collaboration entre différents organes. De plus, la précision concernant l'information à l'autorité cantonale de surveillance, qui figurait dans l'ordonnance, sera désormais inscrite dans la loi.

Le DDPS ou le service cantonal compétent est chargé de mettre en œuvre les recommandations de l'AS-Rens, indépendamment de l'organe auquel celles-ci sont adressées, en vertu du nouvel art. 78*a,* qui reprend l'actuel art. 78, al. 1, LRens. Le nouvel al. 4 introduit une nouvelle procédure pour la validation des recommandations relevant de la compétence cantonale et, le cas échéant, pour leur rejet par les autorités cantonales. La compétence décisionnelle au sein des cantons est ainsi réglée de manière analogue à l'échelon fédéral (cf. al. 2), et il est tenu compte d'une demande de la DélCdG.

Art. 78b

L'al. 2 de l'ancien art. 78, qui concerne la coordination interne des activités de l'autorité de surveillance indépendante, est repris dans un article distinct.

Art. 78c

Les principes de la coordination de la surveillance des services de renseignement avec les autorités étrangères sont désormais réglementés par la LRens. Les détails de cette coordination internationale sont définis dans l'OSRens. Les raisons de cette adaptation sont les suivantes.

La transmission mutuelle d'informations, notamment de données personnelles, a augmenté parallèlement à l'intensification de la collaboration transfrontalière des services de renseignement et aux évolutions techniques. Cet échange d'informations et de données avec les services de renseignement étrangers fait partie du travail quotidien du SRC. Il peut être effectué sous diverses formes, par oral ou par écrit. Compte tenu de l'internationalisation continue des activités de renseignement, la collaboration entre les autorités de surveillance gagne en importance. Cette collaboration est souvent nécessaire pour assurer une surveillance efficace des services de renseignement actifs au niveau international. C'est pourquoi l'AS-Rens doit avoir la possibilité d'échanger des informations et des expériences avec ses partenaires internationaux en matière de surveillance, à l'instar d'autres autorités de surveillance suisses (par ex. la FINMA ou le PFPDT). En principe, tout mandat de surveillance des autorités de surveillance est strictement national, raison pour laquelle la collaboration entre les services de renseignement ainsi que leurs flux de données ne peuvent être contrôlés dans leur intégralité. Il existe donc une lacune en matière de surveillance. C'est dans ce contexte que la nouvelle norme de l'art. 78*c* entre en jeu.

La LRens régit aujourd'hui déjà la collaboration ainsi que la communication bilatérale et multilatérale de données entre les services de renseignement. Elle ne fournit toutefois pas de base juridique spécifique pour la collaboration ou la communication entre autorités de surveillance lorsqu'il s'agit de données personnelles. Contrairement à celui des services de renseignement, le travail des autorités de surveillance ne peut pas s'étendre au-delà des frontières. La surveillance porte uniquement sur des mandats nationaux. Cet aspect ne traduit toutefois qu'un côté de la communication des données: la surveillance se concentre soit sur la collecte et la fourniture de données, soit sur leur réception et leur utilisation. Les autorités de surveillance ne peuvent ni obtenir un aperçu global de la communication de données personnelles, ni vérifier la légalité du processus de collaboration dans son ensemble ou du stockage des données à l'étranger.

L'AS-Rens contribue actuellement à un groupe de travail international, tout comme l'ancien service interne de surveillance du DDPS. Elle échange également des informations aux niveaux bilatéral et multilatéral, dans le cadre de rencontres et de séminaires. Faute d'une base juridique qui permettrait à l'AS-Rens de communiquer des données concrètes à ses partenaires étrangers, la collaboration atteint ses limites. Bien qu'il ait jusqu'à présent été possible de présenter son organisation et ses méthodes, toute discussion approfondie ou participation à un projet commun est actuellement exclue. L'AS-Rens se voit désormais conférer une base juridique explicite pour ses activités internationales. De plus, elle doit être en mesure de communiquer des données personnelles à des autorités de surveillance étrangères, dans le respect de conditions strictes et dans des cas particuliers. Ces données ne peuvent être communiquées que si les services de renseignement concernés se les sont déjà transmises. L'AS-Rens peut ainsi vérifier si la communication des données dans un but donné est d'une part licite et d'autre part appropriée et efficace au vu de l'objectif visé. Par conséquent, les autorités de surveillance doivent respecter le degré de protection en matière de droits personnels garanti par le service destinataire. Le degré de protection des droits personnels qu'offre le service auquel les données sont destinées constitue un élément important pour évaluer la proportionnalité d'une communication de données spécifique.

La coordination internationale avec des partenaires externes joue également un rôle important dans la formation des membres de l'AS-Rens en matière de renseignement. Le développement des connaissances de l'AS-Rens comme de ses membres ne peut pas se fonder uniquement sur les informations fournies par les autorités soumises à la surveillance.

Art. 78d

L'art. 78*d* reprend la formulation de l'actuel art. 78, al. 3.

Art. 80

Etant donné que les collaborateurs des services nationaux peuvent eux aussi être dotés d'une identité d'emprunt (cf. art. 18), l'information du Conseil fédéral et de la DélCdG concernant le but et le nombre des identités d'emprunt est étendue. Sur demande de la DélCdG, il doit en outre être précisé que le rapport fournit également des informations sur la dotation des sources humaines en identités d'emprunt.

La LRens emploie le terme « autorités d'exécution cantonales », aussi la formulation de l'al. 4 est harmonisée en ce sens.

Art. 83

Les décisions rendues dans le cadre de l'exploration du réseau câblé se voient retirer tout effet suspensif, ceci pour les mêmes raisons que pour les autres décisions. Il n'est pas possible d'attendre l'issue d'une procédure de recours: les informations fournies ultérieurement risquent d'être déjà obsolètes, donc inutilisables. De plus, dans le cas où les délais de conservation légaux ont déjà expiré, les données risquent de ne plus exister du tout.

Chapitre 6a: Dispositions pénales, juridiction et communication

Avec ce nouveau chapitre, toutes les dispositions pénales figurent à la fin du texte de loi, comme à l'accoutumée.

Art. 83a et 83b

L'art. 83*a* reprend les alinéas abrogés 4, 4bis et 5 de l'art. 74. Le libellé correspond à la version adoptée par le Parlement le 25 septembre 2020 en lien avec la mise en œuvre de la Convention du Conseil de l'Europe pour la prévention du terrorisme. Il est entré en vigueur au 1er juillet 2021.

Les explications justifiant l'introduction de la disposition pénale concernant l'interdiction d'exercer une activité figurent à l'art. 83*c*.

Comme les décisions relatives à l'interdiction d'exercer une activité et à l'interdiction d'organisations sont rendues par le Conseil fédéral, les dispositions pénales correspondantes obéissent à des règles de poursuite pénale différentes de celles des autres infractions visées à l'art. 83*c*.

Art. 83c, al. 1 et 2

Le SRC ne prévoit à ce jour aucune sanction exécutive ou pénale particulière (telle que des dispositions pénales) pour le cas où les personnes concernées s'opposeraient à une demande de renseignements de la part du SRC, notamment en vertu de l'art. 25, al. 1, LRens Les moyens de contrainte administratifs servent à faire respecter les obligations légales des personnes qui n'observent pas les obligations qui leur incombent. Ainsi, le SRC ne dispose actuellement que des outils prévus par le droit procédural (art. 40 s. de la loi du 20 décembre 1968 sur la procédure administrative[26]) pour faire exécuter une ordonnance en vertu de l'art. 25, LRens. La seule possibilité est de menacer la personne concernée d'une amende pour insoumission en vertu de l'art. 292 du Code pénal[27] (CP). Conformément à l'art. 106, al. 1, CP, le montant maximum d'une telle amende s'élève à 10 000 fr. Si la disposition n'est pas respectée, le SRC peut déposer une plainte auprès du ministère public cantonal compétent pour insoumission à une décision de l'autorité.

Le SRC peut rendre des décisions en rapport avec les obligations de fournir des renseignements qui incombent aux particuliers (art. 25). Le service chargé de l'exploration du réseau câblé peut en outre rendre des décisions impliquant un exploitant de réseaux filaires ou un opérateur de télécommunications afin d'obtenir des données (art. 43). Conformément à l'art. 26 ORens, le service chargé de l'exploration est le Centre des opérations électroniques, situé sur l'actuelle Base d'aide au commandement de l'armée.

Si les obligations découlant de cette loi sont violées et que l'accomplissement des tâches légales du SRC s'en trouve entravé, une nouvelle disposition doit permettre de sanctionner les personnes responsables. Cette disposition se base sur la disposition pénale de la loi du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (LSCPT[28], art. 39) et reprend la même menace de peine. L'ampleur de cette sanction est notamment justifiée par le fait qu'une amende doit avoir un effet répressif approprié. Dans le domaine de l'exploration du réseau câblé en particulier, il est peu probable qu'une amende dont le maximum s'élèverait à seulement 10 000 fr. produise l'effet escompté sur les personnes responsables, ceci pour de nombreux fournisseurs de services de télécommunication. Par analogie à l'art. 39 LSCPT, la punition visée à cet article n'est que subsidiaire à des dispositions plus strictes qui pourraient s'appliquer simultanément en vertu d'autres lois. Les violations d'obligations ayant trait au secret professionnel (et éventuellement à l'abus d'autorité), qui sont réglementées en détail dans le CP, doivent notamment être prises en considération. La falsification de titres visée à l'art. 251 CP doit également être envisagée.

Dans le cadre de l'exploration du réseau câblé, tout exploitant de réseaux filaires ou opérateur de télécommunications qui ne fournit pas les données exigées par le service chargé de l'exploration est passible de poursuites. Il est concevable qu'un exploitant de réseaux filaires doive fournir des données pour plusieurs explorations distinctes. Si l'exploitant ne s'acquitte pas de ses obligations dans le cadre de plusieurs explorations du réseau câblé, les personnes responsables sont passibles de poursuites à plusieurs reprises. L'amende peut être augmentée en cas de récidive.

La divulgation d'informations à des tiers conformément aux art. 19, al. 3, et 20, al. 2, équivaut à une violation du secret de fonction au sens de l'art. 320 CP. C'est pourquoi la LRens ne contient pas de disposition pénale spécifique à ce sujet, mais seulement une disposition pénale visant les particuliers. Jusqu'à présent, la divulgation d'informations à des tiers était non punissable pour les particuliers.

Le nouvel al. 2 crée la possibilité, dans les cas mineurs, de condamner la personne morale à payer une amende pour non-respect des obligations d'un collaborateur de l'entreprise. Cette disposition permet aux autorités d'éviter des frais d'enquête disproportionnés.

Art. 83d

Al. 1

26 RS **172.021**
27 RS **311.0**
28 RS **780.1**

Lors d'explorations du réseau câblé, cette disposition permet au SRC ainsi qu'au service chargé de l'exploration de prendre des mesures contre toute personne qui ne s'acquitte pas de ses obligations, conformément aux principes du droit pénal administratif. Le même principe s'applique à la violation de l'obligation de garder le secret. Dans le cadre de ces procédures, le service chargé de l'exploration du réseau câblé rend des décisions, raison pour laquelle il est également mentionné dans cet alinéa.

Al. 2

Cet alinéa reprend l'art. 74, al. 6 (abrogé). Il est complété par la poursuite et le jugement de la violation de l'interdiction d'exercer une activité.

Art. 83e

Cet article reprend le contenu de l'art. 74, al. 7 (abrogé). Il concerne l'infraction à l'interdiction d'organisations et à l'interdiction d'exercer une activité. Le terme générique « décisions » couvre tous les types de décisions telles que jugements, ordonnances pénales, décisions pénales, mandats de répression et décisions ou ordonnances de non-lieu.

Art. 85, al. 2

Cet alinéa peut être supprimé, la disposition qu'il contient figurant désormais à l'art. 9, al. 3.

Annexe

Remarques générales concernant les ch. 1 et 6

Les modifications de la LMSI et de la LSIP tiennent compte de la mise en œuvre de la motion Rieder 17.3862 « Interdiction de se rendre dans un pays donné pour les extrémistes potentiellement violents ».

Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure[29]

Art. 2

L'*al. 2, let. f*, complète les mesures policières préventives existantes par les mesures contre les activités relevant de l'extrémisme violent en vertu des *art. 24h* ss. L'interdiction de se rendre dans un pays donné se réfère toutefois uniquement aux événements à l'étranger. Il convient néanmoins de s'attendre à ce que cette mesure préventive contribue aussi à renforcer la sûreté intérieure de la Suisse. Des groupements suisses souhaitant participer à des affrontements à l'étranger sont ainsi globalement affaiblis dans leurs actions et leurs objectifs. Les interdictions de se rendre dans un pays donné les empêchent de disposer d'une tribune pour faire valoir leurs revendications au moyen d'un usage extrême de la violence. C'est pourquoi les interdictions de se rendre dans un pays donné appliquées aux extrémistes violents sont inscrites dans la liste des mesures visant au maintien de la sûreté intérieure.

Titre intermédiaire Section 5b: Mesures contre les actes de violence lors de défilés et de manifestations

Un titre intermédiaire et une section supplémentaires sont nécessaires pour les nouvelles mesures contre les actes de violence lors de défilés et de manifestations. La section est insérée à la suite de la section 5*a* (mesures contre la violence lors de manifestations sportives).

Art. 24h Interdiction de se rendre dans un pays donné

L'*al. 1* établit que fedpol, en tant qu'autorité policière de la Confédération, peut ordonner une interdiction de se rendre dans un pays donné à l'encontre d'extrémistes potentiellement violents. L'alinéa définit les conditions dans lesquelles une interdiction de se rendre dans un pays donné peut être ordonnée.

Selon la *let. a*, la personne doit déjà avoir commis des violences par le passé, et ce directement lors d'un défilé ou d'une manifestation en Suisse ou à l'étranger. Par « défilés » et « manifestations », on entend les événements portant sur des idées, et dont l'objectif est de lancer un appel relayé par de nombreuses personnes. Lorsqu'un groupe qui cherche à faire entendre une revendication politique se tient en un endroit donné, il s'agit d'une manifestation. Les défilés se caractérisent par un lieu de rassemblement initial, un itinéraire et un lieu de manifestation final. Les participants doivent se déplacer du lieu initial au lieu final.

Par preuve d'un comportement violent lors d'un événement par le passé, on entend en règle générale un jugement ou une ordonnance pénale dans laquelle un tribunal ou un ministère public constate qu'une personne a commis des actes punissables contre des personnes ou des biens. Les violences contre des personnes ou des biens peuvent constituer diverses infractions. Pour concrétiser ce critère, l'ordonnance inclut une énumération non exhaustive des délits possibles. Cette liste doit se baser sur les dispositions de l'ordonnance du 4 décembre 2009 sur les mesures de police administrative de l'Office fédéral de la police et sur le système d'information HOOGAN (OMAH)[30] de lutte contre le hooliganisme, puisque la menace posée par les extrémistes violents lors de défilés et de manifestation est comparable à celle posée par les hooligans lors de manifestations sportives. Les actes de violence à l'étranger étant aussi enregistrés, les jugements étrangers peuvent également servir de preuve.

Si une voie de recours est déposée contre un jugement ou une ordonnance pénale, jusqu'à cinq années peuvent s'écouler en pratique jusqu'à ce qu'une personne soit condamnée par un jugement exécutoire pour un acte de violence lors d'un défilé ou d'une manifestation. Le fait de devoir attendre plusieurs années avant de pouvoir ordonner une interdiction de se rendre dans un pays donné irait à l'encontre des objectifs préventifs de cette mesure: les personnes qui participent à plusieurs reprises à des affrontements violents lors d'un événement le font en règle générale pour une durée limitée. L'expérience montre que cette « phase aiguë » de l'usage de la violence dure

29 RS **120**
30 RS **120.52**

quelques années. Si ces personnes sont condamnées en première instance et qu'un recours est déposé contre cette décision, plusieurs années peuvent s'écouler jusqu'à ce qu'un jugement exécutoire soit rendu. Cette période est toutefois décisive pour le développement du comportement violent. C'est donc précisément durant celle-ci que la mesure doit intervenir.

De ce fait, il doit être possible, à titre exceptionnel, d'apporter la preuve d'un comportement violent par le passé lors d'un défilé ou d'une manifestation d'une autre manière qu'au moyen d'un jugement. L'*al. 2* fournit une liste de preuves policières de ce type à titre d'exemple. Celle-ci s'appuie sur les preuves servant à ordonner des interdictions de se rendre dans un pays donné à l'encontre de hooligans (art. 5 OMAH).

Compte tenu de ses attributions, la police dispose de connaissances sur des personnes et des milieux faisant notoirement preuve de violence lors de défilés et de manifestations. Les preuves d'un comportement violent reposent par conséquent aussi sur les activités policières. Par plaintes pénales reposant sur des constatations policières, on entend les plaintes déposées par la police elle-même. Les plaintes pénales de particuliers ne sont donc pas prises en compte. La pratique courante veut qu'une décision de renvoi et une décision d'interdiction d'accès soient ordonnées à l'encontre des personnes qui commettent des violences lors de défilés et de manifestations et qui ont pu être arrêtées par la police. De telles décisions peuvent aussi faire office de preuve.

L'interdiction de se rendre dans un pays donné est un instrument de police préventif. Cette mesure vise à empêcher qu'une menace concrète qui se situe dans le futur puisse porter atteinte à des personnes ou des choses. Compte tenu du caractère préventif de l'interdiction de se rendre dans un pays donné, il est nécessaire de travailler sur la base de prévisions. Celles-ci doivent reposer sur des critères objectifs et être suffisamment vérifiables pour remplir les exigences de l'État de droit. Au cumul avec l'al. 1, let. a, on doit par conséquent disposer d'indices concrets et actuels sur la base desquels il convient de partir du principe que la personne concernée veut prendre part à des affrontements violents lors d'un défilé ou d'une manifestation (let. b).

Le défilé ou la manifestation au sens de la let. b doivent présenter un caractère international. On inclut ainsi les événements revêtant une certaine signification en matière de politique économique ou sociale, à l'instar des sommets du G7/G20, des visites d'État de haut rang, des conférences, des congrès de partis politiques ou des défilés de milieux extrémistes entretenant des liens au-delà des frontières. Le champ d'application inclut toutefois aussi les événements survenant en marge de ces événements de grande envergure, notamment les contre-manifestations. La police doit régulièrement faire face à des débordements massifs à de telles occasions. Ce fut p. ex. le cas lors du sommet du G20 en 2017 à Hambourg, à la suite duquel de nombreux Suisses ont été condamnés pour des actes de violence. En 2016, un Suisse a été condamné en France à sept ans de détention en raison d'un recours massif à la violence lors d'un défilé. Une interdiction de se rendre dans un pays donné pourrait empêcher la venue de personnes depuis la Suisse et, partant, des dommages aux personnes et aux choses.

En règle générale, le lieu et la date des événements visés à l'al. 1, let. b (revêtant une dimension de politique économique ou sociale importante), sont connus longtemps à l'avance. Les défilés et manifestations en marge de ces événements, qu'ils soient opposés ou en faveur des revendications de l'événement principal, peuvent cependant aussi survenir spontanément. Les informations policières et l'expérience déterminent s'il convient de s'attendre à des actes de violence lors de ces événements.

On dispose p. ex. d'indices concrets et actuels laissant présumer une sortie du pays à des fins de recours à la violence lors d'un défilé ou d'une manifestation, lorsque la personne a annoncé des projets de voyage concrets pour se rendre à un défilé ou une manifestation à l'étranger où il convient de s'attendre selon toute vraisemblance à des violences considérables contre les choses ou les personnes. L'autorité requérante au sens de l'art. 24*i* est tenue de motiver suffisamment ces indices auprès de fedpol.

En règle générale, les personnes entrant en ligne de compte pour une mesure au sens de l'art. 24*h* sont connues de la police ou du service de renseignement en raison de leurs antécédents. Au vu des expériences accumulées jusqu'à présent, il est vraisemblable que les interdictions de se rendre dans un pays donné ne concerneront qu'un nombre très restreint de personnes (nombre bas à deux chiffres) et qu'elles ne s'appliqueront qu'à un petit nombre d'événements.

L'interdiction de se rendre dans un pays donné en tant qu'instrument préventif est proportionnelle: ordonner une telle interdiction nécessite fondamentalement des indices concrets et factuels qui rendent suffisamment vraisemblable le fait que la personne a l'intention de se rendre à un défilé ou une manifestation. L'obligation de preuve visée à la let. b constitue un sérieux obstacle pour les autorités. À cela s'ajoute le fait que la personne doit déjà s'être distinguée par le passé en raison de son comportement violent et que la preuve correspondante doit être apportée. Les obstacles cumulés des let. a et b sont nécessaires pour assurer le principe de proportionnalité de l'action étatique. Lorsque toutes ces conditions sont réunies dans un cas particulier, l'interdiction de se rendre dans un pays donné est ordonnée pour une durée limitée et un espace géographique restreint (cf. art. 24*h*, al. 2). Le principe de proportionnalité est par ailleurs également assuré par la possibilité d'accorder des dérogations pour de justes motifs (al. 3).

Le fait d'empêcher des personnes de participer à des événements politiques porte en principe atteinte à leur droit à la liberté d'expression. La présente réglementation ne s'applique néanmoins qu'aux personnes qui participeront très probablement à des actes de violence. L'expression de son opinion par la violence contre d'autres personnes ou objets ne relève pas du champ d'application du droit à la liberté d'expression et n'est donc pas protégée[31]. L'interdiction prévue de se rendre dans un pays donné ne porte donc pas atteinte au droit fondamental de la liberté d'expression. Bien au contraire, les extrémistes violents s'immiscent souvent dans les événements visés à l'al. 1, empêchant d'autres participants pacifiques d'exprimer leur opinion. Il arrive aussi que des extrémistes violents prennent le contrôle d'événements pacifiques contre la volonté des organisateurs et les détournent pour servir leurs intérêts, commettre des violences et lancer des appels à la violence.

Toute infraction à l'interdiction de se rendre dans un pays donné est punie d'une amende (insoumission à une décision de l'autorité en vertu de l'art. 292 CP). La loi ne prévoit aucune sanction supplémentaire en cas d'infraction à l'interdiction de se rendre dans un pays donné.

L'*al. 3* prévoit que l'interdiction ne s'applique pas uniquement au voyage direct vers le pays de destination, mais aussi à tous les voyages dans d'autres pays qui permettraient de contourner l'interdiction. On vise ainsi à empêcher des personnes concernées de participer malgré tout à l'événement en empruntant des itinéraires alternatifs. L'interdiction de se rendre dans un pays donné inclut par conséquent aussi les voyages vers certains pays tiers afin d'empêcher de pouvoir rejoindre le pays de destination par ce biais. Des dérogations motivées peuvent être accordées lorsque la personne invoque de justes motifs crédibles. Un mariage ou des obsèques peuvent donner lieu à une dérogation. La décision en matière de dérogation incombe à fedpol dans le cadre d'une pesée des intérêts.

[31] ATF 143 I 147, consid. 3.2.

L'*al. 4* prévoit l'inscription de l'interdiction de se rendre dans un pays donné dans le système de recherches informatisées de police selon l'art. 15 LMSI (RIPOL) afin que les autorités disposant d'un accès à RIPOL soient informées et qu'elles puissent exécuter cette interdiction. Le système de recherches RIPOL est régulièrement consulté par le Corps des gardes-frontière, qui reçoit également une notification visant à le sensibiliser durant la période concernée. Fedpol informe en outre les autorités policières compétentes à l'étranger, de sorte qu'elles puissent réagir aux interdictions de se rendre dans un pays donné, p. ex. en ordonnant une restriction d'entrée. La partie nationale du Système d'information Schengen (N-SIS ; art. 16 LMSI) ne prévoyant aucune catégorie de notice pour les interdictions de se rendre dans un pays donné qui concernent les extrémistes violents, l'information ne peut pas passer par le canal du SIS. La communication des données aux autorités suisses et étrangères se fonde sur l'art. 24*l*, al. 3, en relation avec l'art. 24*h*, al. 4.

Les expériences avec les hooligans montrent que les interdictions de se rendre dans un pays donné exercent une action préventive: la personne frappée d'une telle interdiction renonce généralement à quitter le pays en raison de la menace de poursuites pénales.

Art. 24i Demande

À l'instar des mesures de lutte contre le terrorisme, les mesures contre les extrémistes potentiellement violents sont aussi ordonnées, en règle générale, à la demande du SRC et des autorités cantonales. Le droit de soumettre une demande incombe donc en premier lieu aux autorités qui disposent d'ores et déjà d'informations au sujet des personnes concernées (connaissances découlant de la menace pour la sûreté intérieure et extérieure, ainsi que connaissances découlant de la poursuite pénale d'infractions motivées par l'extrémisme violent). Une action de fedpol de sa propre initiative ne doit cependant pas être exclue. Si les cantons ont confié des tâches de sécurité aux communes, celles-ci peuvent aussi demander directement des mesures à fedpol.

La demande adressée à fedpol par le SRC ou par l'autorité cantonale ou communale compétente doit être suffisamment motivée. Fedpol constate les faits et vérifie si les conditions pour l'interdiction de se rendre dans un pays donné en vertu des art. 24*h* et 24*k* sont réunies. Lorsque le SRC dispose p. ex. d'indices concrets selon lesquels une personne compte se rendre à une contre-manifestation en marge d'une conférence internationale en Allemagne et que cette personne a déjà été condamnée pour émeute au sens de l'art. 260 CP en lien avec des lésions corporelles graves au sens de l'art. 122 CP dans le cadre d'un défilé ou d'une manifestation, le SRC demande à fedpol d'ordonner une interdiction de se rendre dans un pays donné en vertu de l'art. 24*h*. Fedpol vérifiera si l'ensemble des conditions énoncées à l'art. 24*h* sont réunies et, le cas échéant, ordonnera l'interdiction de se rendre dans un pays donné.

Art. 24j Durée de l'interdiction de se rendre dans un pays donné

La restriction de la liberté de mouvement ne peut durer qu'aussi longtemps qu'elle est absolument nécessaire pour empêcher la personne concernée de participer à des actes de violence. De ce fait, l'interdiction de se rendre dans un pays donné ne peut être ordonnée que pour une période s'étendant de trois jours maximum avant l'événement au dernier jour de l'événement. Cette mesure permet de garantir que la restriction ne s'applique que pour une durée proportionnée.

Art. 24k Limite d'âge

Les interdictions de se rendre dans un pays donné visant à lutter contre les activités relevant de l'extrémisme violent peuvent être ordonnées à partir de 16 ans. Cette limite d'âge basse tient compte du fait que certains mineurs présentent également une forte disposition à la violence, et elle souligne le caractère préventif de la mesure. La pratique de la police montre en effet qu'un certain nombre de personnes très jeunes sont déjà instrumentalisées par des groupements extrémistes violents pour servir leurs intérêts. En 2018, 40 mineurs ont ainsi participé à une manifestation non autorisée en Suisse où des personnes masquées ont provoqué des dégâts matériels à hauteur de quelque 100 000 fr. Au total, 147 personnes, dont 21 mineurs, ont fait l'objet d'une plainte pour des délits divers (notamment émeute, insoumission à une décision de l'autorité, empêchement d'accomplir un acte officiel, violence et menace contre les fonctionnaires, infraction à la loi sur les explosifs, dégâts matériels). La personne la plus jeune était âgée de 13 ans au moment de son arrestation. Une interdiction de se rendre dans un pays donné remplit donc aussi un rôle de protection de la jeunesse au sens que celle-ci est confrontée à une injonction des autorités qui l'empêche de participer à des violences organisées.

Art. 24l Traitement et communication des données

Al. 1 et 2: l'autorité requérante et l'autorité de décision ont besoin de traiter des données personnelles sensibles pour motiver la demande d'interdiction de se rendre dans un pays donné et la décision d'interdiction (art. 24*h*), pour vérifier si les conditions sont réunies, ainsi que pour exécuter l'interdiction de se rendre dans un pays donné. Ces dispositions créent la base légale formelle nécessaire en vertu de l'actuel art. 17, al. 2, LPD.

L'*al. 3* prévoit que les collaborateurs de l'Office fédéral de la douane et de la sécurité des frontières (OFDF) chargés du contrôle des personnes sont autorisés à traiter des données personnelles, y compris des données personnelles sensibles, pour appliquer l'interdiction de se rendre dans un pays donné.

L'*al. 4* autorise l'échange de données personnelles entre les autorités qui disposent des informations nécessaires à la décision de fedpol et celles qui accomplissent des tâches dans le domaine de la lutte contre les activités relevant de l'extrémisme violent. L'amélioration de l'échange d'informations entre les autorités constitue l'une des exigences du plan d'action national de lutte contre la radicalisation et l'extrémisme violent (PAN; voir mesure 15, let. a)[32].

L'*al. 5* règle la communication des données aux autorités de sécurité étrangères (gardes-frontière et police). Les interdictions de se rendre dans un pays donné impliquant des données sensibles au sens de l'art. 3, let. c, ch. 4, LPD, une base légale formelle est indiquée (art. 17, al. 2, LPD). Une communication à l'étranger n'est autorisée que lorsqu'un niveau de protection adéquat des données peut être assuré dans le pays concerné (art. 6 LPD).

La mesure ne peut produire son effet préventif que lorsque la personne concernée est au courant qu'elle risque d'être identifiée aussi bien au franchissement de la frontière que dans le pays de destination. La communication des données aux gardes-frontière et aux autorités étrangères doit donc figurer dans la décision. Cette transparence est aussi imposée pour des raisons de protection des données.

32 https://www.fedpol.admin.ch/dam/ejpd/fr/data/aktuell/news/2017/2017-12-04/171204-nap-f.pdf

Il est dans l'intérêt des autorités de sécurité du pays dans lequel l'événement est organisé d'être informées de telles interdictions, car la menace est souvent très élevée lors d'événements politiques de ce type, et les dispositifs de sécurité sont conséquents.

Art. 24m Voies de droit

Les décisions peuvent faire l'objet d'un recours auprès du Tribunal administratif fédéral. Le recours n'a en principe pas d'effet suspensif pour ne pas rendre inopérant le but de l'interdiction de se rendre dans un pays donné. Il peut toutefois être accordé par le tribunal lorsque le but de la mesure n'en est pas compromis.

Loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration[33]

L'accès au système d'information en vue de l'établissement des documents de voyage suisses et des autorisations de retour pour étrangers (ISR) pour l'identification d'une personne est indispensable afin d'assurer des recherches et des identifications sans faille. Sans cet accès, le SRC n'est souvent pas en mesure d'identifier une personne et devrait recourir à d'autres mesures susceptibles de constituer une atteinte plus importante aux droits de la personnalité. Toutes les informations sur des voyages potentiels et l'obtention de documents sont importantes, p. ex. pour l'identification précoce des voyageurs potentiels du djihad ou pour empêcher les voyages en zone de guerre. Cet accès à l'ISR permet au SRC d'employer des moyens moins radicaux, en meilleure adéquation avec la protection de la personnalité.

Pour certaines catégories d'étrangers, l'ISR constitue le pendant au système d'information relatif aux documents d'identité (ISA) visé à l'art. 11 de la loi du 22 juin 2001 sur les documents d'identité[34]. L'accès du SRC à ISA a déjà été réglé par le Parlement le 25 septembre 2020 avec la loi sur les mesures policières de lutte contre le terrorisme (MPT)[35].

Code pénal[36]

Un renvoi est modifié suite à l'abrogation resp. déplacement partiel de l'art. 74, al. 4, LRens.

Loi fédérale du 13 décembre 2002 sur l'Assemblée fédérale[37]

L'intégration de l'AS-Rens dans l'art. 142, al. 2, LParl, constitue le pendant de l'art. 77, al. 2, LRens. Ce faisant, on peut tenir pleinement compte de l'exigence d'une base légale formelle. Le Conseil fédéral estime que l'AS-Rens devrait aussi être intégrée à l'art. 142, al. 3, LParl, et que celle-ci est la mieux placée pour défendre son budget devant l'Assemblée fédérale lorsque cela s'avère nécessaire. Le libellé se base sur la version adoptée par le Parlement le 25 septembre 2020 en lien avec la révision de la loi sur la protection des données.

Loi fédérale du 20 mars 1981 sur l'entraide internationale en matière pénale[38]

La version actuelle de l'art. 11*a*, al. 3, de la loi sur l'entraide pénale internationale (EIMP) est en vigueur depuis le 1er janvier 2010 et contient encore une référence à l'exécution de la LMSI[39] par le SRC. On distinguait à l'époque la recherche de données en Suisse de celle à l'étranger. Celles-ci étaient réglées dans deux actes distincts (aLFRC et LMSI). Cette distinction a été abrogée avec l'entrée en vigueur de la LRens. Les activités mentionnées dans cet article sous l'exécution de la LMSI par le SRC sont intégrées dans la LRens à l'heure actuelle. La modification de l'EIMP a été oubliée au moment où la LRens a été adoptée. Son contenu ne change pas. Les ordonnances sont modifiées en conséquence.

Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération[40]

Art. 15, al. 1, let. h

Conformément à l'art. 24*h*, al. 4 LMSI (voir ci-dessus), les interdictions de se rendre dans un pays donné sont inscrites dans le système RIPOL. La base légale pour RIPOL est complétée avec la let. h.

Art. 18, al. 5, let. d

La let. d supplémentaire élargit la liste des tâches du système de gestion des affaires et des dossiers de fedpol afin de permettre d'y traiter les mesures ordonnées par fedpol en vertu de l'art. 24*h*, al. 3, LMSI (voir ci-dessus). Le libellé se base sur la version adoptée par le Parlement le 25 septembre 2020 en lien avec la MPT.

Art. 18a

Al. 1

En ajoutant à l'art. 7 les al. 1, let. e à h, et 1bis à 3, AP-LRens, le SRC introduit des mesures supplémentaires de protection et de sécurité de ses collaborateurs, de ses installations et des données qu'il traite (voir ci-dessus). Deux de ces nouvelles mesures, à savoir le contrôle

33 RS **142.20**
34 RS **143.1**
35 FF **2020** 7499
36 RS **311.0**
37 RS **171.10**
38 RS **351.1**
39 RS **120**
40 RS **361**

de collaborateurs déjà liés par un rapport de travail et celui de personnes se trouvant dans une procédure d'engagement sont également nécessaires à l'Office fédéral de la police (fedpol). Les tâches que fedpol accomplit couvrent l'ensemble des activités de police judiciaire liées à la grande criminalité et s'étendent à l'exploitation des systèmes d'information de police et à la protection des magistrats, des bâtiments de la Confédération ainsi que des personnes et des bâtiments devant être protégés en vertu du droit international public. L'accomplissement de ces tâches pose des exigences élevées en termes de loyauté des collaborateurs.

S'agissant des personnes se trouvant dans une procédure d'engagement, fedpol vérifie aujourd'hui déjà si elles font l'objet d'une procédure administrative ou pénale en cours, si une sanction correspondante a été prononcée à leur encontre ou si d'autres faits relevant du droit pénal sont constatés. Ces vérifications se fondent sur leur consentement préalable conformément à l'art. 17, al. 2, let. c, LPD. Il s'est toutefois avéré que cette mesure devait pouvoir être appliquée en tous les cas à l'avenir. Par ailleurs, si des indices concrets laissent présumer une menace pour la sécurité de fedpol et de ses collaborateurs, de tels contrôles doivent pouvoir viser les personnes déjà engagées par fedpol. En raison de cette extension matérielle, les contrôles doivent désormais pouvoir se fonder sur une base légale formelle spécifique, qui est créée avec le nouvel art. 18*a* AP-LSIP. La formulation de cet article s'inspire largement de la réglementation prévue par le SRC à l'art. 7, al. 1, let. f et g, et 1bis, AP-LRens. La notion de "contrôle en matière de personnel par fedpol" se distingue de celle de "contrôle de sécurité relatif aux personnes" au sens de la LSI et de celle de "contrôle de loyauté" prévue à l'art. 20*b* nLPers[41]. En effet, ces contrôles en matière de personnel visent tant les personnes déjà liées par un rapport de travail (let. a) que celles figurant parmi les derniers candidats en lice pour un emploi; le contrôle doit impérativement être effectué avant la prise de fonction à fedpol (let. b).

Concrètement, il s'agira d'interroger en priorité les systèmes d'information suivants régis par la LSIP: JANUS (art. 10, 11 et 13), IPAS (art. 12 et 14), RIPOL (art. 15), l'index national de police (art. 17) et ORMA (art. 18), ainsi que le système d'information HOOGAN, visé à l'art. 24*a* LMSI. Pour que fedpol puisse effectuer les contrôles prévus à l'al. 1, let. a et b, la personne concernée doit y avoir préalablement consenti, comme c'est le cas pour les contrôles de sécurité relatifs aux personnes visés à l'art. 7, al. 1, let. f et g, AP-LRens. Si, dans les cas visés à la let. a, fedpol soupçonne un comportement fautif, il porte plainte auprès des autorités de poursuite pénale compétentes.

Contrairement au SRC, qui se fonde sur la LRens pour accomplir ses tâches, fedpol ne dispose d'aucune loi au sens formel qui règlemente les siennes de façon exhaustive. Il convient dès lors d'insérer dans la LSIP la nouvelle disposition légale qui réglemente les contrôles en matière de personnel par fedpol. En effet, cette loi réglemente déjà les systèmes d'information sur lesquels fedpol s'appuie principalement pour effectuer ces contrôles. Par ailleurs, elle contient déjà, à son nouvel art. 17, al. 4, let. l (version selon la LSI[42]), une autre disposition légale qui touche aux contrôles de sécurité relatifs aux personnes. Ce contenu, qui relève du droit du personnel, n'est donc pas une nouveauté dans la LSIP.

Al. 2

Le contrôle d'une personne liée à fedpol par un rapport de travail en vertu de l'al. 1, let. a, constitue une atteinte juridique d'une autre nature que celui d'une personne se trouvant dans une procédure d'engagement, car il peut, dans le pire des cas, entraîner un licenciement. C'est pour cette raison que l'accord écrit d'un membre de la direction de fedpol est requis. Si un employé de fedpol ne consent pas à un contrôle en matière de personnel, l'accord écrit du membre de la direction prévaut alors sur ce refus. Il ne serait pas possible sinon de confirmer ou d'infirmer de façon définitive les indices concrets d'une menace pour la sécurité de l'office et de ses collaborateurs.

Loi fédérale du 3 février 1995 sur l'armée et l'administration militaire[43]

Art. 99, al. 5

Suite aux modifications des dispositions relatives à l'autorité de surveillance indépendante AS-Rens dans la LRens, une référence est modifiée.

Loi fédérale du 20 juin 1997 sur les armes, les accessoires d'armes et les munitions[44]

Art. 9, al. 2

L'art. 9 de la loi sur les armes (LArm) est en vigueur depuis le 12 décembre 2008. À cette date, les tâches de fedpol et du service de renseignement intérieur étaient réglées dans la LMSI, et les autorités d'exécution cantonales étaient les mêmes pour ces deux offices. Avec l'entrée en vigueur de la LRens, leurs tâches ont été clairement séparées sur le plan légal. Un canton peut ainsi spécifier une autorité d'exécution pour l'exécution de la LMSI, et une autre autorité d'exécution pour celle de la LRens. Étant donné qu'en pratique, l'autorité d'exécution au sens de la LRens prend position sur l'acquisition d'armes, il suffit de modifier la référence à la LRens dans l'art. 9 LArm.

Art. 32c

L'accès au système d'information commun harmonisé (ARMADA) visé à l'art. 32*a*, al. 3, LArm, permet au SRC de mieux évaluer le potentiel de menace d'une personne, puisqu'il est en mesure de fournir des renseignements quant à la possession d'une arme, au retrait d'une arme ou au refus d'un permis d'acquisition d'armes. À la lumière de plusieurs tueries (comme celle de Christchurch ou de Hanau) perpétrées par des extrémistes de droite, ce sujet a encore gagné en importance. On sait par ailleurs que des personnes issues de milieux salafistes ou islamistes enclins à la violence tentent d'acquérir des armes. Il est impératif de pouvoir enquêter dans les meilleurs délais afin d'évaluer sérieusement la menace pour la sûreté intérieure ou extérieure.

La loi sur les douanes étant également en cours de révision, une coordination sera nécessaire en fonction de l'avancement des travaux.

41 LSI, annexe 1 (Modification d'autres actes), ch. 4: LPers, nouvel art. 20*b* (FF **2020** 9699).
42 LSI, annexe 1 (Modification d'autres actes), ch. 11: LSIP, nouvel art. 17, al. 4, let. l (FF **2020** 9702).
43 RS **510.10**
44 RS **514.54**

Loi fédérale du 17 juin 2016 sur le casier judiciaire informatique VOSTRA[45]

Il s'agit d'une modification de la terminologie. La LRens emploie le terme « source humaine » au lieu de « informateur ». L'art. 9 LRens fixe les autorités cantonales qui collaborent avec le SRC. La LRens les désigne par le terme « autorité d'exécution ». L'entrée en vigueur de la LRens a rendu caduque la mention à la LMSI. De ce fait, on revoie dorénavant à l'article pertinent de la LRens.

Cette loi devrait entrer en vigueur en 2023.

Loi du 18 mars 2005 sur les douanes[46]

Les membres de milieux terroristes sont particulièrement connus pour leurs voyages et contacts à l'étranger. Des voyageurs du djihad, mais aussi des relations entre des milieux islamistes locaux et des cercles islamistes dans les pays voisins, sont également connus et documentés par le SRC. Le « système d'information de l'OFDF » de l'Administration fédérale des douanes contient des données présentant un intérêt et une importance considérables pour des contrôles détaillés des antécédents.

Les données du système d'information de l'OFDF peuvent s'avérer utiles dans le domaine de l'espionnage pour savoir avec qui et quel véhicule une personne a voyagé. Ces données sont par ailleurs aussi importantes dans le domaine de la non-prolifération pour examiner les importations et exportations de biens ou le transport de sommes d'argent potentiellement considérables.

Une modification de l'annexe 4 de l'ordonnance du 23 août 2017 sur le traitement des données dans l'AFD[47] est nécessaire en raison du nouvel accès dont dispose le SRC. Cette modification sera apportée dans le cadre de la révision des ordonnances à l'issue de la révision de la LRens.

La loi sur les douanes étant également en cours de révision, une coordination sera nécessaire en fonction de l'avancement des travaux, ou les modifications prévues ici seront caduques.

Loi du 19. décembre 1958 sur la circulation routière[48]

Avec l'entrée en vigueur partielle, le 1er janvier 2019, de la modification du 15 juin 2012 de la loi du 19 décembre 1958 sur la circulation routière (LCR), les accès en ligne du SRC aux systèmes de l'Office fédéral des routes, qui ont été remplacés par le nouveau système d'information relatif à l'admission à la circulation (SIAC) et dont une partie avait été fixée avec l'entrée en vigueur de la LRens, ont été supprimés par inadvertance. Il s'agit d'une erreur législative qui se voit corrigée par le présent complément.

Loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication[49]

Art. 14a

Le SRC n'exploitant plus de systèmes d'information, cette disposition parle désormais uniquement de données. Les informations contenues dans le système de traitement sont décrites à l'article 8 LSCPT et contiennent également les données sur les services de télécommunication (art. 8 let. c LSCPT), donc les renseignements (art. 7 let. c LSCPT). Leur contenu demeure inchangé. Les données peuvent encore être copiées électroniquement et transmises au SRC afin que celui-ci puisse les traiter. Les mesures au sens de l'al. 1 let. b correspondent aux mesures de recherche prévues dans la LRens.

Art. 39, al. 4

Comme dans l'art. 83*c* LRens, il convient également d'appliquer la réglementation prévue à l'art. 7 DPA sur les amendes ne dépassant pas 20 000 fr. à la disposition pénale administrative visée à l'art. 39 LSCPT et de créer la possibilité d'infliger une sanction efficace à l'encontre des personnes morales soumises à la LSCPT si elles ne respectent pas leurs obligations. La disposition pénale actuelle visée à l'art. 39 est entrée en vigueur le 18 mars 2018. En pratique, des difficultés ont été rencontrées avec des entreprises récalcitrantes qu'il n'a jusqu'à présent guère été possible de tenir pour responsables. Les présentes dispositions devraient remédier à la situation. En Suisse, on punit en principe les personnes physiques qui ont commis l'acte punissable. Cette « punition » des personnes morales constitue une atteinte à ce principe. Elle a toutefois fait ses preuves dans le domaine des enquêtes pénales administratives, notamment en matière de législation sur la valeur ajoutée, de législation douanière et de législation sur les produits thérapeutiques. On renvoie également aux explications relatives à l'art. 83*c*, al. 3, LRens.

Modification d'autres actes: ch. 13 à 17

La LRens emploie le terme « autorités d'exécution cantonales », aussi la formulation de ces lois est harmonisée en ce sens.

3 Conséquences

3.1 Conséquences pour la Confédération en termes de finances et de ressources humaines

L'AS-Rens peut compenser la charge de travail supplémentaire engendrée par la reprise des tâches de l'ACI grâce à des gains d'efficacité obtenus dans le cadre de la consolidation de son organisation et de ses tâches.

45 FF **2016** 4703
46 RS **631.0**
47 RS **631.061**
48 RS **741.01**
49 RS **780.1**

Les nouvelles tâches en vertu de la LMSI entraînent une certaine charge de travail supplémentaire pour fedpol et le SRC. On peut supposer que l'interdiction de se rendre dans un pays donné ne concernera qu'un nombre très restreint de personnes (quelques dizaines au plus) et qu'elle ne s'appliquera qu'à un petit nombre d'événements. Comparables, les interdictions de se rendre dans un pays donné dans le cadre des mesures contre la violence lors de manifestations sportives (art. 24*c* LMSI) entraînent une charge de travail de 1 à 2 jours en moyenne par décision, tandis qu'un recours entraîne une charge de travail de 3 à 5 jours. Fedpol maîtrisera cette charge supplémentaire avec les ressources actuelles.

Les autres modifications demandées n'entraînent aucune charge supplémentaire en termes de finances ou de ressources humaines pour la Confédération, puisque l'effectif du SRC est actuellement augmenté afin qu'il puisse s'acquitter durablement de ses tâches.

3.2 Conséquences pour les cantons et les communes, ainsi que pour les centres urbains, les agglomérations et les régions de montagne

Les nouvelles interdictions de se rendre dans un pays donné au sens de la LMSI peuvent entraîner une charge de travail supplémentaire pour les cantons puisqu'ils sont tenus de motiver les demandes qu'ils adressent à fedpol.

Les modifications demandées n'entraîneront aucune conséquence notable en termes de finances ou de ressources humaines en ce qui concerne les cantons, les communes, les centres urbains, les agglomérations et les régions de montagne.

3.3 Conséquences pour l'économie, la société et l'environnement

Aucune conséquence négative pour l'économie, la société et l'environnement n'est à attendre. En revanche, les modifications proposées améliorent l'exécution de la LRens, ce qui exercera un impact positif sur la situation de la Suisse en matière de sécurité.

La nouvelle mesure en vertu de la LMSI contribue à la sécurité publique en Suisse et à l'étranger (en empêchant l'exportation d'activités relevant de l'extrémisme violent). Elle exerce en outre un effet protecteur préventif, notamment sur les jeunes au sein d'un milieu extrémiste violent et donc confrontés à un environnement violent ou enclin à la violence.

4 Relation avec le programme de la législature et avec les stratégies du Conseil fédéral

Le projet est annoncé dans le message du 29 janvier 2020 sur le programme de la législature 2019 à 2023[50].

5 Aspects juridiques

5.1 Constitutionnalité

L'avant-projet se fonde sur l'art. 54, al. 1, de la Constitution (Cst.)[51], concernant la sûreté extérieure de la Suisse, et pour la protection de l'État en Suisse, sur la compétence inhérente de la Confédération à prendre les mesures nécessaires pour assurer sa protection ainsi que celle de ses organes et institutions (pour laquelle l'art. 173, al. 2, Cst., est mentionné en préambule).

Avec la présente révision, le Conseil fédéral ne va pas au-delà de ce qui relève d'ores et déjà de la responsabilité de la Confédération en vertu de la Constitution. Il s'appuie par conséquent sur une base constitutionnelle suffisante. Des explications détaillées sont fournies dans le message concernant la LRens (FF 2014 2151).

La question de la conformité avec le droit constitutionnel et international du renoncement à une voie de droit ordinaire pour la personne concernée en cas de restriction ou de refus du droit d'accès est encore controversée et sera éclaircie lors de la procédure de consultation.

5.2 Conséquences en matière de protection des données

Le présent projet de révision se fonde sur une analyse d'impact relative à la protection des données que le SRC avait élaborée avec le soutien de David Rosenthal, auteur du commentaire relatif à la loi suisse sur la protection des données, en vue de l'élaboration de la réglementation alternative de la conservation des données. L'analyse d'impact inclut une description du traitement actuel des données relevant du renseignement ainsi qu'une évaluation des risques pour la personnalité et les droits fondamentaux des personnes concernées, présente les mesures de protection de la personnalité et des droits fondamentaux des personnes concernées, et identifie les points faibles de même que les possibilités d'amélioration. Elle tient également compte des recommandations de la DélCdG et de l'AS-Rens.

L'analyse énumère la multitude de mesures issues des domaines du classement et de la gestion des documents, de la garantie des suppressions, de la garantie de la qualité des données entrantes et sortantes, du contrôle de qualité et de la garantie d'une gouvernance appropriée. En parallèle, elle présente les risques pour les personnes concernées ainsi que des risques supplémentaires en matière de protection des données. Les risques sont mis en regard avec les causes potentielles, les dommages potentiels et les mesures techniques et opérationnelles déjà prises par le SRC pour prévenir les dommages. Une évaluation des risques estime ensuite l'ampleur des dommages et leur degré de probabilité. Enfin, le SRC a élaboré pour chaque risque une déclaration quant à la manière dont il traite celui-ci, y c. les mesures qu'il souhaiterait mettre en œuvre dans ce contexte.

Le présent projet apporte une contribution significative en matière de protection des données selon les conclusions de cette évaluation. Il se distingue du régime actuel par une neutralité technologique, une focalisation sur les processus et une complexité nettement moindre. De plus, les risques moyens à élevés suivants, identifiés dans l'analyse d'impact, sont atténués comme suit:

50 FF **2020** 1709, 1829
51 RS **101**

- Le risque que le SRC traite des données sur des personnes ne relevant pas de la LRens est atténué par l'introduction d'un contrôle initial détaillé (art. 45). Les communications lui parvenant ne sont plus évaluées dans leur globalité, mais de manière détaillée. Le SRC anonymise tous les contenus qui ne présentent aucun lien avec ses tâches ou qui tombent sous le coup des restrictions de traitement des données. Dans le cas de données provenant de sources accessibles au public et de données provenant de mesures de recherche soumises à autorisation enregistrées de manière distincte, le contrôle des restrictions de traitement des données est effectué préalablement à l'utilisation de ces données en tant que données de travail. Dans l'intervalle, elles sont soumises à un embargo d'utilisation. En outre, le SRC est désormais tenu d'informer les autorités d'exécution cantonales lorsque celles-ci lui font parvenir des rapports qui contiennent des données ne présentant aucun lien avec les tâches visées à l'art. 6 ou contrevenant aux restrictions de traitement des données visées à l'art. 5, al. 5. Ces données doivent être détruites ou anonymisées, tant au sein du SRC que des autorités d'exécution cantonales (art. 58*c*, al. 2).
- Le risque que le SRC traite des données erronées sur des personnes et que les produits du SRC relevant du renseignement soient élaborés sur la base de données erronées est atténué par le fait que les données brutes ne peuvent être utilisées qu'après un contrôle de leur exactitude (art. 51, al. 1). Dans l'intervalle, elles sont soumises à un embargo d'utilisation. Le service de contrôle de qualité du SRC dispose par ailleurs d'un accès systématique à toutes les données du SRC et des autorités d'exécution cantonales.
- Le risque que les personnes concernées ne savent pas qui est responsable du traitement des données les concernant par le SRC et les autorités d'exécution cantonales est atténué par le fait que la responsabilité en la matière est clairement attribuée au SRC à l'art. 9, al. 4. De plus, les personnes concernées n'ont plus qu'un interlocuteur, ce qui facilite l'exercice de leurs droits.
- Le risque d'une expérience inquiétante (une personne sait ou pense que le SRC traite des données à son sujet, mais pas pourquoi) est atténué par le fait que le droit d'accès est soumis au régime comparable de la LSIP. Les personnes peuvent dès lors être informées beaucoup plus rapidement que ce qui était possible jusqu'à présent en fonction de la conception du droit.
- Le risque que des données soient traitées plus longtemps que nécessaire est atténué par la renonciation à des silos de données séparés dans les différents systèmes d'information. On ne travaille désormais plus avec des copies des données qui, dans certaines conditions, ne sont pas corrigées, anonymisées ou supprimées en même temps que les originaux. Cela atténue aussi le risque que les mêmes données soient soumises à différentes règles de traitement en fonction du système d'information (p. ex. comme actuellement où elles sont anonymisées dans IASA-EXTR SRC, mais pas dans GEVER SRC, ou supprimées après 15 ans dans IASA-EXTR SRC, mais après 20 ans seulement dans GEVER SRC). En parallèle, il sera dorénavant possible de piloter les données individuellement via leurs métadonnées (p. ex. en ce qui concerne les droits d'accès et les délais de conservation) et d'assurer leur qualité, alors que le traitement actuel repose encore sur des répertoires électroniques.
- Le risque qu'une personne soit soupçonnée par le SRC plus longtemps que nécessaire est atténué par le fait que le SRC a également le droit de traiter des données à décharge et de les ajouter aux données à charge jusqu'à ce que les soupçons soient entièrement levés et que les données puissent être supprimées (art. 52, al. 3).

Le fait de renoncer à définir les systèmes d'information est compatible avec la conception de la nLPD, puisque l'on ne réglemente plus des fichiers de données, mais des activités de traitement. L'accent n'est plus mis sur l'emplacement où les données sont enregistrées, mais sur ce que l'on en fait. Les données personnelles traitées sont désormais associées à ces activités de traitement (art. 49). Leur traitement peut donc être réglementé de manière neutre sur le plan technologique. Cette modification tient également compte des progrès des technologies de l'information. Aucune extension du traitement des données n'est donc impliquée ou envisagée; au contraire, on vise à mieux contrôler ce traitement.

Dans la phase actuelle du processus législatif, encore très précoce, l'établissement d'une nouvelle analyse d'impact sur la base du présent projet ne semble pas pertinent. Elle sera cependant élaborée en temps utile, tel que l'exige la LPD en vue de la présentation du projet final au Parlement.

5.3 Compatibilité avec les engagements internationaux de la Suisse

Les modifications de la LRens proposées sont compatibles avec les engagements internationaux de la Suisse.

5.4 Forme de l'acte législatif

Conformément à l'art. 164 Cst. et à l'art. 22, al. 1, LParl, l'Assemblée fédérale édicte sous la forme d'une loi fédérale toutes les dispositions importantes qui fixent des règles de droit.

5.5 Frein aux dépenses

Le présent avant-projet n'est pas soumis au frein des dépenses selon l'art. 159, al. 3, let. b, Cst., puisqu'il ne contient aucune nouvelle disposition relative à des subventions et ne prévoit pas la création d'un crédit d'engagement ou d'un plafond des dépenses.

5.6 Respect du principe de subsidiarité et du principe de l'équivalence fiscale

5.7 Conformité à la loi sur les subventions

L'avant-projet n'introduit aucune disposition, nouvelle ou modifiée, qui affecte les principes de la loi sur les subventions.

5.8 Délégation de compétences législatives

Le Conseil fédéral reste chargé de régler les modalités du traitement des données. Il s'agit de l'adaptation logique de l'ancienne délégation concernant les systèmes d'information et de stockage de données actuels.

5.9 Protection des données

L'avant-projet réglemente le but, le contenu et le cercle d'utilisateurs du traitement des données, de même que le droit d'accès qui repose désormais sur les dispositions de la nLPD.

La transmission et le traitement des données personnelles sensibles nécessite une base légale formelle (art. 34, al. 1, nLPD). La présente base légale formelle assure le respect des prescriptions en matière de protection des données.